LISTA DE COMPROBACIÓN DE AKAMAI

Lista de comprobación de las capacidades de protección de aplicaciones web y API

El despliegue de una solución de seguridad para aplicaciones web y API a la hora de planificar, implementar u optimizar su estrategia de seguridad de la información proporcionará a su organización la capacidad de entender riesgos de seguridad específicos, abordar brechas de seguridad y detectar amenazas. Necesita una solución de protección de aplicaciones web y API (WAAP) que le proporcione una visibilidad continua con información completa, así como la capacidad de detectar y detener los ataques más sofisticados.

Esta lista de comprobación puede utilizarse para evaluar las capacidades de los proveedores o consultar los requisitos de implementación de una solución WAAP eficaz.

Categoría 1: Requisitos de la plataforma

Existe una gran variedad de organizaciones con diferentes tipos de requisitos. Su solución de seguridad para aplicaciones web debe ser flexible, escalable y fácil de gestionar.

- [ ] Escalabilidad para responder a los picos de 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

Categoría 2: Protección adaptable de aplicaciones web y contra DDoS

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

- [ ] Una detección de ataques que supere el modelo basado en firmas con un sistema de puntuación por anomalía y riesgo
- [ ] 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 recursiva en las aplicaciones
- [ ] 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
- [ ] 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

Categoría 3: Visibilidad, control y protección de las API

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.

- [ ] 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
- [ ] Reglas de inspección de API personalizadas para cumplir los requisitos específicos del usuario
- [ ] Capacidad de predefinir formatos 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)
- [ ] Alertas, generación de informes y paneles en tiempo real a nivel de 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 la API con control de versiones
- [ ] Autenticación y autorización seguras a través de la validación de JSON Web Tokens (JWT)
- [ ] 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)

Categoría 4: Gestión flexible

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.

- [ ] API e interfaz de línea de comandos (CLI) abiertas para integrar tareas de configuración de la seguridad en los procesos de CI/CD
- [ ] Integración con aplicaciones de gestión de eventos e información de seguridad (SIEM) en entornos locales y en la nube
- [ ] Entorno de ensayo (*Staging*) completo y la capacidad de implementar un control de los cambios
- [ ] Protecciones de seguridad autorreguladas que se adapten automáticamente al tráfico
- [ ] Paneles, informes y capacidades heurísticas de alerta en tiempo real
- [ ] Interfaz de usuario (UI) centralizada para ver en detalle la telemetría de ataques y analizar eventos de seguridad
- [ ] Flexibilidad para gestionar la WAAP mediante controles altamente personalizados y protecciones totalmente automatizadas
- [ ] Servicios de seguridad totalmente gestionados para descongestionar o aumentar la gestión de la seguridad, el control y la mitigación de amenazas

Akamai Connected Cloud obtiene información de millones de ataques a aplicaciones web, miles de millones de solicitudes de bots y billones de solicitudes de API cada día. Estos datos, junto con el aprendizaje automático avanzado y la investigación de amenazas, nos permiten mejorar continuamente, detectar nuevas amenazas y crear soluciones innovadoras.

Para obtener más información, visite akamai.com o póngase en contacto con su equipo de ventas de Akamai.

 | Asistencia | Publicado en octubre de 2023