Akamai

WHITE PAPER

13 domande da porre al fornitore della vostra soluzione per la sicurezza delle API

Introduzione

La rete delle API business-to-business sta crescendo in modo esponenziale. Un universo di dispositivi IoT (Internet of Things) in continua espansione sta offrendo agli sviluppatori nuove opportunità per inserire dati realistici nelle applicazioni tramite le API.

Tuttavia, le API, pur offrendo tante nuove opportunità di crescita e innovazione, introducono anche una nuova serie di sfide legate alla sicurezza, tra cui:

- Furto di credenziali delle API
- Mancato riconoscimento delle API
- Errata configurazione delle procedure di autenticazione e autorizzazione
- Mancata protezione delle API ombra e zombie
- Esecuzione di codice remoto, injection, LFI (Local File Inclusion) e altre tecniche di attacco
- Fuga o esfiltrazione di dati
- Scraping delle API
- Abuso della logica aziendale

I fornitori di soluzioni per la sicurezza offrono molte opzioni per rilevare e mitigare queste sfide e altre minacce alle API, che, tuttavia, non sono ugualmente efficaci o facili da usare.

Le 13 domande riportate di seguito vi aiuteranno a inquadrare le discussioni da condurre con i fornitori di soluzioni per la sicurezza delle API e a valutare l'efficacia dei loro prodotti per soddisfare le specifiche esigenze della vostra organizzazione.

1 La vostra soluzione per la sicurezza delle API è in grado di eseguire un rilevamento delle API a livello aziendale?

Uno dei maggiori problemi che i team addetti alla sicurezza si trovano ad affrontare è la mancanza di un inventario completo e accurato di tutte le API utilizzate dalla loro organizzazione. Molte delle API ombra non documentate, che i team addetti alla sicurezza non riescono a rilevare, non fanno parte del sistema strutturato di sicurezza e gestione delle API. È anche normale che le API zombie (ossia quelle che la vostra organizzazione ha ritenuto fossero state ritirate) risultino ancora accessibili. Infine, anche tra le API autorizzate e documentate, possono esistere parametri non documentati che è possibile sfruttare. Pertanto, è fondamentale eseguire il rilevamento di tutte le API (nord-sud, est-ovest e in uscita). L'unico modo per garantire una visibilità delle API completa a livello aziendale consiste nell'esaminare i dati sull'attività delle API esistenti ricavati da un'ampia gamma di tecnologie e piattaforme cloud.

2 La vostra soluzione esegue un rilevamento costante delle API e, in tal caso, questo processo è manuale?

Le API appaiono e scompaiono regolarmente a causa dei processi DevOps in rapida evoluzione. Pertanto, gli inventari delle API in tempo reale non sono sufficienti. La vostra soluzione per la sicurezza delle API deve eseguire un rilevamento costante per garantire che le nuove API documentate vengano inventariate, analizzate e protette. Inoltre, deve rilevare eventuali future istanze delle API ombra o zombie. Anche i prodotti che gravano continuamente sul vostro team per interpretare i risultati e agire di conseguenza non saranno sostenibili nel lungo termine. Al contrario, i prodotti che applicano l'automazione e l'apprendimento automatico al rilevamento e alla valutazione delle API favoriranno l'esecuzione ottimale delle operazioni aziendali anziché aggiungere altre attività manuali all'elenco delle cose da fare per il vostro team.

3 In che modo la vostra soluzione può aiutare i miei processi e strumenti di documentazione sulle API?

L'integrazione dell'approccio alla documentazione con la piattaforma di sicurezza delle API offre molti vantaggi, pertanto vi conviene verificare se il vostro fornitore dispone di questa funzionalità. Ad esempio, il caricamento automatico della documentazione Swagger esistente nella vostra piattaforma di sicurezza delle API come parte di un continuo processo di integrazione/delivery (CI/CD) migliora l'accuratezza dell'identificazione dei parametri e del rilevamento delle API ombra (se il fornitore dispone della capacità di confrontare i parametri delle API rilevate con i parametri già documentati). La vostra piattaforma di sicurezza deve anche riuscire a creare facilmente file Swagger personalizzati per qualsiasi API di cui manca la documentazione, il che aiuterà i vostri sviluppatori a iniziare e migliorare il loro processo di documentazione.

