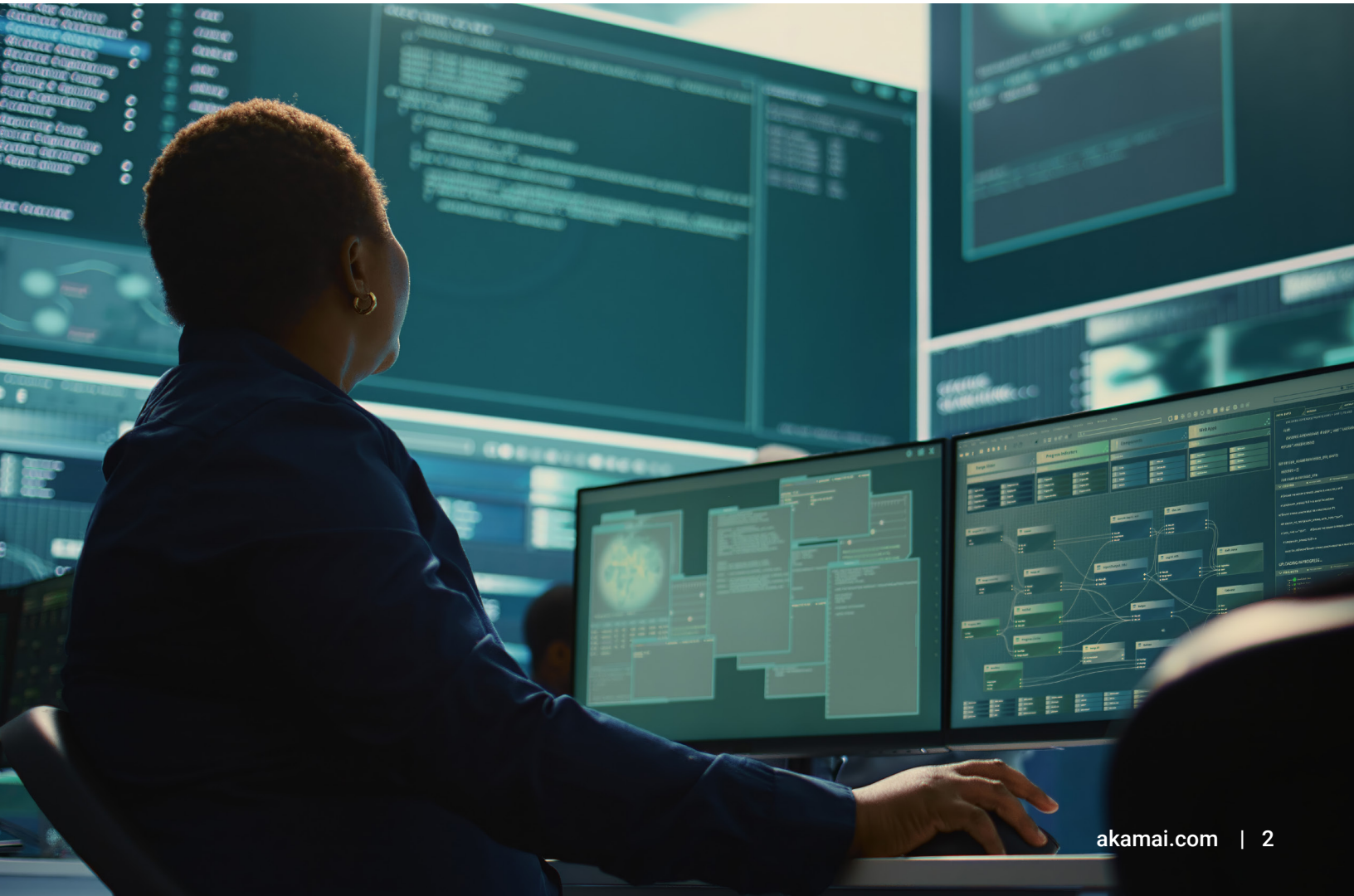
Akamai

WHITE PAPER

Sicurezza e conformità delle API

I requisiti impliciti ed espliciti per la protezione dei dati

In questo rapporto



Introduzione

Dimostrare la conformità alle normative in materia di protezione dei dati ha, tradizionalmente, implicato l'utilizzo di grandi quantità di energie e risorse per tenere il passo con i rischi più comuni. Le cose però stanno cambiando. L'odierna superficie di attacco si sta evolvendo rapidamente per includere minacce che la maggior parte dei programmi di conformità aziendali non tengono nella giusta considerazione, in parte perché gli stessi organismi di regolamentazione non riescono sempre a tenere il passo e ad esplicitare ogni aspetto della copertura necessaria per evitare eventuali violazioni.

