Guida all’acquisto di una soluzione per la sicurezza delle API

Prepararsi ad affrontare la sfida alla sicurezza delle API

Man mano che le organizzazioni diventano sempre più digitali e incentrate sul cloud, le API crescono in termini di ambito e portata, aumentando il loro valore. Ora le API:

- Operano al centro delle applicazioni e dei servizi utilizzati dai vostri clienti e partner, incluse le innovazioni più recenti nel campo dell'intelligenza artificiale
- Sono incorporate negli ambienti cloud, dai servizi utilizzati dagli sviluppatori fino ai carichi di lavoro spostati dai tecnici in modalità "lift-and-shift"
- Generano flussi di entrate, aiutando ad espandere le vostre attività aziendali e a creare un ecosistema di sviluppatori

Tuttavia, se come il 78% dei professionisti del settore IT e della sicurezza avete subito incidenti legati alla sicurezza delle API[1], vi siete resi conto di persona del crescente rischio rappresentato dalle API. Le API vulnerabili o non correttamente configurate sono prevalenti, non protette e facili da violare. Molte organizzazioni, spesso, non conoscono neanche tutte le loro API, il che le rende vulnerabili. Queste API inattive o zombie sono i principali vettori di attacco.

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. La maggior parte delle organizzazioni non ha ancora implementato le funzionalità e i controlli appropriati per prevenire gli attacchi alle API. Certamente, molte aziende dispongono di strumenti per le API nel loro stack esistente, inclusi gateway API e soluzioni WAF (Web Application Firewall). Tuttavia, anche se questi strumenti possono offrire una certa protezione, non sono progettati per fornire il grado di visibilità, sicurezza in tempo reale ed esecuzione continua dei test necessario per difendersi dai moderni attacchi alle API.

1. Akamai Technologies, “API Security Disconnect Report,” 2023

Cosa serve quindi per garantire una protezione completa al vostro patrimonio delle API? Anche se negli ultimi anni è emersa una schiera di prodotti per la sicurezza delle API, barcamenarsi tra il crescente numero di vendor e le loro funzionalità può risultare difficile.

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. Questa guida all'acquisto descrive le funzionalità principali di cui deve disporre una soluzione per la sicurezza delle API completa, definendo le funzioni e i controlli di sicurezza necessari per sviluppare e mantenere le API sicure, individuando e proteggendo, al contempo, ogni API presente nel vostro ecosistema.

Le funzionalità principali di una soluzione per la sicurezza delle API completa

Per stabilire le funzioni di sicurezza delle API che vi servono, è importante capire la natura delle sfide che vi trovate ad affrontare.

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 di terze parti, che potrebbero o meno dare priorità alla sicurezza delle API.

Inoltre, è difficile ottenere informazioni in tempo reale sui seguenti elementi:

- La posizione in cui vengono instradate le API
- Il modo con cui vengono configurate
- Quali dati sensibili spostano
- Quali rischi rappresentano

Poiché le aziende sviluppano e implementano rapidamente nuove applicazioni e API, la superficie di attacco cresce in modo esponenziale. Come per le API obsolete, l'organizzazione potrebbe aver creato e prodotto un gruppo di API anni fa, prima che la sicurezza delle API finisse per emergere come una necessità di importanza critica.

La mancanza di visibilità conduce ad alcuni risultati preoccupanti: solo 4 professionisti della sicurezza su 10 che dispongono di inventari completi delle API sanno quali delle loro API restituiscono dati sensibili quando vengono chiamate. Molte di queste chiamate API provengono da criminali che mettono alla prova le vulnerabilità e, una volta individuata una lacuna, sferrano attacchi spesso implacabili.

Al momento di esaminare i fornitori di soluzioni per la sicurezza che affermano di poter garantire una protezione completa delle API, è importante assicurarsi di aver stabilito l'esecuzione di funzionalità e controlli in fase di produzione in quattro aree critiche.

Di seguito, potrete trovare alcune checklist utili per gli acquirenti che desiderano esaminare le funzionalità dei vendor.

