Akamai

WHITE PAPER

Semplificazione della sicurezza delle applicazioni web

Gli attacchi alle applicazioni web

Le moderne applicazioni web sono diventate complesse, soprattutto con la crescente adozione di architetture basate sui microservizi. L'elevata dipendenza dalle API praticamente in ogni interazione online contribuisce ad aumentare questa complessità e crea nuovi potenziali punti di accesso per gli hacker. Le vulnerabilità web note, nel frattempo, continuano a esistere e vengono reintrodotte nelle applicazioni da tutte le nuove generazioni di programmatori. In risposta, gli odierni criminali si sono evoluti utilizzando attacchi multivettore, DDoS-for-hire e bot per prendere di mira applicazioni web, API e, persino, le vulnerabilità sul lato client.

Tuttavia, gli attacchi opportunistici sono la forma più comune di attacchi web: non colpiscono l'organizzazione direttamente, ma solo dopo aver rilevato una vulnerabilità. Gli scanner usano bot automatizzati per eseguire il crawling dei siti web in modo casuale, alla costante ricerca di una delle migliaia di vulnerabilità. Quando viene rilevata una vulnerabilità, gli autori di attacchi possono portare un database a svelare dati riservati, caricare file dannosi in un server web o sovraccaricare un sito con una travolgente ondata di traffico.

Quali sono i rischi associati agli attacchi web?

Le organizzazioni con una bassa tolleranza al rischio hanno bisogno di un elevato livello di sicurezza per creare una relazione di fiducia, sia internamente (tra sistemi, supply chain, operazioni, ecc.) che esternamente (con partner, clienti, organi direttivi, ecc.). In particolare, le API, dai semplici flussi interni tra le parti di un'applicazione di microservizi alle principali transazioni da azienda ad azienda, devono essere protette accuratamente perché fungono da "collante" digitale per connettere vari sistemi ed ecosistemi di partner e per offrire customer experience digitali e omnicanale.

Sfortunatamente, i criminali informatici dispongono di un arsenale praticamente infinito di metodi di attacchi web progettati per causare il massimo danno. Un attacco riuscito che provoca l'esfiltrazione di dati sensibili o un attacco DDoS che rende i siti non disponibili può compromettere questa relazione di fiducia e causare danni significativi dovuti alla perdita della fedeltà dei clienti, a sanzioni normative, ad azioni legali e al danneggiamento della reputazione del brand.

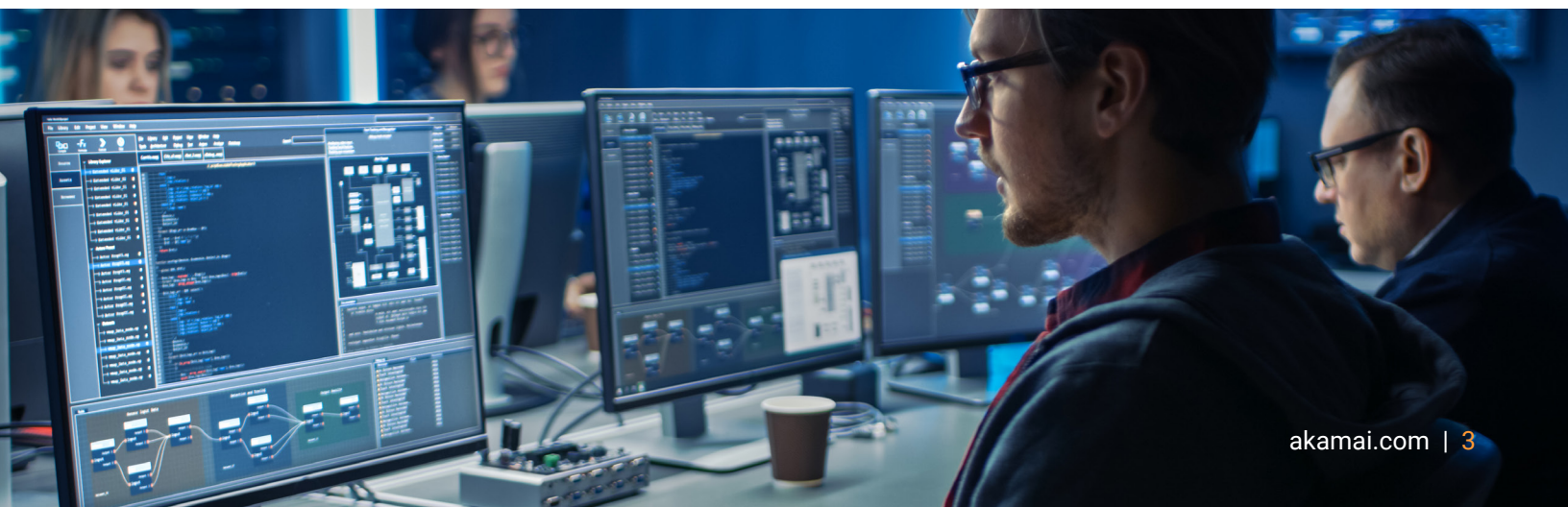
Le sfide legate alla sicurezza delle applicazioni web