È questo il caso della protezione delle API. Ogni volta che un cliente, un partner o un vendor interagiscono con la vostra azienda in modo digitale, c'è un'API "dietro le quinte" che facilita un rapido scambio di informazioni, che spesso includono dati sensibili. I criminali ora sanno che è più semplice rubare questi dati prendendo di mira direttamente le API.

Probabilmente, avrete già visto nuovi linguaggi nelle normative a indicare la necessità di inventariare, valutare o proteggere le API. Tuttavia, anche se non è incluso uno specifico linguaggio sulle API, il fatto che siano diventate un chiaro vettore di attacco *implica* che ne è richiesta un'adeguata protezione.

Non sorprende, quindi, che l'emergere delle API sia diventato un serio problema di conformità. Le API vulnerabili o non correttamente configurate sono prevalenti, facili da violare e spesso non protette. Inoltre, è sufficiente una sola API violata per riuscire a rubare milioni di dati. I numeri parlano da soli:

- Il 78% delle organizzazioni ha subito un incidente relativo alla sicurezza delle API.[1]
- Il 44% delle organizzazioni è stato sanzionato dagli enti di controllo per problemi di sicurezza alle API.[2]

In che modo questo approccio influisce sul vostro programma di conformità? Gli enti di controllo devono verificare che la vostra organizzazione stia prendendo le misure adeguate per proteggere tutti i punti di accesso ai dati sensibili. Pertanto, dovete dimostrare che la vostra organizzazione può:

- Dare conto di tutte le API di cui dispone, incluse quelle ombra più elusive
- Individuare e correggere eventuali vulnerabilità delle API
- Applicare controlli personalizzati per prevenire le violazioni di dati relative alle API

Questo white paper descrive la natura dei crescenti rischi per le API, evidenzia sei esempi di regolamenti e quadri normativi che richiedono la protezione (esplicita o implicita) delle API e offre consigli su come soddisfare i requisiti di conformità tramite le best practice di sicurezza delle API.

1., 2. Akamai Technologies, "The API Security Disconnect", 2023

I rischi per le API

Le API sono il fulcro dei prodotti digitali, dei servizi e degli ambienti cloud della vostra azienda. Il loro costante accesso ai dati le rende capaci non solo di favorire i ricavi, ma anche di creare rischi per le operazioni aziendali. Il problema è che la maggior parte delle aziende (anche quelle che hanno messo in atto rigorosi programmi di sicurezza) non dà priorità alle minacce correlate alle API al livello con cui si focalizzano su altre minacce, come il phishing o il ransomware.

Alcune organizzazioni si affidano ai gateway API e alle soluzioni WAF (Web Application Firewall) per una protezione basilare delle API, ma questi strumenti non sono progettati per fornire il grado di visibilità, protezione in tempo reale ed esecuzione continua dei test che le soluzioni specializzate per la sicurezza delle API possono offrire. Ecco perché questi strumenti non sono adeguati:

- I gateway API e le soluzioni WAF possono osservare solo il traffico delle API *gestito* che viene instradato attraverso di essi.
- Questi strumenti non possono proteggere le API non gestite, che, secondo le previsioni degli analisti, entro il 2025 rappresenteranno quasi la metà dell'ecosistema delle API di un'azienda tipica.
- Di conseguenza, i team addetti alla sicurezza non sono completamente preparati a proteggere la parte della loro superficie di attacco, caratterizzata da un'espansione rapidissima, poiché conoscono poco sul punto in cui vengono instradate le API, come vengono configurate, quali tipi di dati sensibili si scambiano e i rischi che creano.

