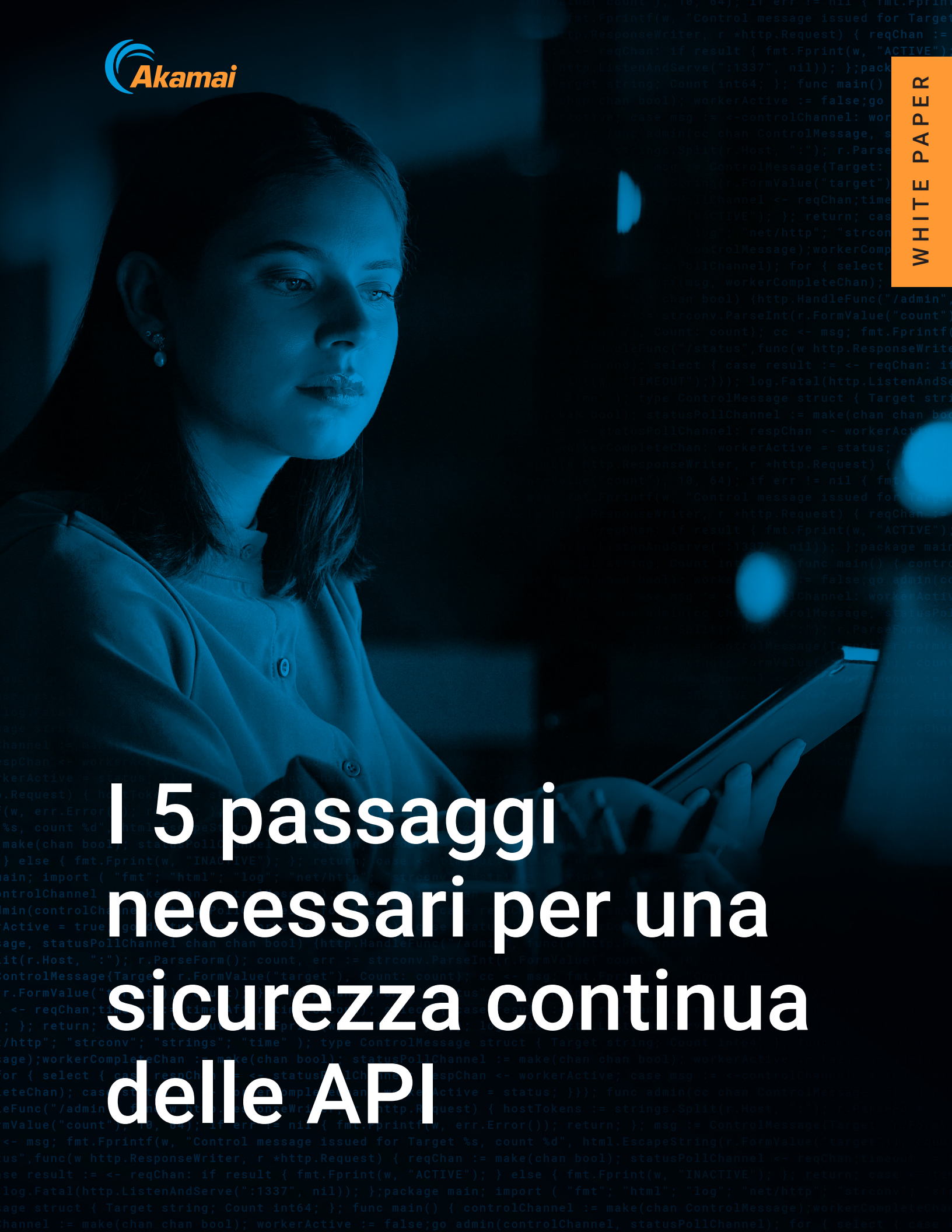
Akamai

WHITE PAPER



I 5 passaggi necessari per una sicurezza continua delle API

In questo rapporto

La sfida legata alla sicurezza delle API

Integrate in ogni iniziativa digitale o cloud avviata dalle organizzazioni, le API (Application Programming Interface) caratterizzano un crescente ecosistema che favorisce un'innovazione redditizia. Il problema è che le API si sono distinte rapidamente per diventare uno dei principali vettori di attacco.