4 Quanto tempo e quanto impegno sono necessari per implementare la vostra soluzione nel mio ambiente?

Il modo più veloce ed efficace per iniziare consiste nell'utilizzare una soluzione SaaS (Security-as-a-Service) per la sicurezza delle API in grado di acquisire e analizzare in modo non invasivo i dati dell'attività delle API dai sistemi esistenti. Potete integrare un'architettura SaaS per la sicurezza delle API ben progettata nel vostro ambiente in pochi minuti per accelerare il time-to-value in ordine di grandezza ed eliminare i costi ricorrenti e i rischi associati agli aggiornamenti del sistema. Per acquisire una maggiore flessibilità, potete affidarvi ad un fornitore in grado di offrire soluzioni WAAP (Web Application and API Protection) e un sistema di rilevamento e risposta alle API per distribuire facilmente i dati del traffico delle API tra la soluzione che protegge il traffico in entrata e la soluzione che protegge tutto il traffico delle API all'interno della vostra organizzazione.

5 In che modo la vostra soluzione aiuta a individuare e dare priorità alle API rilevate che comportano dei rischi?

Vedere un inventario completo della API per la prima volta può sembrare incoraggiante, ma travolgente. Molti team addetti alla sicurezza subiscono il sovraccarico di informazioni e si sforzano di identificare le aree a cui dare priorità per la sicurezza delle API. Il modo migliore per evitare questi problemi è scegliere una soluzione per la sicurezza delle API in grado di svolgere al vostro posto gran parte di queste attività, tra cui:

- Enfatizzare la presenza di API in grado di rendere accessibili i dati sensibili
- Etichettare automaticamente i dati sensibili per tipo (ad es., informazioni di identificazione personale, indirizzi e-mail, dati delle carte di credito, ecc.)

La vostra piattaforma di sicurezza delle API deve anche consentirvi di creare categorie di etichette personalizzate per garantire ai team che si occupano di API e sicurezza di parlare la stessa lingua, in linea con gli obiettivi e i problemi di sicurezza della vostra azienda.

6 La vostra soluzione usa l'analisi comportamentale per stabilire uno standard di comportamenti previsti e per individuare eventuali anomalie?

È possibile rilevare molti tipi di attacchi tramite le firme degli attacchi per bloccare il livello WAAP. Tuttavia, non è possibile rilevare in questo modo molti tipi di attacchi riportati nell'elenco OWASP (Open Web Application Security Project) con i 10 principali rischi per la sicurezza delle API nel 2023, come la violazione dell'autorizzazione a livello di oggetto (BOLA). Questi tipi di attacchi, infatti, sono più passivi e focalizzati sull'abuso aziendale, pertanto sono più difficili da rilevare. L'unico modo per difendersi in modo efficace da tutte le minacce alle API consiste nell'utilizzare l'analisi comportamentale e l'apprendimento automatico. L'analisi dei comportamenti reali richiede grandi dataset e algoritmi di apprendimento automatico in grado di apprendere le specifiche del vostro ambiente, nonché la flessibilità e l'agilità necessarie per aggiornarsi e adattarsi automaticamente in base alle informazioni globali. Un modello SaaS è l'unico modo pratico per eseguire queste attività su larga scala.

7 Potete acquisire e analizzare i dataset abbastanza significativi per stabilire in modo efficace uno standard di comportamenti normali e per individuare eventuali anomalie?

Molte soluzioni per la sicurezza delle API si focalizzano sul monitoraggio delle singole chiamate API o, al più, delle attività delle sessioni a breve termine. Questo approccio non è sufficiente poiché molti processi aziendali legittimi (e molti attacchi) si verificano per un periodo di tempo molto più lungo. È necessario analizzare l'utilizzo delle API su un arco di tempo più lungo (almeno 30 giorni) per avere un quadro più accurato e completo dei comportamenti previsti, inclusi i processi aziendali che si verificano solo una volta al mese (ad es., la fatturazione). Inoltre, questo approccio consente di rilevare gli attacchi eseguiti lentamente per più giorni o settimane (e con numerose sessioni delle API).

