Akamai

WHITE PAPER

Nozioni fondamentali sulla sicurezza delle API: migliorare le competenze e garantire la sicurezza aziendale

Introduzione

Le API hanno subito un'evoluzione molto rapida, trasformandosi da dettaglio di implementazione a fattore trainante dell'innovazione digitale. Ogni volta che un cliente, un partner o un vendor interagisce con un'azienda in modo digitale, c'è un'API "dietro le quinte" che facilita un eccellente scambio dei dati.

Tuttavia, le API proliferano come i rischi correlati. Nella corsa alla creazione e al rilascio di nuove applicazioni e servizi basati sull'intelligenza artificiale sempre più rapidamente, le API sottostanti vengono troppo spesso configurate in modo errato, non dispongono di controlli di sicurezza e sono vulnerabili ad attacchi eseguiti facilmente.

Di conseguenza, poiché le API sono emerse come vettore di attacco principale, molti team addetti alla sicurezza faticano a tenere il passo con le relative strategie di sicurezza. Pertanto, la sicurezza delle API sta rapidamente diventando una delle principali priorità strategiche dei responsabili della sicurezza e dell'ambiente IT.

Sia a chi cerca di conoscere le nozioni fondamentali sulla sicurezza delle API o di stilare un elenco delle domande più appropriate da porsi, questa guida offre tutto ciò che serve sapere, tra cui:

- **I diversi tipi di API**
- **L'importanza della sicurezza delle API per le aziende di oggi**
- **Le best practice utili per affrontare i rischi per la sicurezza delle API**
- **I metodi di abuso e attacco alle API più comuni**

Per accedere direttamente alle best practice per la sicurezza delle API, passare a pagina 10.

Sommario

Nozioni fondamentali sulle API

Che cos'è un'API web?

Un'API web è un'interfaccia di programmazione costituita da uno o più endpoint di un determinato sistema per lo scambio di messaggi di richiesta/risposta, generalmente in formato JSON o XML, che vengono esposti pubblicamente attraverso il web, solitamente tramite un server web basato su HTTP.

In altre parole, un'API web è quello che la maggior parte delle persone associa alla parola "API". Si tratta di un insieme di endpoint costituiti dai percorsi delle risorse, dalle operazioni eseguibili su tali risorse e dalla definizione dei dati delle risorse (ad es., in formato JSON, XML, Protobuf o di altro tipo).

Le API web sono diverse da altri tipi di API, come, ad esempio, quelle esposte dal sistema operativo o dalle librerie delle applicazioni eseguite sullo stesso computer, ma il termine generico "API", di solito, si riferisce ad un'API (web) basata su HTTP, specialmente negli ambiti della trasformazione digitale aziendale e della sicurezza delle API.

Quali sono i tipi più comuni di API?

La seguente tabella contiene termini che si riferiscono ai diversi modelli di utilizzo e approcci tecnici per l'implementazione delle API. Le API web sono definite come API basate su HTTP e oggi possono essere suddivise in quattro tipologie principali, ovvero RESTful, SOAP, GraphQL e gRPC, che sono anch'esse riportate nelle seguente tabella, insieme ad altri tipi di API.

Modello di utilizzo delle API	Descrizione
API pubblica	API che viene condivisa su Internet e resa liberamente disponibile a tutti gli sviluppatori
API esterna	Spesso utilizzato con il significato di API pubblica, questo termine indica un'API che viene esposta su Internet
API privata	API implementata in un data center o in un ambiente cloud protetto e riservata all'uso da parte di sviluppatori affidabili
API interna	Questo termine viene spesso utilizzato con il significato di API privata
API di terze parti	Consente di accedere a livello di programmazione a funzionalità specializzate e/o dati provenienti da fonti di terze parti, per utilizzarli in un'applicazione
API per i partner	API di terze parti che viene resa disponibile esclusivamente ai partner commerciali autorizzati
API autenticata	API accessibile solo agli sviluppatori a cui è stato consentito l'accesso (o a criminali che hanno ottenuto l'accesso non autorizzato alle credenziali)
API non autenticata	API accessibile a livello di programmazione, senza utilizzare credenziali specifiche
API HTTP	API che utilizza l'HTTP (HyperText Transfer Protocol) come protocollo di comunicazione per le chiamate API

API RESTful	Un'API RESTful (Representational State Transfer) è il tipo più comune di API web che utilizza testo non formattato, HTML, XML, YAML o JSON per distribuire i dati; le API RESTful sono semplici da utilizzare per i moderni sistemi front-end (ad es., React e React Native) e facilitano lo sviluppo delle applicazioni web e mobili; infine, questo tipo di API è diventato lo standard più utilizzato per le API web, incluse le API B2B
GraphQL	Le API GraphQL sono il nuovo standard sviluppato da Facebook che fornisce l'accesso ai database tramite un solo endpoint POST (di solito, /graphql) e risolve un comune problema delle API RESTful, ossia il fatto di richiedere più chiamate per compilare una pagina dell'interfaccia utente
SOAP	SOAP utilizza il linguaggio XML (eXtensible Markup Language) dettagliato per le chiamate di procedura remota (RPC, Remote Procedure Call), che viene ancora utilizzato nelle API legacy
XML-RPC	XML-RPC è un metodo per l'esecuzione di chiamate procedurali su Internet, che utilizza una combinazione di XML per la codifica e HTTP come protocollo di comunicazione
gRPC	Le API gRPC sono un protocollo binario ad alte performance sviluppato da Google tramite HTTP/2.0 che viene utilizzato soprattutto per le comunicazioni est-ovest (nella rete interna)
OpenAPI	OpenAPI è una descrizione e una specifica di documentazione per le API. Potrebbe risultare utile sapere che il termine Swagger si riferisce alla specifica originale e che OpenAPI si riferisce allo standard aperto sviluppato dall'iniziativa OpenAPI

Qual è la differenza tra API ed endpoint?