I criminali sanno che le API possono fornire un percorso rapido e diretto ai dati più sensibili di un'azienda. Le vulnerabilità sono molte: spesso, le API entrano in fase di produzione con errori di configurazione, scarsi controlli di autenticazione e una visibilità non prevista in Internet, tutte caratteristiche che un criminale può sfruttare facilmente.

Allora perché queste vulnerabilità delle API non vengono individuate e mitigate prima che le applicazioni vengano rese disponibili per gli utenti finali? Desideriamo quindi indagare le cause principali di questo problema e come possiamo risolverlo.

Avrete probabilmente sentito il vecchio detto secondo cui tutte le aziende dipendono dal software. Oggi si dovrebbe dire, invece, che ogni business unit aziendale dipende da applicazioni sviluppate in modo indipendente, al fine di soddisfare velocemente la domanda dei clienti. Una situazione meno lineare, certamente, ma, spesso, è questa la realtà.

Anche se ancora persiste il passaggio tradizionale dal reparto IT centralizzato, molte aziende assistono ad un vortice di innovazione condotto da iniziative dei segmenti aziendali favorite dall'urgenza e dagli obiettivi commerciali, anziché da processi calibrati. L'imperativo di agire rapidamente e di favorire le opportunità commerciali ha eclissato una considerazione accorta delle implicazioni legate alla sicurezza, portando ad una situazione da alcuni definita come il "debito della cybersicurezza". Gli sviluppatori che non appartengono ad organizzazioni IT centralizzate (e che magari devono riferire ai segmenti aziendali) possono avviare rapidamente nuove applicazioni, strumenti per siti web e servizi basati sull'intelligenza artificiale generativa, bypassando così i controlli interni. Inoltre, in molti casi, i team addetti alla sicurezza non hanno visibilità su questi progetti e, pertanto, non possono valutare accuratamente i rischi.

Per vari anni, questo flusso ha rappresentato la realtà per i vettori di attacco ben noti, facendo sì che gli esperti del settore implorassero le aziende di potenziare i loro sistemi di difesa dai ransomware, proteggere le password e molto altro. Tuttavia, molte aziende non hanno esteso questa urgenza alla protezione delle API facendo diventare la situazione problematica perché le API sono integrate in tutte le applicazioni e i servizi online creati da un'organizzazione, che scambiano costantemente i dati e raramente vengono protetti in modo adeguato.

Modello finanziario

I budget sono cambiati perché sono stati spostati dai costi IT centralizzati alle spese operative dei segmenti aziendali, tuttavia i loro processi non si sono evoluti per riflettere i maggiori rischi per la sicurezza. Le business unit potrebbero non comprendere appieno quanto allocare per la sicurezza e, di conseguenza, spesso non viene allocato nulla per garantire la protezione dei dati.

Migrazione nel cloud

Le applicazioni vengono spostate negli ambienti cloud pubblici e privati. Lo spostamento di dati e carichi di lavoro aggiunge complessità, riduce il controllo e aumenta il numero di terze parti nell'ambiente. Le organizzazioni hanno bisogno di ulteriori pratiche di sicurezza per mitigare questi fattori di rischio e potrebbero non disporre delle competenze, dell'esperienza o delle risorse necessarie per implementarle in modo efficace.

Containerizzazione

Il passaggio ai microservizi causa un incremento esponenziale della superficie di attacco. Queste istanze possono presentarsi rapidamente e poi collassare. Si tratta di un ambiente difficile da proteggere a causa della sua natura altamente dinamica, anche perché gli strumenti tradizionali su cui si basano molte organizzazioni sono stati progettati per ambienti più statici. È questo un altro caso di API onnipresenti e ad elevato rischio. Oggi, l'architettura delle applicazioni basate sui microservizi e sui container ha bisogno di più API per funzionare e, anche se le aziende che dispongono di inventari delle API conoscono l'esatto numero delle API presenti nei loro ambienti, spesso non sanno quali restituiscono dati sensibili.

Sviluppo agile

La velocità con cui si prevede che gli sviluppatori implementino nuove applicazioni, servizi e funzioni favorisce in modo particolare i rischi. I team addetti allo sviluppo affrontano la pressione delle scadenze con determinazione grazie alle metodologie CI/CD (Continuous Integration and Continuous Delivery) e alle funzioni automatizzate per lo sviluppo, l'integrazione e l'esecuzione di test che consentono di lavorare in modo efficiente.

