WHITE PAPER

Come prevenire una violazione delle API

Ecco 5 tipi di violazioni delle API e come potete proteggervi

In questo rapporto

Introduzione

Le API connettono la vostra azienda scambiando dati con partner, fornitori e clienti, eppure, la sicurezza delle API rimane tutt'altra che completa nella maggior parte delle organizzazioni. In realtà, negli ultimi anni le API sono diventate una vulnerabilità presa di mira dai criminali che le sfruttano per accedere ai dati sensibili, per venderli ad altri malintenzionati o per pubblicarle in modo da renderle visibili pubblicamente. Nel 2024, i brand globali dei settori delle telecomunicazioni, del computing aziendale e della collaborazione virtuale hanno notato che, a causa delle violazioni delle API, sono state sottratte enormi quantità di dati dei clienti e altre informazioni sensibili, il che ha implicato enormi costi finanziari e danni alla reputazione.

Che cos'è una violazione delle API?

In breve, una violazione delle API è un abuso intenzionale o un uso improprio di un'API, spesso, per ottenere l'accesso ai dati sensibili. È possibile suddividere i tipi di violazione delle API in base a vari criteri. Per identificare i rischi ed evitare le violazioni in fase di produzione, è utile considerare lo schema seguente, che suddivide i rischi in cinque categorie:

1. **Vulnerabilità note**
   - I criminali sfruttano le vulnerabilità note che non sono state corrette con patch.
2. **API, nascoste, non autorizzate, zombie e obsolete**
   - Le API non gestite e dimenticate possono lasciare le aziende vulnerabili.
3. **Vulnerabilità esterne**
   - Credenziali, chiavi e altre vulnerabilità possono esulare dal vostro controllo.
4. **Errori di configurazione e dell'operatore**
   - Gli errori di configurazione nel sistema di sicurezza dell'infrastruttura e dei servizi possono creare punti di ingresso sfruttabili da parte dei criminali.
5. **Vulnerabilità e problemi non rilevati**
   - I criminali cercano di identificare i problemi e le vulnerabilità che si sono creati nell'ambiente di produzione nonostante i vostri migliori sforzi.

Questo eBook spiega dove si verificano le lacune di sicurezza in ciascuno di questi cinque tipi di violazione delle API e come prevenirli. Inoltre, questo eBook si propone di aiutarvi ad eliminare specifiche vulnerabilità presenti nel vostro programma di sicurezza delle API per ottimizzare la sicurezza delle API e minimizzare i rischi.

Tipo di violazione: vulnerabilità note

Le violazioni delle API che sfruttano vulnerabilità note (che non sono state corrette con patch) sono forse le più comuni. Per accedere ai vostri dati, i criminali informatici, di solito, controllano innanzitutto se la vostra organizzazione ha lasciato eventuali backdoor aperte.

A gennaio 2024, uno strumento di gestione dei progetti ampiamente usato è stato violato da un criminale che ha sfruttato un endpoint delle API privo di controlli di autenticazione. Dopo aver violato l'API, il criminale ha ottenuto un accesso non autorizzato alle informazioni di milioni di utenti e, mesi dopo, ha esfiltrato oltre 21 GB di dati, inclusi indirizzi e-mail e sottoscrizioni ai consigli di amministrazione, su Internet.

Tra i problemi più comuni delle API, figurano quelli relativi alle procedure di autenticazione e autorizzazione. I 10 principali rischi per la sicurezza delle API riportati nell'elenco OWASP forniscono informazioni sulle 10 vulnerabilità delle API più importanti, da cui le organizzazioni devono proteggersi, inclusa la violazione dell'autenticazione.