Quando parlano di "API", spesso gli utenti si riferiscono di fatto a un singolo endpoint delle API. Le API, note anche come servizi o prodotti API, sono insiemi di endpoint che forniscono una funzione aziendale. Un singolo endpoint, invece, indica una risorsa o il percorso di una risorsa, noto anche come un URI (Uniform Resource Identifier), insieme all'operazione eseguita su di esso (creazione, lettura, aggiornamento o eliminazione). Nelle API RESTful, tutte queste operazioni sono solitamente mappate ai metodi HTTP (POST, GET, PUT e DELETE).

Che cos'è un'API nord-sud?

Si tratta di un'API che l'azienda mantiene accessibile agli utenti esterni, soprattutto per consentire le interazioni con i propri partner commerciali. In questo caso, si parla di esposizione dell'API, come, ad esempio:

> **Le banche che adottano l'open banking possono utilizzare le API per rendere visibili i propri dati ad altre organizzazioni di tecnofinanza o ai fornitori di servizi finanziari.**

> **Le aziende sanitarie possono utilizzarle per rendere visibili le cartelle cliniche dei pazienti alle compagnie di assicurazione e ad altre strutture mediche.**

> **Nel settore alberghiero, le API possono essere utilizzate per rendere visibili i sistemi di prenotazione di un hotel agli agenti di viaggio o agli aggregatori.**

Le API sono il tessuto connettivo che consente a varie organizzazioni di scambiare dati fra loro. In genere, le API nord-sud sono considerate sicure perché il loro accesso richiede procedure di autorizzazione e autenticazione. Questa è la tipologia di API che si sta diffondendo più rapidamente e, di conseguenza, rappresenta la superficie di attacco più estesa per la maggior parte delle organizzazioni.

Che cos'è un'API est-ovest?

È un'API utilizzata internamente da un'organizzazione e, pertanto, non dovrebbe essere accessibile all'esterno dell'azienda. Le API di questo tipo vengono utilizzate per collegare le applicazioni interne oppure per connettere fra loro i diversi reparti o business unit. Gli sviluppatori potrebbero anche erroneamente rendere visibili API est-ovest che non erano state programmate per risultare accessibili o, persino, note all'esterno dell'azienda; tuttavia, si possono verificare violazioni quando i criminali riescono ad individuare le API est-ovest accessibili tramite Internet.

Quali sono le differenze tra le API B2C e B2B?

Le API B2C (da azienda a consumatore) sono alla base delle applicazioni web e mobili. Vengono solitamente utilizzate dai moderni client front-end per consentire agli utenti finali autenticati di accedere alle funzionalità aziendali.

Le API B2B (da azienda ad azienda) sono offerte da un'organizzazione ad altre organizzazioni per consentire di svolgere attività aziendali e, talvolta, fornire valore anche ai clienti congiunti.

Le API B2B aiutano a semplificare le interazioni delle aziende con fornitori, rivenditori e altri partner, nonché a migliorare le experience offerte ai clienti.

Le API B2B includono ad esempio:

API di open banking

API di gestione della supply chain

API utilizzate per la fatturazione elettronica e per i pagamenti fra partner commerciali

Poiché i consumer delle API possono essere molto diversi, anche i controlli di sicurezza disponibili per la protezione di tali API possono variare notevolmente. Fino a poco tempo fa, il settore si è concentrato sugli scenari di utilizzo delle API B2C, ma, anche in questi casi, poiché l'attenzione era completamente dedicata alla protezione delle applicazioni web, la sicurezza di queste API veniva trascurata. Gli strumenti e i controlli di sicurezza solitamente utilizzati per la protezione delle applicazioni web B2C offrono alcuni vantaggi, come, ad es., le soluzioni WAF (Web Application Firewall)/WAAP (Web Application and API Protection), ma non possono fornire i livelli di visibilità, monitoraggio in tempo reale e protezione richiesti per proteggere le API B2C dagli attacchi.

Il problema della protezione delle API B2B sta diventando sempre più cruciale. Queste API, spesso, sono bersagli più facili da attaccare per i criminali perché, di frequente, non dispongono dei meccanismi di protezione essenziali. Gli strumenti per la sicurezza delle API del passato offrivano una visibilità limitata sulle API B2B e non riuscivano a proteggere le API che facilitavano l'accesso ai dati in blocco per conto di utenti condivisi, come nel caso dell'open banking, in cui le aziende di tecnofinanza e le istituzioni finanziarie condividono i dati dei clienti che hanno rilasciato il loro consenso. Per affrontare in modo efficace questi problemi, le soluzioni per la sicurezza delle API più recenti, tuttavia, offrono funzionalità di analisi comportamentale e sono in grado di riconoscere le attività anomale.

Quali sono le differenze tra API pubbliche e private?

Le API private, a volte chiamate anche API interne, sono destinate agli sviluppatori e ai collaboratori di un'azienda. Spesso parte di un'iniziativa SOA (Service-Oriented Architecture), le API private hanno lo scopo di semplificare lo sviluppo interno, consentendo a business unit o reparti diversi di accedere in modo efficace ed efficiente ai dati delle rispettive controparti.

Al contrario, le API pubbliche, note anche come API esterne, vengono rese accessibili a consumatori all'esterno dell'azienda. Le loro manifestazioni più estreme, come le API aperte, possono essere utilizzate liberamente da chiunque. In tutti i casi, richiedono una gestione rigorosa e una documentazione eccellente per poter essere utilizzate anche da tecnici esterni all'azienda.