Ma a chi è affidata la gestione dei rischi? Il passaggio al DevOps implica modifiche al codice più frequenti che esulano il controllo dei team addetti alla sicurezza. Un maggior numero di organizzazioni sta passando ad un modello Shift-Left per lo sviluppo delle applicazioni nel complesso. È questo un passo verso la giusta direzione, tuttavia, il concetto di eseguire i test in modo tempestivo e frequente deve essere applicato anche alle API che si trovano all'interno delle applicazioni: le organizzazioni ne hanno di lavoro da fare per mettersi al passo.

Quindi, da dove iniziare? Una delivery continua richiede una sicurezza continua. Di seguito, vengono riportati cinque passaggi da eseguire per avviare una protezione delle API completa e always-on durante il rapido processo di innovazione della vostra azienda.

I 5 passaggi necessari per una sicurezza continua delle API

1. Seminate la cultura della sicurezza continua

Comprendere e gestire la sicurezza delle API non è compito facile perché richiede ai dirigenti aziendali di promuovere una cultura della sicurezza nell'intera organizzazione, specialmente nel ciclo di vita dello sviluppo del software. Se avete già compiuto progressi nel costruire una cultura della sicurezza di questo tipo, il passaggio successivo è usarla per risolvere le complessità delle API e i rischi operativi associati allo scopo di migliorare la visibilità, la governance e la collaborazione.

Di seguito, vengono riportate alcune operazioni pratiche che la vostra organizzazione può effettuare per sviluppare e mantenere una cultura della sicurezza duratura:

- **Decentralizzate il team addetto alla sicurezza.** Integrate figure di esperti all'interno dei gruppi dedicati allo sviluppo e alle linee dei prodotti per migliorare la visibilità e la governance. Incoraggiate l'adozione di policy più flessibili che si basano sul contesto fornito da queste figure di esperti integrate.
- **Assicuratevi che i team addetti alla sicurezza prendano parte a tutte le implementazioni digitali**, non solo per la creazione delle policy, ma attivamente dal lancio di ogni servizio. I proprietari di segmenti aziendali, i loro team e gli sviluppatori devono disporre di linee di comunicazione dirette con il personale addetto alla sicurezza.
- **Designate esperti di sicurezza dedicati.** Identificate, all'interno delle business unit, le persone dedicate a costruire e sostenere le relazioni più importanti per lavorare rapidamente. Disporre di esperti di sicurezza dedicati vi consentirà di ribadire l'importanza della cultura della sicurezza e metterà i team interfunzionali nella condizione di responsabilizzarsi a vicenda.
- **Includete tutte le persone coinvolte.** La formazione sulla sicurezza è imprescindibile, non solo per sviluppatori e tecnici, ma per tutte le persone coinvolte nel processo di sviluppo del software e oltre.

2. Valutate il sistema di sicurezza delle API

Molte organizzazioni sottovalutano le dimensioni del loro patrimonio delle API. Le aziende che dispongono di inventari potrebbero non solo perdersi gran parte delle loro API, ma anche non sapere quali pongono i maggiori rischi. La creazione di un inventario completo e accurato vi consente di valutare l'intera superficie di attacco delle API.

Di seguito vengono riportati alcuni consigli da seguire per ottenere una piena visibilità sul sistema di sicurezza delle API:

- **Create un inventario completo.** Cercate di acquisire una visione chiara e accurata delle potenziali vulnerabilità della vostra organizzazione e del reale aspetto della vostra superficie di attacco per API e applicazioni web. Utilizzate uno strumento di individuazione delle API in grado di individuare e inventariare in modo completo tutte le API, tra cui:
  - API ombra
  - API zombie
  - API inattive
- **Identificate tutte le API e i rischi associati.** Cercate di comprendere i tipi di dati sensibili con cui interagisce ogni API, come vengono instradati, le risorse fisiche associate e le business unit o l'applicazione a cui appartengono.
- **Esaminate le allocazioni delle risorse dei team addetti alla sicurezza.** Analizzate il numero di API che ogni membro del team AppSec deve gestire. Stabilite se un maggior numero di conoscenze tecnologiche o sessioni di formazione possono mantenere il vostro sistema allo stesso livello o migliorarlo.

