CHECKLIST AKAMAI

Checklist delle capacità WAAP (Web Application and API Protection)

Implementare una soluzione per la protezione delle applicazioni web e delle API nelle fasi di pianificazione, di implementazione o di ottimizzazione della strategia di sicurezza delle informazioni può offrire alla vostra organizzazione la capacità di comprendere i propri rischi, individuare eventuali falle e rilevare le minacce. Vi serve una soluzione per la protezione delle applicazioni web e delle API (WAAP) in grado di fornire una visibilità continua, completa di informazioni dettagliate e funzionalità complete per identificare e bloccare gli attacchi più sofisticati.

Questa checklist risulta utile per valutare le funzionalità dei fornitori o come promemoria dei requisiti necessari per implementare una soluzione WAAP efficace.

Categoria 1. Requisiti della piattaforma

Poiché le forme e le dimensioni delle organizzazioni possono essere diverse come i loro requisiti, la vostra soluzione per la sicurezza delle applicazioni web deve risultare flessibile, scalabile e facile da gestire.

- [ ] Scalabilità in grado di soddisfare le varie richieste di traffico e fornire una protezione continua senza peggiorare le performance
- [ ] Architettura in grado di superare le sfide correlate alle applicazioni distribuite in varie aree geografiche
- [ ] Funzionalità dei registri di controllo per garantire un corretto utilizzo
- [ ] Protezione delle origini dei siti on-premise, su cloud privati o pubblici (inclusi multicloud o cloud ibridi)
- [ ] Mitigazione degli attacchi DDoS (Distributed Denial-of-Service) a livello di rete [L3/4] con uno SLA (accordo sul livello di servizio) immediato
- [ ] Visibilità sugli autori e sulla frequenza/gravità degli attacchi grazie ad un'intelligence proveniente da varie fonti sulla piattaforma
- [ ] Proxy inverso con traffico web tramite le porte 80 e 443
- [ ] Sistemi di protezione della privacy di rete con crittografia SSL/TLS

Categoria 2. Protezione adattiva dagli attacchi DDoS e alle applicazioni web

La sicurezza delle applicazioni web deve superare i limiti del tradizionale sistema di rilevamento basato su firme per passare a forme più avanzate di protezione adattiva dagli attacchi DDoS e per le applicazioni web per raggiungere una sicurezza più precisa e affidabile.

- [ ] Sistema di rilevamento degli attacchi basati su firme con assegnazione di punteggi in base al rischio e alle anomalie
- [ ] Funzionalità di apprendimento automatico, data mining e rilevamento basato sull'analisi euristica per identificare le minacce in rapida evoluzione
- [ ] Aggiornamenti automatici delle regole WAF (Web Application Firewall) con un'intelligence continua sulle minacce in tempo reale proveniente dai ricercatori sulla sicurezza
- [ ] Possibilità di collaudare regole WAF nuove o aggiornate rispetto al traffico in tempo reale prima dell'implementazione in produzione
- [ ] Protezione (almeno) da attacchi SQL injection, XSS, File Inclusion, Command Injection, SSRF, SSI e XXE
- [ ] Regole predefinite completamente personalizzabili per soddisfare le specifiche esigenze dei clienti
- [ ] Protezione dagli attacchi DoS (Denial-of-Service) volumetrici a livello di applicazione [L7] progettati per sovraccaricare i server web con attività delle applicazioni ricorsive
- [ ] Regole WAF totalmente gestite per evitare di doverle continuamente configurare e aggiornare
- [ ] Intelligence e assegnazione di punteggi di Client Reputation per indirizzi IP singoli e condivisi
- [ ] Regole personalizzate in grado di proteggere rapidamente da specifici modelli di traffico (patching virtuale)
- [ ] Limiti del tasso di richieste per proteggere dal traffico di bot automatizzato o eccessivo
- [ ] Protezione da attacchi mirati direct-to-origin
- [ ] Controlli di indirizzi IP/aree geografiche tramite più elenchi di reti per bloccare o consentire il traffico proveniente da specifici indirizzi IP, sottoreti o aree geografiche
- [ ] Protezione da client automatizzati, come strumenti di analisi delle vulnerabilità e attacchi web

Categoria 3. Visibilità, protezione e controllo delle API

Poiché i sistemi di protezione delle API sono diventati una parte fondamentale nella sicurezza delle applicazioni web, vi serve una soluzione WAAP con solide funzionalità di rilevamento, protezione e controllo delle API per mitigare le relative vulnerabilità e ridurre la superficie di rischio.