È importante notare che le API private accessibili tramite Internet non sono veramente private nel senso stretto del termine. Prendiamo, ad esempio, l'API B2C di ACME sviluppata internamente dai tecnici ACME, che viene utilizzata esclusivamente dalle app mobili ACME. Si potrebbe avere la tentazione di considerarla privata, ma poiché il traffico verso tale API arriva da Internet, e quindi dall'esterno dell'azienda, non è veramente un'API privata, ma è semplicemente un'API non accessibile ad utenti esterni. Le API di questo tipo vengono attaccate regolarmente dagli hacker, che intercettano il traffico e retroingegnerizzano le app mobili per individuare le API corrispondenti.

Che cosa si intende per sicurezza delle API

Che cos'è la sicurezza delle API?

La sicurezza delle API è una strategia che mira ad ottenere visibilità, eseguire test rigorosi e proteggere le API presenti in un'azienda, incluse le API che sono parte integrante di applicazioni, processi aziendali e carichi di lavoro nel cloud. Tuttavia, poiché le API sia interne che esterne vengono prodotte in modo estremamente rapido e in enormi quantità, non è sempre facile avere un quadro completo dell'intero panorama delle API presenti in un'organizzazione. Molte organizzazioni non sanno quante API hanno effettivamente e quali API restituiscono dati sensibili quando vengono chiamate. Per identificare e mitigare i rischi per la sicurezza delle API, sono richiesti controlli di sicurezza abbastanza sofisticati da fornire questo tipo di visibilità e analisi dei dati. Le API che necessitano di protezione possono includere:

- API che semplificano l'accesso ai dati da parte di clienti o partner aziendali.
- API utilizzate dai partner aziendali.
- API implementate e utilizzate internamente allo scopo di mettere le funzionalità e i dati delle applicazioni a disposizione di vari sistemi e interfacce utente, in modo scalabile e standardizzato.

Una strategia efficace per la sicurezza delle API deve includere tecniche sistematiche per la valutazione dei rischi e dei potenziali effetti, oltre all'esecuzione di misure di contenimento adeguate. Per valutare i rischi, occorre innanzitutto creare un inventario di tutte le API, approvate e non, utilizzate dall'organizzazione, che deve includere attributi quali:

- Classificazioni dei dati che, come minimo, distinguono tra dati "non sensibili", "sensibili" e "molto sensibili".
- Indicatori di rischio, quali vulnerabilità ed errori di configurazione delle API.

Inoltre, la visibilità delle API e le misure di mitigazione dei rischi devono considerare varie potenziali minacce, tra cui:

- Rilevamento e prevenzione dell'utilizzo delle "API ombra" non autorizzate (vedere a lato)
- Identificazione e correzione delle vulnerabilità e degli errori di configurazione nelle API, che potrebbero essere sfruttati dai criminali
- Prevenzione degli scenari di utilizzo inappropriato delle API, come la violazione della logica aziendale e lo scraping dei dati

Qual è la differenza tra la sicurezza delle API e la sicurezza delle applicazioni?

Anche se la sicurezza delle API e la sicurezza delle applicazioni tradizionali sono discipline correlate, la sicurezza delle API costituisce un problema a sé stante per i suoi livelli di portata e complessità.

Scalabilità superiore

La rapida diffusione delle API è dovuta soprattutto a tre fattori:

1. Aumento del ricorso ai microservizi, un'architettura che impone l'uso delle API per la comunicazione fra i servizi.
2. Nel canale degli utenti diretti, i moderni framework delle applicazioni front-end, come React, Angular e Vue, utilizzano le API e stanno sostituendo le app web legacy.
3. Le API vengono aggiunte anche per gestire canali completamente nuovi, ad es., partner, IoT e automazione aziendale.

Complessità superiore dovuta all'aumento della flessibilità

A differenza delle applicazioni web, le API sono progettate per essere utilizzate a livello di programmazione e in molti modi diversi. Proprio per questo, è estremamente difficile distinguere gli utilizzi legittimi dagli attacchi e dalle violazioni.

Esiste una tassonomia delle API che i team di sicurezza dovrebbero conoscere?

Di seguito sono riportate le categorie e le descrizioni comuni delle API che possono presentarsi in un contesto di sicurezza.

API autorizzate

API pubblicata (con documentazione Swagger o simile)

API non autorizzate

- API ombra
- API non autorizzata
- API zombie
- API nascosta

API obsolete

- API obsoleta
- API legacy
- API zombie
- API orfana

Quali sono le best practice consigliate per la protezione delle API?

Per migliorare la sicurezza delle API, è possibile iniziare con le best practice elencate di seguito:

- Integrazione delle procedure e degli standard di sicurezza delle API con il ciclo di sviluppo del software utilizzato dall'organizzazione.
- Integrazione della documentazione e dei test di sicurezza automatizzati delle API nelle pipeline di integrazione continua/delivery continua (CI/CD, Continuous Integration/Continuous Delivery).
- Applicazione garantita di controlli di autenticazione e autorizzazione appropriati ed efficaci in tutte le API.
- Implementazione di misure di limitazione della velocità, per evitare lo sfruttamento o la compromissione delle API.
- Aumento della limitazione della velocità e delle altre misure a livello di applicazione, tramite reti per la distribuzione dei contenuti e/o gateway specializzati, allo scopo di mitigare il rischio di attacchi DDoS (Distributed Denial-of-Service).
- Integrazione dei test di sicurezza delle API nei processi di test delle applicazioni in generale.
- Rilevamento continuo delle API.
- Implementazione di un approccio sistematico con lo scopo di identificare e correggere le vulnerabilità più comuni delle API, come quelle incluse nell'elenco OWASP con i 10 principali rischi per la sicurezza delle API.
- Utilizzo del rilevamento e della prevenzione delle minacce basate su firma, come livello di protezione base contro gli attacchi noti alle API.
- Miglioramento del rilevamento basato su firma con l'intelligenza artificiale e l'analisi comportamentale per rendere il rilevamento delle minacce alle API più scalabile, accurato, rilevante per l'azienda e resiliente alle nuove minacce.
- Estensione dei processi di monitoraggio e analisi della sicurezza delle API per più settimane e sessioni API diverse.
- Integrazione del monitoraggio della sicurezza delle API, e della generazione degli avvisi relativi, con l'accesso on-demand all'inventario delle API e ai dati relativi alle attività destinati a ricercatori di minacce informatiche e sviluppatori, oltre che al personale DevOps e di supporto.