3. Mitigate, automatizzate e integrate

Le aziende devono comprendere l'accesso, l'utilizzo e il comportamento delle API. Tuttavia, le API sono complesse da analizzare. Comprendere il panorama della sicurezza delle API in tutta la sua complessità, di solito, richiede vari processi, come l'analisi dei registri, l'acquisizione dei dati dei cataloghi, la revisione delle configurazioni, l'esecuzione di test sulla sicurezza e la valutazione delle configurazioni dei dispositivi. Senza gli strumenti appropriati, la mitigazione può risultare onerosa sia perché tecnicamente difficoltosa sia perché richiede una notevole dose di tempo e fatica. Tuttavia, la mitigazione viene spesso attuata in modo automatizzato o semi-automatizzato per eliminare le vulnerabilità note e per mitigare i rischi immediati e richiede una minima o nessuna interazione degli utenti.

Di seguito vengono riportate alcune indicazioni utili per prevenire gli attacchi e risolvere gli errori di configurazione:

- **Effettuate l'integrazione con i sistemi di gestione dei workflow IT esistenti.** Dovete assicurarvi che i problemi vengano assegnati ai team appropriati non appena identificati. Le integrazioni devono attivare i workflow di automazione in grado di risolvere eventuali problemi legati alle API presenti all'interno dell'organizzazione.
- **Adottate sistemi di mitigazione automatizzati multifase.** Inizialmente, prima di intraprendere nuove azioni di mitigazione, affidatevi a persone competenti. Assicuratevi che le business unit siano tra loro coordinate per adottare una mitigazione semi-automatizzata. Non è sufficiente dire semplicemente agli sviluppatori che il codice non va bene, ma è necessario fornire loro le giuste informazioni da poter usare. In caso contrario, è una perdita di tempo sia da parte vostra che da parte loro. Se alcuni problemi si ripetono, utilizzate un sistema completamente automatizzato per accelerare il processo di mitigazione.
- **Cercate eventuali comportamenti dannosi.** Utilizzate i dati cronologici relativi alle tattiche di sfruttamento delle API per stabilire un comportamento anomalo che potrebbe rivelare l'intenzione del criminale. Utilizzate risposte automatizzate o semi-automatizzate per mitigare gli attacchi.
- **Effettuate l'integrazione con i sistemi SIEM (Security Information and Event Management) esistenti.** Questa integrazione garantisce al team più ampio di poter utilizzare i dati sulla sicurezza delle API.

4. La sicurezza delle API Shift-Left

Quando si tratta di sicurezza delle API, non è solo una questione di eseguire i test delle API, ma anche di *quando* eseguirli. Il modello tradizionale colloca i test più vicino alla fase di implementazione, che è vitale, ma è un metodo inadeguato e può condurre a vulnerabilità gravi. L'approccio "Shift-Left" consente di spostare varie attività nelle prime fasi del processo di sviluppo. Con la sicurezza e l'esecuzione dei test integrate in ciascuna fase dello sviluppo delle API, un approccio Shift-Left garantisce agli sviluppatori di riuscire a monitorare le vulnerabilità per l'intero ciclo di vita delle API. In tal modo, le organizzazioni possono accelerare l'innovazione e rafforzare il proprio vantaggio competitivo considerando la sicurezza delle API l'elemento fondamentale.

Ecco alcuni suggerimenti che possono aiutarvi ad adottare un approccio Shift-Left all'esecuzione dei test delle API:

- **Definite gli obiettivi.** Poiché l'approccio Shift-Left richiede un cambiamento aziendale e culturale, i dirigenti devono prima definire gli obiettivi del processo per garantire che eventuali nuovi strumenti o processi introdotti nel ciclo di sviluppo siano allineati con le metodologie di sviluppo e di esecuzione dei test attualmente utilizzati dal team.
- **Cercate di comprendere la supply chain.** Cercate di capire come e dove l'organizzazione sviluppa app e software prima di progettare un programma di sicurezza Shift-Left completo. Il livello di rischio per la sicurezza della supply chain dipende perlopiù dalle competenze in materia di sicurezza degli altri componenti della catena, il che aiuta anche gli sviluppatori ad identificare le aree in cui collocare i test tempestivamente nel ciclo di vita.
- **Automatizzate i processi di sicurezza.** Con il lancio dei microservizi da parte dei team di sviluppo, assicuratevi che gli strumenti per la sicurezza delle API vengano usati dagli esperti di sicurezza integrati fin dalle prime fasi per poter monitorare i rischi legati alla containerizzazione.
- **Utilizzate strumenti coerenti.** Incoraggiate i team addetti alla sicurezza ad adottare l'interfaccia principale degli sviluppatori, nonché la lingua, le piattaforme e gli strumenti da loro utilizzati. Ad esempio, è possibile inserire vulnerabilità e risultati negli stessi backlog dei prodotti per nuovi requisiti funzionali delle applicazioni come storie di utenti regolari.
- **Rendete il team AppSec una fonte di innovazione.** Utilizzate i principi della delivery continua per sviluppare microservizi di sicurezza in grado di mitigare i rischi allo scopo di consentire alle organizzazioni di effettuare operazioni che altre aziende del settore non riescono a fare.