Le soluzioni per la protezione delle applicazioni web e delle API (WAAP) su cloud di Akamai sono progettate per mitigare varie forme di attacchi alle applicazioni web, DDoS e basati sulle API. Una delle sfide principali associate ai firewall, tuttavia, è rappresentata dal fatto che i team AppSec devono analizzare e ottimizzare costantemente le regole man mano che le applicazioni cambiano, le minacce si evolvono e gli aggiornamenti diventano disponibili. Assumere addetti alla sicurezza esperti rimane una sfida perché i più competenti spesso cambiano ruolo ogni due anni. Spesso, si tratta di un processo manuale che richiede tempo e operatori qualificati e non è scalabile per la maggior parte delle organizzazioni a causa dei turni, dei cicli dell'apprendimento e delle architetture specializzate per l'integrazione delle tecnologie.

Le policy di sicurezza obsolete possono diventare fonte di frustrazione poiché la complessità degli avvisi riduce drasticamente la capacità di differenziare accuratamente i falsi positivi dagli attacchi reali. I team addetti alla sicurezza che non sono in grado di mettere a punto regole efficaci possono arrivare a sospendere i loro sistemi di protezione e accettare consapevolmente un maggior rischio nel timore di avere un impatto sugli utenti legittimi e interrompere le attività aziendali.

Perché una soluzione WAAP di Akamai?

Akamai App & API Protector è una soluzione WAAP basata su cloud, che include funzionalità di mitigazione e visibilità sui bot, progettata per proteggere applicazioni e API su larga scala da un'ampia gamma di minacce a livello di rete e applicazioni con il minimo sforzo e ridotti costi fissi. La procedura guidata di onboarding self-service di Akamai riduce la necessità di disporre di conoscenze pregresse poiché fornisce la guida e le informazioni necessarie per proteggere le vostre risorse in modo rapido e semplice. Il nostro processo di configurazione automatizzato analizza gli avvisi di sicurezza e apprende il comportamento delle applicazioni per ottimizzare automaticamente i sistemi di protezione, offrendo, pertanto, un maggior risparmio sulle risorse. App & API Protector elimina molti degli odierni problemi relativi ai firewall che costituiscono una fonte di attrito all'interno dell'organizzazione, un onere operativo e un ostacolo all'implementazione.



I sistemi di protezione automatizzati, completamente gestiti da Akamai, vengono applicati sulla piattaforma più distribuita al mondo, pertanto consentono di adottare un approccio automatico alla sicurezza delle applicazioni e alla protezione delle API. La protezione automatica da attacchi web come SQL injection, XSS (Cross-Site Scripting) ed LFI (Local File Inclusion) offre un'ampia copertura senza richiedere praticamente una manutenzione costante. Inoltre, l'applicazione dell'apprendimento automatico e dell'euristica ci consente di migliorare l'identificazione dei modelli di falsi positivi nel traffico sulla base di singole policy, non un controllo generico a livello di rete, per risultati più pertinenti e funzionali.