La protezione delle informazioni degli utenti è prioritaria per gli enti di controllo, che infliggono sanzioni severe alle aziende non capaci di proteggere adeguatamente i dati dei clienti dagli accessi non autorizzati. Considerando che solo 4 professionisti della sicurezza su 10 con inventari completi delle API sanno quali delle loro API restituiscono dati sensibili[3] e che molte chiamate API vengono originate dai criminali per verificare la presenza di eventuali vulnerabilità, le violazioni di dati tramite le API sono destinate solo a crescere, soprattutto perché gli attacchi alle API sono attualmente alquanto semplici da sferrare.

3. Akamai Technologies, "The API Security Disconnect", 2023

Quattro attacchi alle API con implicazioni di conformità

In che modo una violazione delle API può influire sul livello di conformità di un'azienda? Di seguito, vengono riportati alcuni esempi.

- Una famosa applicazione di gestione dei progetti è stata violata da un criminale che ha sfruttato un endpoint delle API privo di controlli di autenticazione. Il criminale ha violato l'API, ha ottenuto un accesso non autorizzato alle informazioni di milioni di utenti e, mesi dopo, ha esfiltrato oltre 21 GB di dati, inclusi indirizzi e-mail e sottoscrizioni ai consigli di amministrazione, su Internet.
- Più di 11 milioni di dati appartenenti ai clienti di una grande società di telecomunicazioni sono stati resi visibili, sembra perché un'API, che non richiedeva autenticazione, è stata inconsapevolmente esposta a Internet. I criminali hanno violato l'API, si sono resi conto che non disponeva di un identificatore univoco, hanno individuato il suo numero identificativo e hanno richiesto facilmente dati sensibili.
- Pare che un'azienda di social media sia stata colpita due volte negli ultimi anni da una tattica di scraping resa possibile tramite un uso improprio delle API. Nel primo caso, i dati privati sono stati esfiltrati da 500 milioni di profili utente e poi venduti. Nel secondo caso, un criminale ha creato un database, completo dei numeri di telefono e dei dati dei salari esfiltrati da 700 milioni di utenti.
- Questa stessa tecnica è stata usata contro un'altra azienda di social media per esfiltrare i dati su milioni di utenti. L'azienda è stata sanzionata con una multa di 5 miliardi di dollari perché un vendor di terze parti ha usato l'API dell'azienda per raccogliere dati sensibili. Indipendentemente dal fatto che il vendor abbia abusato dell'API, la *stessa* società è stata multata perché non è riuscita a monitorare la sua applicazione.

Sei esempi di regolamenti e quadri normativi relativi alla sicurezza delle API

Molti regolamenti e quadri normativi non fanno necessariamente esplicito riferimento alle API, ma le normative si focalizzano chiaramente sulla protezione di applicazioni e infrastrutture all'interno della quali operano le API, come ad esempio:

- Il PCI DSS (Payment Card Industry Data Security Standard) v4.0 offre indicazioni utili per verificare che il software di un'organizzazione utilizzi le funzioni di componenti esterni in modo sicuro, incluse le API che trasmettono i dati dei pagamenti da un'app mobile ad un sistema bancario.
- Il NIST Secure Software Development Framework offre indicazioni utili per proteggere adeguatamente i software con un livello di sicurezza costante e per risolvere le vulnerabilità. Le API sono al centro dello sviluppo dei software.

In molti casi, le normative prevedono obiettivi generici per la protezione dei dati, come il regolamento generale sulla protezione dei dati (GDPR) in cui si parla di "misure di sicurezza appropriate". Le vostre API potrebbero ricevere milioni di chiamate al giorno che richiedono la trasmissione di tali dati da parte di clienti *e* criminali. Siete voi che dovete stabilire quali controlli di sicurezza sono necessari e dimostrare come funzioneranno.

Analizziamo ora in modo più approfondito i regolamenti e i quadri normativi che influiscono direttamente sull'ecosistema delle vostre API.