8 La vostra soluzione riesce a identificare ogni entità, relazione e attività presente all'interno dei dati relativi alle API per fornire un maggior contesto aziendale?

Il miglior modo per utilizzare i dati relativi all'attività delle API consiste nell'arricchirli di contesto sulle implicazioni aziendali derivanti dall'utilizzo delle API. Le seguenti funzioni di identificazione e di etichettatura sono essenziali per la vostra piattaforma di sicurezza delle API al fine di valutare e profilare le relazioni tra le varie entità:

- Rappresentazioni di utenti delle API (entità degli utenti), come indirizzi IP, chiavi API, token di accesso, userID, partnerID, merchantID, supplierID, ecc.
- Rappresentazioni di processi aziendali (entità dei processi aziendali), come prenotazioni, pagamenti, fatturazione, contabilità, ecc.

Un'analisi granulare a questo livello è l'unico modo per trasformare la vasta quantità di dati generati dalle API in uno standard significativo e comprensibile di comportamenti previsti.

9 La vostra soluzione riesce a tracciare ogni attività eseguita da ogni entità nelle API in un arco temporale per mostrare i cambiamenti dei comportamenti nel corso del tempo?

Anche se la comprensione e il monitoraggio delle attività e delle minacce alle API ad un macro-livello sono fondamentali, la capacità di restringere l'analisi su specifiche entità è ugualmente importante. Ad esempio, se viene identificato un comportamento anomalo per uno specifico partner aziendale, la capacità di visualizzare tutte le attività di questa entità in un arco temporale è molto importante. Lo stesso vale per le entità dei processi aziendali. Vedere tutta la storia di ciò che è successo (e quando è successo) in un periodo di tempo per ogni entità all'interno delle vostre API è una potente capacità che rende ovvia la storia dell'uso normale e dell'abuso aziendale. La capacità di ripercorrere l'attività per vedere ciò che è successo prima e dopo un avviso è uno strumento potente che aiuta a comprendere l'abuso della logica aziendale.

10 In che modo posso integrare la vostra soluzione con gli strumenti, i processi e i workflow esistenti?

L'invio di avvisi alla vostra soluzione SIEM (Security Information and Event Management) è utile, ma è solo un punto di partenza. Un numero sempre maggiore di team addetti alla sicurezza utilizza strumenti SOAR (Security Orchestration, Automation and Response) più sofisticati per avviare workflow predefiniti quando vengono rilevati incidenti e minacce alla sicurezza. Inoltre, poiché molti problemi di sicurezza delle API richiedono un intervento da parte di sviluppatori che non fanno parte dei team addetti alla sicurezza, la vostra piattaforma di sicurezza delle API deve integrarsi anche con gli strumenti di gestione dei workflow e di monitoraggio dei problemi utilizzati dai team di sviluppo. Se uno strumento di sicurezza analizza il traffico delle API, ha senso utilizzare le API anche come aiuto per coordinare le risposte nella CDN, nella soluzione WAF (Web Application Firewall) o nel gateway API e per creare propri playbook.

11 Posso utilizzare i dati relativi alle attività e alle API della vostra soluzione per la mitigazione dei rischi e la ricerca delle minacce in modo proattivo?

Gli strumenti di sviluppo e sicurezza integrati non possono essere semplicemente delle "scatole nere" che inviano avvisi unidirezionali alle vostre soluzioni. I team addetti alla sicurezza e alle API devono poter analizzare i dati che hanno originato un avviso o un problema. A tal scopo, è consigliabile utilizzare piattaforme di sicurezza delle API in grado di consentire agli utenti di esaminare i dati relativi alle API direttamente da un'interfaccia web integrata o tramite le API che consentono di integrare la piattaforma di sicurezza delle API con altre interfacce e strumenti di propria scelta. In tal modo, il vostro team addetto alla sicurezza potrà condurre una ricerca proattiva delle minacce in maniera efficace ed efficiente. Questo approccio, inoltre, aiuterà i vostri sviluppatori e le altre parti interessate che non fanno parte del team addetto alla sicurezza a capire come le API vengono prese di mira (e utilizzate in modo legittimo) dai criminali.