- [ ] Operazioni automatiche di rilevamento e profilazione di API sconosciute e/o modificabili (inclusi endpoint, caratteristiche e definizioni delle API)
- [ ] Ispezione automatica delle richieste XML e JSON per il rilevamento di attacchi basati sulle API
- [ ] Regole di ispezione delle API personalizzate per soddisfare specifici requisiti degli utenti
- [ ] Capacità di predefinire i formati XML e JSON supportati in grado di limitare le dimensioni, il tipo e la portata delle richieste API
- [ ] Protezione delle infrastrutture di back-end delle API da attacchi ad attività bassa e lenta progettati per esaurire le risorse (ad es. Slow POST, Slow GET)
- [ ] Generazione di rapporti, avvisi e dashboard in tempo reale a livello delle API
- [ ] Controlli della velocità (limitazione delle richieste) per endpoint basati su chiavi API
- [ ] Elenchi di reti API (consentiti/bloccati) basati su indirizzi IP/aree geografiche
- [ ] Gestione del ciclo di vita delle API con controllo delle versioni
- [ ] Protezione dell'autenticazione e dell'autorizzazione tramite convalida JWT (JSON Web Token)
- [ ] Definizione delle richieste API consentite per chiave (quota per ogni chiave definita in modo indipendente) per un controllo completo sul consumo
- [ ] Onboarding API tramite definizioni API standard (Swagger/OAS e RAML)

Categoria 4. Gestione flessibile

Vi servono workflow semplici e automatizzati per massimizzare il vostro investimento e migliorare l'efficienza operativa. Sia che si tratti di proteggere applicazioni nuove o in continua evoluzione, adottare nuove regole WAF o estendere la protezione alle API, il processo deve risultare semplice e intuitivo.

- ☐ API e CLI (Command-Line Interface) aperte per integrare le attività di configurazione dei sistemi di sicurezza nei processi CI/CD
- ☐ Integrazione con le applicazioni SIEM (Security Information and Event Management) on-premise e basate su cloud
- ☐ Ambiente di staging completo e capacità di implementare il controllo delle modifiche
- ☐ Sistemi di protezione con ottimizzazione automatica che si adattano automaticamente al vostro traffico
- ☐ Funzionalità di generazione di rapporti, avvisi e dashboard basate sull'analisi euristica in tempo reale
- ☐ Interfaccia utente centralizzata per accedere a dati telemetrici dettagliati sugli attacchi e analizzare gli eventi di sicurezza
- ☐ Flessibilità di gestione della soluzione WAAP tramite sistemi di protezione completamente automatizzati e/o controlli di alto livello
- ☐ Servizi di sicurezza totalmente gestiti per migliorare la gestione della sicurezza, il monitoraggio e la mitigazione delle minacce o per alleggerire il carico di lavoro delle risorse dedicate

Akamai Connected Cloud raccoglie informazioni da milioni di attacchi alle applicazioni web, miliardi di richieste di bot e migliaia di miliardi di richieste API ogni giorno. Questo livello di informazioni, insieme ad un'avanzata tecnologia di apprendimento automatico e ricerca sulle minacce, ci consente di apportare continui miglioramenti, rilevare nuove minacce e sviluppare capacità innovative.

Per ulteriori informazioni, visitate il sito akamai.com o contattate il team di vendita di Akamai.

 | Supporto | Data di pubblicazione: 10/23