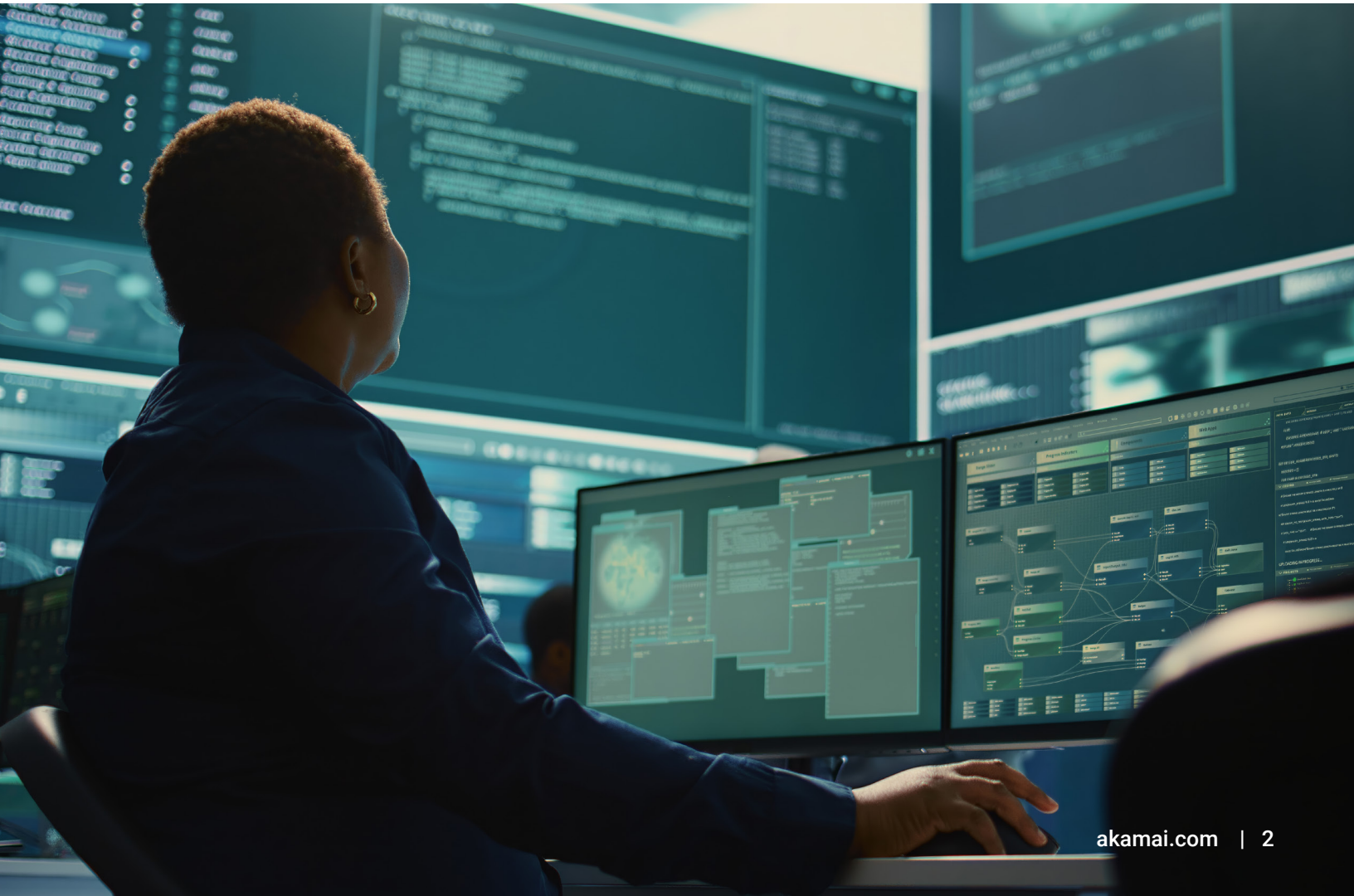
Akamai

WHITE PAPER

Cumplimiento y seguridad de las API

Requisitos implícitos y explícitos de protección de datos

En este informe



Introducción

Demostrar el cumplimiento de las normativas de protección de datos siempre ha sido sinónimo de tener que dedicar grandes cantidades de energía y recursos a hacer frente a los riesgos más conocidos. Sin embargo, eso está cambiando. La superficie de ataque actual está evolucionando rápidamente para incluir amenazas que la mayoría de los programas de cumplimiento empresariales no tienen plenamente en cuenta. Esto se debe, en parte, a que los propios organismos reguladores no siempre pueden mantener el ritmo e indicar exactamente cada uno de los aspectos de cobertura necesarios para evitar las infracciones.

Esto es lo que ocurre con la protección de API. Cada vez que un cliente, partner o proveedor interactúa digitalmente con su empresa, existe una API entre bastidores que facilita un intercambio rápido de información, que a menudo incluye datos confidenciales. Los atacantes ahora saben que pueden simplificar su estrategia para robar esos datos teniendo como objetivo directamente a las API.

Es posible que ya se haya percatado del nuevo lenguaje en las normativas que habla de la necesidad de inventariar, evaluar o proteger las API. No obstante, incluso cuando no se incluye un lenguaje específico sobre las API, el hecho de que se hayan convertido en un claro vector de ataque *implica* que es necesario protegerlas correctamente.

No es sorprendente la aparición de las API como un importante problema de cumplimiento. Las API expuestas o mal configuradas prevalecen, son fáciles de vulnerar y, a menudo, no están protegidas. Y la vulneración de una sola API puede provocar el robo de millones de registros. Los números hablan por sí solos:

- El 78 % de las organizaciones ha sufrido un incidente de seguridad relacionado con las API.[1]
- Los reguladores han impuesto sanciones a un 44 % de las organizaciones por incidentes de seguridad relacionados con las API.[2]

¿Cómo afecta esto a su programa de cumplimiento? Los reguladores deben comprobar que su organización está tomando medidas para proteger todos los puntos de acceso a los datos confidenciales. Esto significa que debe demostrar que su organización puede:

- Controlar todas las API, incluidas las API en la sombra.
- Descubrir y corregir cualquier vulnerabilidad de las API.
- Aplicar controles personalizados para evitar filtraciones de datos centradas en las API.

En este white paper se analiza la naturaleza de los crecientes riesgos de las API, se destacan seis ejemplos de normativas y marcos que exigen protecciones de las API (ya sea explícita o implícitamente), además de ofrecerse consejos sobre cómo ajustarse a los requisitos de cumplimiento a través de las prácticas recomendadas de seguridad de las API.

1., 2. Akamai Technologies, "El API Security Disconnect", 2023

Comprensión de los riesgos de las API

Las API residen en el centro de los productos digitales, servicios y entornos de nube de su empresa. Su acceso constante a los datos las convierte en un factor de ingresos y en un riesgo operativo. El problema es que la mayoría de las empresas, incluso aquellas con programas de seguridad consolidados, no priorizan las amenazas relacionadas con las API en la medida en que se centran en otras amenazas, como el phishing o el ransomware.

Algunas organizaciones confían en las puertas de enlace de API y los firewalls de aplicaciones web (WAF) para la protección básica de las API, pero estas herramientas no están diseñadas para proporcionar el grado de visibilidad, protección en tiempo real y pruebas continuas que pueden proporcionar las soluciones de seguridad de API especializadas. Estas son las razones por las que estas herramientas no son suficientes:

- Las puertas de enlace de API y los WAF solo pueden observar el tráfico de API *gestionado* que pasa a través de ellos.
- No pueden proteger las API no gestionadas, que los analistas predicen que constituirán casi la mitad del ecosistema de API de una empresa típica para 2025.
- De esta forma, los equipos de seguridad no están completamente preparados para proteger la parte de su superficie de ataque que se expande más rápidamente, ya que saben poco sobre dónde se enrutan las API, cómo están configuradas, qué tipos de datos confidenciales intercambian y los riesgos que representan.

