Storie di clienti Akamai

Un'importante società di telecomunicazioni asiatica ha protetto le sue API dalle minacce

Questa società ha guadagnato la visibilità (e la protezione) su ogni API presente nel suo patrimonio

Individuazione delle API non gestite

Miglioramento della protezione delle API

Protezione dei dati sensibili

Il settore delle telecomunicazioni in Asia sta investendo ingenti capitali nello sviluppo di nuove tecnologie, espandendo, al contempo, le reti per soddisfare la domanda di migliori servizi digitali da parte dei clienti in seguito alla proliferazione dei dispositivi mobili. Le API "dietro le quinte" forniscono:

- La connettività necessaria per consentire la trasformazione del settore delle telecomunicazioni, accelerando, al contempo, i processi dei team DevOps
- La base per offrire servizi di telefonia mobile, accesso a Internet e altri prodotti per le telecomunicazioni ai clienti di tutto il continente
- La capacità di offrire soluzioni maggiormente personalizzate e, in definitiva, di migliorare le customer experience

Una delle più importanti società di telecomunicazioni dell'Asia ha intravisto anche la grande opportunità resa possibile dalle API, specificamente nell'offerta di nuove soluzioni digitali per voce e dati. Inoltre, con l'avvicinarsi dell'era del 5G, la società ha puntato gli occhi oltre la telefonia, rivolgendo la sua attenzione su big data, intelligenza artificiale, dispositivi IoT e altre nuove applicazioni digitali, sapendo, tuttavia, che le API stanno proliferando non solo di numero, ma anche nei rischi correlati. Dopo aver visto altri importanti provider di servizi di telecomunicazione subire gli effetti degli attacchi alle API nel 2022 e nel 2023, la società si è rivolta a Noname Security (ora acquisita da Akamai).

Telecommunications Company

Sede

Asia

Settore

Operatori di rete

Soluzione

Akamai API Security

La necessità di una visibilità su tutte le API e sui rischi correlati

Come per molte organizzazioni, la mancanza di visibilità sulle API e sui rischi correlati è la sfida maggiore per i team addetti alla sicurezza. Secondo la nostra ricerca, solo 4 organizzazioni su 10 che dispongono di un inventario completo delle API sanno quali delle loro API restituiscono dati sensibili. Utilizzando il modulo di individuazione della nostra soluzione API Security, abbiamo stabilito che il nostro cliente che opera nel settore delle telecomunicazioni stava riscontrando un problema simile.

Prima di collaborare con Akamai, questo cliente aveva utilizzato controlli per la sicurezza delle API costituiti principalmente da una piattaforma tradizionale per la gestione delle API e da una soluzione WAF (Web Application Firewall). Questa combinazione risultava adeguata per la sicurezza di applicazioni e API, tuttavia nessuna delle due soluzioni riusciva a fornire gli elevati livelli in termini di controlli di sicurezza e visibilità richiesti per garantire una protezione completa delle API dagli odierni metodi di attacco. Il motivo principale consiste nel fatto che non tutte le API vengono instradate tramite un proxy come una soluzione WAF o un gateway API, pertanto queste API non gestite diventano bersagli allettanti per i criminali.

Tuttavia, anche con un controllo accurato dell'inventario delle sue API, la società aveva comunque bisogno delle funzionalità necessarie per proteggere le API durante il loro normale funzionamento e la gestione delle richieste. In breve, sarebbe improponibile, per il team addetto alla sicurezza di un'organizzazione, identificare manualmente eventuali comportamenti dannosi nel suo ambiente.

Esistono centinaia, se non migliaia, di endpoint delle API da dover proteggere in tempo reale. Le soluzioni AppSec comunemente usate, di solito, non riescono a tenere il passo con tutte le chiamate API nell'ambiente di un cliente, rendendo così l'ambiente IT di una società potenzialmente vulnerabile agli attacchi informatici senza le appropriate funzionalità di protezione del runtime delle API.

Come ottenere la visibilità su tutte le API e la loro protezione dalle minacce

La prima fase di questo approccio ha previsto un'implementazione pilota allo scopo di individuare le API interne dell'azienda, valutare le configurazioni e comprendere i tipi di dati trasmessi tramite le API. Il cliente è rimasto subito favorevolmente colpito dalla velocità con cui è stato eseguito il rilevamento, dall'accuratezza dell'inventario e dai dati sensibili resi vulnerabili che lo strumento ha identificato.

In seguito ai risultati positivi di questa fase pilota, il cliente ha quindi ampliato l'area di copertura della piattaforma Noname API Security (ora parte di Akamai API Security) all'intero patrimonio delle sue API interne ed esterne. In tal modo, il cliente è riuscito a rilevare un maggior numero di API nascoste in fase di produzione e a far emergere le minacce al suo ambiente più imminenti.

Abbiamo notato che il cliente aveva bisogno di difendersi maggiormente da importanti vulnerabilità in termini di sicurezza per proteggere le sue API da attacchi futuri. Con l'implementazione di Akamai API Security, il cliente ora può rilevare le anomalie dei comportamenti sospetti e attivare gli appropriati protocolli di risposta agli incidenti in tempo reale. In tal modo, le organizzazioni possono evitare di doversi basare su registri di rapporti e accessi non aggiornati per ricavare le informazioni necessarie per i loro processi di mitigazione. Una volta rilevati con Akamai API Security, i comportamenti sospetti vengono segnalati al gateway API, al sistema SIEM e ad altri motori per la sicurezza delle informazioni del cliente allo scopo di informare l'intero team addetto alla sicurezza. Il cliente può scegliere di far risolvere il problema al suo personale interno manualmente o automaticamente (oppure con una combinazione di queste modalità), a seconda del caso di utilizzo e della gravità della vulnerabilità.

 | Data di pubblicazione 09/24