La capacità di implementare queste best practice dipende dal livello raggiunto nella strategia di sicurezza delle API (vedere a lato).

Fasi del processo di sicurezza delle API

Fase 1. Visibilità e rilevamento

È la fase di individuazione di tutte le API e dei microservizi da esse supportati tramite un approccio automatizzato. L'ampiezza della copertura è fondamentale perché le API trascurate (come quelle non più utilizzate) sono un obiettivo di primo piano per i criminali

Fase 2. Esecuzione dei test

È la fase in cui vengono eseguiti i test di tutte le API per garantirne la corretta codifica e il funzionamento previsto. I test eseguiti prima dell'implementazione di un'API rappresentano la fase finale di questo processo; i rischi vengono eliminati prima che l'API entri in fase di produzione e le correzioni eventualmente necessarie sono molto meno costose.

Fase 3. Controllo dei rischi

L'intero ambiente delle API viene continuamente controllato allo scopo di identificare le API configurate in modo errato o altri tipi di errori. Inoltre, queste verifiche garantiscono un'adeguata documentazione di tutte le API e stabiliscono se le API contengono dati sensibili o non sono sottoposte agli appropriati controlli di sicurezza.

Fase 4. Protezione del runtime

Viene utilizzata una soluzione con una protezione del runtime automatizzata, che riesce a distinguere le attività delle API normali da quelle anomale. Monitorando in tal modo le interazioni delle API, è possibile rilevare i comportamenti che indicano una minaccia in tempo reale.

Fase 5. Risposta

Vengono implementate soluzioni in grado di rispondere ai comportamenti sospetti delle API, come una soluzione WAF o un gateway API che blocca il traffico sospetto prima che possa accedere alle risorse critiche. Queste soluzioni utilizzano regole personalizzate e automatizzate.

Fase 6. Ricerca delle minacce

Vengono eseguite regolarmente analisi approfondite sui dati relativi alle minacce precedenti per scoprire se gli avvisi hanno identificato correttamente le minacce e se sono emersi modelli che attivano una ricerca proattiva delle minacce con una combinazione di strumenti sofisticati e intelligenza umana.

Rischi e violazioni della sicurezza delle API

Che cos'è la vulnerabilità di un'API?

In un'API, una vulnerabilità è un bug del software o un errore di configurazione del sistema, che può essere sfruttato da un criminale per accedere ai dati sensibili o alle funzionalità di un'applicazione oppure per utilizzare l'API in modo inappropriato. I 10 principali rischi per la sicurezza delle API riportati nell'elenco OWASP offrono un'interessante panoramica su alcune delle vulnerabilità delle API più ampiamente violate, che le organizzazioni devono tentare di identificare e risolvere.

Le vulnerabilità delle API vengono tutte registrate nell'elenco OWASP con i 10 principali rischi per la sicurezza delle API?

L'elenco OWASP con i 10 principali rischi per la sicurezza delle API costituisce un ottimo punto di partenza per le organizzazioni che cercano di migliorare il proprio approccio alla sicurezza delle API. Le sue categorie coprono una vasta gamma di potenziali rischi per le API, tuttavia quelle incluse nell'elenco OWASP con i 10 principali rischi per la sicurezza delle API sono numerose, pertanto è importante esaminare a fondo le sottoaree per ciascuna di essi. Gli autori di attacchi alle API tentano spesso di sfruttare i problemi di autorizzazione (ampiamente coperti dall'elenco OWASP), ma esistono anche minacce che non rientrano completamente nell'OWASP con i 10 principali rischi per la sicurezza delle API, come lo sfruttamento dei bug logici.

Quali sono le modalità di utilizzo improprio delle API?

Le API possono essere attaccate e sfruttate in vari modi, ma i più comuni includono:

- **Sfruttamento delle vulnerabilità.** Le vulnerabilità tecniche dell'infrastruttura sottostante possono causare la compromissione del server. Gli esempi di questo tipo variano dalle vulnerabilità Apache Struts (CVE-2017-9791, CVE-2018-11776) alle vulnerabilità Log4j (CVE-2021-44228).

- **Violazioni della logica aziendale.** Si verifica una violazione della logica quando un criminale sfrutta i difetti di progettazione o implementazione delle applicazioni per dare origine a un comportamento imprevisto e non autorizzato. Questi scenari sono fonte di preoccupazione per i CISO e i loro team poiché i controlli di sicurezza tradizionali sono inutili contro questi attacchi.

- **Accesso non autorizzato ai dati.** Un'altra forma comune di abuso delle API è lo sfruttamento di meccanismi di violazione delle autorizzazioni per accedere a dati che non dovrebbero essere accessibili. Queste vulnerabilità hanno molti nomi diversi, come BOLA (Broken Object Level Authorization), IDOR (Insecure Direct Object Reference) e BFLA (Broken Function Level Authorization).