La protección de la información de los usuarios es una prioridad para los reguladores, quienes imponen multas severas a las empresas que no protegen razonablemente los datos de sus clientes frente al acceso no autorizado. Dado que solo 4 de cada 10 profesionales de la seguridad con inventarios de API completos saben cuáles de sus API devuelven datos confidenciales[3] y que muchas llamadas a API proceden de atacantes que prueban vulnerabilidades, las filtraciones de datos a través de API solo aumentarán, especialmente porque los ataques de API son, hoy por hoy, bastante fáciles de llevar a cabo.

3. Akamai Technologies, "El API Security Disconnect", 2023

Cuatro ataques a API con implicaciones de cumplimiento

¿Cómo puede afectar una vulneración de API a la estrategia de cumplimiento de una empresa? A continuación, se incluyen algunos ejemplos:

- Una aplicación de gestión de proyectos conocida se vio comprometida por un atacante que aprovechó un terminal de API que carecía de controles de autenticación. El atacante vulneró la API, obtuvo acceso no autorizado a la información de millones de usuarios y, meses después, filtró más de 21 GB de datos en Internet, incluidas las direcciones de correo electrónico y los miembros de la junta.
- Más de 11 millones de registros de clientes de una gran empresa de telecomunicaciones quedaron expuestos, supuestamente debido a una API que, sin saberlo, se encontraba expuesta a Internet y que no requería autenticación. Los atacantes vulneraron la API, vieron que carecía de un identificador único, adivinaron su número de ID y solicitaron fácilmente datos confidenciales.
- Se ha informado de que una empresa de redes sociales se ha visto afectada dos veces en los últimos años por una táctica de scraping que ha sido posible gracias al uso inadecuado de API. En el primer caso, se extrajeron datos privados de 500 millones de perfiles de usuario que se vendieron posteriormente. En el segundo caso, un atacante creó una base de datos que incluía números de teléfono y datos salariales extraídos de 700 millones de usuarios.
- Esta misma técnica se utilizó contra otra empresa de redes sociales para exfiltrar datos de millones de usuarios. La empresa recibió una sanción de 5000 millones de dólares porque un proveedor externo utilizó la API de la empresa para recopilar datos confidenciales. No importaba que el proveedor usara de forma indebida la API; la *propia* empresa fue sancionada porque no supervisaba su aplicación.

Seis ejemplos de normativas y marcos sobre seguridad de las API

En muchas normativas y marcos, las API no necesariamente 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. Por ejemplo:

- La Norma de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) v4.0 ofrece orientación para confirmar que el software de una empresa utiliza de forma segura las funciones de los componentes externos. Aquí se incluyen API que transmiten datos de pago desde una aplicación móvil hasta el sistema de un banco.
- El marco de desarrollo de software seguro del Instituto Nacional de Normas y Tecnología (NIST) proporciona orientación para crear software que esté bien protegido en todo momento y responder a las vulnerabilidades. Las API son la base del desarrollo de software.

En muchos casos, las normativas sugieren objetivos definidos de forma poco estricta para proteger los datos, como el requisito del Reglamento General de Protección de Datos (RGPD) que sugiere "medidas de seguridad adecuadas". Es posible que sus API reciban millones de llamadas al día, de clientes *y* de atacantes, para proporcionar esos datos. Depende de usted determinar qué controles de seguridad son necesarios y, a continuación, demostrar cómo funcionarán.

Analicemos más detenidamente las normativas y los marcos con implicaciones directas para su ecosistema de API.

