La guida definitiva all'individuazione delle API

Sommario

L'importanza dell'individuazione delle API

Se state avviando un sistema di sicurezza delle API o desiderate migliorare ulteriormente la vostra strategia, individuare e inventariare tutte le API della vostra organizzazione sono operazioni fondamentali. Perché? Dietro ogni applicazione realizzata dalla vostra azienda, ogni carico di lavoro migrato nel cloud e ogni strumento utilizzato dai dipendenti per collaborare, ci sono delle API che si occupano dello scambio di dati spesso sensibili. Il problema è che la maggior parte delle organizzazioni (anche quelle che comprendono l'importanza di un inventario completo) non riesce a vedere effettivamente un numero consistente delle API di cui dispongono.

Ed è impossibile proteggersi da ciò che non si vede.

Man mano che le organizzazioni diventano sempre più digitali e incentrate sul cloud, il patrimonio delle loro API cresce in termini di ambito, portata e complessità. Le API sono, spesso, diffuse in più ambienti, dagli ambienti on-premise al cloud ibrido. A complicare la situazione, l'ecosistema delle API si estende probabilmente ben oltre il perimetro di rete e il cloud. Pensiamo alla miriade di connessioni che le API hanno stabilito con app, servizi e sistemi che appartengono agli ecosistemi di sviluppatori e terze parti.

Man mano che le API aumentano di ambito, portata e complessità, è difficile ottenere informazioni in tempo reale sui seguenti elementi:

- Dove si trovano le API nelle varie business unit che, in molti casi, dispongono di propri team di sviluppatori
- Come vengono configurate le API, dove sono instradate e se dispongono di appropriati controlli di autenticazione e autorizzazione
- Se le API restituiscono dati sensibili quando vengono chiamate e chi può ottenere l'accesso a questi dati

A complicare la situazione, molte API accumulate dalle organizzazioni non sono gestite, sono invisibili e, spesso, non sono protette, tra cui le API inattive, nascoste e zombie, che, in molti casi, non vengono rilevate dai sistemi di difesa degli strumenti comunemente usati, come gateway API e WAF (Web Application Firewall). Anche se questi strumenti offrono indubbi vantaggi e una protezione basilare, l'attuale panorama delle minacce per le API richiede un maggior livello di visibilità, protezione in tempo reale ed esecuzione continua dei test rispetto a quanto riescano a fornire le soluzioni specializzate per la sicurezza delle API.

Individuando tutte le API, riuscirete a costruire una solida base per le successive operazioni essenziali, come valutare i rischi per tutte le API, comprendere il livello di sicurezza delle API della vostra organizzazione e utilizzare le informazioni acquisite per applicare una protezione in tempo reale allo scopo di prevenire gli attacchi. In questo white paper, troverete:

- Informazioni sugli elementi che rendono alcuni tipi di API così elusivi per i team addetti alla sicurezza
- Dettagli sulle funzionalità di individuazione delle API che possono aiutarvi ad ottenere visibilità e a prevenire gli attacchi

Perché le API sono così difficili da individuare?

Non è raro disporre di API non gestite in fase di produzione di cui nessuno nei team addetti alle operazioni/sicurezza sa nulla, il che rende l'azienda vulnerabile ad una serie di rischi per la cybersicurezza e di problemi operativi. Le API vulnerabili o non correttamente configurate sono prevalenti, non protette e facili da violare per i criminali. In più, la posta in gioco è alta. Gli attacchi sferrati contro le API possono mettere a rischio i profitti, la resilienza e la conformità normativa di un'azienda.

Ecco di seguito quattro modi che possono dare luogo alle API non autorizzate:

1. Errori nei comandi rapidi e nei processi delle API

Alcune API non autorizzate 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 il team IT oppure gli sviluppatori potrebbero essere più preoccupati dell'esecuzione che delle procedure. Anche le API che sono state "ereditate" in seguito ad un'acquisizione aziendale vengono frequentemente dimenticate. Questi tipi di API non autorizzate vengono spesso indicate come API ombra.

2. Versioni delle API obsolete

In molti casi, una vecchia versione di un'API, possibilmente con un livello di sicurezza inferiore o una vulnerabilità nota, non viene mai rimossa perché, ad esempio, deve coesistere con una nuova versione per il periodo di tempo richiesto per l'aggiornamento del software. Tuttavia, cosa succede se il responsabile della disattivazione delle API lascia l'azienda, si occupa di un nuovo incarico o, semplicemente, si dimentica di arrestare la versione precedente?
Le API possono anche essere dismesse ufficialmente, ma rimangono attive per la supervisione operativa.
Entrambi i casi determinano ciò che viene spesso indicato come API zombie.

3. API ereditate

Le API che sono state "ereditate" in seguito a fusioni o acquisizioni aziendali vengono frequentemente dimenticate e diventano API ombra. Gli inventari (se esistenti), spesso, si perdono nel difficile e complicato lavoro di integrazione dei sistemi. Le grandi imprese che effettuano numerose acquisizioni di aziende più piccole sono particolarmente a rischio perché le API delle aziende più piccole, spesso, proliferano e non sono documentate.

4. API commerciali

Alcuni pacchetti software commerciali includono le API per la connessione ad altre applicazioni e fonti di dati esterne. Talvolta, queste API possono essere attivate a nostra insaputa.

Che cos'è l'individuazione delle API?