- **Controllo degli account.** Dopo un furto di credenziali o persino un attacco XSS, è possibile assumere il controllo di un account. Quando questo accade, è possibile abusare persino delle API meglio scritte e perfettamente protette. L'utilizzo di una soluzione per la sicurezza delle API in grado di offrire funzionalità di analisi comportamentale consente di distinguere le attività autenticate dall'utilizzo illecito.
- **Scraping dei dati.** Quando le organizzazioni rendono disponibili i loro dataset tramite API pubbliche, gli autori delle minacce possono interrogare queste risorse in maniera aggressiva, per acquisire in maniera indiscriminata enormi dataset preziosi.
- **Attacchi DoS (Denial-of-Service) alle aziende.** Chiedendo al back-end di svolgere attività molto gravose, gli autori di attacchi alle API possono causare un rallentamento graduale del servizio, fino ad arrivare al blocco completo (DoS, Denial-of-Service) a livello di applicazione. Questa vulnerabilità è molto comune in GraphQL, ma può presentarsi in qualunque implementazione degli endpoint delle API che utilizza le risorse in modo intensivo.

Che cos'è un'API zombie?

Le API sono in continua evoluzione, spinte dall'evoluzione dei requisiti aziendali e di mercato. Quando vengono rilasciate nuove implementazioni degli endpoint per soddisfare nuove esigenze aziendali, correggere i bug e introdurre miglioramenti tecnici, le versioni precedenti di questi endpoint diventano obsolete. Ma poiché il ritiro dei vecchi endpoint è tutt'altro che semplice da gestire, le implementazioni obsolete degli endpoint rimangono spesso accessibili e funzionanti, trasformandosi in zombie.

Come si identificano i vari tipi di API ombra?

Uno dei modi che consente di effettuare il rilevamento delle API ombra a livello aziendale consiste nell'acquisire e nell'analizzare il traffico delle API sulla rete. Alcuni esempi di origini del traffico delle API includono i seguenti:

Una volta raccolti i dati non elaborati provenienti da tutte le fonti disponibili, è possibile utilizzare le tecniche dell'intelligenza artificiale per trasformarli in un inventario completo di tutti gli endpoint, le API e i parametri. A questo punto è possibile eseguire ulteriori analisi per classificare tali elementi e identificare le API ombra, che dovrebbero essere eliminate o introdotte nei processi di governance formali.

Come si possono proteggere le API interne e le API B2B?

In realtà dipende tutto da cosa si intende per "interno". Alcuni team considerano "API interne" le API che vengono esposte su Internet per essere utilizzate dalle applicazioni web e mobili della propria organizzazione. Anche se la documentazione di tali API può essere effettivamente accessibile solo ai dipendenti e ai collaboratori dell'azienda, gli hacker sono ormai esperti nell'analisi delle app e nella retroingegnerizzazione delle API tramite toolkit di disassemblaggio delle app e proxy come Burp Suite.

In ogni caso, se le "API interne" sono definite come API est-ovest, inaccessibili dall'esterno dell'organizzazione, il pericolo principale si riduce alle minacce interne. Per proteggere le API est-ovest e le API B2B, come per la maggior parte delle altre API, occorre proteggere innanzitutto il ciclo di sviluppo sicuro del software (SSDLC, Secure Software Development Lifecycle), quindi garantire un accesso autenticato e autorizzato, gestendo anche le quote, i limiti di velocità e gli arresti in caso di picchi di traffico improvvisi, oltre che utilizzando le soluzioni WAF/WAAP per la protezione delle API dalle minacce note. A causa della natura sensibile e spesso massiva delle transazioni nelle API B2B, è possibile considerare l'aggiunta di rigorosi meccanismi di autenticazione, come mTLS.

Sia per le API est-ovest che per le API B2B, è consigliabile utilizzare l'analisi comportamentale, soprattutto se le entità coinvolte sono numerose, il che può rendere difficile distinguere i comportamenti legittimi da quelli illegittimi. Ad esempio:

> **Come si può sapere se le credenziali API di uno specifico utente sono state violate?**

> **Come si può sapere se un partner che elenca i numeri delle fatture sta violando l'API di fatturazione allo scopo di rubare i dati degli account?**

La protezione delle API est-ovest e delle API B2B richiede un contesto aziendale che non può essere ricavato analizzando solamente gli elementi tecnici, come indirizzi IP e token API. L'unico modo per comprendere e gestire efficacemente i rischi consiste nell'utilizzare l'apprendimento automatico e l'analisi comportamentale per ottenere visibilità sulle entità aziendali rilevanti. Il contesto aziendale e i benchmark storici per l'uso normale delle API da parte di entità specifiche come utenti o partner, ma anche processi aziendali (fatture, pagamenti, ordini, e così via), consentono di rilevare anomalie che altrimenti passerebbero inosservate.

I gateway API offrono un'adeguata protezione dai rischi?

Molte organizzazioni che adottano un approccio strategico alle API utilizzano i gateway API, la maggior parte dei quali è dotata di funzioni di sicurezza integrate molto utili alle organizzazioni, a partire dall'autenticazione (e dell'autorizzazione, se è possibile utilizzare OpenID Connect). Tuttavia, da sole, l'autenticazione, l'autorizzazione e la gestione delle quote a livello di gateway API non sono sufficienti, e per diversi motivi:

Lacune nel rilevamento eseguito dai gateway API: i gateway API hanno visibilità e controllo solo sulle API che sono configurati per gestire, ma sono completamente inefficaci nel caso degli endpoint e delle API ombra.

Lacune di sicurezza dei gateway API: i gateway API possono applicare l'autenticazione e, in parte, gli schemi di autorizzazione, ma non ispezionano i payload (come WAF e WAAP) né creano un profilo comportamentale in grado di rilevare le violazioni.

Quali sono gli errori più comuni nella configurazione delle API?