1. PCI DSS v4.0

La norma PCI DSS, creada por el Payment Card Industry Data Security Council (Consejo sobre Normas de Seguridad de la PCI), se ha convertido en un estándar global para la protección de los datos de pago. Si su empresa acepta las principales tarjetas de crédito y trata, almacena o transmite electrónicamente los datos de los titulares de tarjetas, debe cumplir esta norma.

Los requisitos de la versión original abarcan los pilares fundamentales de seguridad que son tan importantes actualmente como lo eran cuando se publicó la norma PCI DSS en 2006, como la asignación de acceso a los datos del sistema y de los titulares de tarjetas según sea necesario y la definición de los requisitos de acceso por roles.

No obstante, con la norma PCI DSS v4.0 en vigor, las empresas necesitan adaptar sus programas de cumplimiento para tener en cuenta a los atacantes que tienen como objetivo las miles de API que incluyen las tecnologías de pago. En general, la norma PCI DSS v4.0 se centra en cuatro objetivos clave:

1. Seguir satisfaciendo las necesidades de seguridad del sector de pagos.
2. Abogar por la seguridad como un proceso continuo.
3. Ofrecer a las empresas flexibilidad (por ejemplo, nuevas herramientas o nuevos controles) para cumplir los requisitos.
4. Mejorar los métodos y procesos de validación.

El requisito 6.2.3 de la norma PCI DSS v4.0 se centra en la necesidad de que las organizaciones revisen el código de las aplicaciones hechas a medida (es decir, el código desarrollado por un proveedor externo, pero no de las aplicaciones comerciales estándar disponibles en el mercado) para garantizar que no se transmita ninguna vulnerabilidad a la fase de producción. Este requisito, específico de las API, ofrece orientación para confirmar que el software de una organización utiliza de forma segura las funciones de los componentes externos (bibliotecas, marcos, API, etc.). Requisitos como estos subrayan el papel tan importante que desempeñan las API en la cadena de suministro de software y lo que se necesita para protegerlas.

Las API se han convertido en el método predeterminado de conectividad e intercambio de datos en los entornos de aplicaciones modernos. Teniendo esto en cuenta, proteger las API tanto con una perspectiva de preproducción ("shift-left") como con una perspectiva de posproducción ("shield-right") es esencial para que su empresa digital pueda resistir los ataques. A continuación se presentan algunas prácticas recomendadas de seguridad de API para cumplir el requisito 6.2.3:

- Confirmar el uso de componentes basados en API y su nivel de seguridad (por ejemplo, detectar errores de configuración que provoquen vulnerabilidades, incluido el uso de métodos de cifrado débiles).
- Validar el comportamiento normal y esperado del uso de la API e implementar controles para bloquear a los agentes sospechosos de manera que no vulneren sus sistemas (por ejemplo, comprobar el comportamiento de la aplicación para detectar vulnerabilidades lógicas).
- Detectar los marcos de terceros que utiliza para implementar las API y determinar si alguno de ellos está obsoleto y es vulnerable.
- Crear un inventario completo de todas las API, incluidas las diferentes versiones de API que está ejecutando; esto proporciona información sobre las puertas traseras y las posibles funciones no documentadas que debe gestionar.
- Validar la seguridad de su código de API y evitar transmitir cualquier vulnerabilidad relacionada con las API a la fase de producción.
- Implementar prácticas recomendadas de codificación segura para las API, lo que le permitirá adoptar un enfoque programático para distribuir código de forma segura y continua.

2. Reglamento General de Protección de Datos (RGPD)

El RGPD es una legislación de la Unión Europea (UE) cuyo objetivo es reforzar y unificar la protección de datos de las personas dentro de la UE. Sin embargo, el RGPD no se limita a las empresas con sede en la UE; cualquier organización que ofrezca bienes o servicios de consumo en la UE debe cumplirlo.

El reglamento establece que los datos personales son información que se puede relacionar o conectar con una persona individual. Los datos regulados por el RGPD pueden incluir el nombre, la información de contacto, los datos bancarios y financieros y la información médica de una persona. En el ámbito más técnico, los datos cubiertos también incluyen datos de geolocalización, como direcciones IP y cookies web.