Oltre a proteggere le API dai tipi di rischi inclusi nell'elenco OWASP, le organizzazioni devono anche proteggere il relativo codice dalle CVE (Common Vulnerabilities and Exposure), il cui elenco completo è stato creato dal FFRDC (Federally Funded Research and Development Center), un centro di ricerca sulla cybersicurezza negli Stati Uniti gestito da MITRE. Probabilmente, vi ricorderete della nota vulnerabilità Apache Log4j 2 (CVE-2021-44228), anche definita "Log4Shell". A causa di un bug presente nella libreria Log4j, una nota libreria di registrazione open source per il linguaggio di programmazione Java, i criminali sono riusciti ad eseguire codice arbitrario da remoto per ottenere l'accesso al sistema preso di mira. I sistemi aziendali vengono regolarmente sondati dai criminali alla ricerca di vulnerabilità note, come quella riportata qui sopra.

Negli Stati Uniti, la CISA (Cybersecurity and Infrastructure Security Agency) si occupa di stilare un catalogo delle vulnerabilità CVE note e cataloghi simili vengono redatti anche in altri paesi.

L'elenco OWASP con i 10 principali rischi per la sicurezza delle API è stato creato nel 2019 e poi aggiornato nel 2023. Tuttavia, anche se è utile, questo elenco non riesce a stare al passo con lo scenario degli attacchi in continua evoluzione. Solo nel 2024, sono state aggiunte al catalogo della CISA più di 24.000 nuove CVE, di cui oltre 500 sono correlate alle API (fino a metà agosto 2024).

Per proteggere completamente la vostra organizzazione dalle vulnerabilità note, è necessario un duplice approccio:

1. Assicurarsi che i processi di sviluppo ed esecuzione dei test siano abbastanza solidi da evitare di introdurre vulnerabilità note in fase di produzione.

2. Correggere le nuove vulnerabilità con le patch appropriate il più rapidamente possibile dopo averle identificate.

Molte organizzazioni incontrano difficoltà con entrambe queste operazioni. Inoltre, utilizzano il codice e le API provenienti da terze parti, che possono introdurre ulteriori vulnerabilità. Nel 2022, un team di ricercatori ha individuato vulnerabilità critiche legate alle API, che hanno interessato diversi produttori che operano nell'industria automobilistica. Queste vulnerabilità avrebbero potuto rendere visibili i dati sensibili dei clienti e, persino, la posizione di un veicolo, consentendo di aprire, avviare o disattivare un'auto tramite la violazione del sistema di gestione da remoto.

Come prevenirle

Per proteggere la vostra organizzazione dalle violazioni delle API causate da vulnerabilità note, uno dei metodi più comuni consiste nell'aggiornare rapidamente software e sistemi non appena vengono rilasciate le patch di sicurezza. È anche fondamentale garantire che i processi di sviluppo ed esecuzione dei test siano completi e basati sulle best practice per la sicurezza delle API, che includono:

- **Protezione della supply chain dei software:** assicuratevi che le librerie, i software open source (OSS) e altro codice di terze parti in uso siano sicuri.
- **Implementazione dei test sulla sicurezza Shift-Left:** eseguite i test sui software e sulla sicurezza delle API all'inizio del processo di sviluppo. In tal modo, potrete rilevare eventuali vulnerabilità, come errori di codifica e configurazione commessi dagli sviluppatori nell'urgenza di rilasciare rapidamente software o aggiornamenti.
- **Gestione del sistema di sicurezza delle API:** questo approccio combina l'individuazione delle API con l'identificazione dei dati sensibili e il rilevamento delle vulnerabilità, garantendo di focalizzare le operazioni di mitigazione prima sulle API più importanti.

Come Akamai API Security può aiutarvi

Akamai API Security consente ai vostri team di ridurre le vulnerabilità note per ogni nuova build senza rallentare i processi. API Security è una soluzione per l'esecuzione di test sulla sicurezza delle API appositamente progettata per fornire una copertura completa delle vulnerabilità specifiche delle API. La funzione dei test attivi aiuta le organizzazioni a preparare ed eseguire i test sulla sicurezza delle API in ogni fase dello sviluppo.

