Akamai

WHITE PAPER

La sicurezza delle API nell'ecosistema dell'open banking

Bilanciare innovazione e sicurezza per le banche europee nell'era del digitale

Analisi riassuntiva

Nel 2023, le banche dell'area EMEA (Europa, Medio Oriente e Africa) hanno registrato una notevole redditività e per il prossimo anno si prevede lo stesso trend. Le API (Application Programming Interface), che costituiscono il 31% di tutto il traffico web, sono state determinanti in questa crescita poiché hanno facilitato vari servizi, come le operazioni bancarie, il deposito di assegni da remoto e gli sportelli bancomat assistiti da GPS, insieme ad altri servizi di terze parti. La rapida adozione delle API ha, tuttavia, ampliato lo scenario delle minacce informatiche, richiedendo alle istituzioni finanziarie di investire in modo sostanziale nella cybersicurezza.

La direttiva rivista relativa ai servizi di pagamento (PSD2) dell'Unione europea e l'attesa PSD3 hanno svolto un ruolo cruciale nel dare forma allo scambio di dati tra le banche tradizionali e le società di tecnofinanza. Gli standard RTS (Regulatory Technical Standard) impongono un utilizzo sicuro delle API, incorporando un solido meccanismo di autenticazione dei clienti (SCA) e standard di comunicazione comuni e aperti (SCA-RTS). La direttiva PSD2, anche se principalmente focalizzata sui pagamenti, ha favorito l'utilizzo del termine "open banking" nel Regno Unito, ribadendo l'importanza della condivisione dei dati dei conti bancari dei clienti che ne hanno fornito l'autorizzazione e aprendo la strada a soluzioni di "open finance" più complete, il cui fulcro è rappresentato proprio dalle API.

Favorita dalle API, la trasformazione digitale in atto nei servizi finanziari dell'area EMEA mette in evidenza l'adattabilità di questo settore e l'impegno volto a soddisfare le esigenze dei clienti in continua evoluzione. Tuttavia, nel corso di questa trasformazione è essenziale vigilare per rafforzare la cybersicurezza, risolvere eventuali vulnerabilità e garantire che i vantaggi dell'innovazione digitale prevalgano sull'onnipresente minaccia degli attacchi informatici. McKinsey riferisce che alcune banche importanti stanno pensando di investire il 14% dei loro budget in programmi per le API, riflettendo l'attuale impennata nell'utilizzo delle API e richiedendo notevoli investimenti in cybersicurezza. Le istituzioni finanziarie ora danno priorità alla salvaguardia dei loro sistemi interni e alla protezione delle risorse e dei dati dei clienti con una particolare attenzione rivolta al rilevamento delle minacce, alle strategie di risposta e alla collaborazione per contrastare i rischi informatici in modo efficace.

La crescente importanza delle API

L'area EMEA è interessata da una rivoluzione digitale basata sul desiderio di fornire servizi e prodotti più efficienti e personalizzati ai clienti dei servizi finanziari. Le API svolgono un ruolo cruciale poiché offrono livelli impareggiabili di convenienza, velocità e sicurezza ai clienti che accedono ai prodotti bancari. Inoltre, le API consentono alle applicazioni di terze parti di connettersi con gli strumenti, i servizi e le risorse più importanti delle banche al fine di semplificare le connessioni per entrambe le parti. I clienti ora possono usufruire dei vantaggi offerti da un'ampia gamma di attività finanziarie, che ha trasformato le customer experience e spinto il settore finanziario verso l'era del digitale. Le API, da semplici strumenti di comunicazione, sono diventate la colonna portante del traffico Internet, supportando varie applicazioni.