12 Cosa fate per garantire la protezione dei dati sensibili relativi alle mie attività aziendali da voi raccolti?

L'avanzata analisi comportamentale richiesta per proteggere le API dall'odierno scenario delle minacce è possibile solo se effettuata nel cloud. Considerando le dimensioni e il livello di riservatezza del dataset delle vostre API, è importante pretendere la protezione dei vostri dati dal fornitore della vostra soluzione per la sicurezza. Verificare le pratiche adottate dal vostro fornitore per proteggere la vostra infrastruttura cloud è importante, ma è solo il punto di partenza. Potete richiedere al fornitore della vostra soluzione per la sicurezza delle API di utilizzare tecniche come la tokenizzazione, ossia sostituire i dati sensibili con token anonimizzati prima di trasmetterli al cloud. In tal modo, viene garantita la privacy dei dati anche se il fornitore (o il loro provider di servizi cloud) riscontra un problema di sicurezza.

13 La vostra soluzione fornisce un accesso granulare ai dati sulle attività delle API?

I dati sono un elemento strategico per tutto, dalla conformità al contesto necessario per la prevenzione degli attacchi. Molti fornitori offrono proprie versioni per l'archiviazione dei dati delle API nel tempo, tuttavia cercate di capire bene cosa vi offrono realmente. Le soluzioni che propongono solo l'invio di avvisi non vi consentono di avere un quadro completo della situazione perché le attività delle API violate possono verificarsi lentamente nel tempo, non solo nel momento in cui viene inviato un avviso. In alternativa, il fornitore di una soluzione completa che tiene traccia di tutte le attività delle API vi offre un quadro chiaro di tutta la situazione e vi fornisce gli strumenti necessari per esaminare queste attività in dettaglio invece di perderle in un modello di apprendimento automatico non accurato. È importante disporre di questo accesso granulare ai vostri dati perché in questo modo potete monitorare le minacce in modo proattivo invece di intervenire retroattivamente dopo aver ricevuto l'avviso di un attacco.

13 domande da porre al fornitore della vostra soluzione per la sicurezza delle API

1. La vostra soluzione per la sicurezza delle API è in grado di eseguire un rilevamento delle API a livello aziendale?
2. La vostra soluzione esegue un rilevamento costante delle API e, in tal caso, questo processo è manuale?
3. In che modo la vostra soluzione può aiutare i miei processi e strumenti di documentazione sulle API?
4. Quanto tempo e quanto impegno sono necessari per implementare la vostra soluzione nel mio ambiente?
5. In che modo la vostra soluzione aiuta a individuare e dare priorità alle API rilevate che comportano dei rischi?
6. La vostra soluzione usa l'analisi comportamentale per stabilire uno standard di comportamenti previsti e per individuare eventuali anomalie?
7. Potete acquisire e analizzare i dataset abbastanza significativi per stabilire in modo efficace uno standard di comportamenti normali e per individuare eventuali anomalie?
8. La vostra soluzione riesce a identificare ogni entità, relazione e attività presente all'interno dei dati relativi alle API per fornire un maggior contesto aziendale?
9. La vostra soluzione riesce a tracciare ogni attività eseguita da ogni entità nelle API in un arco temporale per mostrare i cambiamenti dei comportamenti nel corso del tempo?
10. In che modo posso integrare la vostra soluzione con gli strumenti, i processi e i workflow esistenti?
11. Posso utilizzare i dati relativi alle attività e alle API della vostra soluzione per la mitigazione dei rischi e la ricerca delle minacce in modo proattivo?
12. Cosa fate per garantire la protezione dei dati sensibili relativi alle mie attività aziendali da voi raccolti?
13. La vostra soluzione fornisce un accesso granulare ai dati sulle attività delle API?

Come dovreste aver già capito, la soluzione Akamai API Security può offrire un efficace sistema di protezione, come consigliato in questa sede. Scoprite la nostra soluzione.

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