- **Individuate ed eseguite i test di ogni API** in base alla logica aziendale dell'applicazione.
- **Eseguite test di tipo Shift-Left** con integrazioni nell'intero ciclo di sviluppo del software. I team acquisiscono una visibilità dinamica delle API in vari stadi e ambienti del processo CI/CD.
- **Offrite agli sviluppatori** le funzioni più intuitive del settore, tra cui semplici operazioni di configurazione e automazione, risultati dei test online e istruzioni contestuali per risolvere i problemi identificati.

Inoltre, la gestione del sistema offerta da API Security fornisce una visione completa sul traffico, sul codice e sulle configurazioni per poter valutare il livello di sicurezza delle API della vostra organizzazione. API Security effettua una ricerca sul maggior numero possibile di fonti per rilevare eventuali vulnerabilità, inclusi i file di registro, le riproduzioni del traffico storico, i file di configurazione e molto altro. Inoltre, la soluzione rileva tutte le vulnerabilità riportate nell'elenco OWASP con i 10 principali rischi per la sicurezza delle API (per ulteriori informazioni sulla gestione del sistema, potete consultare la sezione sugli errori di configurazione e dell'operatore).

Tipo di violazione: API nascoste, non autorizzate, zombie e obsolete

È impossibile fermare ciò che non si vede: in molte aziende, un gran numero di API non sono gestite, il che rende le API nascoste, non autorizzate, zombie e obsolete (come viene illustrato nella barra laterale alla pagina successiva) bersagli che risultano invisibili o che vengono trascurati all'interno del patrimonio delle API. Inoltre, i criminali, spesso, cercano varianti delle API da poter sfruttare esaminando le API vulnerabili di un'organizzazione e, quindi, confondendo o modificando i valori per individuare le versioni più vecchie.

Questo è quanto è successo ad un'importante società di telecomunicazioni australiana che ha erroneamente reso visibili pubblicamente più di 11,2 milioni di dati dei suoi clienti, inclusi nomi, indirizzi, date di nascita e numeri di carte d'identità. L'attacco ha sfruttato un'API utilizzata per l'esecuzione dei test che è diventata in qualche modo accessibile sull'Internet pubblico. Poiché questa API non autorizzata non prevedeva controlli di autenticazione, un criminale è riuscito a richiedere e ricevere milioni di dati.

La maggior parte delle organizzazioni utilizza sia API nuove che già esistenti. Non è raro trovare una combinazione di API non autorizzate, zombie e nascoste, che rendono l'azienda vulnerabile ad una serie di rischi per la cybersicurezza e di problemi operativi.

Queste API invisibili sono di vario tipo:

- **API commerciali:** alcuni pacchetti software commerciali includono le API per la connessione ad altre applicazioni e fonti di dati esterne. Queste API possono essere attivate senza che nessuno se ne renda conto (un problema che può essere risolto mediante la funzione di individuazione delle API).
- **Versioni delle API obsolete:** in molti casi, una vecchia versione di un'API, possibilmente con un livello di sicurezza inferiore o una vulnerabilità nota, potrebbe non venire mai rimossa. Una versione obsoleta potrebbe dover coesistere con una nuova versione per un certo periodo di tempo durante l'aggiornamento del software, tuttavia, se il processo non riesce ad impedire la disattivazione delle API obsolete, queste diventano API zombie.
- **Errori nei comandi rapidi e nei processi:** alcune API nascoste derivano dal fatto di non aver informato le persone giuste. Ad esempio, un team LOB (Line of Business) potrebbe creare le API necessarie per soddisfare specifiche esigenze senza informare i team addetti alla sicurezza o IT oppure gli sviluppatori potrebbero non seguire la procedura.
- **API ereditate:** le API che sono state "ereditate" in seguito a fusioni o acquisizioni aziendali vengono frequentemente dimenticate e diventano API nascoste.
- **Codice riattivato:** in alcuni casi, le versioni obsolete delle API potrebbero venire erroneamente riattivate.