Visto l'elevato numero delle possibili modalità di utilizzo delle API, gli errori di configurazione che si possono commettere sono praticamente infiniti. In una configurazione errata, si rilevano, tuttavia, alcuni temi ricorrenti:

Autenticazione inefficace o assente

L'autenticazione è fondamentale per proteggere i dati sensibili resi disponibili tramite le API. Occorre innanzitutto garantire che tutte le API che trasportano dati sensibili utilizzino l'autenticazione, ma è importante anche proteggere i meccanismi di autenticazione dagli attacchi di forza bruta, dal credential stuffing e dall'uso di token di autenticazione rubati, limitando la velocità. Possono, inoltre, verificarsi errori di configurazione che consentono ai consumer delle API di ignorare i meccanismi di autenticazione, spesso in relazione alla gestione dei token, come nel caso dei problemi noti di convalida dei JWT o della mancanza di controllo dell'ambito dei token.

Autorizzazione inefficace

Le API vengono spesso utilizzate per fornire accesso a dati o contenuti, comprese le informazioni sensibili. L'autorizzazione è un processo che consente di verificare l'idoneità di un consumer delle API ad accedere ai dati richiesti, prima di renderli disponibili. Questa operazione può essere eseguita a livello di oggetto o di risorsa (ad esempio, un utente può accedere ai propri ordini, ma non a quelli degli altri) oppure a livello di funzione (come spesso accade con le funzionalità amministrative). L'autorizzazione è difficile da implementare correttamente, a causa dell'elevato numero di casi e condizioni sull'edge, oltre che della moltitudine dei flussi possibili per le chiamate API tra i microservizi. Se non utilizza un motore di autorizzazione centralizzato, l'implementazione dell'API potrebbe includere alcune di queste vulnerabilità, come BOLA e BFLA.

Errata configurazione della sicurezza

Oltre ai problemi di autenticazione e autorizzazione menzionati in precedenza, è possibile anche commettere diversi tipi di errori di configurazione della sicurezza, che includono comunicazioni non sicure (come l'uso di suite di crittografia vulnerabili o l'assenza del protocollo SSL/TLS), soluzioni di storage su cloud non protette e policy eccessivamente permissive per la condivisione delle risorse tra origini diverse.

Mancanza di risorse e limitazione della velocità

Quando le API vengono implementate senza limitare il numero delle chiamate eseguibili dai relativi consumer, i criminali possono sovraccaricare le risorse del sistema determinando un peggioramento del servizio o sferrando un attacco DoS su vasta scala. I limiti di velocità dovrebbero essere applicati, come minimo, all'accesso a qualsiasi endpoint non autenticato (gli endpoint di autenticazione rivestono un'importanza critica); in caso contrario, attacchi di forza bruta, credential stuffing e convalida delle credenziali sono semplicemente inevitabili.

Che cosa sono gli attacchi alle API?

Gli attacchi alle API sono tentativi di utilizzare le API per scopi dannosi o non autorizzati. Gli attacchi alle API possono assumere varie forme, tra cui:

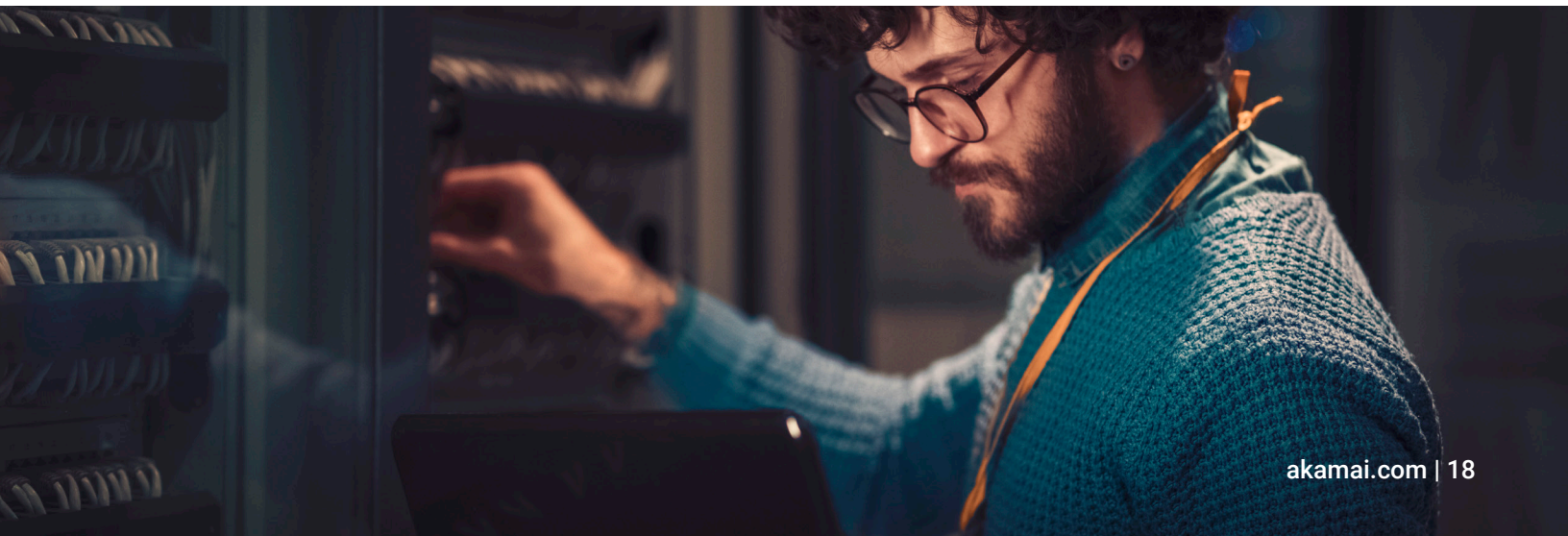
- Sfruttamento delle vulnerabilità tecniche presenti nelle implementazioni delle API
- Utilizzo di credenziali rubate e di altre tecniche per il controllo degli account, che consentono ad un criminale di spacciarsi per un utente legittimo
- Violazione della logica business che consente l'utilizzo delle API con modalità impreviste

Che cos'è il credential stuffing per le API?

