CAPACIDADES DE PROTEÇÃO DE APLICAÇÕES WEB E APIS:

Uma lista de verificação para instituições financeiras

As interfaces de programação de aplicações (APIs) têm um enorme potencial e capacidade de suportar interconexões entre todos os tipos de dispositivos, aplicações e dados. São a tecnologia que sustenta uma diversidade crescente de estratégias e atividades bancárias internas e externas. Têm a promessa de uma maior abertura para maior concorrência e benefícios para os clientes. No entanto, o rápido crescimento das APIs em serviços financeiros expandiu a superfície de ataque e introduziu novos riscos de segurança.

Incorporar uma solução de segurança para aplicações Web e APIs enquanto você planeja, implementa ou otimiza sua estratégia de segurança das informações fornecerá à sua organização a capacidade de avaliar riscos específicos, abordar lacunas de segurança e detectar ameaças. Para permanecerem competitivas, as instituições financeiras precisam de uma solução de proteção de aplicações Web e de API (WAAP) que ofereça visibilidade contínua com insights abrangentes e a capacidade total de identificar e interromper os ataques mais sofisticados.

Estas listas de verificação podem ser usadas para avaliar os recursos do fornecedor ou servir de lista dos requisitos necessários para implementar uma solução WAAP eficaz.

01. REQUISITOS DA PLATAFORMA

02. APLICAÇÃO WEB ADAPTÁVEL E PROTEÇÃO CONTRA ATAQUES DDoS

03. VISIBILIDADE, PROTEÇÃO E CONTROLE DA API

04. GERENCIAMENTO FLEXÍVEL

01 REQUISITOS DA PLATAFORMA

- Escalabilidade para atender às demandas de tráfego e fornecer proteção contínua sem perda de desempenho
- Arquitetura que possa superar os desafios de aplicações geograficamente dispersas
- Recursos de registro de auditoria para garantir o uso adequado
- Proteção de origens de website no local, privados ou em nuvem pública (incluindo multinuvem ou nuvem híbrida)
- Atenuação de DDoS (distributed denial-of-service) na camada de rede [L3/4] com contrato de nível de serviço de zero segundo
- Visibilidade de quem está atacando, da frequência e da gravidade dos ataques com inteligência de ataque em toda a plataforma
- Proxy reverso com tráfego da Web pelas portas 80 e 443
- Proteções de privacidade de rede com criptografia SSL/TLS
- Líder comprovado na categoria de solução há pelo menos 5 anos por uma empresa terceirizada imparcial
- Detecte e alerte automaticamente quando e onde as Informações de Identificação Pessoal (PII) estão sendo transmitidas para se proteger contra vazamentos de dados

As instituições financeiras são responsáveis por proteger seus próprios dados financeiros confidenciais e de clientes contra ameaças à segurança em rápida evolução. Em resposta, a sua solução de segurança de aplicações Web deve ser flexível, dimensionável e fácil de administrar.

APLICAÇÃO WEB ADAPTÁVEL E PROTEÇÃO CONTRA ATAQUES DDoS 02

A segurança de aplicações Web deve ir além da detecção tradicional baseada em assinaturas e adotar formas mais avançadas de aplicação Web adaptável e proteção contra ataques DDoS, para obter resultados de segurança mais precisos e confiáveis.

- Detecção além de ataques baseados em assinatura com classificação baseada em anomalias e riscos
- Regras de WAF totalmente gerenciadas para eliminar a necessidade de configuração e atualizações contínuas
- Pontuação e inteligência de reputação do cliente para endereços IP individuais e compartilhados
- Recursos de machine learning, mineração de dados e detecção baseada em heurística para identificar ameaças em rápida evolução
- Atualizações de regras de WAF (Web Application Firewall) automáticas com inteligência contra ameaças em tempo real desenvolvida por pesquisadores de segurança
- Capacidade de testar regras WAF novas ou atualizadas em relação ao tráfego em tempo real antes de implantar na produção
- Proteção (no mínimo) contra injeção de SQL, XSS, inclusão de arquivo, injeção de comando, SSRF, SSI e XXE
- Regras predefinidas totalmente personalizáveis para atender aos requisitos específicos do cliente
- Proteção contra ataques DoS volumétricos à camada de aplicação [L7] projetados para sobrecarregar servidores da Web com atividade de aplicação recursiva
- Regras personalizadas para proteger rapidamente contra padrões de tráfego específicos (aplicação virtual de patches)
- Limites de taxa de solicitação para proteger contra tráfego automatizado ou excessivo de bots
- Proteção contra ataques diretos na origem
- Controles de IP/localização geográfica por meio de várias listas de rede para bloquear ou permitir o tráfego de IP, sub-rede ou áreas geográficas específicas
- Proteção contra clientes automatizados, como ferramentas de verificação de vulnerabilidades e de ataques da Web