Come prevenirle

Un audit delle API manuale, condotto allo scopo di documentare tutti gli input che devono essere accuratamente inventariati, può richiedere varie ore, specialmente considerando il tempo necessario per valutare e intervenire su ogni API individuata. Questa attività non è certo realistica per i team addetti alla sicurezza già oberati di lavoro. Per proteggere la vostra azienda dallo sfruttamento delle API non autorizzate, zombie e nascoste, è necessario automatizzare l'individuazione delle API per identificare tutte le API in uso, di qualsiasi tipo esse siano. È fondamentale individuare e inventariare tutte le API presenti nella vostra azienda, rilevando anche le API e i relativi domini non gestiti da un gateway API.

Come Akamai API Security può aiutarvi

API Security sfrutta una vasta gamma di fonti di integrazione per acquisire i dati delle API, come traffico non elaborato, registrazioni e molto altro. Grazie ai dati ricavati da queste fonti, API Security è in grado di identificare le API, nonché gli errori di configurazione, le vulnerabilità e gli episodi di abuso che le interessano. I nostri strumenti di individuazione riescono a rilevare tutte le vulnerabilità riportate nell'elenco OWASP con i 10 principali rischi per la sicurezza delle API.

Ulteriori funzioni di individuazione vi consentono di:

- Individuare e inventariare tutte le API, indipendentemente dalla configurazione o dal tipo, tra cui RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC
- Rilevare le API inattive, legacy e zombie
- Identificare i domini ombra dimenticati, trascurati o non conosciuti
- Stilare gli inventari e garantire un'accurata documentazione delle API

Le API non gestite ad alto rischio che cercano i criminali

Le API nascoste (dette anche "API non documentate") esistono e operano all'esterno dei canali ufficialmente monitorati di un'organizzazione. Queste API possono essere create per scopi leciti da sviluppatori che desiderano accelerare il loro lavoro o possono essere tracce di versioni software precedenti.

Le API non autorizzate sono create per scopi dannosi e, quindi, rappresentano un rischio per la sicurezza di un sistema o di una rete.

Le API zombie includono tutte le API che vengono lasciate eseguire anche una volta sostituite da nuove versioni o da altre API.

Le API obsolete non sono più consigliate per l'uso a causa delle modifiche apportate alle API. Anche se vengono comunque implementati campi, classi e metodi obsoleti, è possibile rimuoverli nelle future implementazioni, quindi non è necessario usarli nel nuovo codice.

Tipo di violazione: vulnerabilità esterne

Le vulnerabilità esterne delle API sono, di solito, il risultato di pratiche inadeguate o errori procedurali, come fuga di chiavi e credenziali delle API, esposizione di schemi e codice delle API, documentazione approssimativa e archivi vulnerabili. La capacità di rilevare potenziali vettori di attacco al di fuori dei confini della vostra azienda è diventata fondamentale. L'anno scorso, numerose violazioni di alto profilo sono state causate dall'esposizione accidentale di chiavi API o di altre credenziali da parte di fonti esterne. Ad esempio, gli hacker hanno utilizzato una campagna di phishing per ottenere un accesso non autorizzato a 130 archivi di codici sorgente di Dropbox e poter così accedere alle chiavi API archiviate in modo improprio su GitHub. Questo tipo di vulnerabilità è diventato così comune che GitHub ha messo in atto misure appropriate per bloccare le fughe di chiavi API e altri segreti, ma altri archivi pubblici possono comunque risultare vulnerabili.

Nel caso di un'altra vulnerabilità esterna ben nota, i ricercatori hanno rilevato più di 3.000 app mobili che hanno reso visibili pubblicamente le chiavi API di Twitter. Questo tipo di errore è sorprendentemente comune perché gli sviluppatori, spesso, integrano le chiavi API nel codice delle applicazioni durante lo sviluppo per motivi di praticità. Se queste chiavi integrate non vengono poi rimosse prima di rilasciare le applicazioni pubblicamente, diventano una potenziale vulnerabilità.