¿Qué significa esto para la seguridad de las API? Tanto si desarrolla aplicaciones o microservicios como dispositivos del Internet de las cosas (IoT), las API que constituyen la base de estas tecnologías probablemente intercambien datos regulados por el RGPD. Por lo tanto, las organizaciones que desarrollan API accesibles a través de Internet deben incluir la protección de datos en su diseño desde el principio, no después.

Tenga en cuenta el principio de privilegio mínimo, que requiere garantizar que los usuarios solo tengan los permisos mínimos necesarios para realizar su trabajo.

El artículo 25 del RGPD tiene *sus raíces* en los mínimos privilegios, lo que exige a las empresas que implementen "medidas técnicas y organizativas apropiadas con miras a garantizar que, de forma predeterminada, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento". A su vez, los desarrolladores de API deben implementar controles de autenticación y autorización de usuarios para proteger los datos confidenciales que fluyen a través de sus API. Los equipos de desarrollo de API también deben garantizar la confidencialidad de los datos en tránsito mediante el uso de protocolos de comunicación seguros para cifrar el intercambio de información entre el cliente y el servidor.

Sin embargo, ¿qué ocurre con el ecosistema existente de API que las organizaciones han creado en los últimos años o incluso décadas? Una parte importante de las API empresariales no se gestiona, queda olvidada o se ejecuta de forma permanente sin controles ni ajustes. En estos casos, el cumplimiento del RGPD requiere:

- Detectar todas las API del entorno de TI.
- Evaluar sus factores de riesgo (por ejemplo, los tipos de datos que han estado intercambiando y quién o qué puede acceder a esos datos).
- Corregir cualquier vulnerabilidad, como errores de configuración o mecanismos de autenticación débiles.
- Probar las API continuamente para garantizar la resiliencia frente a los métodos tradicionales y emergentes de ataque y vulneración.

3. Ley de Resiliencia Operativa Digital (DORA)

Dado el papel del sector financiero de la UE como operador de infraestructuras críticas, los requisitos del reglamento DORA tienen por objeto ayudar a las organizaciones de los estados miembros de la UE a resistir y recuperarse de los ciberataques. Con la ley DORA, el sector tendrá un marco vinculante y amplio de gestión de riesgos para las tecnologías de la información y las comunicaciones (TIC). El objetivo de la ley es armonizar y endurecer los requisitos para las empresas financieras de la UE, ya que el panorama actual conlleva innumerables reglamentos y normas.

En total, la ley DORA afecta a más de 22 000 instituciones financieras y proveedores de servicios de TI de la UE. Cabe destacar que aquí se incluyen terceros que proporcionan a las empresas financieras de la UE sistemas y servicios de TIC, entre ellos, los proveedores de servicios en la nube. La ley exige a las instituciones financieras que desarrollen estrategias en materia de riesgos de TIC de terceros y actúen con la debida cautela para determinar la idoneidad de los proveedores.

La ley DORA establece varios requisitos relacionados con la seguridad de las API, como la estabilidad operativa digital, que requiere que las organizaciones implementen programas de pruebas periódicas para identificar posibles brechas, vulnerabilidades o deficiencias en la estabilidad operativa digital. Piense en pruebas de seguridad de red, pruebas de penetración, pruebas de aplicaciones web y muchas más. Es importante realizar revisiones obligatorias con base en pruebas de penetración para la detección de amenazas (TLPT), según el tamaño, el riesgo y el perfil empresarial de la institución financiera. Es igualmente importante probar periódicamente sus API para detectar vulnerabilidades.