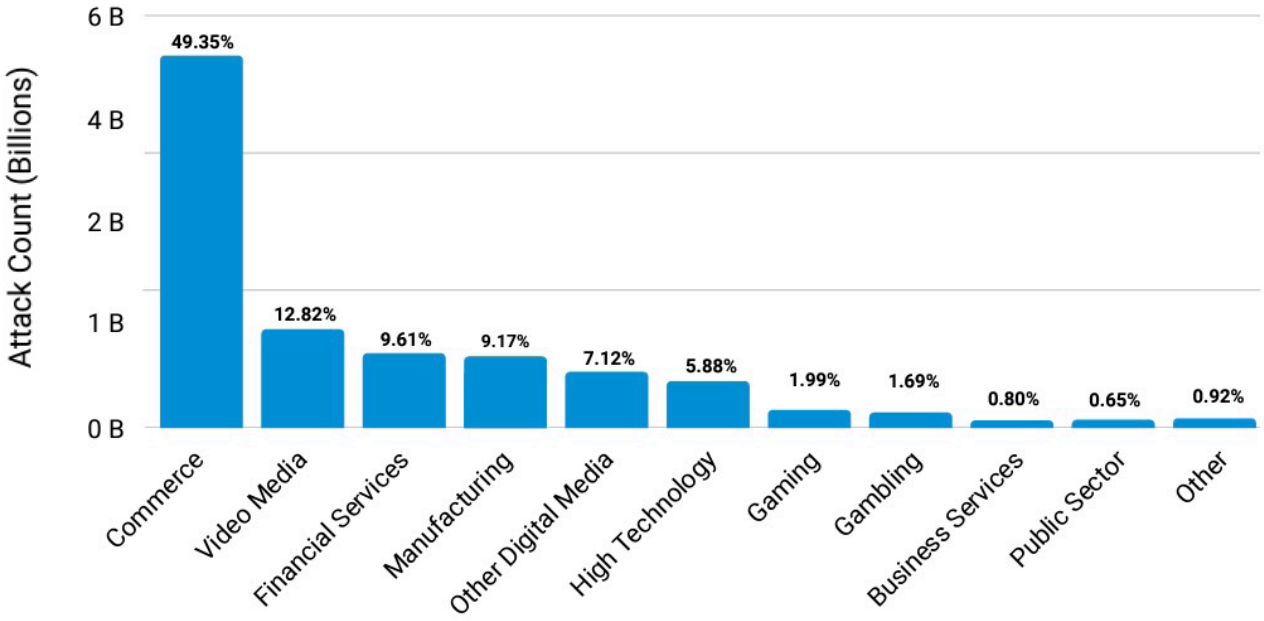
Secondo Allied Market Research, il mercato dell'open banking in Europa ha raggiunto i 6,14 miliardi di dollari nel 2020 e si prevede che arriverà a toccare i 48,30 miliardi di dollari entro il 2030 con un tasso di crescita annuale composito del 23,18% dal 2021 al 2030. Questa adozione viene accelerata da iniziative come l'Open Bank Project, gestita dalla TESOBE con sede a Berlino. Collaborando con più di 40 banche a livello globale, l'Open Bank Project consente alle banche di offrire ai propri clienti app e servizi di terze parti tramite uno store di app e API aperte. In Francia, il consolidamento dell'API STET, fornita dal centro di smistamento STET (Systèmes technologiques d'échange et de traitement), agevola l'implementazione dei pagamenti dell'open banking. Le API sono all'avanguardia nel rapido rimodellamento dello scenario finanziario che caratterizza l'area EMEA e il resto del mondo.

Le minacce correlate alle API nell'area EMEA

I servizi finanziari risultano il terzo settore maggiormente preso di mira nell'area EMEA poiché hanno subito quasi il 10% dell'elevato numero di attacchi alle applicazioni web e alle API registrati tra gennaio 2022 e giugno 2023. Questo dato si traduce in 1 miliardo di attacchi web su un totale di 11 miliardi di attacchi sferrati contro tutti i settori nell'area EMEA, che ha registrato un aumento significativo del 119% su base annua tra il 2° trimestre 2022 e lo stesso periodo del 2023. Analizzando la situazione in maggior dettaglio, riscontriamo che il Regno Unito è stato il paese maggiormente colpito con un 59,2% di attacchi alle applicazioni web, facendo registrare la crescita annua più elevata pari al 79%, seguito dai Paesi Bassi (16,2%) e dalla Germania (10,7%).

EMEA: i principali settori verticali colpiti dagli attacchi alle applicazioni web e alle API

1° gennaio 2022 - 30 giugno 2023



I servizi finanziari sono il terzo settore verticale più colpito dagli attacchi nell'area EMEA

I principali rischi per la sicurezza delle API

Le API sono potenzialmente vulnerabili ad un'ampia gamma di rischi di sicurezza, il che può condurre a violazioni di dati, accessi non autorizzati e altre forme di abusi. Tra i principali rischi per la sicurezza delle API, figurano le API ombra, la vulnerabilità e l'abuso delle API, la condivisione eccessiva di informazioni sensibili e gli attacchi di credential stuffing.