1. PCI DSS v4.0

Creato dal Payment Card Industry Data Security Council, il PCI DSS è diventato uno standard globale per la protezione dei dati dei pagamenti. Se la vostra azienda accetta le principali carte di credito e si occupa di elaborare, archiviare o trasmettere i dati dei titolari di carte di credito in modo elettronico, deve ottemperare a questo standard.

I requisiti della versione originale riguardano principi di sicurezza che sono importanti oggi come lo erano quando il PCI DSS è stato pubblicato nel 2006, come l'assegnazione dell'accesso ai sistemi e ai dati dei titolari di carte di credito solo a chi ne ha necessità per motivi lavorativi e la definizione dei requisiti di accesso in base al ruolo.

Ora, tuttavia, con l'entrata in vigore del PCI DSS v4.0, le aziende devono adattare i loro programmi di conformità per contrastare i criminali che prendono frequentemente di mira le migliaia di API presenti nelle tecnologie di pagamento. In generale, lo standard PCI DSS v4.0 è incentrato su quattro obiettivi chiave:

1. Continuare a soddisfare le esigenze di sicurezza del settore dei pagamenti
2. Sostenere la sicurezza come processo continuo
3. Dare alle aziende la possibilità di soddisfare i requisiti in modo flessibile (ad es., nuovi strumenti, nuovi controlli)
4. Ottimizzare metodi e processi di convalida

Il requisito 6.2.3 del PCI DSS v4.0 impone alle organizzazioni di rivedere il proprio codice applicativo personalizzato (ossia, il codice sviluppato da un fornitore di terze parti, ma non le applicazioni commerciali preconfezionate standard) per garantire di non immettere vulnerabilità in fase di produzione. Specifico per le API, questo requisito offre indicazioni utili per verificare che il software di un'organizzazione utilizzi le funzioni di componenti esterni (librerie, modelli, API, ecc.) in modo sicuro. Questi requisiti evidenziano il ruolo chiave delle API nella supply chain dei software in generale e che cosa serve per proteggerle.

Le API sono diventate il metodo predefinito per la connettività e lo scambio dei dati nei moderni ambienti applicativi. Tenendo conto di ciò, proteggere le API sia in fase di pre-produzione (Shift-Left) che in fase di post-produzione (Shield-Right) è essenziale per rendere le vostre attività digitali resilienti agli attacchi. Riportiamo di seguito sei best practice per la sicurezza delle API utili per garantire la conformità al requisito 6.2.3:

- Verificare l'utilizzo di componenti basati su API e il relativo sistema di sicurezza (ad es., individuare configurazioni errate che portano a vulnerabilità, incluso l'uso di una crittografia debole).
- Convalidare i comportamenti normali e previsti di utilizzo delle API e implementare i controlli necessari per impedire a criminali sospetti di violare i propri sistemi (ad es., verificare il comportamento dell'applicazione per rilevare le vulnerabilità logiche).
- Individuare i framework di terze parti utilizzati per implementare le API, stabilendo se possono essere obsoleti e vulnerabili.
- Creare un inventario completo di tutte le API, incluse le diverse versioni in esecuzione, per ottenere informazioni su potenziali funzionalità e backdoor non documentati che devono essere gestiti.
- Verificare la sicurezza del codice delle API ed evitare di immettere in produzione vulnerabilità legate alle API.
- Implementare best practice di codifica protetta delle API, che consentono di adottare un approccio programmatico per la distribuzione sicura del codice su base continua.

2. Regolamento generale sulla protezione dei dati (GDPR)

Il GDPR è una legge dell'Unione europea (UE) che mira a rafforzare e unificare la protezione dei dati delle persone all'interno dell'UE. L'obbligo di conformità al GDPR, tuttavia, non è limitato alle aziende che operano nell'UE, ma riguarda tutte le organizzazioni che offrono beni o servizi all'interno dell'UE.

Il regolamento stabilisce che i dati personali sono informazioni che possono essere collegate o connesse ad un individuo. I dati regolamentati ai sensi del GDPR possono includere il nome di una persona, le informazioni di contatto e i dati bancari, finanziari e sanitari. Da un punto di vista più tecnico, queste informazioni includono anche i dati di geolocalizzazione, come gli indirizzi IP e i cookie web.