La fuga di ID utente e password da siti web e piattaforme SaaS (Software-as-a-Service) è ormai un problema abituale. Questi incidenti comportano spesso la condivisione online di moltissimi set di credenziali. Il credential stuffing è una pratica che consiste nell'utilizzare le credenziali di autenticazione ottenute da siti web violati in precedenza per effettuare tentativi di accesso automatici ad altri siti web. Questa tecnica si basa sul presupposto che molti utenti utilizzano le stesse credenziali per accedere siti diversi. In numero sempre maggiore, i criminali ora puntano direttamente alle API e prendono di mira i loro meccanismi di autenticazione in modo da poter automatizzare più facilmente gli attacchi dato che le API vengono create proprio per semplificare l'utilizzo.

Che cos'è l'esfiltrazione dei dati tramite le API?

L'esfiltrazione dei dati è il risultato più comune che deriva dall'abuso e dagli attacchi sferrati contro le API. In alcuni casi, si riferisce al furto di informazioni altamente sensibili e riservate, eseguito da un criminale tramite un attacco alle API. Tuttavia, può indicare anche tipi di violazioni meno gravi, incluso lo scraping di dati pubblicamente disponibili condotto in modo aggressivo per accumulare grandi dataset che, in forma aggregata, forniscono informazioni preziose.



Tendenze e soluzioni per la sicurezza delle API

Quali sono le ultime tendenze in materia di sicurezza delle API?

Di seguito sono riportate le tendenze principali che i responsabili della sicurezza dovrebbero prendere in considerazione nello sviluppo di una strategia di sicurezza delle API:

Analisi comportamentale e rilevamento delle anomalie: anziché cercare di prevedere i possibili attacchi e affidarsi esclusivamente al rilevamento basato su firme e alle policy predefinite (come le soluzioni WAF) per mitigare i rischi, le organizzazioni stanno integrando sempre più spesso l'apprendimento automatico e l'analisi comportamentale per visualizzare le attività delle API in un contesto aziendale e per rilevare le anomalie.

Transizione dagli ambienti on-premise a SaaS: mentre molti prodotti per la sicurezza delle API di prima generazione sono stati implementati on-premise, gli approcci basati su SaaS sono sempre più diffusi a causa dei loro livelli di velocità e facilità di implementazione, a cui si aggiunge la possibilità di sfruttare la potenza dell'apprendimento automatico su vasta scala.

Analisi di finestre temporali più ampie: gli approcci alla sicurezza delle API che analizzano solamente le singole chiamate API o le attività nelle sessioni a breve termine vengono sostituiti da piattaforme che possono analizzare le attività delle API nel corso di alcuni giorni, e talvolta di settimane, dall'ottimizzazione automatizzata delle policy WAF di base all'analisi dei comportamenti fino al rilevamento delle anomalie.

Metodologia DevSecOps estesa anche agli stakeholder non esperti di sicurezza: uno dei metodi più efficaci per contenere i rischi legati alle API consiste nel creare legami più stretti fra le strategie e gli strumenti di sicurezza delle API, gli sviluppatori e i sistemi coinvolti nella creazione, nell'implementazione e nella configurazione delle API.

Sicurezza delle API basata su API: anche se è essenziale rilevare e mitigare le violazioni e gli attacchi in corso contro le API, le organizzazioni più lungimiranti stanno cercando soluzioni per utilizzare l'accesso on-demand ai dati e alle informazioni dettagliate sulla sicurezza delle API per migliorare la ricerca delle minacce, la risposta agli incidenti e le pratiche di sviluppo delle API.

Che cos'è la sicurezza delle API basata su firma?

Le tecniche di sicurezza delle API basate su firme monitorano le caratteristiche e i modelli di attacco noti allo scopo di generare avvisi e altre risposte automatizzate quando rilevano una discrepanza. Questo è il comportamento tipico delle soluzioni WAF (Web Application Firewall). Se un'organizzazione scopre che il traffico API in entrata è compromesso o presenta comportamenti anomali, può utilizzare la sicurezza delle API basata su firma per bloccare immediatamente tale minaccia.

È consigliabile scegliere una soluzione WAF inserita in una piattaforma WAAP più ampia in grado di offrire funzioni di rilevamento avanzate basate sull'apprendimento automatico, che apprende dai modelli di firma degli attacchi e rimane agile anche quando viene utilizzata su vasta scala. Una piattaforma WAAP integrata con una soluzione per la sicurezza delle API che offre analisi comportamentale e risposte personalizzate offre il meglio di entrambi gli approcci. Insieme, queste soluzioni offrono un livello completo di visibilità, rilevamento e risposta delle API, sia internamente che esternamente.

Che cosa sono le attività di rilevamento e risposta delle API?

Le attività di rilevamento e risposta delle API rientrano in una nuova categoria della sicurezza delle API, incentrata sull'analisi approfondita dei dati storici con lo scopo di:

- Identificare uno schema di comportamento base per tutti i consumer API.
- Rilevare attacchi e anomalie che indicano possibili violazioni e utilizzi inappropriati delle API.

Per essere efficaci su vasta scala, le soluzioni di rilevamento e risposta delle API devono essere basate su un modello SaaS, a causa delle enormi dimensioni dei dataset richiesti dalle tecniche di apprendimento automatico a uso intensivo di risorse.

Che cos'è la protezione avanzata dalle minacce alle API?

La protezione avanzata dalle minacce alle API è un approccio SaaS alla sicurezza delle API, che combina l'analisi comportamentale con la ricerca delle minacce allo scopo di:

- Rilevare tutte le API utilizzate da un'organizzazione, incluse le API ombra o zombie.
- Applicare l'apprendimento automatico per sovrapporre il contesto aziendale e determinare le modalità di utilizzo e violazione delle API.
- Eseguire l'analisi comportamentale e la ricerca delle minacce, sia sulle API che sui dati relativi alle loro attività.

