Storie di clienti Akamai

Un retailer Fortune 100 protegge le sue attività digitali con API Security

conformandosi alle principali normative per bloccare potenziali attacchi DDoS e fughe di dati

Il settore del retail sta subendo una significativa trasformazione in seguito all'adozione dei processi digitali favoriti dalle potenzialità delle API (Application Programming Interface). Le API stanno rivoluzionando il modo con cui i retailer operano, interagiscono con i clienti e gestiscono le loro attività aziendali.

I retailer integrano i loro sistemi con vari servizi e applicazioni di terze parti tramite le API, offrendo interazioni perfette su diverse piattaforme. Ad esempio, le API consentono ai retailer di integrare le loro piattaforme di e-commerce con i gateway di pagamento, i provider di servizi di spedizione e i sistemi di gestione dell'inventario. Tuttavia, man mano che l'ecosistema scala, crea un enorme numero di potenziali vulnerabilità in termini di sicurezza.

La sicurezza delle API è importantissima nell'odierno scenario digitale. Poiché le organizzazioni si affidano sempre di più alle API per connettere i sistemi, condividere i dati ed effettuare le loro integrazioni, garantire la sicurezza di queste interfacce assume un'importanza critica. Ecco perché questo retailer Fortune 100 si è rivolto a Noname Security (ora acquisita da Akamai) per proteggere la sua superficie di attacco delle API.

Che cos'è la superficie di attacco delle API?

L'individuazione delle API svolge un ruolo cruciale nel controllo della proliferazione delle API, con cui si intende la crescita incontrollata del numero di API all'interno di un'organizzazione. In questa situazione in cui le aziende utilizzano sempre più le API per favorire la trasformazione digitale e promuovere l'innovazione, è essenziale adottare un approccio sistematico per individuare e gestire le API in modo efficace. Inoltre, nell'ecosistema del retail digitale in rapida crescita, è innanzitutto fondamentale garantire la protezione delle API.

Designer Merchandise Retailer

Sede

Stati Uniti

Settore

Retail

Soluzione

Akamai API Security

Risultati principali

- Prevenzione dell'esposizione dei dati
- Individuazione della superficie di attacco delle API
- Riduzione di rischi e costi

Akamai

Questa azienda leader nel settore del retail non aveva visibilità sul traffico e sull'inventario delle API. Senza una governance sulle diverse piattaforme utilizzate (on-premise e nel cloud), non era possibile sviluppare una protezione scalabile del ciclo di vita dello sviluppo del software (SDLC) delle API. L'azienda si è così rivolta al nostro team per richiedere un'individuazione continua delle risorse delle API allo scopo di ridurre rischi e costi identificando eventuali configurazioni errate, vulnerabilità e componenti non conformi, nonché per integrarsi con i suoi workflow SecOps esistenti (ad es. Splunk).

Prevenire l'esposizione dei dati sensibili

Nel settore del retail, le organizzazioni devono attenersi a numerose normative sulla conformità, che mirano a proteggere i diritti dei consumatori, a garantire pratiche commerciali eque e a tutelare la sicurezza e la privacy dei dati. Le aziende devono avere visibilità sulle API di gestione dei dati sensibili e devono riuscire a proteggerle per conformarsi alle normative e agli standard di settore più importanti, evitando, al contempo, eventuali conseguenze legali e danni alla reputazione.

Il team di Akamai ha aiutato a prevenire l'esposizione pubblica dei dati sensibili per un retailer Fortune 100, che stava usando una vecchia versione di Jira da cui si era originato un bug a causa del quale erano stati resi visibili i nomi dei dipendenti, i nomi utente di Jira e gli indirizzi e-mail. Anche le API pubbliche presentavano per l'azienda un livello di rischio elevato.

La soluzione Akamai API Security è riuscita a risolvere le falle nel sistema di sicurezza delle API dell'azienda e a mitigare le configurazioni errate presenti nel suo ambiente. Ad esempio, la configurazione dell'architettura di scarsa qualità aveva aumentato il rischio di subire attacchi DDoS e fughe di dati.

Le mosse per il futuro

Il cliente collabora attivamente con il team di Akamai con cui si incontra ogni settimana per agevolare il percorso aziendale e, nel futuro, intende esaminare la possibilità di eseguire altre integrazioni con i suoi workflow esistenti. Akamai API Security identifica e assegna le priorità in modo intelligente alle potenziali vulnerabilità, che possono essere risolte manualmente o automaticamente (oppure con una combinazione di queste modalità) tramite apposite integrazioni nelle soluzioni WAF, nei gateway API, nei processi SIEM e ITSM, negli strumenti dei workflow o in altri servizi. Inoltre, considerando i suoi strumenti tecnologici in rapida espansione, il cliente sta esaminando varie integrazioni da poter implementare nel futuro.

 | Data di pubblicazione 08/24