Storie di clienti Akamai

Un retailer Fortune 100 che opera nel settore bevande protegge API e dati

Dati dei clienti protetti mediante l'identificazione di importanti vulnerabilità delle API e la mitigazione di precedenti episodi di frodi, abusi e furti

Le API (Application Programming Interface) consentono ai retailer di creare experience personalizzate per i clienti, semplificando, al contempo, le operazioni aziendali. Ogni variabile che mette una bevanda nelle mani dei consumatori, tra cui dati di inventario e posizione, inoltro di ordini, pagamenti e, persino, programmi premi, viene distribuita dalle API. Le API hanno rivoluzionato l'experience di acquisto connettendo l'ecosistema dei retailer, i loro partner e i loro clienti, tuttavia, la loro costante vicinanza ai dati sensibili le rende anche un rischio.

Benché i consumatori possano usufruire della nuova experience del retail digitale, sono spesso preoccupati del livello di protezione delle loro informazioni personali. E giustamente: le API stanno diventando sempre più uno dei vettori di attacco preferiti dai criminali informatici. Ecco perché un retailer Fortune 100 che opera nel settore bevande si è rivolto a Noname Security (ora acquisita da Akamai) per mitigare le vulnerabilità presenti nel suo sistema di sicurezza delle API.

Le sfide derivanti dalla crescita del patrimonio delle API

Nei nostri colloqui iniziali, l'azienda si era mostrata preoccupata circa la sua incapacità di raggiungere un elevato livello di governance e sicurezza delle API su scala globale. Per raccogliere le prove necessarie, ha commissionato un programma Bug Bounty pubblicamente documentato che ha identificato un'enorme vulnerabilità, a causa della quale avrebbero potuto essere esfiltrati nomi, indirizzi, e-mail e numeri di telefono di quasi 100 milioni di utenti. Fortunatamente, si è trattato di un programma Bounty, pertanto è stato possibile risolvere i problemi senza alcun danno.

Retail Beverage Company

Sede

Stati Uniti

Settore

Retail, viaggi e turismo

Soluzione

Akamai API Security

Risultati principali

- Più di un miliardo di chiamate API al giorno protette
- 5.000 richieste al secondo protette
- Oltre 200 problemi identificati e risolti

Akamai

Inoltre, l'azienda, disponendo di un livello inadeguato di visibilità e monitoraggio delle API, non riusciva a valutare adeguatamente i rischi e i suoi dati Apigee non fornivano dettagli contestuali (ad es. tipi di dati, comportamento degli utenti, modelli di riferimento, indagini sulle vulnerabilità). A causa di queste vulnerabilità delle API, ne sono derivati episodi di frodi, abusi e furti, che hanno fatto aumentare i costi operativi del retailer.

Rafforzare il suo sistema di sicurezza delle API

La piattaforma Noname API Security (ora parte di Akamai API Security) è riuscita ad inventariare le API del cliente e a fornire funzioni di analisi comportamentale, rilevamento di attacchi in tempo reale e gestione delle vulnerabilità, tra cui l'esecuzione di test AppDev specifici delle API. Di conseguenza, il cliente è stato in grado di rilevare e mitigare gli attacchi alle API che i controlli esistenti non erano riusciti ad individuare. Il team addetto alla sicurezza delle applicazioni o AppSec è riuscito ad incrementare l'efficienza e a migliorare la prioritizzazione dei problemi ad alto rischio.

Akamai supporta anche fino a 50.000 API per motore senza alcuna latenza operativa. Utilizzando la nostra piattaforma come componente fondamentale, il cliente ha sviluppato un programma globale per la sicurezza delle API e ora può usufruire di una piena visibilità sull'inventario delle API con dati sulle API contestualmente rilevanti. Inoltre, l'azienda ha ottenuto preziose informazioni che non erano disponibili con gli strumenti esistenti, migliorando così i costi per garantire un'efficace gestione delle vulnerabilità delle API e un rilevamento delle minacce in tempo reale.