Come prevenirle

Per ridurre o eliminare questi tipi di vulnerabilità esterne, è necessario un duplice approccio:

- Adottare procedure rigorose per identificare o eliminare le origini delle vulnerabilità, come fuga di chiavi e credenziali, uso improprio degli archivi, ecc.
- Esaminare regolarmente la superficie di attacco esterna per rilevare e mitigare le vulnerabilità.

Per proteggersi da un'ampia gamma di minacce per le API, è necessario adottare le funzioni di individuazione dall'interno verso l'esterno (come descritto nella sezione "Violazioni dalle API non autorizzate") e dall'esterno verso l'interno per identificare le vulnerabilità e ridurre la superficie di attacco esterna.

Come Akamai API Security può aiutarvi

API Security vi aiuta a stare al passo con i criminali simulando le tecniche di ricognizione utilizzate dagli hacker e consentendovi di individuare e risolvere rapidamente i problemi riscontrati. Con l'individuazione dall'esterno verso l'interno, API Security effettua una scansione automatica della vostra superficie di attacco esterna ad intervalli regolari per individuare le vulnerabilità prima dei criminali, consentendovi di:

- **Individuare le vulnerabilità pubbliche:** individuate e risolvete rapidamente i problemi più importanti, come la fuga di chiavi e credenziali delle API, l'esposizione del codice, gli errori di configurazione, le vulnerabilità degli archivi e molto altro.
- **Individuare i domini e i sottodomini correlati alla vostra azienda:** sfruttate i dati raccolti da varie fonti, inclusi i registrar di Internet e dei certificati e i programmi open source.
- **Incorporare i metodi di attacco reali:** simulate un criminale mentre esegue una ricognizione all'esterno per raccogliere informazioni eseguendo un numero limitato di query ai domini o ai sottodomini dell'azienda.

Tipo di violazione: errori di configurazione e dell'operatore

Molti criminali informatici riescono ad ottenere l'accesso ai sistemi sfruttando gli errori di configurazione di server, reti, gateway API e firewall che trattano e proteggono il traffico delle API. Da uno studio condotto da IBM Security X-Force, è emerso che due terzi delle violazioni del cloud sono legati alle API non configurate correttamente. Gli errori di configurazione della sicurezza possono essere causati da configurazioni predefinite non sicure, un'archiviazione sul cloud senza controllo degli accessi (sorprendentemente comune) e configurazioni incomplete o ad hoc. Man mano che la vostra presenza digitale si espande, le vostre attività aziendali potrebbero espandersi in altre posizioni, incluse più zone di disponibilità del cloud pubblico o cloud pubblici come AWS, Microsoft Azure e Google Cloud. Questi ambienti, spesso, operano con diversi controlli di sicurezza, pertanto diventa complesso e difficile garantire la corretta configurazione del sistema di sicurezza ovunque.

Come prevenirle

Uno dei modi migliori per proteggersi dagli errori di configurazione della sicurezza nell'infrastruttura è evitare il più possibile di configurare manualmente server, dispositivi di rete, gateway e firewall. Se i team amministrativi della vostra azienda configurano da sempre manualmente i controlli di sicurezza delle applicazioni e dell'infrastruttura (o li "modificano" regolarmente), aumentano le possibilità di introdurre vulnerabilità a livello di configurazione.

L'automazione è il vostro miglior alleato quando si tratta di garantire la sicurezza. Alcune aziende stanno adottando il concetto di infrastruttura immutabile come modo per evitare di commettere errori manuali.

Ma anche se avete fatto tutto quanto è in vostro potere per garantire la protezione completa dell'infrastruttura, dei servizi e delle API che utilizzate, comunque dovete gestire il sistema delle API. La gestione del sistema delle API vi fornisce gli strumenti necessari per gestire, monitorare e mantenere la sicurezza delle API per tutto il loro ciclo di vita.

