



La guida definitiva alla gestione del sistema di sicurezza delle API

Sommario

Perché la sicurezza delle API è diventata imprescindibile	3
Perché adottare una gestione del sistema di sicurezza?	6
Le funzioni indispensabili del sistema di gestione della sicurezza	8
L'approccio alla gestione del sistema di sicurezza offerto da Akamai	11
Come un sistema di gestione della sicurezza delle API può aiutarvi	13

Perché la sicurezza delle API è diventata imprescindibile

Le API consentono agli sviluppatori di un'organizzazione di migliorare la loro efficienza in una professione in cui la velocità non può scendere a compromessi. Tuttavia, anche se le API sono intuitive per gli sviluppatori (e fondamentali per garantire l'interoperabilità delle risorse software e dei dati), la sicurezza delle API non è riuscita a tenere il passo con la velocità dell'innovazione.

L'84% delle organizzazioni ha riscontrato un problema di sicurezza delle API negli ultimi 12 mesi, con un aumento rispetto al 78% del 2023¹, in parte, perché le API offrono anche una migliore efficienza ai criminali. Molte API, infatti, vengono create

con errori di configurazione/codifica senza controlli di autenticazione. Di conseguenza, un attacco alle API può risultare alquanto semplice da sferrare e un modo diretto per sottrarre dati.

Inoltre, quando si tratta di dati, solo il 27% delle aziende con un inventario completo delle API sa quali API restituiscono dati sensibili, dalle informazioni sui clienti alla proprietà intellettuale, una percentuale in calo rispetto al 40% del 2023². Considerando l'aumento nel numero di attacchi e la riduzione della visibilità, alle aziende serve un modo per valutare e migliorare il proprio sistema di sicurezza delle API.

1, 2. Akamai, Studio sull'impatto della sicurezza delle API 2024

Come si presenta un sistema completo per la sicurezza delle API

Parallelamente alla diffusione dell'utilizzo delle API da parte delle aziende, aumenta anche la loro superficie di attacco, il che crea nuove sfide in termini di sicurezza.

Per quanto riguarda la sicurezza delle API, gli strumenti tradizionalmente usati dalle organizzazioni, come gateway API e soluzioni WAF (Web Application Firewall), possono fornire un certo livello di protezione. Tuttavia, poiché il patrimonio delle API diventa sempre più complesso, ad esempio, per la proliferazione delle API non gestite che sono difficili da individuare e proteggere, qualcosa nella loro sicurezza deve cambiare.

Le API meritano di occupare un posto di rilievo in una strategia di sicurezza aziendale. Inoltre, una soluzione dedicata per la sicurezza delle API, ossia progettata per affrontare gli odierni metodi di attacco e i rischi per le API, può fornire la visibilità e le funzionalità necessarie per mettere in atto questa strategia. Non si tratta di una difesa approfondita, in cui gli strumenti si completano l'un l'altro per coprire ogni fase del percorso dell'attacco.



Una piattaforma completa per la sicurezza delle API, ossia progettata per fornire funzionalità di individuazione delle API, gestione del sistema di sicurezza, protezione del runtime ed esecuzione dei test di sicurezza, può aiutarvi ad individuare i rischi nascosti per le API, identificare i percorsi degli attacchi alle API e mitigare le minacce non rilevate in tempo reale.

Nel nostro eBook correlato, *La guida definitiva all'individuazione delle API*, viene descritto il primo elemento fondamentale nella sicurezza delle API: l'individuazione delle API. Una volta individuate e inventariate tutte le API in uso nella vostra organizzazione, la fase successiva consiste nel migliorare il sistema di sicurezza delle API.

La gestione del sistema di sicurezza può risultare particolarmente importante per le aziende che acquistano applicazioni da provider di terze parti e le utilizzano, le brandizzano e le vendono come proprietarie. Ad esempio, tutte

le nuove auto prodotte negli ultimi cinque anni presentano praticamente le stesse identiche funzionalità telematiche. Se un criminale individua le vulnerabilità presenti negli endpoint delle API di un produttore, può ottenere un semplice punto di accesso per sferrare attacchi per il controllo degli account e di violazione di dati da remoto.

Argomenti trattati in questa guida

La gestione del sistema di sicurezza delle API vi fornisce gli strumenti necessari per gestire, monitorare e mantenere la sicurezza delle API per tutto il loro ciclo di vita. Questa guida definitiva si focalizza sui requisiti principali della gestione del sistema di sicurezza delle API, tra cui il rilevamento delle vulnerabilità e la protezione dei dati sensibili. Inoltre, presenta i metodi e le funzioni di gestione del sistema di sicurezza disponibili nella soluzione Akamai API Security.

