Akamai

WHITE PAPER

8 cose da fare e da non fare per la sicurezza delle API

I fattori critici per garantire un efficace sistema di sicurezza delle API

Perché la protezione delle API è così complicata?

La sicurezza delle API è in cima alla lista delle priorità di molti dirigenti IT e per una serie di buoni motivi. Considerate quanto segue:

"L'esplosione delle API fornisce una superficie di attacco allettante e la sicurezza delle API continua a sconcertare i responsabili della sicurezza".

- Le 8 componenti della sicurezza delle API, Forrester Research, Inc., 28 settembre 2023

Cosa ha causato l'aumento del rischio per le API

Per fronteggiare questi rischi, le organizzazioni devono comprendere quanto segue prima di iniziare ad implementare un efficace sistema di sicurezza delle API:

Le API sono dei bersagli in costante movimento	
Consapevolezza interna delle API	**Esposizione delle API all'esterno**
I processi DevOps creano e rimuovono le API in continuazione, determinando la presenza di un inventario delle API incompleto	Se le pratiche relative alle API non sono mature, si genera un'imprevista esposizione delle API sensibili a parti esterne, incluse molte API ombra

Le API sono vulnerabili a due diversi tipi di minacce	
Vulnerabilità tecniche	**Abuso e uso improprio**
I criminali possono sfruttare le configurazioni errate e le vulnerabilità dei software, incluse le 10 principali vulnerabilità per la sicurezza delle API riportate nell'elenco OWASP	L'abuso della logica aziendale e altri comportamenti, come uno scraping dei dati aggressivo, possono verificarsi indipendentemente dalla presenza di una vulnerabilità tecnica

Affrontare la complessa sfida correlata con la sicurezza delle API richiede un approccio ben ponderato, che include:

Integrazione delle ultime innovazioni tecnologiche

Eliminazione delle barriere aziendali

Analisi di tutte le minacce alle API

Di seguito vengono riportate alcune strategie essenziali da implementare (e le insidie da evitare) durante lo sviluppo di un approccio più sofisticato alla sicurezza delle API della vostra organizzazione.

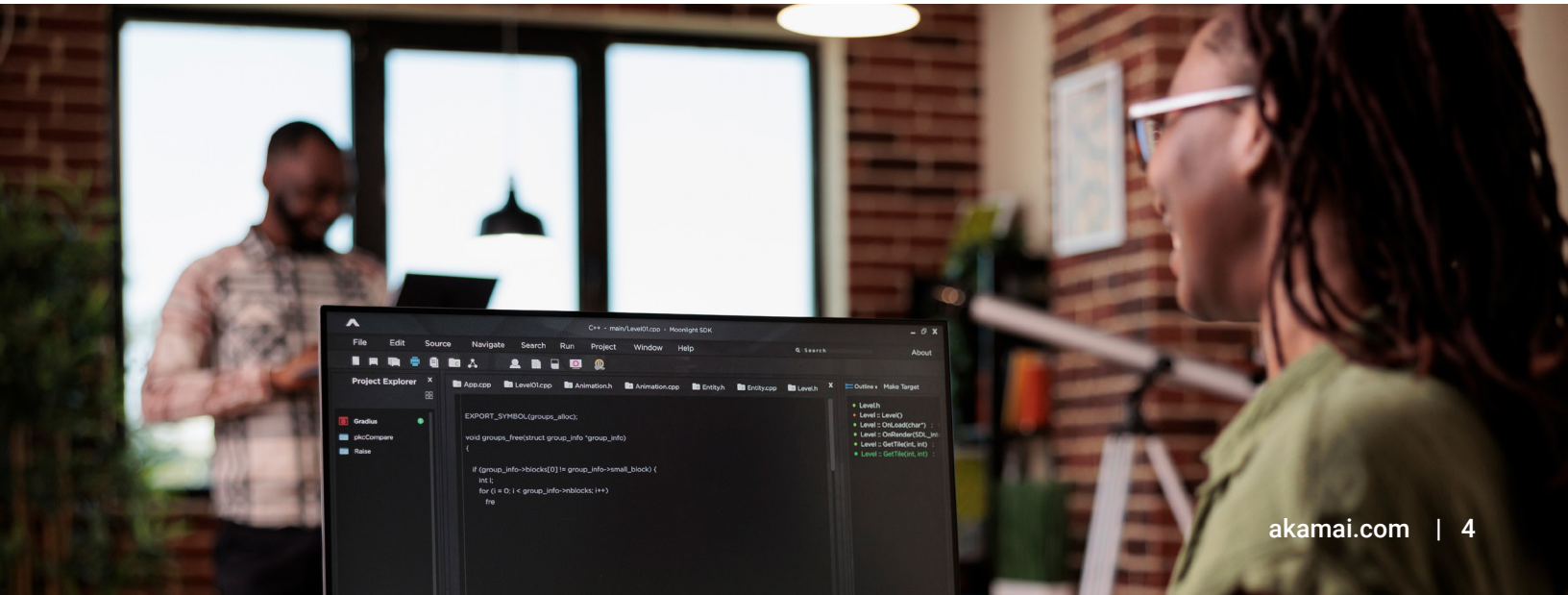
Le 8 cose da fare e da non fare per un'efficace sicurezza delle API