5. Eseguite test continui

Come abbiamo appena descritto, un approccio di sicurezza Shift-Left sposta i test alle prime fasi del processo per consentire al team di eseguirli tempestivamente nel ciclo di vita. Al contrario, in un approccio Shift-Right i test vengono eseguiti con scenari e utenti reali che non si trovano nell'ambiente di sviluppo. L'approccio Shift-Right garantisce la stabilità e le performance dei programmi software reali eseguendo i test negli ambienti di produzione e migliorando le user experience tramite la raccolta di feedback e recensioni dagli utenti delle applicazioni. La verità è che nessun approccio è meglio di un altro. Per minimizzare i rischi potenziali, un'organizzazione deve eseguire test di continuo.

Di seguito, vengono riportati alcuni suggerimenti utili per sviluppare e mantenere una cultura della sicurezza duratura:

- **Eseguite i test delle API in modo attivo.** Come parte del ciclo di vita dello sviluppo del software delle API, è consigliabile eseguire i test sulla sicurezza delle API per risolvere potenziali problemi in fase di pre e post-produzione. Controllate l'integrità di ogni API prima e dopo la loro implementazione.
- **Monitorate continuamente il traffico delle API.** Tenete traccia dell'utilizzo delle API e analizzate i metadati relativi al traffico delle API. L'analisi del traffico in tempo reale identifica nuove API e le modifiche apportate alle API esistenti. Il processo dell'analisi deve essere automatizzato, ripetibile e fattibile.
- **Cercate eventuali vulnerabilità ed errori di configurazione.** I test devono essere continui ed eseguiti in parallelo con gli sviluppatori e devono implicare una comunicazione continua tra clienti, sviluppatori e addetti ai test. L'esecuzione dei test deve identificare i problemi in modo da poterli risolvere prima che vengano sfruttati. Eventuali ritardi nell'analisi offrono agli hacker tempo in più per trarre vantaggio dalle vulnerabilità. Inoltre, altrettanto importante, dovete segnalare eventuali modifiche apportate alle policy o alle funzionalità e aggiornare i sistemi SIEM.
- **Registrate il traffico delle API.** Assicuratevi di registrare il traffico delle API nel caso in cui sia necessario creare rapporti forensi per specifiche chiavi API, token, indirizzi IP e identità degli utenti.

Riepilogo

La minaccia per la sicurezza delle API è un pericolo reale e presente per molte organizzazioni. Le API, spesso, non sono gestite, quindi rimangono nascoste al rilevamento degli strumenti tradizionali e presentano costantemente errori di configurazione e codifica senza richiedere controlli di autenticazione. Di conseguenza, le API sono un obiettivo allettante per i criminali e possono essere violate all'insaputa delle organizzazioni.

La soluzione a questa situazione è una sicurezza continua, ossia integrata nei processi degli sviluppatori e nelle stesse API una volta create e spostate in fase di produzione. Di seguito, vengono riportate quattro best practice che le organizzazioni devono tenere a mente:

1. Sviluppate una nuova cultura per integrare esperti AppSec nel team di progettazione della vostra organizzazione
2. Create un inventario completo delle API per gestire il profilo di rischio per la sicurezza delle API della vostra organizzazione
3. Date priorità ai processi di mitigazione, automatizzate le correzioni (ove possibile) e integrate in modo agevole la struttura di sicurezza delle API negli attuali sistemi di protezione delle applicazioni
4. Sorvegliate ed eseguite i test delle API in modo continuo per assicurarvi che le nuove vulnerabilità vengano identificate e mitigate rapidamente

Anche se questo approccio richiede una nuova concezione, diversi processi e una collaborazione tra i vari team, è una sfida che può essere superata.

Scoprite 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 by demo personalizzata su Akamai API Security.

Akamai Security protegge 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.