Perché adottare una gestione del sistema di sicurezza?

Una gestione di questo tipo vi garantisce di iniziare con il piede giusto per garantire la sicurezza delle API. Questo sistema vi aiuta a comprendere il rischio delle API individuate trovando i tipi di dati che vengono scambiati, se sono presenti vulnerabilità o errori di configurazione, se le API sono correttamente autenticate e molto altro. La capacità di identificare le vulnerabilità delle API e la relativa mitigazione vi consente di agire rapidamente prima che si verifichi un attacco.

Una gestione completa del sistema di sicurezza vi fornisce una visibilità su tutte le attività relative alle API per consentirvi di applicare le policy di sicurezza appropriate, garantire la conformità alle normative e verificare i cambiamenti nell'ecosistema delle API. Inoltre, protegge e salvaguarda le API da attacchi, utenti non autorizzati e tentativi di violazione dei

Solo il 27% delle aziende con un inventario completo delle API sa quali API restituiscono dati sensibili, una percentuale scesa dal 40% registrato nel 2023³.

3. Akamai, Studio sull'impatto della sicurezza delle API 2024

dati, tutti problemi che possono causare significativi danni alla reputazione, perdita di affari e sanzioni normative.

L'implementazione di best practice per la gestione del sistema di sicurezza minimizza la superficie di attacco delle API e mitiga gran parte dei rischi correlati. Stilare inventari accurati delle API e degli archivi di dati sensibili è fondamentale per ottimizzare la gestione del sistema di sicurezza. Alla pagina successiva, verranno descritti altri elementi che caratterizzano il sistema di gestione della sicurezza delle API: rilevamento delle vulnerabilità, monitoraggio delle API e mitigazione dei problemi.

- **Rilevamento delle vulnerabilità**

Analisi: il codice sorgente viene esaminato per individuare le vulnerabilità comuni, capire in che modo le API interagiscono con i sistemi esterni e valutare le sue funzioni di autorizzazione e autenticazione.

Osservazione: il traffico delle API in entrata e in uscita viene esaminato per identificare errori di configurazione, rilevare le vulnerabilità e comprendere il comportamento standard delle API.

La gestione del sistema di sicurezza è solo una parte di un programma completo per la sicurezza delle API, pertanto, è cruciale eseguire test completi prima della produzione per impedire alle vulnerabilità di raggiungere questa fase.

- **Monitoraggio delle API**

Potete identificare e monitorare le chiamate delle API in fase di produzione, tenere traccia delle richieste delle API, rilevare le deviazioni dall'utilizzo standard e creare avvisi quando l'utilizzo delle API supera le soglie prestabilite.

- **Mitigazione**

Potete risolvere le lacune o le vulnerabilità identificate per rendere le API più sicure e conformi cambiando il codice, ottimizzando le impostazioni di sicurezza o applicando le patch appropriate per mitigare i difetti delle API. Una buona gestione del sistema di sicurezza consente di mitigare le vulnerabilità prima che possano essere sfruttate.

Le funzioni indispensabili del sistema di gestione della sicurezza

Come già sapete (o forse sospettate), il vostro sistema di sicurezza delle API non è configurato per offrirvi il massimo livello di protezione. Ecco quindi alcune importanti funzioni che i vostri strumenti per la gestione del sistema di sicurezza devono includere:

- **Classificazione dei dati sensibili**

Un'API che fornisce i dati sul meteo ricavati da fonti pubbliche può creare molti più problemi rispetto ad un'API che trasmette informazioni sulle carte di credito. Gli strumenti per la gestione del sistema di sicurezza delle API devono riuscire ad identificare il numero di API che sono in grado di accedere a varie informazioni, come dati delle carte di credito, numeri di telefono, codici fiscali e altri dati sensibili, insieme al numero degli utenti che possono accedere ai dati sensibili tramite le API.

- **Valutazione della configurazione**

Molti attacchi informatici consentono ai criminali di accedere ai sistemi presi di mira grazie a semplici errori di configurazione di reti, gateway API o firewall che trattano e proteggono il traffico delle API. Un solido sistema di gestione della sicurezza deve effettuare regolarmente una scansione delle configurazioni dell'infrastruttura e del software, inclusi i file di registro e di configurazione. In tal modo, potrete scoprire errori di configurazione e vulnerabilità, identificando, al contempo, i rischi creati dai cambiamenti apportati alla configurazione.

- **Punteggio di affidabilità dei criminali**

Cercate un motore in grado di fornirvi la valutazione dell'affidabilità dei criminali che utilizza gli algoritmi di apprendimento automatico per valutare i 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 e altri fattori contestuali. In tal modo, potrete stabilire il livello di affidabilità in base al quale un incidente di runtime rilevato è il risultato di un'attività dannosa. Questa funzionalità esclusiva consente ai clienti di intervenire rapidamente sulle minacce critiche e creare flussi automatici di mitigazione e notifica per gli attacchi ad alto impatto.