Cosa implica il regolamento per la sicurezza delle API? Sia per lo sviluppo di applicazioni, microservizi o dispositivi IoT (Internet-of-Things), è probabile che le API su cui si basano queste tecnologie scambino dati regolamentati dal GDPR. Pertanto, le organizzazioni che sviluppano API accessibili a Internet devono tener conto della protezione dei dati nella progettazione delle API fin dall'inizio, non in un secondo momento.

Consideriamo il principio del privilegio minimo, che richiede di concedere agli utenti solo le autorizzazioni minime necessarie per svolgere le proprie mansioni lavorative.

L'articolo 25 del GDPR si *basa* sul principio del privilegio minimo, che richiede alle aziende di implementare misure tecniche e organizzative tali da garantire che, per impostazione predefinita, vengano trattati solo i dati personali necessari per ogni scopo specifico. A loro volta, gli sviluppatori delle API sono tenuti ad implementare adeguati controlli di autenticazione e autorizzazione degli utenti per salvaguardare i dati sensibili che vengono distribuiti tramite le API. I team addetti allo sviluppo delle API devono anche assicurarsi che i dati rimangano riservati durante il transito utilizzando protocolli per le comunicazioni sicure allo scopo di crittografare lo scambio di informazioni tra client e server.

Tuttavia, cosa possiamo dire dell'attuale ecosistema delle API che le organizzazioni hanno costruito nel corso degli ultimi anni o, persino, decenni? Una parte notevole delle API aziendali non sono gestite, vengono ignorate o sono eseguite in modo continuo senza eseguire controlli e adeguamenti. In questi casi, la conformità al GDPR richiede:

- L'identificazione di tutte API presenti nel vostro ambiente IT
- La valutazione dei loro fattori di rischio (ad es., i tipi di dati che scambiano e chi o cosa può accedere a questi dati)
- La mitigazione di eventuali vulnerabilità, come configurazioni errate o deboli meccanismi di autenticazione
- L'esecuzione continua di test sulle API per verificare la loro resilienza a violazioni e attacchi condotti con metodi nuovi e tradizionali

3. DORA (Digital Operational Resiliency Act)

Considerando il ruolo del settore finanziario dell'UE come operatore di infrastrutture critiche, i requisiti del DORA sono concepiti per aiutare le organizzazioni degli stati membri dell'UE a resistere e a riprendersi dagli attacchi informatici. Con il DORA, il settore potrà disporre di un quadro normativo completo e vincolante per la gestione dei rischi nei servizi ICT (Information and Communication Technology). Questo atto mira ad armonizzare e ad inasprire i requisiti a cui devono conformarsi le società finanziarie dell'UE nell'attuale scenario costituito da una miriade di regolamenti e standard.

In totale, più di 22.000 istituzioni finanziarie e provider di servizi IT dell'UE rientrano nell'ambito del DORA, soprattutto terze parti che forniscono alle società finanziarie dell'UE sistemi e servizi ICT, inclusi i provider di servizi cloud. Questo atto richiede alle istituzioni finanziarie di sviluppare strategie di mitigazione dei rischi causati da terze parti che forniscono servizi ICT e di agire con la dovuta diligenza per esaminare l'idoneità dei provider.

Il DORA stabilisce vari requisiti relativi alla sicurezza delle API, tra cui la stabilità operativa digitale, che richiede alle organizzazioni di implementare programmi regolari di test per identificare potenziali lacune, vulnerabilità e/o assenza di funzionalità nei sistemi. Pensiamo ai test sulla sicurezza della rete, ai test di penetrazione, ai test sulle app web e molti altri. È importante condurre revisioni obbligatorie sulla base dei test di penetrazione per la ricerca di eventuali minacce (TLPT), a seconda delle dimensioni, del livello di rischio e del profilo aziendale della società finanziaria. Ugualmente importante è sottoporre regolarmente le API a test per cercare eventuali vulnerabilità.

