CAPACIDADES DE PROTECCIÓN DE APLICACIONES WEB Y API:

lista de control para instituciones financieras

Las interfaces de programación de aplicaciones (API) tienen un gran potencial y la capacidad de facilitar las interconexiones entre todo tipo de dispositivos, aplicaciones y datos. Son la tecnología en la que se apoya una creciente variedad de estrategias y actividades tanto internas como externas de los bancos. Además, prometen una mayor apertura para aumentar la competencia en beneficio de los clientes. Sin embargo, el rápido crecimiento de las API en el sector de los servicios financieros ha ampliado la superficie de ataque y ha introducido nuevos riesgos para la seguridad.

Integrar una solución para la protección de las API y las aplicaciones web a la hora de planificar, implementar u optimizar su estrategia de seguridad de la información permitirá a su empresa entender los riesgos específicos a los que se enfrenta, identificar las posibles lagunas y detectar las amenazas. Para seguir siendo competitivas, las instituciones financieras necesitan una solución de protección de aplicaciones web y API (WAAP) que les proporcione una visibilidad continua, con información detallada, así como la capacidad de detectar y detener los ataques más sofisticados.

Estas listas de control pueden utilizarse para evaluar las capacidades de los proveedores o consultar los requisitos de implementación de una solución WAAP eficaz.

01. REQUISITOS DE LA PLATAFORMA

02. PROTECCIÓN ADAPTABLE DE APLICACIONES WEB Y CONTRA DDoS

03. VISIBILIDAD, CONTROL Y PROTECCIÓN DE LAS API

04. GESTIÓN FLEXIBLE

01 REQUISITOS DE LA PLATAFORMA

- Escalabilidad para responder a las exigencias del tráfico y proporcionar protección continua sin que afecte al rendimiento
- Arquitectura capaz de superar los desafíos que supone la dispersión geográfica de las aplicaciones
- Capacidades de registro de auditoría para garantizar un uso adecuado
- Protección de los orígenes del sitio en entornos locales y de nube privada o pública (incluidos los entornos multinube y de nube híbrida)
- Mitigación de ataques DDoS en la capa de red [L3/4] con un acuerdo de nivel de servicio de cero segundos
- Visibilidad de los atacantes, así como de la frecuencia y la gravedad de los ataques, en toda la plataforma gracias a la inteligencia colectiva
- Proxy inverso con tráfico web a través de los puertos 80 y 443
- Protección de la privacidad en la red con cifrado SSL/TLS
- Líder demostrado en la categoría a la que corresponda la solución durante al menos 5 años según un tercero imparcial
- Detección y alerta automáticas que indiquen cuándo y dónde se está transmitiendo información de identificación personal (PII) para protegerla de las filtraciones de datos

Las instituciones financieras tienen la responsabilidad de proteger la información confidencial y financiera de sus clientes ante las amenazas de seguridad, que no paran de evolucionar. Para responder ante ellas, su solución de seguridad para aplicaciones web debe ser flexible, escalable y fácil de gestionar.

PROTECCIÓN ADAPTABLE DE APLICACIONES WEB Y CONTRA DDoS 02

La seguridad debe ir más allá de la detección tradicional basada en firmas y adoptar formas más avanzadas y adaptables de protección de las aplicaciones web y contra ataques DDoS, a fin de obtener resultados más fiables y precisos.

- Detección de ataques que supere el modelo basado en firmas con un sistema de puntuación por anomalía y riesgo
- Reglas de WAF totalmente gestionadas para eliminar la necesidad de configurarlas y actualizarlas continuamente
- Puntuación de reputación del cliente e inteligencia para las direcciones IP individuales y compartidas
- Funciones de aprendizaje automático, minería de datos y detección heurística para identificar las amenazas de rápida evolución
- Actualización automática de las reglas de firewall de aplicaciones web (WAF) con inteligencia contra amenazas en tiempo real proporcionada por expertos en seguridad
- Capacidad para realizar pruebas de las reglas de WAF nuevas o actualizadas sobre el tráfico en vivo antes de implementarlas en producción
- Protección (como mínimo) contra ataques de inyección SQL, XSS, inclusión de archivos, inyección de comandos, SSRF, SSI y XXE
- Reglas predefinidas totalmente personalizables para satisfacer los requisitos específicos del cliente
- Protección contra ataques DoS volumétricos a la capa de la aplicación [L7] diseñados para saturar los servidores web con una actividad incesante en las aplicaciones
- Reglas personalizadas para ofrecer una protección rápida contra patrones de tráfico específicos (aplicación de parches virtuales)
- Limitación del índice de solicitudes para ofrecer protección contra el tráfico de bots automatizado o excesivo
- Protección contra ataques dirigidos directamente al origen
- Controles por dirección IP y área geográfica a través de múltiples listas de redes para bloquear o permitir el tráfico procedente de direcciones IP, subredes o zonas geográficas específicas
- Protección contra clientes automatizados, como el análisis de vulnerabilidades y las herramientas de ataque web