1 Impegnatevi a garantire una visibilità delle API completa

Vale la pena ripeterlo: non potete proteggere le API che non sapete di avere. Più un'API non viene identificata e monitorata, maggiori sono le probabilità che diventi il bersaglio di un criminale Il miglior modo per raggiungere una visibilità completa è garantire che la vostra piattaforma di sicurezza delle API sia in grado di acquisire informazioni dalla più ampia gamma di origini dati, tra cui gateway API, dispositivi di rete, soluzioni di coordinamento dei microservizi, provider di servizi cloud e molto altro. Nello specifico, la vostra soluzione per la sicurezza delle API deve essere in grado di garantire:

Quando	Dove
• Rilevare le API continuamente • Monitorare le singole chiamate API • Registrare l'attività delle sessioni a breve termine • Analizzare il comportamento delle API nel tempo	• Rilevare le API nell'azienda • Rilevare le API legacy • Individuare le API ombra

Una visibilità completa delle API vi aiuta a prevenire eventuali violazioni di dati relativi alle API, specialmente perché l'ultima tecnica adottata in questo ambito richiede ai criminali l'utilizzo di attacchi ad attività bassa e lenta per acquisire i dati dalle API. Sapere dove si trovano tutte le vostre API è il primo passo per prevenire questo tipo di attacco emergente.



2 Non temete il cloud

Le soluzioni WAF (Web Application Firewall) utilizzano tecniche basate sulle firme per prevenire l'accesso di API non autorizzate all'interno della vostra organizzazione. Man mano che gli attacchi alle API si evolvono, vi serve un ulteriore livello per difendere totalmente le API da una serie completa di possibili rischi tramite l'analisi comportamentale. Ora, è fondamentale monitorare il comportamento delle API all'interno della vostra organizzazione, non solo quelle vulnerabili all'esterno.

Per utilizzare l'analisi comportamentale in modo efficace, è necessario analizzare il traffico delle API nel cloud. I team addetti alla sicurezza, a volte, sono riluttanti ad inviare informazioni sensibili sull'attività della propria organizzazione nel cloud. Tuttavia, l'esecuzione di analisi dei comportamenti reali tramite l'utilizzo di estese tecniche di rilevamento e risposta sul volume dei dati delle API generati dalla maggior parte delle aziende è impossibile da mettere in pratica senza la scalabilità e l'elasticità fornite dal cloud.

Inoltre, poiché i team addetti alla sicurezza sono sempre più a corto di risorse, le procedure di implementazione dei prodotti lunghe e complesse sono un ostacolo notevole al progresso. Considerando il crescente rischio posto da un uso più ampio delle API, i team addetti alla sicurezza non possono permettersi di rimanere ancora indietro. Ecco perché è fondamentale adottare il cloud inserendolo nella vostra strategia di sicurezza delle API.

3 Rendete il contesto aziendale centrale per la vostra strategia

Il rilevamento delle API e l'identificazione dei rischi alla sicurezza rappresentano solo l'inizio del percorso che mira a ridurre la superficie di attacco delle API. Considerate le tre domande seguenti:

1. Come fate a sapere se le credenziali API di uno specifico partner sono state violate?

2. Come fate a sapere se si sta verificando un episodio di spionaggio aziendale sotto forma di scraping dei dati su un'API?

3. Come fate a sapere se è in atto una violazione della vostra API di fatturazione da parte di un utente che elenca i numeri delle fatture per rubare i dati degli account?

Nel primo caso, l'attività sembrerà avere origine da un utente legittimo. Pertanto, l'unico modo per rilevare eventuali intenzioni malevole consiste nel notare un cambiamento rispetto al comportamento previsto sull'API in questione. Anche il secondo e il terzo caso sono esempi di comportamenti non autorizzati che sfruttano modelli di accesso alle API legittimi. Esistono altri casi in cui è fondamentale comprendere il contesto aziendale, oltre a quanto si verifica da un punto di vista tecnico.