- **API ombra.** Molte istituzioni finanziarie non dispongono di un team o di una persona responsabile della gestione di tutte le API. Questa mancanza di supervisione crea una notevole falla nella sicurezza. Il rilevamento e la classificazione delle API all'interno di un'organizzazione è fondamentale per la loro gestione e la loro protezione. Inoltre, è importante colmare il divario esistente tra sviluppatori e team addetti alla sicurezza rilevando le API ombra nel proprio ambiente. Questo rilevamento continuo consente di essere sempre aggiornati sulle nuove API o sulle modifiche apportate a quelle esistenti in modo da poter eliminare le API ombra.

- **Vulnerabilità delle API.** Una volta rilevate le API, le istituzioni finanziarie devono valutare il loro livello di rischio e identificare eventuali vulnerabilità, soprattutto per le API che contengono dati sensibili. Questo passaggio è vitale per dare priorità alla sicurezza in modo efficace.

- **Abuso delle API.** Con l'incremento della digitalizzazione, il numero di attacchi alle applicazioni web nell'area EMEA continua ad aumentare. I criminali prendono incessantemente di mira le API, richiedendo solide misure di sicurezza per contrastarne l'abuso e l'utilizzo improprio.

- **Condivisione eccessiva di informazioni sensibili.** Le app moderne spesso condividono i dati sensibili in modo eccessivo, offrendo nuovi vettori di attacco. I criminali possono intercettare il traffico e ottenere un accesso non autorizzato alle informazioni sensibili.

- **Attacchi di credential stuffing.** Le API vengono utilizzate dai criminali per automatizzare gli attacchi di credential stuffing sferrati contro le istituzioni finanziarie.

Le sfide alla sicurezza delle API

Inventario delle API

Secondo un recente sondaggio SANS, l'inventario delle API rimane cruciale per le istituzioni finanziarie, che potrebbero non conoscere tutte le API presenti all'interno della loro infrastruttura, creando un punto cieco in termini di governance e sicurezza. Questa mancanza di visibilità può rappresentare uno dei fattori principali che spesso contribuiscono ad evitare il rilevamento e la segnalazione degli attacchi alle API. Per proteggere le API, è necessario innanzitutto rilevarle e classificarle in modo completo.

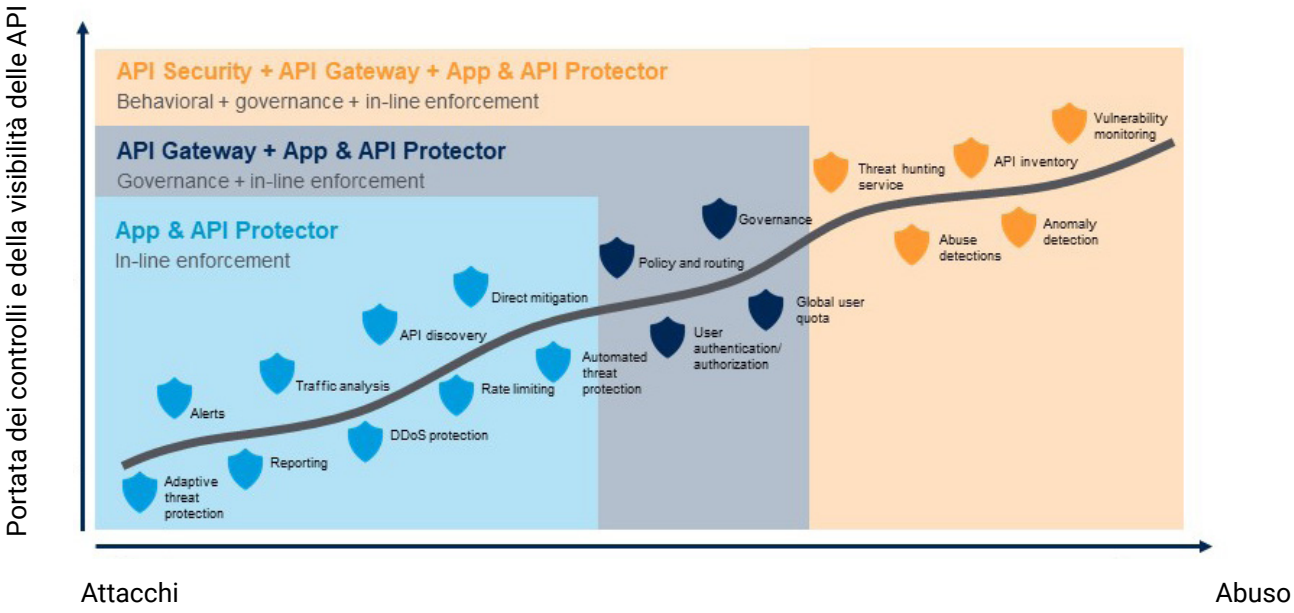
L'impatto di attacchi alle API devastanti

L'interruzione della disponibilità di applicazioni web e API può influire notevolmente sulla soddisfazione dei clienti e sulla fedeltà al brand. Con la crescente adozione di un approccio principalmente digitale, le API sono diventate ancora più importanti per il successo delle istituzioni finanziarie, specialmente nel caso dell'open banking adottato dalle società di tecnofinanza e dalle banche tradizionali.