Come API Security può aiutarvi

Il modulo di gestione di API Security analizza le chiamate e l'infrastruttura delle API per identificare gli errori di configurazione, che sono, solitamente, problemi di bucket di Amazon S3, presenza di dati sensibili sulle API non autenticate ed errori di configurazione basati sull'accesso a diversi sistemi Kubernetes.

Il modulo di gestione di API Security fornisce una visibilità completa sul traffico, sul codice e sulle configurazioni, offrendo una panoramica sull'intera superficie di attacco per le API e le applicazioni web, incluse tutte le forme di dati sensibili che attraversano le API, come le informazioni di identificazione personale. Inoltre, il modulo di gestione vi aiuta anche a verificare che lo strumento di gestione delle API stia utilizzando sequenze cifrate e protocolli complessi per evitare di adottare una crittografia debole che potrebbe rendere visibili questi dati sensibili. Inoltre, le API non devono accettare token JWT (JSON Web Token) non più validi perché, in caso contrario, potrebbero consentire accessi non autorizzati e aumentare i rischi per la sicurezza. Il modulo aiuta anche a prevenire gli errori di configurazione, come l'ascolto degli strumenti di bilanciamento del carico delle applicazioni su porte non sicure senza funzioni di reindirizzamento. Insieme, tutte queste misure rafforzano il sistema di sicurezza delle API, garantendo una difesa più resiliente dalle potenziali minacce.

Tipo di violazione: vulnerabilità non rilevate

Come con la maggior parte dei tipi di violazione, i criminali informatici che sondano la vostra infrastruttura cercano regolarmente la presenza di eventuali CVE, le 10 principali vulnerabilità per la sicurezza delle API riportate nell'elenco OWASP e altri comuni errori di configurazione, come le API non autorizzate, zombie e nascoste. Inoltre, i criminali esaminano le API rese visibili pubblicamente alla ricerca di nuove vulnerabilità da poter sfruttare nelle librerie, nel codice open source e in altri tipi di codice pubblico, nonché nei bug e negli errori di codifica e di configurazione presenti nel patrimonio delle API. Queste vulnerabilità consentono ai criminali informatici di manipolare le chiamate API e inserire stringhe di fuzzing nelle richieste. Di conseguenza, le tecniche utilizzate dai criminali informatici si evolvono continuamente.

Come prevenirle

Per prevenire questi problemi, è importante garantire che il codice sia il più possibile privo di bug e vulnerabilità (per ulteriori informazioni, potete consultare la sezione "Vulnerabilità note"). Tuttavia, dovete comunque considerare la possibilità che i criminali riusciranno ad individuare i bug oppure ad ottenere l'accesso alle chiavi o alle credenziali necessarie per violare le API.

La protezione del runtime delle API è progettata per identificare gli hacker che cercano di sfruttare una qualsiasi vulnerabilità, più o meno nota. È l'unico modo che consente di proteggere il patrimonio delle API dai bug e dagli errori di configurazione non identificati e passati in fase di produzione, nonché la miglior protezione dai tentativi di violazione di credenziali e chiavi.

La protezione del runtime identifica anomalie e schemi insoliti nell'utilizzo delle API e nell'accesso ai dati per consentire di identificare e mitigare gli attacchi in corso, che potrebbero sfuggire ai controlli, prima che vengano estratti migliaia (o milioni) di dati.

La protezione del runtime delle API runtime vi aiuta ad identificare e bloccare le richieste delle API dannose, tra cui:

- Attacchi che acquisiscono elevati volumi di dati sensibili da un'API
- Attacchi di violazione dell'autorizzazione a livello di oggetto (BOLA)

Una soluzione per la protezione del runtime delle API può rilevare:

- Fughe di dati
- Violazioni delle policy relative ai dati
- Attacchi alla sicurezza delle API
- Manomissione dei dati
- Comportamenti sospetti

Inoltre, la protezione del runtime include funzioni di registrazione del traffico delle API, monitoraggio dell'accesso ai dati sensibili, rilevamento delle minacce e blocco o mitigazione dei vettori di attacco.