4 Non rendete i dati una strada a senso unico

Una delle funzionalità fondamentali di un efficace approccio alla sicurezza delle API consiste nella capacità di inviare avvisi ed eventi agli strumenti di monitoraggio della sicurezza e workflow IT che preferite. Un errore comune che viene commesso dai fornitori di soluzioni per la sicurezza (e dai team che implementano gli avvisi) è visualizzare gli avvisi di sicurezza e le risposte automatizzate come un flusso di comunicazione unidirezionale.

Proprio come molti processi aziendali legittimi, gli attacchi possono verificarsi per un lungo periodo di tempo. Per risultare efficace, è necessario eseguire l'analisi comportamentale dell'utilizzo delle API su un periodo di almeno 30 giorni. In tal modo, potete ottenere un quadro più completo e accurato del comportamento standard previsto. Inoltre, questo approccio consente di rilevare gli attacchi eseguiti lentamente per più giorni o settimane (e con numerose sessioni delle API). Considerate un attacco di scraping dei dati ad attività bassa e lenta che rientra in un limite di velocità definito: questo comportamento risulterebbe solo da un'analisi a livello cronologico condotta sulla base di un cambiamento.

Un avviso inviato senza il supporto di informazioni, probabilmente, fa più male che bene. Un avviso completo di contesto sulle cause e sull'impatto dell'attacco, invece, è molto più utile. Tuttavia, la cosa migliore è fornire un avviso utile e completo di contesto per offrire al destinatario la possibilità di interrogare un dataset più vasto per analizzare l'incidente. Quindi, potete utilizzare i vostri sistemi di protezione WAF per bloccare immediatamente il traffico che presenta una potenziale minaccia per la vostra azienda.

5 Date priorità alla collaborazione tra i reparti

Alcuni dei maggiori miglioramenti nella sicurezza delle API derivano dalla capacità di evitare in modo proattivo eventuali vulnerabilità durante le fasi di progettazione, sviluppo e implementazione. Per raggiungere questo obiettivo in modo efficace, è richiesta la collaborazione tra i vostri team.

Per avviare questo processo collaborativo, dovete fornire ai team addetti alle API la visibilità sul modo di utilizzo (e abuso) delle API in situazioni realistiche. Nel corso del tempo, questa esposizione favorirà una cultura che pensa alla sicurezza nelle fasi preliminari dei processi di sviluppo e distribuzione delle applicazioni. Inoltre, assicuratevi che:

- Siano presenti vantaggi non legati alla sicurezza in grado di aiutare i team addetti alle API a lavorare in modo più efficace oltre alle principali funzioni di sicurezza del vostro approccio
- Sia semplice per gli utenti non legati alla sicurezza, come gli sviluppatori, visualizzare e cercare informazioni sulle attività e nell'inventario delle API
- Vengano utilizzate risposte contestuali, ad esempio l'integrazione in strumenti di sviluppo, come Jira, in grado di aprire in modo proattivo ticket per la risoluzione dei problemi di sicurezza da parte degli sviluppatori

Pensare alla sicurezza delle API come un impegno che tutti devono assumersi e semplificare il coinvolgimento delle parti interessate che non fanno parte del team di sicurezza elimina eventuali accuse e consente ai team addetti allo sviluppo, alle operazioni e alla sicurezza di collaborare in modi reciprocamente vantaggiosi.

6 Non sottovalutate le API di terze parti

Un altro errore comune nella strategia di sicurezza delle API da evitare consiste nel supporre che dovete preoccuparvi solo delle vostre API. Benché sia desiderabile credere che il gateway WAF o API che avete acquistato riesca a standardizzare tutta la vostra strategia di sicurezza delle API, non è sempre questo il caso.

Ad esempio, proprio perché viene implementata una strategia centralizzata per il gateway API, non dovete supporre che le API ombra non riusciranno ad eludere l'approccio fondamentale alla governance delle API. Se la vostra azienda si basa su API di terze parti, il vostro gateway le considererà autenticate, anche se sono state violate prima che siano state correlate al vostro ecosistema.

La vostra strategia di protezione delle API deve integrarsi con le vostre principali tecnologie in questo ambito, come i gateway API, raccogliendo anche quante più informazioni possibili da altre fonti, come dispositivi di rete, piattaforme cloud e strumenti di coordinamento dei microservizi. Questo è l'unico modo possibile per disporre di un quadro completo della superficie di attacco delle vostre API e per predisporre per il futuro la vostra strategia di sicurezza man mano che si verificano le inevitabili transizioni a livello di tecnologie e infrastrutture.