01

Individuazione delle API

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 inattive, legacy e zombie
- ☑ Identificare i domini ombra dimenticati, trascurati o non conosciuti
- ☑ Eliminare i punti ciechi e scoprire i potenziali percorsi degli attacchi

02

Gestione del sistema delle API

Anche un semplice errore di configurazione delle API può lasciare campo libero ai criminali, che, una volta penetrati nel sistema, possono accedere ed esfiltrare rapidamente i dati sensibili. Per capire come sono configurate tutte le vostre API, dovete:

- ☑ Eseguire una scansione automatica dell'infrastruttura per scoprire eventuali configurazioni errate e rischi nascosti
- ☑ Creare workflow personalizzati per informare le principali persone coinvolte sulle vulnerabilità
- ☑ Identificare le API e gli utenti interni che possono accedere ai dati sensibili
- ☑ Classificare i problemi rilevati in base ai livelli di gravità per dare priorità alla mitigazione

03

Rilevamento e mitigazione degli attacchi alle API

Gli attacchi alle API stanno diventando impossibili da evitare. Per rilevare e mitigare le minacce in modo efficace, dovete:

- ☑ Monitorare gli episodi di manomissione e fuga di dati, violazioni delle policy, comportamenti sospetti e abuso delle API
- ☑ Analizzare il traffico delle API proveniente da tutte le fonti ed effettuare le opportune integrazioni con i workflow esistenti (creazione di ticket, Security Information and Event Management, ecc.) per avvisare i team addetti alle operazioni/sicurezza
- ☑ Prevenire gli attacchi e gli abusi in tempo reale con una mitigazione parzialmente o totalmente automatizzata

04

Esecuzione di test sulla sicurezza delle API

La velocità è essenziale per ogni applicazione creata dagli sviluppatori, il che, tuttavia, rende più difficile rilevare una vulnerabilità o un difetto di progettazione. Per eseguire test accurati delle API, dovete:

- ☑ Eseguire un'ampia serie di test automatizzati che simulano il traffico dannoso e seguono la logica aziendale sottostante delle API
- ☑ Individuare le vulnerabilità prima che le API entrino in fase di produzione per ridurre il rischio di un attacco
- ☑ Esaminare le specifiche delle API sulla base delle regole e delle policy di governance stabilite
- ☑ Eseguire test sulla sicurezza delle API on-demand o come parte di una pipeline CI/CD

Individuazione delle API: un'analisi approfondita delle funzionalità principali

Molte organizzazioni utilizzano sia API nuove che già esistenti. 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 non autorizzate possono derivare da vari fattori, come comandi rapidi, errori nei processi e la loro mancata interruzione una volta dismesse. Alla pagina successiva, vengono forniti esempi chiave da poter consultare.

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 a nostra insaputa.

Errore di disattivazione

Le API possono anche essere dismesse ufficialmente, ma rimangono attive per la supervisione operativa e, a volte, vengono definite API zombie.

Versioni delle API obsolete

A volte, una versione precedente di un'API non viene dismessa 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?

Comandi rapidi ed errori nei processi

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.

Durante i colloqui con i vendor, chiedete di spiegarvi come riescono a far sì che le API non autorizzate, legacy, zombie e nascoste vengano identificate e gestite prima che possano essere sfruttate. Le API legacy e zombie sono spesso l'anello più debole nella sicurezza delle API. Pertanto, è fondamentale individuare le API che non sono gestite da un gateway API e localizzarle, inventariarle e stabilire se devono essere mitigate o dismesse.

Le principali funzioni di individuazione delle API

Una soluzione per la sicurezza delle API deve includere le seguenti funzioni di individuazione:

Rilevamento delle risorse e inventario granulare delle API

Uno strumento di individuazione delle API deve essere in grado di bloccare e identificare le API di cui si dispone, indipendentemente dalla configurazione o dal tipo, tra cui RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC. La soluzione 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 delle API inattive, legacy e zombie

Le API legacy e zombie possono influire negativamente sulle iniziative della sicurezza delle API di un'organizzazione perché, di solito, non sono gestite e funzionano senza alcuna visibilità o controlli di sicurezza. Uno strumento di individuazione delle API deve essere in grado di trovare questo tipo di API.

Individuazione dei domini nascosti

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 essere in grado di identificare i domini nascosti dimenticati, trascurati o non conosciuti, che potrebbero rappresentare un rischio per la sicurezza.

Scansioni automatiche

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.

Sviluppo personalizzato limitato

Infine, con lo strumento di individuazione delle API appropriato, non avete bisogno di 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.

Gestione del sistema delle API: un'analisi approfondita delle funzionalità principali

Le minacce al patrimonio delle API stanno crescendo rapidamente in seguito a varie tendenze, come il passaggio da operazioni IT centralizzate ad operazioni LOB decentralizzate, il maggior uso delle risorse cloud e la transizione ad architetture basate su microservizi.

