Storie di clienti Akamai

Una società di servizi finanziari individua e mette al sicuro le API

Una banca ha protetto le sue iniziative digitali individuando le API nascoste, valutando e mitigando i rischi per le API e soddisfando gli obblighi normativi

Visibilità completa

Miglioramento dell'approccio alla sicurezza

Protezione delle iniziative digitali

Il settore dei servizi finanziari sta rapidamente adottando la trasformazione digitale per rimanere competitivo in un mercato in continua evoluzione. Utilizzando le funzionalità digitali come l'intelligenza artificiale e l'analisi dei big data, le istituzioni finanziarie sono in grado di offrire prodotti innovativi, ridurre i costi e fornire servizi più efficienti e personalizzati ai loro clienti.

Allo stesso tempo, tuttavia, la trasformazione digitale porta con sé un maggior rischio di subire attacchi informatici. Per combattere questo problema crescente, la cybersicurezza è diventata ora parte essenziale di ogni strategia di trasformazione digitale. Le società di servizi finanziari devono garantire che i propri sistemi siano sicuri e resilienti per proteggere i dati e le risorse dei loro clienti dai criminali.

Una delle più importanti banche commerciali dell'Asia si è rivolta rapidamente a Noname Security (ora acquisita da Akamai) per rafforzare il proprio sistema di sicurezza delle API. Le violazioni delle API sono aumentate con una velocità allarmante: Tech Wire Asia ha segnalato che "oggi, su 13 incidenti informatici, 1 può essere attribuito ad una vulnerabilità delle API", sottolineando anche che "le vulnerabilità delle API costano alle aziende fino a 75 miliardi di dollari all'anno".

Considerando che i nostri clienti dispongono di più di 700 miliardi di dollari di risorse in totale, oltre 5000 clienti aziendali e una reputazione nella gestione patrimoniale rinomata a livello internazionale, era fondamentale garantire di riuscire a mitigare tutte le vulnerabilità delle API nel minor tempo possibile.

Financial Services

Sede

Asia

Settore

Servizi finanziari

Soluzione

Akamai API Security

Akamai

La necessità di una maggiore visibilità sulle API e sui rischi correlati

L'istituzione aveva già implementato una piattaforma di gestione delle API per eseguire il controllo del traffico e delle autenticazioni, ma non era sicura della sua capacità di riuscire a prevenire attacchi informatici e abusi delle API. Anche se i gateway API forniscono i necessari controlli basilari per la sicurezza delle API, non sono sufficienti per proteggere adeguatamente le organizzazioni dalle specifiche minacce alle API.

Ad esempio, la violazione dell'autorizzazione a livello di oggetto, a cui spesso ci si riferisce con l'acronimo BOLA, si presenta come un normale traffico delle API verso i gateway. Questa mancanza di consapevolezza contestuale tra le richieste delle API e le relative risposte consente agli attacchi BOLA di passare indisturbati e di accedere ai servizi di back-end critici. Non solo questa falla può lasciare le organizzazioni vulnerabili ai tentativi di sfruttamento BOLA, ma può anche dare adito ad altri attacchi e all'abuso della logica aziendale.

Un'altra limitazione della visibilità è mantenere un inventario delle API accurato. Come per la maggior parte delle organizzazioni, questa banca riscontrava problemi con le API sconosciute all'interno del suo ambiente. La realtà è che le aziende devono gestire migliaia di API, molte delle quali non vengono instradate tramite un proxy, come un gateway API, e vengono definite API non autorizzate o zombie. Queste API erano state implementate in precedenza da ex dipendenti o prima che l'organizzazione adottasse un approccio sistematico nei confronti della sicurezza delle API. Indipendentemente dal motivo per cui queste API esistono, il gateway API della banca non riusciva ad individuarle, pertanto era molto probabile finire con il sottovalutare il numero esatto di API di cui l'organizzazione disponeva.

Prepararsi ad affrontare la sfida alla sicurezza delle API

L'organizzazione ha implementato la piattaforma Noname API Security completa (ora parte di Akamai API Security), incluse le soluzioni per la gestione del sistema delle API, la protezione del runtime e l'esecuzione dei test nel suo ambiente. Il livello di sicurezza del cliente è migliorato in modo esponenziale: ora l'organizzazione è in grado di rilevare e mitigare le vulnerabilità legate ad uno dei vettori di attacco meno conosciuti al mondo.

Ora è inoltre possibile individuare e rilevare le API sconosciute all'interno della piattaforma, raggiungendo un livello completo di visibilità e mitigazione dei rischi. L'istituzione ha ridotto notevolmente la proliferazione delle sue API e ha migliorato il processo di conformità in quanto Akamai API Security classifica i dati sensibili per aiutare a soddisfare i requisiti dei regolamenti vigenti, come il GDPR, l'HIPAA e molti altri.

La banca ora ha anche la capacità di bloccare gli attacchi in tempo reale e di proteggere i dati dei clienti. La soluzione di protezione del runtime rileva e classifica in modo intelligente le potenziali minacce assegnando le priorità necessarie e monitorando continuamente, nel contempo, l'attività delle API. Integrandosi con le soluzioni WAF (Web Application Firewall), i gateway API, i processi SIEM (Security Information and Event Management) e ITSM (Information Technology Service Management) e altri strumenti dei workflow, la nostra piattaforma consente di mitigare le minacce manualmente o automaticamente (oppure con una combinazione di queste modalità).

Risultati

Le API sono diventate rapidamente uno dei vettori di attacco preferiti dagli hacker e il numero di attacchi sferrati non accenna a diminuire. Ad esempio, abbiamo osservato "una crescita del 257 percento nel numero di attacchi sferrati contro i servizi finanziari su base annuale" nel 2022. Grazie alla soluzione Akamai API Security, questa società di servizi finanziari sarà ben attrezzata per evitare di diventare una delle prossime vittime degli attacchi e per difendersi da questa tendenza crescente. In particolare, i team addetti alla sicurezza dei clienti potranno comprendere meglio i pericoli rappresentati dalle API e creare sistemi ancora più sicuri.