Storie di clienti Akamai

Un'importante banca statunitense protegge il traffico delle API

mantenendo una rigorosa conformità alle normative di settore con un'impareggiabile visibilità sulla superficie di attacco delle API

Negli ultimi anni, il settore del banking sta subendo una significativa trasformazione, favorita dall'adozione delle API (Application Programming Interface). La proliferazione delle API ha consentito alle banche di sfruttare nuove opportunità, migliorare le customer experience e favorire la propria espansione aziendale.

Le API hanno svolto un ruolo cruciale nel promuovere un'eccellente integrazione tra diversi sistemi e applicazioni all'interno dell'ecosistema del banking. Esponendo i propri servizi e dati tramite le API, le banche ora possono collaborare con sviluppatori di terze parti, startup FinTech e altre istituzioni finanziarie per creare soluzioni innovative ed espandere le soluzioni offerte. Tuttavia, nonostante questi ovvi vantaggi, l'esposizione delle API comporta anche rischi per la sicurezza, che possono minacciare in modo significativo la riservatezza, l'integrità e la disponibilità di un'API. Tra questi rischi, figurano accessi non autorizzati, attacchi di tipo injection o DoS (Denial-of-Service), trasmissione dei dati non sicura, inappropriata escalation dei privilegi e delle autorizzazioni, mancanza di convalida dell'input, archiviazione delle credenziali non protetta e operazioni di registrazione e monitoraggio non adeguate. Per gestire tali rischi, la banca si è rivolta a Noname Security (ora acquisita da Akamai).

Gestione della conformità

Nel settore dei servizi finanziari, la conformità alle normative riveste la massima importanza per garantire pratiche eque e trasparenti, per proteggere i consumatori e per mantenere l'integrità del sistema finanziario. I regolamenti di adeguata verifica del cliente (KYC) e le norme antiriciclaggio (AML) richiedono alle istituzioni finanziarie di verificare l'identità dei loro clienti, di valutare i potenziali rischi

Banking Leader

Sede

Stati Uniti

Settore

Servizi finanziari

Soluzione

Akamai API Security

Risultati principali

- Conformità alle normative rafforzata
- Integrazione con l'ambiente di produzione F5
- Identificazione continua delle API fornita

Akamai

associati con il riciclaggio di denaro illecito e il finanziamento del terrorismo e di segnalare eventuali attività sospette.

Tra le altre normative, figura il PCI DSS (Payment Card Industry Data Security Standard), un insieme di standard di sicurezza stabiliti dalle principali società di carte di credito per proteggere i dati dei titolari di carte di credito. Queste normative sono solo la punta dell'iceberg per quanto riguarda il settore finanziario. Ecco perché conoscere i dati trasmessi tramite le API è risultato cruciale per questa banca leader nel settore dei servizi finanziari.

L'azienda aveva bisogno di capire, gestire e mitigare i rischi migliorando la visibilità complessiva del suo ecosistema delle API, con una particolare attenzione all'individuazione delle API, alla classificazione dei dati, alla vulnerabilità e al rilevamento delle anomalie. Inoltre, una delle massime priorità dell'azienda era l'integrazione con il suo ambiente di produzione F5.

Scoprire il suo patrimonio delle API

La piattaforma Noname API Security (ora parte di Akamai API Security) ha fornito visibilità sul traffico delle API trasmesso verso e dalla rete del cliente, oltre che al suo interno. Il motore di Akamai API Security ha analizzato il traffico e ha individuato tutte le API di questa banca leader nei servizi finanziari. L'analisi del traffico in tempo reale ha identificato nuove API e le modifiche apportate alle API esistenti, quindi i dati sono stati registrati e aggiornati nel dashboard del cliente.

Poiché la piattaforma non si basa su agenti o componenti collaterali e poiché si integra con l'infrastruttura cloud, riesce a vedere tutte le API, indipendentemente se siano o meno registrate con un gateway API. Le API interne ed esterne, le API legacy (precedenti al gateway API) e le API ombra o non autorizzate (non instradate tramite un gateway) sono state tutte individuate, il che ha fornito al cliente un'impareggiabile visibilità sulla superficie di attacco delle API.

Uno sguardo al futuro

Questa banca leader nei servizi finanziari utilizza una serie di criteri per valutare la riuscita del suo sistema di sicurezza delle API. Uno di questi criteri consiste nell'esecuzione di un triage rapido, per cui Akamai fornisce il suo supporto. Un obiettivo importante consiste nel determinare come analizzare la gravità di ciascun risultato in modo da consentire al SOC di valutare, eseguire il triage e rispondere rapidamente ad un avviso.