Una solida individuazione (come descritto nella sezione precedente) è il primo passaggio necessario per garantire la protezione del patrimonio delle API. Dovete individuare ed inventariare tutti i tipi di API attualmente in uso.

Esistono altre funzionalità che sono fondamentali per la gestione del sistema di sicurezza delle API. Dovete essere in grado di identificare quali API accedono e trasmettono i dati sensibili e classificarle di conseguenza, perché le API che trattano dati come le informazioni sui clienti devono essere sicuramente autenticate. È anche importante identificare le vulnerabilità dell'infrastruttura che renderanno le API più vulnerabili.

Valutazione della configurazione

Molti attacchi informatici vengono sferrati con successo grazie a semplici errori di configurazione di reti, gateway API o firewall che trattano e proteggono il traffico delle API.

Una soluzione per la sicurezza delle API deve effettuare regolarmente una scansione delle configurazioni dell'infrastruttura e del software, inclusi i file di registro, le riproduzioni del traffico storico, i file di configurazione e molto altro. In tal modo, potrete scoprire errori di configurazione e vulnerabilità, eliminando, al contempo, il rischio di apportare cambiamenti alla configurazione.

Livelli di gravità personalizzabili

Poiché la soluzione identifica nuove vulnerabilità nell'ambiente, deve anche assegnare un livello di gravità ai problemi rilevati in modo da poter stabilire una priorità per la loro risoluzione. I livelli di gravità devono essere personalizzabili per allinearsi con la tolleranza ai rischi dell'organizzazione, ai requisiti normativi e alle policy interne.

Workflow personalizzati

Insieme ai livelli di gravità personalizzabili, lo strumento ideale per la gestione dei sistemi deve consentirvi di creare workflow personalizzati per intraprendere immediatamente le azioni necessarie una volta identificate le vulnerabilità. Questi workflow possono consentire varie operazioni, dalla creazione di ticket alla notifica dell'aggiornamento delle configurazioni di rete alle principali parti interessate.

Documentazione generata automaticamente

La documentazione sulle API spiega agli utenti delle API che cosa fanno e come utilizzarle. Le organizzazioni devono valutare le API protette per garantirne la conformità rispetto alle specifiche e ad un'accurata documentazione. Una documentazione scarsa o inesistente rende più difficile eseguire i test sulla sicurezza, aumentando il rischio che un'API raggiunga la fase di produzione con una vulnerabilità non rilevata. Questo problema è spesso esacerbato dall'outsourcing dello sviluppo delle API. Indipendentemente dall'origine del problema, una documentazione obsoleta, incompleta e inaccurata non è accettabile se si desidera garantire il successo di un programma per la sicurezza delle API.