En la ley DORA se describen ejemplos de pruebas de seguridad que incluyen pruebas de API y aplicaciones basadas en web. Esto incluye el uso de recursos orientados al público, como el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP). En concreto, los 10 principales riesgos de seguridad de las API según OWASP ayudan a las organizaciones a identificar errores de configuración, puntos débiles, defectos de lógica y problemas de código que permiten a los atacantes obtener acceso, manipular o controlar de cualquier otro modo los recursos de la organización.

4. Ley de transferibilidad y responsabilidad de seguros médicos (HIPAA)

La ley HIPAA se centra en las normas de privacidad y seguridad de los datos para custodiar la información sanitaria protegida (PHI) en los registros sanitarios electrónicos (EHR), las plataformas de prescripción médica electrónica y los sistemas de TI de atención sanitaria. Cualquier proveedor de atención sanitaria, administrador de seguros o centro de compensación de EE. UU. que almacene o transmita electrónicamente la PHI debe cumplir con la HIPAA. Esto implica garantizar la confidencialidad, la integridad y la disponibilidad de la PHI y protegerla contra la revelación no autorizada y el uso inadecuado.

La ley HIPAA es un ejemplo de una normativa que tiene importantes repercusiones para las API, incluso si no menciona explícitamente las API en sus requisitos.

Piense en un proveedor tecnológico que crea portales de pacientes para clínicas de atención médica abiertos ininterrumpidamente. Una función subyacente de estos portales es la capacidad de ofrecer a los pacientes un acceso eficiente y seguro a los datos de sus visitas al médico, los resultados de las pruebas, los pagos y mucho más. Las API facilitan ese intercambio. Tanto la clínica como el proveedor están obligados a cumplir los requisitos de la HIPAA.

La norma de privacidad de la HIPAA especifica que las entidades cubiertas "deben desarrollar e implementar políticas y procedimientos que restrinjan el acceso y los usos de la información sanitaria protegida según las funciones específicas de los miembros de su plantilla". Por lo tanto, los desarrolladores de API de una organización deben integrar medidas de seguridad técnicas como la autenticación, los ID de usuario únicos y los controles de acceso basados en funciones para garantizar que se aplican los mínimos privilegios.

La visibilidad también es esencial para las organizaciones cubiertas por la HIPAA, ya sea un proveedor cuyo equipo de TI crea API personalizadas o un proveedor tercero que desarrolla API para ese proveedor. Las organizaciones necesitan evaluaciones e informes en tiempo real sobre la situación de riesgo de cada API, incluidos los tipos de PHI que transmiten. Esto es relevante para el cumplimiento y para ajustarse al requisito de la HIPAA de responder a las personas que solicitan información sobre cuándo, dónde, por qué y a quién se ha revelado su PHI.

5. Directiva de seguridad de sistemas de redes y de información (NIS2)

La UE adoptó la versión 2.0 de la Directiva NIS en enero de 2023, que se basa en las directrices de la versión original para proteger la infraestructura de TI y notificar incidentes. Aunque la versión 2.0 no menciona específicamente las API, sus requisitos tienen importantes repercusiones para la protección y gestión de estas, ya que son parte integral del funcionamiento de muchos servicios digitales en las organizaciones sujetas a la directiva. Cabe destacar que la directiva NIS2 incluye:

- Una gama más amplia de sectores, por ejemplo, los proveedores de servicios en la nube y las empresas de redes sociales se unen a la lista existente, que incluye a los operadores de infraestructuras críticas. En estos sectores, donde las API se utilizan ampliamente para la integración y la prestación de servicios, garantizar la seguridad de las API se convierte en una prioridad.
- Un nuevo énfasis en proteger las cadenas de suministro: las empresas deben evaluar el riesgo y proteger sus cadenas de suministro de TI y sus relaciones con proveedores externos. Dado que las API se utilizan a menudo para integrar servicios externos, garantizar su seguridad es fundamental para el cumplimiento.
- Un requisito de crear un sistema de gestión de la seguridad de la información que evalúe a las personas, las políticas y la tecnología para proteger los recursos confidenciales y garantizar la resiliencia operativa. Dado que las API son vectores de ataque de rápido crecimiento, deben incluirse en las estrategias de gestión de riesgos.
- La notificación de incidentes de ciberseguridad importantes, incluidas las vulneraciones de API. Por lo tanto, las organizaciones deben establecer mecanismos para supervisar, detectar e informar de incidentes relacionados con las API.