Il DORA evidenzia alcuni esempi di test sulla sicurezza che includono test sulle API e sulle applicazioni basate su web, tra cui l'utilizzo di risorse rivolte al pubblico, come l'OWASP (Open Worldwide Application Security Project). L'elenco OWASP con i 10 principali rischi per la sicurezza delle API, in particolare, aiuta le organizzazioni ad identificare errori di configurazione, punti deboli, difetti di logica e problemi del codice che consentono ai criminali di ottenere l'accesso, manipolare o controllare in altro modo le risorse aziendali.

4. HIPAA (Health Insurance and Portability and Accountability Act)

L'HIPAA si focalizza sulla privacy dei dati e sulle regole di sicurezza necessarie per salvaguardare le informazioni sanitarie protette (PHI) presenti nelle cartelle cliniche elettroniche, le piattaforme di immissione delle ricette elettroniche e altri sistemi IT sanitari. Le aziende sanitarie, gli amministratori di piani assicurativi o i centro di smistamento che si occupano di archiviare o trasmettere le PHI in modo elettronico devono conformarsi ai principi dell'HIPAA. A tal riguardo, devono garantire la riservatezza, l'integrità e la disponibilità delle PHI, nonché la loro protezione da divulgazioni non autorizzate e uso improprio.

L'HIPAA è un esempio di una normativa che influisce notevolmente sulle API, anche se non ne fa esplicito riferimento nei suoi requisiti.

Consideriamo un vendor di servizi tecnologici che realizza portali dei pazienti per le strutture sanitarie 24/7. Una funzione sottostante di questi portali è la capacità di offrire ai pazienti un accesso efficiente e sicuro ai dati relativi a visite mediche, risultati delle analisi, pagamenti e molto altro. Le API facilitano questo scambio. Sia le strutture sanitarie che i vendor sono obbligati ad aderire ai requisiti dell'HIPAA.

La regola sulla privacy dell'HIPAA specifica che le entità interessate devono sviluppare e implementare policy e procedure tali da restringere l'accesso e l'utilizzo delle informazioni sanitarie protette sulla base degli specifici ruoli svolti dai membri della propria forza lavoro. Pertanto, gli sviluppatori delle API di un'organizzazione devono incorporare misure di protezione tecniche, come l'autenticazione, ID utente univoci e controlli degli accessi basati sui ruoli per garantire l'implementazione del principio del privilegio minimo.

Anche la visibilità è essenziale per le organizzazioni che rientrano nell'ambito dell'HIPAA, sia che si tratti di un provider il cui team IT crea API personalizzate o un vendor che sviluppa API per il provider. Alle organizzazioni servono rapporti e valutazioni in tempo reale sul livello di rischio di ciascuna API, inclusi i tipi di PHI che trasmettono. Questi dati sono rilevanti per garantire la conformità e per soddisfare il requisito dell'HIPAA che impone di rispondere alle persone che richiedono informazioni su tempi, motivi e utenti a cui le loro PHI sono state divulgate.

5. Direttiva NIS2 (Network and Information Security)

L'UE ha adottato la versione 2.0 della direttiva NIS a gennaio 2023, che si basa sulle linee guida della versione originale allo scopo di proteggere l'infrastruttura IT e segnalare eventuali problemi. Anche se la versione 2.0 non fa esplicito riferimento alle API, i suoi requisiti influiscono notevolmente sulla protezione e sulla gestione delle API perché sono parte integrante del funzionamento di molti servizi digitali nelle organizzazioni che sono soggette alla direttiva. È importante notare che la NIS2 include:

- Un numero più vasto di settori, ad esempio, sono stati aggiunti all'elenco esistente provider di servizi cloud e aziende di social media, inclusi operatori di infrastrutture critiche. Per questi settori, in cui le API sono ampiamente usate per l'integrazione e la delivery dei servizi, è fondamentale garantire la sicurezza delle API.
- Una nuova enfasi sulla protezione delle supply chain: le aziende devono valutare i rischi e proteggere le proprie supply chain IT, nonché le loro relazioni con i fornitori di terze parti. Poiché le API vengono spesso usate per integrare i servizi esterni, garantire la loro sicurezza è fondamentale per rispettare i requisiti di conformità.
- Un requisito che impone di realizzare un sistema di gestione della sicurezza delle informazioni per valutare le persone, le policy e gli strumenti tecnologici necessari per proteggere le risorse sensibili e per garantire la resilienza operativa. Poiché le API sono vettori di attacco in rapida crescita, devono essere incluse nelle strategie di gestione dei rischi.
- La segnalazione di incidenti di cybersicurezza significativi, incluse le violazioni delle API. Pertanto, le organizzazioni devono mettere in atto meccanismi tali da monitorare, rilevare e segnalare gli incidenti relativi alle API.

