Storie di clienti Akamai

Una società che opera nei settori dello sport e dei media rileva i rischi per le API nascoste

creando un inventario completo delle API e individuando gli errori di configurazione che favoriscono gli attacchi alle API

Creazione di un inventario accurato

Individuazione dei controlli mancanti

Rilevamento degli attacchi SQL injection

Le applicazioni e le piattaforme digitali stanno rivoluzionando i settori dello sport e dei media con il potere delle API. Queste innovazioni tecnologiche stanno trasformando il modo con cui gli eventi live vengono organizzati, promossi e seguiti, creando nuove opportunità per artisti, organizzatori di eventi e spettatori.

Le API condividono con facilità le informazioni sugli eventi, gli aggiornamenti e i collegamenti ai biglietti su vari canali dei social media, aumentando la visibilità e promuovendo le vendite. Inoltre, le API stanno trasformando il modo di seguire gli eventi live. L'integrazione con le applicazioni mobili e i dispositivi indossabili offre funzioni interattive come pianificazioni personalizzate, mappe interattive e notifiche in tempo reale.

È importante notare, tuttavia, che la natura sensibile delle transazioni e dei dati coinvolti nei settori dello sport e dei media rende fondamentale dare priorità alla sicurezza delle API. I controlli della sicurezza delle API svolgono un ruolo fondamentale nel garantire l'integrità, la riservatezza e la disponibilità dei dati: ecco perché questa società rinomata a livello mondiale nei settori dello sport e dei media si è rivolta a Noname Security (ora acquisita da Akamai).

L'adozione della sicurezza delle API

Il cliente era ben consapevole della necessità di adottare un sistema di sicurezza delle API, ma non sapeva esattamente da dove iniziare e a quali aree dare priorità. Tradizionalmente, l'organizzazione si era focalizzata principalmente sulla sicurezza delle applicazioni credendo che gli strumenti esistenti, come gateway API e soluzioni WAF (Web Application Firewall), fossero adeguati per la protezione delle API. Tuttavia, anche se alcuni strumenti simili possono offrire una protezione basilare, non sono progettati per fornire il grado di visibilità, sicurezza in tempo reale ed

Sports and Media Company

Sede

Stati Uniti

Settore

Media & Entertainment

Soluzione

Akamai API Security

Akamai

esecuzione continua dei test che le soluzioni specializzate per la sicurezza delle API sono in grado di fornire. Molti di questi sistemi di protezione non potevano essere gestiti con l'infrastruttura corrente dell'organizzazione. Ad esempio, due aspetti fondamentali della sicurezza delle API sono l'autenticazione e l'autorizzazione. Meccanismi di autenticazione appropriati sono in grado di garantire che solo gli utenti o i sistemi autorizzati possano accedere alle API.

Il rilevamento delle vulnerabilità

Il team che si occupa della soluzione Akamai API Security ha utilizzato i propri moduli di gestione dei sistemi e protezione del runtime per comprendere il sistema di sicurezza delle API attualmente utilizzato dal cliente. Una volta stilato un inventario accurato delle API presenti nell'ambiente del cliente, siamo riusciti a rilevare eventuali vulnerabilità ed errori di configurazione del sistema di sicurezza esistente.

Innanzitutto, abbiamo rilevato che il cliente aveva subito un attacco SQLi (Structured Query Language injection): si tratta di un tipo di vulnerabilità della sicurezza che si verifica quando un criminale riesce a manipolare i parametri immessi durante una richiesta API per eseguire comandi SQL non autorizzati. Le conseguenze di un attacco SQLi riuscito possono essere gravi: i criminali possono guadagnare l'accesso non autorizzato ai dati sensibili, modificare o eliminare i dati oppure, persino, eseguire comandi arbitrari sul server del database sottostante.

In secondo luogo, abbiamo notato che il cliente non disponeva di un sistema di autenticazione appropriato, senza il quale tutti possono accedere agli endpoint delle API e, potenzialmente, recuperare o modificare i dati sensibili. L'eventuale modifica o eliminazione dei dati può determinare relativi problemi di integrità e la potenziale perdita di informazioni critiche, che può condurre a violazioni dei dati, alla divulgazione non autorizzata di informazioni o, persino, alla compromissione completa del sistema.

Uno sguardo al futuro

Dopo aver assunto il controllo delle proprie API in fase di produzione, il cliente sta cercando di capire come affrontare le vulnerabilità presenti nella fase di preproduzione. Per aiutare le organizzazioni ad individuare e mitigare queste vulnerabilità, Akamai API Security include Active Testing, una soluzione per i test della sicurezza delle API appositamente progettata per comprendere la specifica logica aziendale di un'organizzazione e per fornire una copertura completa delle vulnerabilità specifiche delle API. Active Testing può aiutare le organizzazioni a preparare ed eseguire test tempestivi sulla sicurezza delle API in ogni fase dello sviluppo.

 | Data di pubblicazione 09/24