6. Directrices para los reguladores de servicios financieros de EE. UU.

El Consejo Federal de Certificación de Instituciones Financieras (FFIEC) crea las directrices y normas para que los reguladores federales supervisen el sector financiero de EE. UU. Esto incluye la Reserva Federal, la FDIC, la Oficina del Contralor de la Moneda (OCC) y la NCUA. La misión del consejo es proteger a los consumidores e inversores del fraude, el abuso y el uso indebido. Aunque no es una normativa, las directrices de la FFIEC son fundamentales para garantizar que las empresas financieras sepan cómo ajustarse a sus medidas de seguridad recomendadas.

Este es un ejemplo clave de un documento que incluye directrices específicas sobre cómo proteger las API y, a su vez, proteger a los consumidores del fraude y el robo de identidad. A continuación se ofrece una descripción general:

- **Inventario:** la FFIEC recomienda crear un inventario de todos los sistemas de información (incluidas las API) que requieren autenticación y controles de acceso. Esto no solo se aplica a las instituciones financieras, sino también a sus terceros, como los proveedores de servicios en la nube.
- **Autenticación:** la API solo debe permitir el acceso a usuarios autorizados. Es fundamental identificar a todos los usuarios (por ejemplo, clientes) para los que se necesitan controles de acceso. También es importante identificar a los usuarios que requieran controles mejorados, como la autenticación multifactorial.
- **Autorización:** la API solo debe permitir el acceso a recursos específicos a los usuarios autorizados. Dicho esto, la FFIEC recomienda implementar seguridad por capas; por ejemplo, actividades de supervisión, registro y notificación para identificar y hacer un seguimiento del acceso no autorizado.
- **Gestión de riesgos:** existen varias prácticas eficaces de gestión de riesgos que la FFIEC identifica en sus directrices más recientes. Sin embargo, mencionan explícitamente las API en la categoría de inventario de sistemas de información, lo que significa que necesita un inventario preciso de sus API.

Una organización puede estar al día en cuanto a amenazas conocidas, como el phishing o el ransomware, pero la FFIEC pide identificar *cualquier* ciberamenaza con una "probabilidad razonable de afectar a los sistemas de información de las instituciones financieras" y a sus datos. Como se ha mencionado en la introducción, el 78 % de las organizaciones se han enfrentado a incidentes de seguridad relacionados con las API, por lo que puede confiar en que la protección de las API es un imperativo de cumplimiento a medida que los requisitos de los reguladores financieros siguen evolucionando.

Supere los desafíos de cumplimiento con las prácticas recomendadas de protección de las API

El panorama de amenazas actual exige una solución de seguridad de las API completa que proporcione detección de API, gestión de la situación, protección en tiempo de ejecución y pruebas de seguridad de las API. Este enfoque integral funciona como un complemento para cualquier WAF o puerta de enlace de API que ya estén instalados.

1. Detección de las API

Es habitual tener API que nadie conoce. La mayoría de las organizaciones tienen poca o ninguna visibilidad sobre un gran porcentaje de su tráfico de API, a menudo porque asumen que todas sus API se enrutan a través de una puerta de enlace de API. Sin embargo, este no es el caso. Sin un inventario completo y preciso, su empresa está expuesta a toda una serie de riesgos. Capacidades principales necesarias:

- Localización y realización de un inventario de todas sus API, independientemente de cuál sea su configuración o tipo.
- Detección de las API inactivas, heredadas y zombis.
- Identificación de los dominios ocultos olvidados, descuidados o desconocidos.
- Eliminación de los puntos ciegos y descubrimiento de posibles rutas de ataque.

