LISTA DE VERIFICAÇÃO DA AKAMAI

Lista de verificação de recursos de proteção de aplicações Web e APIs

Implantar 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. Você precisa de uma solução de proteção de aplicações Web e de API (WAAP) que ofereça visibilidade contínua com informações abrangentes e a capacidade total de identificar e interromper os ataques mais sofisticados.

Esta lista de verificação pode ser usada para avaliar os recursos do fornecedor ou servir como lista dos requisitos necessários para implementar uma solução WAAP eficaz.

Categoria 1: Requisitos da plataforma

Existem organizações de todas as formas e tamanhos com graus variados de requisitos. Sua solução de segurança de aplicações Web deve ser flexível, dimensionável e fácil de administrar.

- [ ] 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, privadas ou em nuvem pública (incluindo multinuvem ou nuvem híbrida)
- [ ] Mitigação de DDoS (negação de serviço distribuído) na camada de rede [L3/4] com um contrato de nível de serviço de zero segundo
- [ ] Visibilidade sobre quem está atacando, a frequência dos ataques e a 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

Categoria 2: Proteção adaptável de aplicações Web e contra ataques DDoS

Sua segurança de aplicações Web deve ir além da detecção tradicional baseada em assinaturas e adotar formas mais avançadas de proteção adaptável de aplicações Web e 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
- [ ] 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] desenvolvidos para sobrecarregar servidores da Web com atividade de aplicação recursiva
- [ ] Regras de WAF totalmente gerenciadas para eliminar a necessidade de configuração e atualizações contínuas
- [ ] Pontuação e inteligência de reputação do cliente para indivíduos e endereços IP compartilhados
- [ ] 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 específicos
- [ ] Proteção contra clientes automatizados, como ferramentas de verificação de vulnerabilidades e de ataques da Web

Categoria 3: Visibilidade, proteção e controle da API

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.

- [ ] 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
- [ ] Regras de inspeção de API personalizadas para atender aos requisitos específicos do usuário
- [ ] Capacidade de predefinir formatos de 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" desenvolvidos para esgotar recursos (por exemplo, Slow POST, Slow GET)
- [ ] Alertas, relatórios e painéis em tempo real no nível da 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
- [ ] Autenticação e autorização seguras por meio da validação de JWT (JSON Web Token)
- [ ] 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)

Categoria 4: Gerenciamento flexível

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.

- ☐ APIs abertas e a interface de linha de comando (CLI) para integrar tarefas de configuração de segurança em processos de CI/CD
- ☐ Integração com aplicações SIEM (gerenciamento de eventos e de informações sobre segurança) no local e na nuvem
- ☐ Ambiente de staging completo e capacidade de implementar o controle de alterações
- ☐ Autoajuste de proteções de segurança que se adaptam automaticamente ao seu tráfego
- ☐ Painéis em tempo real, geração de relatórios e recursos de alerta baseados em heurística
- ☐ IU (interface de usuário) centralizada para acessar telemetria de ataque detalhada e analisar eventos de segurança
- ☐ Flexibilidade para gerenciar o WAAP por meio de controles de alto nível de intervenção e/ou proteções totalmente automatizadas
- ☐ Serviços de segurança totalmente gerenciados para transferir ou aprimorar seu gerenciamento de segurança, monitoramento e mitigação de ameaças

A Akamai Connected Cloud coleta informações de milhões de ataques a aplicações da Web, bilhões de solicitações de bots e trilhões de solicitações de API todos os dias. Esse nível de informação aliado ao aprendizado de máquina avançado e à pesquisa de ameaças, permite que a Akamai melhore suas soluções, detecte novas ameaças e desenvolva recursos inovadores constantemente.

Para saber mais, acesse akamai.com ou entre em contato com a equipe de vendas da Akamai.