- **Workflow personalizzati**

Insieme ai livelli di gravità personalizzabili, dovete riuscire a creare workflow in grado di intraprendere immediatamente le azioni necessarie una volta identificate le vulnerabilità. I workflow personalizzati possono consentire varie operazioni, dalla creazione di ticket per la risoluzione dei problemi 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. È necessario valutare le API protette per garantirne la conformità rispetto alle specifiche e creare 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 **specificata OpenAPI** (in precedenza nota come Swagger) definisce le caratteristiche di un'interfaccia standard. Gli strumenti per la gestione del sistema di sicurezza devono 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.

Una società leader nel campo assicurativo migliora il sistema di sicurezza delle API con Akamai

In un periodo in cui i consumatori preferiscono l'online ai tradizionali negozi fisici, le società di servizi finanziari devono innovarsi ad un ritmo accelerato. Come molte aziende del suo settore, Aflac, il principale provider di assicurazioni sanitarie integrative negli Stati Uniti, ha dovuto affrontare i crescenti problemi di sicurezza delle API.

Aflac si è rivolta alla piattaforma Noname API Security (ora parte di Akamai API Security) per soddisfare le sue esigenze. Il modulo di gestione del sistema di sicurezza aiuta il team ad identificare i vari tipi di dati che attraversano le API dell'azienda, a fornire visibilità sulle API che accedono ai dati sensibili e a rilevare eventuali anomalie nell'accesso ai dati.

Per ulteriori informazioni, leggete il [case study completo su Aflac](#).



"Eravamo consapevoli che il nostro patrimonio delle API fosse ampio e volevamo essere totalmente sicuri di conoscere ogni API, di avere piena visibilità sul loro funzionamento e di poterle sottoporre continuamente a test per individuare eventuali rischi per la sicurezza.

- DJ Goldsworthy, VP, Security Operations and Threat Management, Aflac

L'approccio alla gestione del sistema di sicurezza offerto da Akamai

Il modulo di gestione del sistema di sicurezza offerto dalla soluzione Akamai API Security fornisce una visione completa sul traffico, sul codice e sulle configurazioni per poter valutare il livello di sicurezza delle API della vostra organizzazione. Akamai stabilisce come si presenta una reale superficie di attacco per le API e le applicazioni web e rileva tutte le forme di dati sensibili che attraversano le API, aiutandovi a proteggerli.

Anche un semplice errore di configurazione delle API può lasciare la vostra azienda vulnerabile ai criminali informatici.

Una volta penetrati nel sistema, gli hacker possono accedere ed esfiltrare i vostri dati sensibili. Il modulo di gestione del sistema di sicurezza offerto dalla soluzione Akamai API Security offre tre funzioni principali:

- Integrazione out-of-band per un'individuazione continua delle API on-premise, in ambienti ibridi e nel cloud pubblico
- Un inventario delle API semplice da consultare, che include informazioni sui modelli, sulla posizione della rete e sui tipi di dati
- Generazione automatizzata della documentazione relativa alle API (OAS/Swagger)
- Analisi contestuale degli errori di configurazione e delle vulnerabilità delle API con assegnazione di priorità
- Rilevamento di tutte le 10 principali vulnerabilità per la sicurezza delle API riportate nell'elenco OWASP
- Individuazione e classificazione automatizzate dei cambiamenti apportati ai dati sensibili e alle API

Esposizione delle API
I problemi e i rischi relativi alla sicurezza delle API non sono da ricercare solo nel codice sorgente. Osservare il comportamento del traffico nel contesto della rete fornisce tutti i dati necessari per ricavare informazioni sui rischi correlati.

Tag	Type	# of Related I
API1:2019	Broken Object Level Authorization	40 12
API2:2019	Broken User Authentication	10 13
API3:2019	Excessive Data Exposure	4 8 2
API4:2019	Lack of Resources & Rate Limiting	4 8 1
API5:2019	Broken Function Level Authorization	4 8 1
API6:2019	Mass Assignment	4 8 1
API7:2019	Security Misconfiguration	4 8 1
API8:2019	Injection	4 8 1
API9:2019	Improper Assets Management	4 8 1
API10:2019	Insufficient Logging & Monitoring	1 2 2

Esposizione delle API

Oltre ad individuare i rischi presenti nel codice delle API, è anche importante osservare il traffico delle API con un'attenzione particolare al loro comportamento (per verificare se si discosta da quello standard) e al contesto della rete.