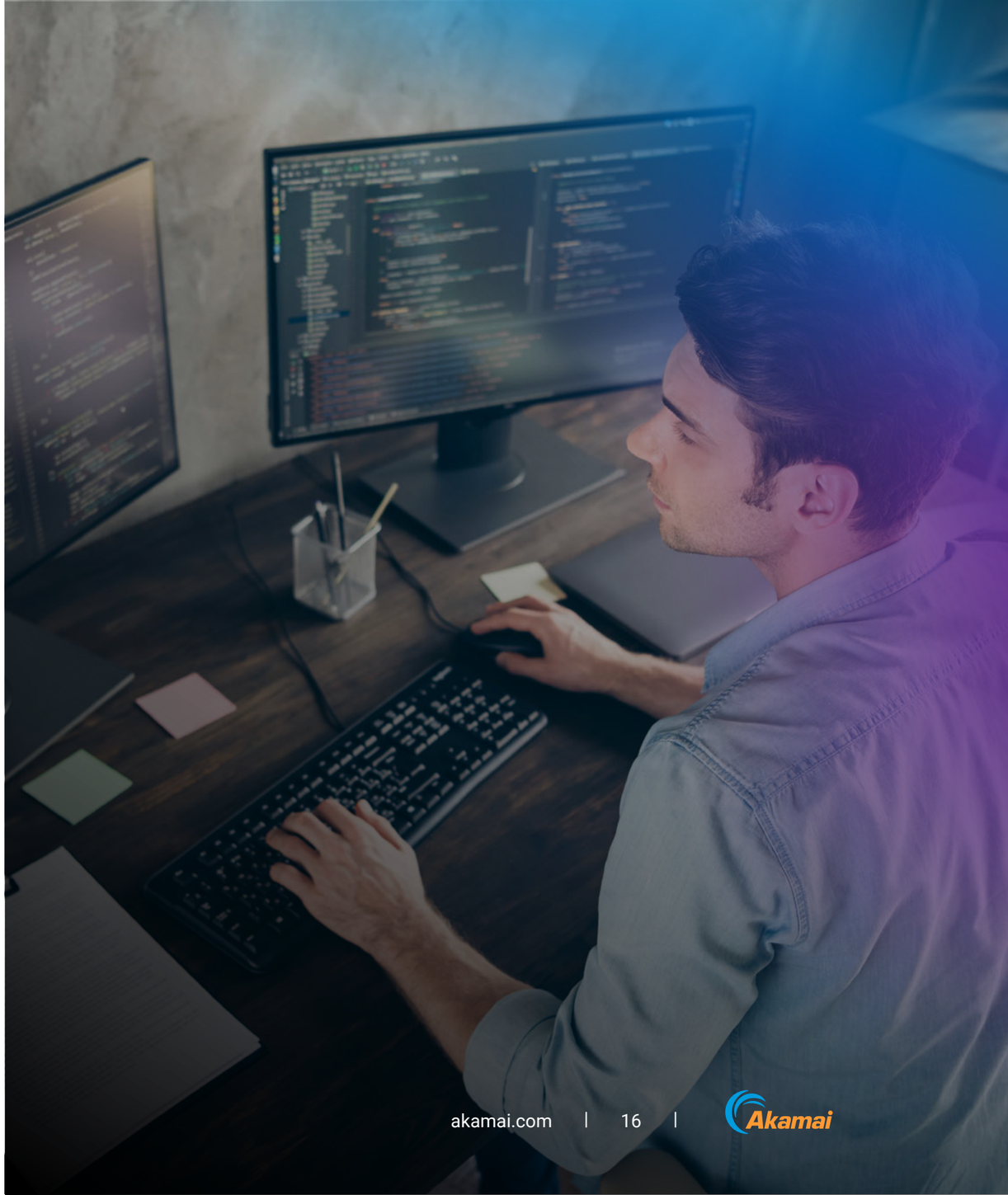
La specifica OpenAPI definisce le descrizioni di un'interfaccia standard. Una soluzione per la sicurezza delle API deve essere in grado di:

- Confrontare le specifiche delle API con il traffico attualmente osservabile e identificare le differenze, consentendo alle organizzazioni di vedere quali delle loro API implementate non rientrano nelle specifiche e, quindi, sono potenzialmente a rischio.
- Generare automaticamente una documentazione OpenAPI completa sulla base dello stato delle API corrente e di quello futuro per aiutare a garantire che tutte le API vengano correttamente documentate e che la documentazione sia aggiornata. 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.

Rilevamento e mitigazione delle minacce alle API: un'analisi approfondita delle funzionalità principali

Gli attacchi che tentano di sfruttare le vulnerabilità delle API sono un dato di fatto. Non è più una questione di "se" un'organizzazione subirà un attacco, ma di "quando e come" lo subirà. È diventato imprescindibile rilevare gli attacchi rapidamente e bloccarli prima che possano arrecare danni significativi, come esfiltrare i dati privati dei clienti. Anche se le vostre API sono, secondo voi, il più possibile sicure, vi serve una protezione attiva del runtime per rilevare episodi di fuga e manomissione di dati, violazioni delle policy relative ai dati, comportamenti sospetti e attacchi alla sicurezza delle API, tra cui la registrazione del traffico delle API, il monitoraggio dell'accesso ai dati sensibili, il rilevamento delle minacce e il blocco o la mitigazione dei vettori di attacco.

Nelle due pagine seguenti, verranno spiegate le funzioni principali che una soluzione per la sicurezza delle API deve includere.



Monitoraggio fuori banda in tempo reale

Il monitoraggio della sicurezza delle API non deve influire sul traffico delle API o rallentarlo. Prendete in considerazione vendor in grado di fornire un approccio senza agenti che offre alle aziende un'implementazione più rapida e una maggiore visibilità sul traffico. Tuttavia, in alcuni casi, se necessario (ad es., in ambienti on-premise complessi), la soluzione deve disporre di una flessibilità sufficiente per supportare anche gli agenti.

Una soluzione per la sicurezza delle API deve riflettere il traffico proveniente da fonti di dati identificate ed eseguire analisi di questi dati in background con avvisi in tempo reale sugli eventuali problemi rilevati.