Che cos'è una piattaforma di sicurezza delle API?

Una piattaforma di sicurezza delle API è una soluzione basata su SaaS, che viene espressamente progettata allo scopo di:

- Creare un inventario, aggiornato continuamente, di tutte le API utilizzate a livello aziendale, incluse quelle non autorizzate.
- Analizzare le API e il relativo utilizzo per scoprire il contesto aziendale e determinare lo schema di base del comportamento previsto.
- Rilevare anomalie nell'utilizzo delle API e, se necessario, generare avvisi e dati di supporto ai flussi di lavoro SIEM (Security Information and Event Management) e SOAR (Security Orchestration, Automation and Response).
- Fornire accesso on-demand all'inventario delle API e alle informazioni relative ad attività e minacce per tutti gli stakeholder, non solo esperti di sicurezza.

Che cos'è un'azienda per la sicurezza delle API?

Ora che i responsabili della sicurezza e IT utilizzano le API in modo più strategico, potrebbero sentire l'esigenza di ricorrere a partner specializzati in materia di API. Queste aziende possono essere suddivise in tre tipologie comuni:

- Aziende che forniscono la tecnologia necessaria per accettare le chiamate API in un sistema centrale, per poi indirizzarle alle risorse di back-end e ai microservizi appropriati.
- Aziende che forniscono piattaforme di sicurezza delle API per garantire alle organizzazioni di riuscire ad identificare tutte le API attive e i loro potenziali rischi, rilevare attacchi e violazioni, eseguire test completi sulla sicurezza e fornire informazioni dettagliate sull'utilizzo delle API.
- Aziende che forniscono piattaforme WAAP e di sicurezza delle API, che possono aiutare i clienti a trasferire in modo trasparente i dati relativi al traffico delle API, offrendo, al contempo, la possibilità di rilevare le API, all'interno e all'esterno della piattaforma, ossia la soluzione ideale per il consolidamento dei fornitori e la risoluzione delle lacune digitali.

Che cos'è la ricerca delle minacce alle API?

La ricerca delle minacce implica l'individuazione attiva di minacce sconosciute o mai rilevate in precedenza. Questo approccio proattivo è cruciale per l'identificazione di minacce nuove ed emergenti mai rilevate in precedenza e per la loro mitigazione prima che possano causare danni significativi. Una delle principali tecniche usate nella ricerca delle minacce è l'analisi comportamentale, che include l'analisi del comportamento delle API per identificare eventuali attività sospette o anomale. Ad esempio, se un'API richiede improvvisamente migliaia di record in un breve periodo di tempo, ciò potrebbe indicare che la logica aziendale dell'API è stata violata. Le moderne soluzioni per la sicurezza delle API forniscono specifiche funzionalità di ricerca delle minacce per consentire ai team addetti alla sicurezza di identificare tempestivamente le minacce potenziali e adottare le contromisure necessarie.

Che cos'è una soluzione WAAP?

Una soluzione WAAP (Web Application and API Protection) è una categorizzazione utilizzata dalla società di ricerche Gartner per classificare le nuove soluzioni per la protezione di applicazioni web e API. Si tratta di un'evoluzione della precedente soluzione WAF introdotta per rispondere alla crescente importanza strategica assunta dalla sicurezza delle API e al passaggio dalle piattaforme WAF sul cloud come servizi SaaS gestiti.

In cosa consiste la documentazione delle API?

Il tipo di documentazione più comune per le API RESTful (che sono le API web più diffuse) è costituito da una raccolta di file Swagger basati sulla specifica OpenAPI. In teoria, la documentazione delle API viene creata dagli sviluppatori durante le relative fasi di progettazione o implementazione, ma in realtà tale documentazione risulta spesso obsoleta e le modalità di utilizzo effettive delle API risultano notevolmente diverse da quelle documentate. Per risolvere il problema, alcune piattaforme di sicurezza delle API possono generare file Swagger a partire dalle attività reali delle API, evidenziando le lacune tra l'uso documentato e quello effettivamente implementato, allo scopo di fornire informazioni essenziali per qualunque valutazione dei rischi associati alle API.

Esiste una lista di controllo per la sicurezza delle API consigliata alle aziende?

Per garantire una sicurezza efficace delle API, è necessario eseguire regolarmente una serie di procedure dettagliate. Di seguito, viene riportata una lista di controllo che può essere utilizzata dai team addetti alla sicurezza come punto di partenza per migliorare il proprio sistema di sicurezza delle API:

- Il sistema di sicurezza delle API include un meccanismo per il rilevamento continuo delle API a livello aziendale?
- La gestione del sistema delle API è integrata in un sistema più ampio costituito dalle pratiche di gestione della sicurezza e dei rischi dell'organizzazione?
- Viene implementato un approccio generale alla sicurezza delle API, non ancorato a specifici modelli di infrastruttura di data center o cloud?
- L'approccio utilizzato offre ai team il contesto aziendale di cui hanno bisogno per comprendere a fondo l'attività delle API e i potenziali rischi osservati?
- Si dispone di una strategia per l'automazione bidirezionale fra la piattaforma di sicurezza delle API e gli altri processi aziendali correlati, come SIEM/SOAR, ricerca delle minacce, documentazione, strumenti DevOps e così via?
- Vengono adottate le misure necessarie per estendere gli strumenti e i processi di protezione delle API anche agli stakeholder che non sono specializzati in materia di sicurezza?

Le soluzioni di sicurezza Akamai proteggono le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o le customer experience. Tramite la scalabilità della nostra piattaforma globale e la visibilità delle minacce, possiamo unire le nostre forze per prevenire, rilevare e mitigare le minacce affinché voi possiate rafforzare la fiducia nel brand e realizzare la vostra visione. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn.
Data di pubblicazione: 09/24.