2. Gestión de la situación de las API

Con un inventario completo de las API, es fundamental conocer qué tipos de datos se transmiten a través de las API y cómo afecta esto a su capacidad para cumplir los requisitos normativos. La gestión de la situación de las API proporciona una visión completa del tráfico, el código y las configuraciones para evaluar el nivel de seguridad de las API de su organización. Capacidades principales necesarias:

- Análisis automático de la infraestructura para detectar errores de configuración y riesgos ocultos.
- Creación de flujos de trabajo personalizados para informar acerca de las vulnerabilidades a los principales interesados.
- Identificación de las API y los usuarios internos que pueden acceder a los datos confidenciales.
- Clasificación de los problemas detectados en función de la gravedad para priorizar la corrección de los más críticos.

3. Seguridad en tiempo de ejecución de las API

Sin duda, ya conoce el concepto de "asumir que se va a producir una filtración". Las filtraciones y los ataques específicos de las API están alcanzando el mismo grado de inevitabilidad. Para todas las API activas en fase de producción, debe ser capaz de detectar y bloquear los ataques en tiempo real. Capacidades principales necesarias:

- Supervisión de la manipulación y filtración de datos, las infracciones de políticas, el comportamiento sospechoso y los ataques a las API.
- Análisis del tráfico de las API sin necesidad de realizar cambios adicionales en la red ni implementar agentes difíciles de instalar.
- Integración de los flujos de trabajo existentes (incidencias, gestión de información y eventos de seguridad [SIEM], etc.) para alertar a los equipos de seguridad y operaciones.
- Prevención de los ataques y del uso indebido de los datos en tiempo real con el proceso de corrección parcial o completamente automatizado.

4. Prueba de seguridad de las API

Los equipos de desarrollo de las API se ven sometidos a la presión de trabajar con la mayor rapidez posible. La velocidad es esencial para todas las aplicaciones desarrolladas, lo que facilita que se produzca una vulnerabilidad o un defecto de diseño y que, posteriormente, no se detecte. Probar las API durante el desarrollo antes de que se envíen a la fase de producción reduce en gran medida tanto el riesgo como el coste de corregir una API vulnerable. Capacidades principales necesarias:

- Ejecución de una amplia variedad de pruebas automatizadas que simulan tráfico malicioso.
- Descubrimiento de las vulnerabilidades antes de poner las API en funcionamiento, lo que reduce el riesgo de que un ataque logre su objetivo.
- Análisis de las especificaciones de sus API con respecto a las políticas y normativas de control establecidas.
- Realización de pruebas de seguridad bajo demanda dirigidas a las API o como parte de un proceso de integración e implementación continuas (CI/CD).

Cómo Akamai API Security puede simplificar las complejidades del cumplimiento en materia de API

Las API son una de las principales causas de las vulneraciones que las normativas actuales buscan prevenir. ¿Qué se necesita para proteger su empresa a medida que se multiplican las API y sus riesgos? Las herramientas existentes que muchas organizaciones utilizan para la protección básica de las API proporcionan cierta protección, pero no es suficiente. Si busca una forma mejor de proteger las API de su organización y demostrar el cumplimiento, nos gustaría ayudarle.

Para todos los requisitos y directrices que se tratan en este white paper, Akamai API Security refuerza la protección que las empresas necesitan, no solo para cumplir las normativas, sino también para proteger los datos y la confianza de sus clientes.

La completa solución de Akamai protege las API en sus etapas iniciales de desarrollo hasta la posproducción, lo que le permite seguir las prácticas recomendadas fundamentales:

- Detección de las API.
- Gestión de la situación.
- Protección en tiempo de ejecución.
- Pruebas de seguridad.

Obtenga más información sobre las API y cómo protegerlas de los ataques**.**

Descubra cómo Akamai API Security puede ayudar a su organización**.**

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 septiembre de 2024.