Rilevamento dello sfruttamento e delle anomalie nelle API

La raccolta passiva di dati non è sufficiente, specialmente considerando che il numero di API e il volume totale del traffico delle API continua ad aumentare. Le attività delle API devono essere analizzate di continuo per rilevare eventi anomali e per avvisare i team addetti alla sicurezza e alle operazioni.

Gli strumenti più avanzati integrano le funzionalità di intelligenza artificiale e apprendimento automatico per analizzare il traffico in tempo reale e per fornire informazioni contestuali tali da identificare le attività anomale che possono indicare episodi di fuga e manomissione di dati, violazioni delle policy relative ai dati e altri attacchi alla sicurezza delle API.

Prevenzione degli attacchi alle API

Una volta identificata un'anomalia o un altro problema e generato un avviso, la tempistica è essenziale. Uno spostamento non autorizzato di dati sensibili tramite le API o un altro abuso sospetto delle API deve essere rilevato e bloccato. Una soluzione per la sicurezza delle API non solo deve bloccare eventuali abusi tramite l'integrazione con i firewall e i gateway API esistenti, ma deve anche fornire una mitigazione parzialmente o totalmente automatizzata oppure una combinazione di questi due metodi per gestire alcuni tipi di avvisi. Riguardo ai problemi ricorrenti identificati in precedenza, dovreste avere la possibilità di fornire una risposta totalmente automatizzata.

Valutazione del livello di fiducia degli attacchi

Alcune soluzioni disponibili sul mercato utilizzano gli algoritmi di apprendimento automatico per valutare segnali interni ed esterni, tra cui il comportamento delle API, i modelli del traffico di rete, i dati di geolocalizzazione e i feed di intelligence sulle minacce. Utilizzando fattori contestuali di questo tipo, una soluzione può stabilire il livello di fiducia secondo cui un incidente di runtime rilevato è il risultato di un'attività dannosa.

Integrazioni per la risposta agli incidenti

Quando si verifica un incidente, una soluzione per la sicurezza delle API deve includere le integrazioni necessarie per garantire che le attività di mitigazione vengano assegnate ai team appropriati. Una volta rilevati, eventuali errori di configurazione, violazioni delle policy relative ai dati o comportamenti sospetti devono essere segnalati al gateway API, al sistema SIEM e ad altri motori per la sicurezza delle informazioni allo scopo di garantire che vengano informate le persone giuste.

Come regola generale, una soluzione per la sicurezza delle API deve integrarsi facilmente con gli altri strumenti di sicurezza, monitoraggio e gestione utilizzati dall'organizzazione.

Esecuzione di test sulla sicurezza delle API: un'analisi approfondita delle funzionalità principali

Un errore commesso da molti team addetti allo sviluppo è aspettare troppo prima di eseguire i test delle API con la conseguenza di farli diventare un collo di bottiglia. I team devono adottare un approccio Shift-Left per garantire che l'esecuzione dei test inizi tempestivamente nel processo di sviluppo per risultare completa. I vantaggi derivanti da un'efficace esecuzione dei test sulla sicurezza delle API sono notevoli:

- **Prevenzione degli attacchi**
  - Individuando le vulnerabilità prima che le API entrino in fase di produzione, potete ridurre il rischio di subire un attacco
- **Migliore conformità**
  - Un'esecuzione completa dei test vi aiuta a garantire la conformità, evitando sanzioni e danni alla reputazione
- **Aumento della fiducia**
  - Un'esecuzione dei test rigorosa ed efficace può aumentare la fiducia dell'organizzazione nei confronti delle API e aiutare a garantire la tempestività dei rilasci da parte degli sviluppatori

Alcuni vendor che operano nel settore possono offrire consigli alle aziende sul modo con cui mitigare i problemi che riscontrano nei loro ambienti, nonché configurare l'esecuzione dei test delle API in modo completo. Tra i consigli, possono figurare i passaggi necessari per configurare le autenticazioni appropriate o per correggere le dipendenze delle API. Il vantaggio: Se riuscite a risolvere i problemi legati alla logica aziendale nel vostro ambiente, potrete aumentare il numero di API ottimizzate per l'esecuzione dei test, che risulterà più completa.