6. Linee guida per gli enti di controllo dei servizi finanziari negli Stati Uniti

Il FFIEC (Federal Financial Institutions Examination Council) si occupa di stilare le linee guida e gli standard adottati dagli enti di controllo statunitensi per vigilare sul settore finanziario negli Stati Uniti, tra cui il Federal Reserve, il FDIC, l'OCC e il NCUA. Il Consiglio si propone di proteggere clienti e investitori da frodi, abusi e atti di cattiva condotta. Anche se non si tratta di normative, le linee guida del FFIEC sono fondamentali per garantire alle società finanziarie di sapere come allinearsi alle sue misure di sicurezza consigliate.

Di seguito viene riportato un esempio di un documento che include specifiche linee guida sulla protezione delle API e, a sua volta, su come proteggere i consumatori dalle frodi e dal furto di identità. Ecco una panoramica:

- **Inventario:** il FFIEC consiglia alle aziende di stilare un inventario di tutti i sistemi informativi (incluse le API) che richiedono controlli di autenticazione e accesso. Questo requisito si applica non solo alle istituzioni finanziarie, ma anche alle loro terze parti, come i provider di servizi cloud.
- **Autenticazione:** le API devono consentire l'accesso solo agli utenti autorizzati. È cruciale identificare tutti gli utenti (ad es., i clienti) per i quali è necessario controllare l'accesso. Inoltre, è importante identificare gli utenti che garantiscono controlli avanzati, come l'autenticazione multifattore.
- **Autorizzazione:** le API devono consentire l'accesso solo a specifiche risorse per gli utenti autorizzati. Ecco perché il FFIEC consiglia di implementare una sicurezza stratificata, ad esempio, monitorando, registrando e generando rapporti sulle attività necessarie per identificare e tenere traccia degli accessi non autorizzati.
- **Gestione dei rischi:** sono numerose le pratiche riportate dal FFIEC nelle sue ultime linee guida che consentono un'efficace gestione dei rischi, ma che fanno esplicitamente riferimento alle API nella categoria relativa all'inventario dei sistemi informativi da stilare, pertanto, in modo accurato.

Un'organizzazione potrebbe essere a regime sulle minacce ben note, come il phishing o il ransomware, ma il FFIEC richiede di identificare *qualsiasi* minaccia informatica con una ragionevole probabilità di influire sui sistemi informativi delle istituzioni finanziarie e sui loro dati. Come già detto nell'introduzione, il 78% delle organizzazioni ha subito incidenti relativi alla sicurezza delle API, pertanto la protezione delle API può essere considerata imprescindibile per raggiungere la conformità vista la continua evoluzione dei requisiti previsti dagli enti di controllo finanziari.

Soddisfare i requisiti di conformità con le best practice per la protezione delle API

L'odierno panorama delle minacce richiede una soluzione completa per la sicurezza delle API in grado di fornire funzioni di individuazione, gestione dei sistemi, protezione del runtime e test della sicurezza delle API. Questo approccio a 360° completa qualsiasi soluzione WAF o gateway API già implementati.

1. Individuazione delle API

Spesso, non si conoscono tutte le API di cui si dispone. La maggior parte delle organizzazioni ha poca (se non nessuna) visibilità sulla gran parte del traffico delle proprie API, spesso perché si dà per scontato che tutte le API vengano instradate tramite un gateway API. Eppure non è così. La vostra azienda è esposta ad una serie di rischi se non viene stilato un inventario completo e accurato. Queste sono le principali funzionalità richieste:

- Individuazione e creazione di un inventario delle API, indipendentemente dalla configurazione o dal tipo
- Rilevamento delle API inattive, tradizionali e zombie
- Identificazione dei domini ombra dimenticati, trascurati o non conosciuti
- Eliminazione dei punti ciechi e individuazione dei potenziali percorsi degli attacchi