L'individuazione delle API consiste in un processo e un insieme di funzionalità che aiutano le organizzazioni a identificare, catalogare e gestire le API, oltre a valutarne i rischi associati. Se condotta correttamente, l'individuazione delle API può aiutare le organizzazioni a:

- Ridurre la proliferazione delle API (ossia, la rapida accumulazione delle API senza un'adeguata documentazione o supervisione) e migliorare il sistema di sicurezza
- Comprendere meglio il loro attuale scenario delle API e prendere decisioni informate sullo sviluppo futuro
- Monitorare e controllare l'accesso alle API, garantendo che solo gli utenti autorizzati possano accedervi

Le principali funzioni di individuazione delle API in grado di migliorare la visibilità e ridurre i rischi

Spesso, non si conoscono tutte le API di cui si dispone. Senza un inventario accurato, tuttavia, la vostra azienda viene esposta ad una serie di rischi. Per creare un inventario accurato delle API, dovete:

Individuare
e inventariare le vostre API, indipendentemente dalla configurazione o dal tipo

Rilevare
le API non gestite, come le API inattive e zombie

Identificare
i domini ombra dimenticati, trascurati o non conosciuti

Eliminare
le lacune di visibilità e scoprire i potenziali percorsi degli attacchi

Durante la valutazione di nuove soluzioni per l'individuazione delle API, tenete presente che uno strumento di individuazione deve includere tutte le funzionalità riportate di seguito:

Individuazione di tutti i tipi di API

Uno strumento di individuazione delle API deve essere in grado di identificare le API di ogni configurazione o tipo, tra cui RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC.

Inventario granulare delle API

Uno strumento di individuazione delle API deve anche essere in grado di creare un inventario che viene aggiornato automaticamente per impedire che diventi obsoleto e deve offrire la possibilità di cercare, etichettare, filtrare, assegnare ed esportare le API in base a qualsiasi attributo.

Rilevamento elusivo delle API

Le API non gestite possono influire negativamente sulle iniziative di sicurezza delle API di un'organizzazione: ad esempio, la proliferazione delle API potrebbe essere iniziata con un team di sviluppatori che hanno lasciato l'azienda perché, di solito, queste API non sono gestite e funzionano senza alcuna visibilità o controlli di sicurezza. È fondamentale per uno strumento di individuazione trovare queste API.

Individuazione dei domini nascosti delle API

Come le API, anche i domini possono essere nascosti, ossia non si sa nulla sui nomi dei domini delle API. Gli strumenti di individuazione delle API devono identificare i domini nascosti dimenticati, trascurati o non conosciuti, che potrebbero rappresentare un rischio per la sicurezza.

Scansione automatica delle API

La scansione è fondamentale per eliminare i punti ciechi e per identificare problemi critici, tra cui:

- Fuga di credenziali e chiavi API
- Esposizione degli schemi e del codice delle API
- Errori di configurazione dell'infrastruttura
- Vulnerabilità presenti nella documentazione, negli archivi GitHub, negli spazi di lavoro Postman, ecc.

L'identificazione di queste e di altre fonti di intelligence sfruttabile può aiutare anche i team a capire i potenziali percorsi di attacco che i criminali informatici potrebbero utilizzare.

Nessuna integrazione richiesta

Uno strumento di individuazione delle API deve essere in grado di rilevare l'intero patrimonio delle API, individuando le API vulnerabili e i domini nascosti, senza richiedere una speciale integrazione o l'installazione di software. Queste funzionalità sono fondamentali per evitare le lacune di visibilità che si verificano solo perché l'installazione degli agenti giusti o la configurazione degli strumenti non è riuscita correttamente.

Sviluppo personalizzato limitato

Infine, uno strumento di individuazione delle API deve essere progettato in modo da evitare la necessità di adottare uno sviluppo personalizzato per le fonti di traffico. Questi strumenti vengono, di solito, preintegrati nei principali componenti infrastrutturali. Lo sviluppo personalizzato, di solito, è dispendioso in termini di tempo e, se vengono apportate modifiche all'origine, potrebbe essere necessario rielaborare un'integrazione, che non è scalabile per i team addetti alla sicurezza IT già sotto pressione.

Come Akamai Security può aiutarvi ad individuare tutte le API

Con funzionalità di individuazione delle API complete e costanti, le organizzazioni possono ottenere i seguenti vantaggi per le loro attività aziendali:

- Conoscere tutta la superficie di attacco delle API
- Ridurre i costi correlati con gli inventari delle API e gli aggiornamenti della documentazione
- Migliorare la conformità con requisiti normativi e policy interne

Oggi, le minacce richiedono una soluzione per la sicurezza delle API completa, che comprende quattro aree critiche: individuazione delle API, gestione dei sistemi, rilevamento e mitigazione delle minacce e, infine, esecuzione di test sulla sicurezza. Akamai API Security fornisce tutti e quattro questi moduli essenziali, proteggendo le API per l'intero ciclo di vita, dallo sviluppo alla produzione. Concepita per le organizzazioni che rendono visibili le API ai loro partner, fornitori e utenti, la nostra soluzione API Security rileva le API, esamina il loro livello di rischio, analizza il loro comportamento e blocca il proliferare delle minacce all'interno.

Leggete ulteriori informazioni sui metodi di attacco alle API, sulle vulnerabilità delle API più comuni e su come proteggere la vostra organizzazione.

Scoprite come possiamo aiutarvi programmando una demo personalizzata su Akamai API Security.

Informazioni sulle soluzioni per la sicurezza di Akamai

Le soluzioni per la sicurezza di 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: 10/24.