L'intero concetto dell'esecuzione di test sulla sicurezza delle API, tuttavia, rimane alquanto nebuloso. I team addetti allo sviluppo potrebbero non comprendere completamente cosa comporta questa operazione. L'esecuzione di test delle API con un approccio Shift-Left è un processo costituito da tre fasi:

1. **Capire le API:** comprendere il caso di utilizzo delle API rende l'esecuzione dei test più informata, specialmente nel caso di complessi problemi alla logica aziendale.
2. **Interagire correttamente con le API:** assicuratevi di riuscire ad utilizzare le API nel modo previsto. Questo passaggio è fondamentale per capire se avete scelto l'API più appropriata per la funzione che vi serve.
3. **Inviare il traffico degli attacchi alle API:** in questa fase, potreste manipolare manualmente le richieste indirizzate alle API, inserire le stringhe di fuzzing nelle richieste o utilizzare uno strumento automatizzato per eseguire i test sulla sicurezza delle API. Come per qualsiasi aspetto dell'IT moderno, l'automazione è spesso il modo migliore per eseguire un'azione su larga scala senza sacrificare la velocità.

Le principali funzioni dei test sulla sicurezza delle API

L'esecuzione di test sulla sicurezza delle API deve includere test statici, dinamici e di penetrazione. Una soluzione per la sicurezza delle API deve includere strumenti tali da facilitare un'esecuzione dei test accurata allo scopo di automatizzare i processi dei test il più possibile. Verificate se una soluzione per la sicurezza delle API offre le seguenti funzioni per l'esecuzione dei test sulle API:

Esecuzione automatizzata e proattiva dei test sulla sicurezza delle API

L'esecuzione automatizzata dei test sulla sicurezza riduce rischi e costi identificando errori di configurazione, vulnerabilità e componenti non conformi prima che un'API entri in fase di produzione.

Governance delle API

È essenziale pensare in precedenza ai problemi di governance come ruoli, responsabilità e policy, tra cui responsabilità a livello di esecuzione per sviluppatori e tecnici addetti alla sicurezza e alla piattaforma, nonché supervisione delle policy e decisioni relative ai rischi. Una soluzione per la sicurezza delle API deve consentirvi di esaminare le specifiche delle API sulla base delle regole e delle policy di governance stabilite.

Integrazione con la pipeline CI/CD e l'archivio dei codici

Il DevSecOps è una variante del DevOps che aggiunge la sicurezza al workflow di sviluppo dei software. La sicurezza delle API deve essere parte delle iniziative del DevSecOps. Una soluzione per la sicurezza delle API deve fornire una serie di test sulla sicurezza delle API da poter eseguire on-demand o come parte di una pipeline CI/CD. L'integrazione CI/CD è essenziale perché consente di eseguire test sulla sicurezza delle API continui e rapidi, che sono necessari per tenere il passo con lo sviluppo delle applicazioni.

Un'unica soluzione per identificare e risolvere le lacune nella sicurezza delle API

Le API sono componenti essenziali per consentire ad un'organizzazione di offrire servizi ai clienti, generare profitti e operare in modo efficiente in un'economia sempre più digitale e incentrata sul cloud. Tuttavia, la crescita continua, la vicinanza ai dati sensibili e la mancanza di controlli di sicurezza delle API le rendono un bersaglio allettante per i criminali moderni.

Gli strumenti che molte organizzazioni usano attualmente per gestire le API e garantire una protezione basilare riducono in qualche modo i rischi, ma non sono sufficienti per contrastare le odierne minacce alle API. Non ci si può affidare ad un solo tipo di protezione.

Al contrario, le organizzazioni devono cercare una soluzione completa per la sicurezza delle API in grado di fornire tutte e quattro le componenti descritte in questa guida all'acquisto: individuazione, gestione dei sistemi, rilevamento e mitigazione delle minacce ed esecuzione di test sulla sicurezza. Non dovete eliminare necessariamente gli strumenti esistenti che si sono dimostrati efficaci in alcune aree, ma cercare semplicemente una soluzione in grado di integrarsi perfettamente con i vostri strumenti esistenti.

Occuparsi della sicurezza delle API non significa dover allocare tante risorse, ma potete cominciare con un progetto pilota misurabile su scala più piccola per risolvere specifiche lacune presenti nel vostro sistema di sicurezza. In alternativa, potete iniziare il vostro percorso verso la sicurezza delle API con un aggiornamento completo. Ogni organizzazione è diversa dalle altre.

Considerando l'aumento degli attacchi alle API, il passaggio più importante è decidere di intervenire. Speriamo che questa guida all'acquisto vi risulti utile.

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**.

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.

Akamai