03

VISIBILIDADE, PROTEÇÃO E CONTROLE DA API

- Detecção e criação automática de perfis de APIs desconhecidas e/ou em alteração (incluindo endpoints, características e definições de API)
- Inspeção automática de solicitações XML e JSON para detectar ataques baseados em API
- Controles de taxa (limitação) para endpoints de API com base na chave de API
- Listas de rede da API (lista de permissões/bloqueios) baseadas em IP/localização geográfica
- Gerenciamento do ciclo de vida da API com controle de versão
- Regras de inspeção de API personalizadas para atender aos requisitos específicos do usuário
- Autenticação e autorização seguras por meio da validação de JWT (JSON Web Token)
- Capacidade de predefinir formatos de objeto XML e JSON aceitáveis que restrinjam o tamanho, o tipo e a profundidade das solicitações de API
- Proteção de infraestruturas de back-end de API contra ataques do tipo "low and slow" projetados para esgotar recursos (por exemplo, Slow Post, Slow Get)
- Definição de solicitações de API permitidas por chave (cota para cada chave definida independentemente) para controle total do consumo
- Integração de API usando definições de API padrão (Swagger/OEA e RAML)

As proteções de API tornaram-se uma parte essencial da segurança de aplicações Web. Você precisa de uma solução WAAP com recursos robustos de detecção, proteção e controle de API para mitigar vulnerabilidades de API e reduzir sua área de risco.

GERENCIAMENTO FLEXÍVEL 04

- APIs abertas e a CLI para integrar tarefas de configuração de segurança em processos de CI/CD
- Painéis de controle em tempo real, geração de relatórios e recursos de alerta baseados em heurística
- Integração com aplicativos SIEM (security information and event management, gerenciamento de eventos e informações de segurança) locais e baseados em nuvem
- IU (interface de usuário) centralizada para acessar telemetria de ataque detalhada e analisar eventos de segurança
- Ambiente de staging completo e capacidade de implementar o controle de alterações
- Autoajuste de proteções de segurança que se adaptam automaticamente ao seu tráfego
- Serviços de segurança totalmente gerenciados para transferir ou aprimorar seu gerenciamento de segurança, monitoramento e mitigação de ameaças

Você precisa de fluxos de trabalho simples e automatizados para maximizar seu investimento e melhorar a eficiência operacional. Seja para proteger aplicações novas ou em constante mudança, adotar novas regras de WAF ou estender proteções a APIs, o processo deve ser simples e intuitivo.

A Akamai oferece proteção de aplicações Web e API às principais instituições financeiras do mundo. Todos os dias, nossa equipe de pesquisa de segurança global obtém insights de milhões de ataques a aplicações Web, bilhões de solicitações de bots e trilhões de solicitações de API. Esse nível de percepção, aliado ao machine learning avançado e à pesquisa de ameaças, permite que a Akamai melhore suas soluções, detecte novas ameaças e desenvolva recursos inovadores constantemente.

As soluções de segurança de aplicações Web e API da Akamai protegerão sua instituição financeira contra as formas mais avançadas de ataques a aplicações Web, DDoS e baseados em API. Fique por dentro de nossas pesquisas mais recentes consultando nosso Hub de ameaças.

Akamai

A Akamai potencializa e protege a vida online. As principais empresas do mundo escolhem a Akamai para criar, entregar e proteger suas experiências digitais, ajudando bilhões de pessoas a viver, trabalhar e jogar todos os dias. Com a plataforma de computação mais distribuída do mundo, da nuvem à edge, nós facilitamos o desenvolvimento e a execução de aplicações para os nossos clientes, enquanto mantemos as experiências mais próximas dos usuários e as ameaças ainda mais distantes. Saiba mais sobre as soluções de segurança, computação e entrega da Akamai em akamai.com/pt e akamai.com/pt/blog ou siga a Akamai Technologies no Twitter e no LinkedIn.