La rapida crescita nel traffico delle API

Il traffico delle API nel settore finanziario è stato interessato da una rapida crescita con un volume addirittura triplicato. Questa crescita mette alla prova i controlli di sicurezza che devono tenersi al passo con lo scenario delle minacce alle API in continua evoluzione.

Attacchi alle API in continua evoluzione



Normative e sicurezza

Le istituzioni finanziarie che sfruttano la potenza delle API e di altre tecnologie innovative si trovano al crocevia tra gli obiettivi delle policy pubbliche e quelli della stabilità finanziaria. Il ruolo importante svolto dalle API nel migliorare gli obiettivi dei clienti le ha rese il metodo predefinito per la connettività e lo scambio di dati all'interno dei moderni ambienti dei servizi finanziari e questa tendenza continuerà anche in futuro. Gli obiettivi principali consistono nell'espandere la gamma delle opzioni finanziarie, favorire la competizione e l'accessibilità, oltre a promuovere l'inclusione finanziaria. Gli organismi di regolamentazione nell'area EMEA si impegnano nell'intento di ampliare la portata dei servizi finanziari a vantaggio dei singoli clienti e delle organizzazioni.

Il ruolo delle normative nella sicurezza delle API

Le normative del settore, come la direttiva PSD2 (e, presto, la PSD3), promuovono la trasparenza richiedendo alle istituzioni tradizionali di dare priorità alla sicurezza e alla privacy degli utenti durante la condivisione dei loro dati con entità esterne. Le istituzioni finanziarie devono ottemperare a queste normative, continuando a perseguire attivamente l'innovazione.

Anche se promuovono la condivisione dei dati, queste normative stabiliscono, inoltre, come le organizzazioni devono archiviare e salvaguardare tali dati. Le istituzioni finanziarie devono disporre di un partner tecnologico in grado di garantire la conformità normativa senza ostacolare il loro percorso verso l'innovazione e di risolvere eventuali problemi relativi alla qualità delle API fornendo alle autorità gli strumenti necessari per far valutare le interfacce API dedicate alle banche e ad altre entità finanziarie.

Secondo l'Autorità bancaria europea (EBA), "l'esperienza acquisita dall'implementazione della direttiva PSD2 evidenzia l'assenza di un unico standard per le API, determinando l'esistenza di varie soluzioni per le API nell'Unione europea. Questo aspetto pone enormi problemi per i fornitori di servizi di terze parti, che devono impegnarsi notevolmente nell'intento di connettersi alle API di vari ASPSP (Account Servicing Payment Service Provider) e adattare le connessioni alle API in continua evoluzione". La speranza è che la nuova PSD3 farà tesoro delle lezioni apprese dalla direttiva PSD2.

I 6 passaggi utili per creare una solida strategia di sicurezza delle API

La strategia di prevenzione degli attacchi basati sulle API tramite la protezione degli endpoint e il controllo delle credenziali non è più sufficiente. Oggi, una solida strategia per la sicurezza delle API deve includere i sei passaggi riportati di seguito.

1. Collaborazione con i partner

Le istituzioni finanziarie e i loro partner dei servizi di sicurezza devono lavorare a stretto contatto, sincronizzando persone, processi e tecnologie, al fine di stabilire una solida difesa contro i rischi che minacciano la sicurezza delle API, tra cui i team addetti allo sviluppo, alle operazioni di sicurezza e rete e alla gestione delle identità, i responsabili dei rischi, gli architetti della sicurezza e i team addetti alla questioni di conformità/legali.

2. Rilevamento e classificazione delle API

Per proteggere le API, è necessario innanzitutto rilevarle e classificarle all'interno dell'organizzazione. Questo processo consente ai tecnici addetti alla sicurezza di comprendere la portata della superficie di attacco e la potenziale esposizione delle informazioni sensibili.