2. Gestione del livello delle API

Dopo aver stilato un inventario completo delle API, è fondamentale capire quali tipi di dati vengono distribuiti tramite le API e come influiscono sulla vostra capacità di soddisfare i requisiti normativi. La gestione del livello delle API fornisce una visione completa sul traffico, sul codice e sulle configurazioni per poter valutare il livello di sicurezza delle API della vostra organizzazione. Queste sono le principali funzionalità richieste:

- Scansione automatica dell'infrastruttura per scoprire configurazioni errate e rischi nascosti
- Creazione di workflow personalizzati per informare le principali persone coinvolte circa le vulnerabilità
- Identificazione delle API e degli utenti interni che possono accedere ai dati sensibili
- Classificazione dei problemi rilevati in base ai livelli di gravità per dare priorità alla mitigazione

3. Sicurezza del runtime delle API

Sicuramente, avete già familiarità con il concetto di dover "presupporre una violazione". Le violazioni e gli attacchi specifici delle API stanno raggiungendo lo stesso grado di inevitabilità. Per tutte le vostre API attualmente in fase di produzione, dovete essere in grado di rilevare e bloccare gli attacchi in tempo reale. Queste sono le principali funzionalità richieste:

- Monitoraggio della manomissione e della fuga di dati, della violazione delle policy, del comportamento sospetto e degli attacchi alle API
- Analisi del traffico delle API senza apportare ulteriori modifiche alla rete o utilizzare agenti difficili da installare
- Integrazione con i workflow esistenti (creazione di ticket, SIEM, ecc.) per avvisare i team addetti alla sicurezza/operazioni
- Prevenzione degli attacchi e degli abusi in tempo reale con una mitigazione parzialmente o totalmente automatizzata

4. Test di sicurezza delle API

I team addetti allo sviluppo delle API sono sotto pressione perché devono lavorare il più rapidamente possibile. La velocità è essenziale per ogni applicazione sviluppata, il che rende più semplice il verificarsi di una vulnerabilità o un difetto di progettazione e, di conseguenza, più difficile che vengano rilevati. L'esecuzione di test sulle API in fase di sviluppo prima che entrino in produzione riduce notevolmente sia i rischi che i costi necessari per mitigare le loro vulnerabilità. Queste sono le principali funzionalità richieste:

- Esecuzione di un'ampia serie di test automatizzati che simulano il traffico dannoso
- Individuazione delle vulnerabilità prima che le API entrino in fase di produzione per ridurre il rischio di un attacco
- Verifica delle specifiche delle API sulla base delle regole e delle policy di governance stabilite
- Esecuzione di test sulla sicurezza delle API on-demand o come parte di una pipeline CI/CD

In che modo Akamai API Security può semplificare i problemi di conformità delle API

Le API sono la causa principale delle violazioni che le normative di oggi devono prevenire. Cosa serve per proteggere le aziende considerando il proliferare delle API e dei rischi correlati? Gli strumenti che molte organizzazioni usano attualmente per garantire una protezione basilare delle API forniscono un certo livello di sicurezza, ma non a sufficienza. Se cercate un modo migliore per proteggere le API della vostra organizzazione e per dimostrare la sua conformità, saremo lieti di aiutarvi.

Per le linee guida e i requisiti trattati in questo white paper, Akamai API Security rafforza la protezione necessaria alle aziende, non solo per rispettare le normative vigenti, ma anche per proteggere i dati e la fiducia dei clienti.

La soluzione completa di Akamai protegge le API in tutte le loro fasi, dallo sviluppo iniziale fino alla post-produzione, offrendovi la possibilità di aderire alle principali best practice:

- Individuazione delle API
- Gestione dei sistemi
- Protezione del runtime
- Test sulla sicurezza

Scoprite ulteriori informazioni sulle API e su come proteggerle dagli attacchi**.**

Scoprite come Akamai API Security può aiutare la vostra organizzazione**.**

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 prevenire, rilevare e mitigare le minacce informatiche in ambienti ransomware 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: 09/24.