Verificate il vostro sistema di sicurezza con il nostro strumento di ricerca delle CVE, che fornisce informazioni dettagliate per ogni CVE, inclusi i livelli delle minacce e informazioni sugli attuali sistemi di protezione di Akamai, per aiutarvi a gestire le vostre strategie interne di sicurezza e sviluppo. Inoltre, potete migliorare l'allineamento internamente e velocizzare il time-to-market con le integrazioni SecDevOps predefinite di Akamai, incluse le integrazioni di Akamai come codice, API, CLI e Terraform.

Standard più elevati con le protezioni adattive

In che modo Akamai App & API Protector è in grado di fornire semplicità e accuratezza? Innanzitutto, Akamai Adaptive Security Engine, la tecnologia su cui si basa la soluzione App & API Protector, è unica perché apprende i modelli di traffico e di attacco esclusivi per ciascun cliente, analizza le caratteristiche di ogni richiesta in tempo reale e utilizza tali informazioni per intercettare e adattarsi alle minacce future. Questa tecnologia facilita le operazioni di sicurezza tenendo conto di tutti i dati anomali o sospetti e assegna un punteggio per le minacce a ciascuna richiesta. Più alto è questo punteggio, più aggressivi sono i sistemi di protezione, che, modificati dinamicamente per adattarli al livello di minaccia rilevato, consentono di identificare anche gli attacchi più insidiosi mantenendo i falsi positivi estremamente bassi.

Gli attacchi alle applicazioni, di solito, comportano una forma di ricognizione, ma è durante la ricerca delle vulnerabilità da parte dei criminali che Akamai costruisce le prove sulle relative tecniche e tattiche da adottare. Ciò non solo consente di identificarli tempestivamente, ma lascia una cronologia del traffico specifico nel caso in cui i criminali dovessero ritornare in futuro. Più frequenti sono i tentativi dei criminali, più potenti saranno i sistemi di protezione adottati.

Akamai dispone di informazioni su:

Oltre 780 milioni
di avvisi sugli attacchi alle applicazioni web giornalieri

Oltre 26 miliardi
di richieste di bot

Oltre 932 TB
di dati analizzati ogni giorno

Intelligence sulle minacce basata sul crowdsourcing

Molti dei siti web più attaccati su Internet appartengono a clienti di Akamai, inclusi 9 dei primi 10 retailer, tutte le 10 principali banche, 9 delle prime 10 case farmaceutiche, tutti i 6 reparti dell'esercito statunitense e l'elenco potrebbe continuare. La nostra visibilità copre oltre 780 milioni di attacchi giornalieri alle applicazioni web e 26 miliardi di richieste di bot. Centinaia di ricercatori sulle minacce e analisti di dati di Akamai esaminano oltre 932 TB di nuovi dati ogni giorno alla ricerca di eventuali minacce. Questo livello di informazioni globali, insieme ad un'avanzata tecnologia di apprendimento automatico, intelligenza artificiale e analisi umana, ci consente di bloccare in modo proattivo e predittivo sia gli attacchi comuni che quelli altamente sofisticati.

Akamai ha mitigato gli attacchi alle applicazioni per più di un decennio, ha protetto i clienti e ha mantenuto la disponibilità dell'infrastruttura, resistendo ad alcuni degli attacchi più imponenti. Proseguendo nel suo intento di analizzare e segnalare le nuove minacce, Akamai, dato che gli attacchi si evolvono fino a diventare sempre più ampi e sofisticati, continua ad innovare e adattare le proprie soluzioni per rimanere al passo con i criminali. Inoltre, poiché si basa sull'Akamai Intelligent Edge Platform, App & API Protector include funzionalità predefinite che sono state concepite per garantire performance ottimali di API, siti web e applicazioni.

Esaminate le vostre esigenze relative alla protezione di applicazioni web e API e scoprite i vantaggi offerti dalla soluzione Akamai App & API Protector con questa prova gratuita.

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 06/24.