3. Test delle vulnerabilità e valutazione dei rischi

Una volta rilevate le API, le istituzioni finanziarie devono eseguire i test delle vulnerabilità e la valutazione dei rischi per identificare e risolvere eventuali vulnerabilità in modo tempestivo. Questo processo deve essere integrato nello sviluppo e nell'aggiornamento delle API per garantire una sicurezza costante.

4. Implementazione del rilevamento dei comportamenti

I sistemi di protezione delle API sono componenti fondamentali della struttura complessiva di sicurezza delle applicazioni. Il rilevamento dei comportamento è una strategia chiave per impedire lo sfruttamento delle API vulnerabili. Questo approccio implica il monitoraggio e l'analisi dei comportamenti delle API in modo costante per identificare le potenziali minacce.

5. Priorità ai controlli dei 10 principali rischi di sicurezza delle API riportati nell'elenco OWASP

Per garantire una protezione completa, le istituzioni finanziarie devono dare priorità ai controlli dei 10 principali rischi di sicurezza delle API riportati nell'elenco OWASP (Open Worldwide Application Security Project), che riguardano le vulnerabilità e i vettori di attacco più importanti a livello delle API.

OWASP API Top 10 coverage by Akamai

- ☑ **API1:2023 — Broken Object Level Authorization:** BOLA vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs.
- ☑ **API2:2023 — Broken Authentication:** BA refers to broad vulnerabilities in the authentication process, exposing the system to attackers that can exploit these weaknesses to compromise API object protection.
- ☑ **API3:2023 — Broken Object Property Level Authorization:** BOPLA is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.
- ☑ **API4:2023 — Unrestricted Resource Consumption:** This is a type of vulnerability, sometimes called API resource exhaustion, where APIs do not limit the number of requests or the volume of data they serve within a given time.
- ☑ **API5:2023 — Broken Function Level Authorization:** BFLA can occur when access control models for API endpoints are incorrectly implemented.
- ☑ **API6:2023 — Unrestricted Access to Sensitive Business Flows:** This risk arises when an API exposes critical operations like business logic without sufficient access control.
- ☑ **API7:2023 — Server Side Request Forgery:** SSRF allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing.
- ☑ **API8:2023 — Security Misconfiguration:** This refers to the improper setup of security controls, which can leave a system vulnerable to attacks.
- ☑ **API9:2023 — Improper Inventory Management:** This is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including deprecated, legacy, and/or outdated APIs — may be left unpatched and vulnerable to attack.
- ☑ **API10:2023 — Unsafe Consumption of APIs:** This refers to the risks associated with the use of third-party APIs without putting proper security measures in place.

6. Acquisizione delle conoscenze del settore

Le istituzioni finanziarie devono imparare da altre aziende dello stesso settore e condividere le best practice acquisite. L'iscrizione al Financial Services Information Sharing and Analysis Center (FS-ISAC) consente alle istituzioni finanziarie di sfruttare la loro piattaforma di intelligence, le loro risorse e un'affidabile rete di esperti del settore per prevedere, mitigare e rispondere alle minacce informatiche. Comprendere chiaramente come altre organizzazioni hanno risolto i problemi di sicurezza delle API può aiutare a migliorare le misure di sicurezza dell'intero settore.

Conclusione

In questa epoca caratterizzata da una rapida trasformazione digitale e da una diffusa adozione delle API, progettata per facilitare un'integrazione flessibile, veloce e vantaggiosa in termini di costi in un'ampia gamma di software, dispositivi e origini dati, la salvaguardia delle API assume un'importanza fondamentale per le istituzioni finanziarie dell'area EMEA. In ogni caso, la sicurezza delle API implica un complesso sistema di equilibri tra varie funzionalità, funzioni e richieste aziendali. Trascurare la sicurezza delle API può condurre a severe conseguenze, tra cui attacchi informatici, violazioni di dati, infrazione delle normative e danni alla reputazione di un'istituzione.

Dai nostri dati emerge che le funzionalità delle API sono tra i principali obiettivi dei criminali che evolvono e adattano continuamente i loro metodi di attacco. Pertanto, è indispensabile trasferire il sistema di sicurezza delle API sull'edge, spostandolo dall'infrastruttura di un'organizzazione e avvicinandolo ai punti di contatto digitali in cui i clienti interagiscono con dati e applicazioni. Questa svolta strategica è cruciale per garantire una solida protezione delle risorse digitali.

Scoprite ulteriori informazioni sulle funzionalità di Akamai per i servizi finanziari. In alternativa, potete contattare Akamai per discutere ulteriormente su questo approccio e su come applicarlo alla vostra organizzazione.

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: 01/24.