7 Non rispondete e andate oltre

Anche se è gratificante rispondere agli avvisi in modo rapido ed efficace, se vi focalizzate solo sulla mitigazione degli avvisi quando si verificano, perdete l'opportunità di evitarli del tutto. Pensate, invece, di eseguire una ricerca delle minacce in modo proattivo. Se il vostro partner per la sicurezza delle API vi consente di eseguire query sui dati, potrete mettere alla prova le vostre ipotesi, comprendere le relazioni sottostanti e identificare le potenziali minacce prima che si trasformino in un problema di sicurezza. Ad esempio, se rilevate un comportamento illecito nell'utilizzo delle API da parte di uno specifico partner, potete cercare rapidamente comportamenti simili condotti da altri partner o fornitori.

Tutti i partner per la sicurezza delle API devono archiviare i dati cronologici in un data lake e fornire l'accesso a questi dati per consentire di eseguire le operazioni di analisi e ricerca delle minacce.

Idealmente, queste avanzate funzionalità di query sono disponibili in due modi:

1. Tramite un'intuitiva interfaccia web

2. Tramite una serie di interfacce API fornite dai provider di soluzioni per la sicurezza delle API da poter utilizzare nello sviluppo di workflow più sofisticati

8 Adottate un approccio alla sicurezza delle API in modo costante

Il modo migliore per integrare la sicurezza delle API direttamente nelle vostre attività aziendali consiste nell'esecuzione di test sulle API. Aggiungendo questo strumento al ciclo di vita delle API, potete limitare le possibilità di immettere in fase di produzione un'API vulnerabile o configurata in modo errato. Queste procedure di test e correzione condotte nelle fasi iniziali del ciclo di sviluppo consentono di ridurre i problemi, risparmiare tempo e limitare le spese.

È consigliabile poi per i team addetti alla sicurezza iniziare a proteggere le API con la creazione di un apposito inventario per l'utilizzo da parte della loro organizzazione. Poiché le API vengono aggiunte e rimosse di continuo, è fondamentale per i team addetti alla sicurezza mantenere un inventario aggiornato delle interfacce API all'interno dei loro repository di dati e delle loro applicazioni sensibili. Se viene eseguito in modo efficace un costante rilevamento delle API, tutte le API ombra, non autorizzate, dimenticate, zombie, orfane e obsolete diventano un problema del passato.

I team addetti alla sicurezza devono disporre della visibilità necessaria per rilevare e mitigare un'ampia gamma di minacce alla sicurezza delle API emergenti. Tuttavia, il rilevamento delle minacce deve anche avvenire durante la fase di runtime. L'abuso della logica aziendale avviene solo sulle API in fase di produzione. Il confronto di un comportamento in fase di runtime con i normali modelli di utilizzo di base aiuta a individuare un comportamento anomalo.

Infine, è importante fermare effettivamente le minacce che possono sfruttare le vostre API in qualsiasi momento durante il runtime. Il blocco automatico condotto dalla soluzione WAF è cruciale in questa fase perché la semplice ricezione di avvisi su qualsiasi problema non è sufficiente per proteggere la vostra azienda al macrolivello. Altre risposte automatizzate possono essere varie e personalizzabili, come la riduzione del limite di velocità per il gateway API, l'apertura di un ticket Jira per consentire ad uno sviluppatore di eseguire un'analisi o l'invio di un'e-mail al team addetto alla sicurezza. La capacità di rispondere in modo appropriato ad ogni minaccia rilevata è possibile solo se si comprende il contesto e se il meccanismo di risposta è personalizzabile.

Riepilogo

Cose da fare	Cose da non fare
✓ Impegnatevi a garantire una visibilità delle API completa	✗ Non temete il cloud
✓ Rendete il contesto aziendale centrale per la vostra strategia	✗ Non rendete i dati una strada a senso unico
✓ Date priorità alla collaborazione tra i reparti	✗ Non sottovalutate le API di terze parti
✓ Adottate un approccio alla sicurezza delle API in modo costante	✗ Non rispondete e andate oltre

Iniziate oggi stesso

Siete pronti a fare il primo passo verso un approccio moderno e sistematico alla sicurezza delle API?

Ulteriori informazioni su Akamai API Security.

L'approccio basato sul cloud di Akamai vi consente di iniziare facilmente in pochi minuti. Nel giro di poche ore, avrete il quadro completo dell'utilizzo delle API nella vostra organizzazione, inclusa una descrizione dettagliata delle relazioni esistenti tra la logica aziendale e le API.

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 12/23