03

VISIBILIDAD, CONTROL Y PROTECCIÓN DE LAS API

- Funciones automáticas de detección y creación de perfiles para API desconocidas y cambiantes (incluidos los terminales, las características y las definiciones de API)
- Inspección automática de solicitudes XML y JSON para detectar ataques a API
- Controles de frecuencia (limitación) para terminales de API basados en claves de API
- Listas de redes de API (de autorización o de bloqueo) basadas en las direcciones IP y en las zonas geográficas
- Gestión del ciclo de vida de las API con control de versiones
- Reglas de inspección de API personalizadas para satisfacer los requisitos específicos del usuario
- Autenticación y autorización seguras a través de la validación de JSON Web Tokens (JWT)
- Capacidad de predefinir formatos de objeto JSON y XML aceptables para restringir el tamaño, el tipo y el alcance de las solicitudes de API
- Protección de las infraestructuras back-end de las API contra ataques de actividad baja y lenta diseñados para agotar los recursos (por ejemplo, POST lento y GET lento)
- Definición de las solicitudes de API permitidas en función de la clave (donde la cuota de cada clave se define de forma independiente) para controlar totalmente el consumo
- Integración de API mediante definiciones de API estándar (Swagger/OAS y RAML)

La protección de las API se ha convertido en una parte esencial de la seguridad en las aplicaciones web. Necesita una solución WAAP con capacidades sólidas de detección, protección y control de las API para mitigar sus vulnerabilidades y reducir la superficie de riesgo.

GESTIÓN FLEXIBLE 04

- API y CLI abiertas para integrar tareas de configuración de la seguridad en los procesos de CI/CD
- Paneles, informes y capacidades heurísticas de alerta en tiempo real
- Integración con aplicaciones de gestión de eventos e información de seguridad (SIEM) en entornos locales y en la nube
- Interfaz de usuario (IU) centralizada para ver en detalle la telemetría de ataques y analizar eventos de seguridad
- Entorno de ensayo (*Staging*) completo y la capacidad de implementar un control de los cambios
- Protecciones de seguridad autorreguladas que se adaptan automáticamente al tráfico
- Servicios de seguridad totalmente gestionados para descongestionar o mejorar la gestión de la seguridad, el control y la mitigación de amenazas

Necesita flujos de trabajo simples y automatizados para optimizar su inversión y mejorar la eficiencia operativa. Tanto si se trata de proteger aplicaciones nuevas o cambiantes, como si hay que aplicar nuevas reglas de WAF o protecciones adicionales a las API, el proceso debe ser fluido e intuitivo.

Akamai ofrece protección de API y aplicaciones web a las principales instituciones financieras del mundo. Cada día, nuestro equipo de investigación de la seguridad global obtiene información de millones de ataques a aplicaciones web y de solicitudes de bots y API. Estos datos, junto con el aprendizaje automático avanzado y la investigación de amenazas, nos permiten mejorar continuamente, detectar nuevas amenazas y crear soluciones innovadoras.

Las soluciones de seguridad para aplicaciones web y API de Akamai le permitirán proteger su institución financiera frente a los ataques DDoS, a las aplicaciones web y de API más avanzados. Manténgase conectado a nuestra investigación más reciente visitando nuestro Centro de seguridad.

Akamai

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Gracias a la plataforma informática más distribuida del mundo, de la nube al Edge, nuestros clientes pueden desarrollar y ejecutar las aplicaciones con facilidad, mientras acercamos las experiencias a los usuarios y mantenemos las amenazas a raya. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com/es y akamai.com/es/blog, o siga a Akamai Technologies en Twitter y LinkedIn.