Come API Security può aiutarvi

Pensate alla protezione del runtime come l'ultima linea di difesa quando tutte le altre misure di prevenzione si sono rivelate insufficienti. La funzione principale della protezione del runtime è rilevare e bloccare gli attacchi alle API in tempo reale. La soluzione utilizza il monitoraggio automatizzato con l'apprendimento automatico (ML) per condurre un'analisi del traffico in tempo reale e per fornire informazioni contestuali sulla fuga e sulla manomissione dei dati, sulle violazioni delle policy relative ai dati, sui comportamenti sospetti e sugli attacchi alla sicurezza delle API. API Security rileva le anomalie e le potenziali minacce nel traffico delle API e semplifica la mitigazione basandosi su policy di risposta agli incidenti predefinite.

Tramite l'ML, API Security crea un modello comportamentale per ogni API. Questo standard di comportamenti normali viene quindi usato per rilevare gli attacchi basati sulla logica aziendale delle API. Ogni problema generato dalla protezione del runtime include informazioni su gravità, stato, associazione con le 10 principali vulnerabilità della sicurezza delle API riportate nell'elenco OWASP e dettagli sul criminale, se disponibili. I problemi includono anche i dettagli sulla sessione del criminale, nonché una copia della richiesta e della risposta delle API per assistere nell'individuazione e nella risoluzione dei problemi.

La protezione del runtime di API Security offre funzioni di individuazione e prevenzione degli attacchi alle API in tempo reale insieme ad un continuo rilevamento degli errori di configurazione delle API, in aggiunta alle integrazioni dei workflow più comuni che semplificano le operazioni e la mitigazione.

Forse, l'aspetto più importante per il vostro team è il fatto che API Security si integra con soluzioni WAF, gateway API, ITSM, SIEM e altri strumenti di workflow per fornire una difesa olistica dagli attacchi. Potete scegliere di automatizzare totalmente la mitigazione delle minacce o richiedere diversi livelli di intervento manuale per migliorare le caratteristiche di visibilità e controllo.

5 tipi di violazioni, 5 principi di prevenzione

Dopo aver compreso meglio come le API vengono utilizzate dai criminali informatici, potete focalizzarvi sulla prevenzione delle loro violazioni. Ecco cinque prospettive strategiche e strumenti di prevenzione che dovete adottare insieme:

1. Sicurezza delle API Shift-Left

- La sicurezza delle API Shift-Left implica un'ampia esecuzione dei test delle API in fase di sviluppo in modo da non rendere visibili ai criminali informatici eventuali vulnerabilità nell'ambiente di produzione

2. Individuazione dall'interno verso l'esterno

- Identificate tutte le API presenti nelle vostre attività aziendali

3. Individuazione dall'esterno verso l'interno

- Identificate ed eliminate le origini delle vulnerabilità (come chiavi/credenziali violate e uso improprio degli archivi) ed esaminate regolarmente la superficie di attacco esterna per rilevare e mitigare le vulnerabilità

4. Gestione completa del sistema di sicurezza

- Fate sempre del vostro meglio quando si tratta di sicurezza delle API evitando errori di configurazione e vulnerabilità

5. Protezione del runtime

- Rilevate attività anomale delle API e proteggetevi da tutte le possibili minacce, incluse le vulnerabilità e i bug non identificati in precedenza

Richiesta di una demo

Provate quanto sia semplice identificare e mitigare gli errori di configurazione presenti nelle vostre API e proteggetevi dagli attacchi alle API guardando Akamai API Security in azione. Scoprite in prima persona perché le principali aziende scelgono la nostra soluzione per la sicurezza delle API.

Richiedete una demo

Akamai