Il sistema di gestione della sicurezza offerto dalla soluzione Akamai API Security effettua una ricerca sul maggior numero possibile di fonti per rilevare eventuali vulnerabilità, inclusi i file di registro, le riproduzioni del traffico storico, i file di configurazione e molto altro. La soluzione rileva tutte le 10 principali vulnerabilità della sicurezza delle API riportate nell'elenco OWASP e protegge le API da fughe di dati, problemi di autorizzazione, abusi, uso improprio e danneggiamento dei dati.

Akamai identifica e assegna le priorità in modo intelligente alle potenziali vulnerabilità, che possono essere risolte manualmente o automaticamente (oppure con una

combinazione di queste modalità), tramite apposite integrazioni nelle soluzioni WAF, nei gateway API, nei processi SIEM e ITSM, negli strumenti dei workflow e in altri servizi.

Protezione dei dati delle API

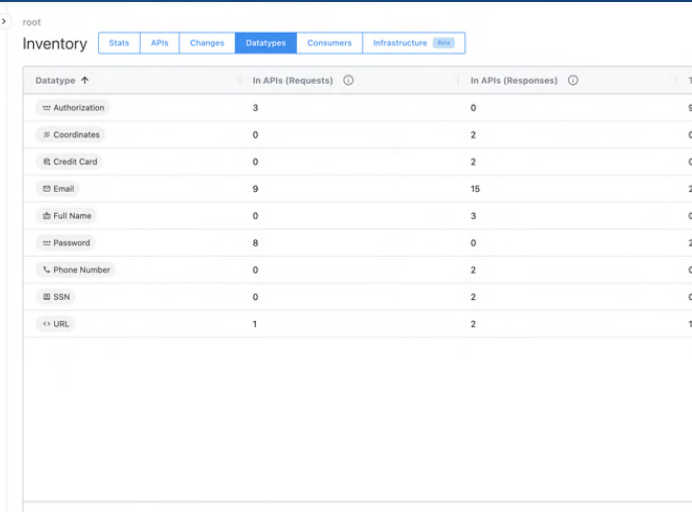
La protezione dei vari tipi di dati sensibili richiede un inventario accurato dei dati che attraversano gli endpoint per applicare di conseguenza le policy e i controlli appropriati (le policy DLP per le API sono intuitive e dettagliate).

La conformità sta assumendo una dimensione completamente nuova in seguito al crescente utilizzo delle API. Nuove normative sono emerse in risposta alla crescente superficie di attacco. I settori altamente regolamentati devono ora includere le API nei loro piani di conformità.

Il modulo di gestione del sistema di sicurezza offerto dalla soluzione Akamai API Security identifica tutte le forme di dati sensibili che attraversano le API, incluse le informazioni di identificazione personale (PII), come dati di carte di credito, codici fiscali, indirizzi, informazioni sulle assicurazioni e molto altro. Limitando l'accesso a questi tipi di dati e implementando un appropriato sistema di gestione, possiamo aiutarvi a garantire che i dati sensibili rimangano nelle posizioni richieste e che vengano protetti dalle minacce.

Protezione dei dati delle API

La protezione dei vari tipi di dati sensibili richiede un inventario accurato dei dati che attraversano gli endpoint per poter applicare di conseguenza le policy e i controlli appropriati (le policy DLP per le API sono intuitive e dettagliate).



Datatype	In APIs (Requests)	In APIs (Responses)	Total
Authorization	3	0	3
Coordinates	0	2	2
Credit Card	0	2	2
Email	9	15	24
Full Name	0	3	3
Password	8	0	8
Phone Number	0	2	2
SSN	0	2	2
URL	1	2	3

Come un sistema di gestione della sicurezza delle API può aiutarvi

Ogni volta che un cliente, un partner o un vendor interagiscono con la vostra organizzazione in modo digitale, c'è un'API "dietro le quinte" che facilita un rapido scambio dei dati (spesso sensibili). Disporre della visibilità su tutte le API presenti nella vostra organizzazione e valutare i relativi attributi di rischio, ad esempio, quali API restituiscono dati sensibili, può aiutarvi a proteggere la vostra azienda da un vettore di attacco in rapida crescita. Un sistema di gestione della sicurezza delle API può aiutarvi anche a garantire la conformità con le normative globali nell'intento di impedire eventuali violazioni di dati.



Scoprite ulteriori informazioni sulle **normative sulla protezione dei dati** che richiedono la visibilità e la protezione di tutte le API.

Scoprite come possiamo aiutarvi programmando una **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 o akamai.com/blog e seguite Akamai Technologies su **X** (in precedenza Twitter) e **LinkedIn**. Data di pubblicazione: 12/24.

