STUDIO SULL'IMPATTO DELLA SICUREZZA DELLE API 2024:

il settore dei servizi finanziari

In un periodo in cui si registra un aumento degli attacchi alle API, scoprite come il settore dei servizi finanziari sta affrontando questo problema di sicurezza e cosa può fare la vostra organizzazione per proteggersi.

L'anno scorso, l'88,7% delle società di servizi finanziari ha subito un attacco alle API che gestiscono i loro dati aziendali e che connettono clienti e partner ai servizi più importanti. Utilizzando metodi sempre più innovativi, i criminali possono accedere ai dati presenti nelle API non protette per rubare informazioni personali e finanziarie, inclusi gli estratti conto e le cronologie delle transazioni.

I team addetti alla sicurezza sono consapevoli dell'impatto esercitato da questa situazione e cercano nuovi modi per migliorare le proprie contromisure. Tuttavia, affrontare un altro vettore di attacco può sembrare scoraggiante, specialmente se sferrato contro le API, i cui errori di configurazione o difetti alla logica aziendale possono essere facilmente individuati e sfruttati.

E come facciamo a saperlo? Akamai ha condotto un sondaggio su oltre 1200 professionisti del settore IT e della sicurezza, dai CISO (Chief Information Security Officer) al personale addetto alla sicurezza delle applicazioni, per sapere come affrontano le minacce correlate alle API.

In questo articolo, abbiamo esaminato i risultati del nostro sondaggio condotto sul settore dei servizi finanziari, in cui i partecipanti hanno affermato che le prime conseguenze dei problemi di sicurezza delle loro API sono state "le sanzioni imposte dagli enti di controllo" e "l'aumento dello stress e/o la pressione esercitata sul mio team/reparto". Queste conseguenze intercorrelate sono semplici da comprendere se si considera che i partecipanti al sondaggio hanno riferito di aver speso 832.800 dollari per risolvere i problemi legati alle API: una percentuale del 40% superiore alla media di tutti gli otto settori oggetto del sondaggio e più alta rispetto a quella di ogni altro settore.

Continuate a leggere per ulteriori approfondimenti di settore tratti dallo studio sull'impatto della sicurezza delle API 2024.

La visibilità in declino con l'aumento degli attacchi

Mentre l'84% delle organizzazioni di vari settori ha riscontrato problemi di sicurezza delle API, le società di servizi finanziari sono state prese di mira più frequentemente rispetto alla media degli altri settori (88,7%). I partecipanti al nostro sondaggio hanno identificato due principali vulnerabilità che favoriscono questi attacchi: i firewall di rete, che non riescono a bloccare le minacce (26,5%), e le vulnerabilità interne alle API negli strumenti basati sull'AI generativa, come i grandi modelli linguistici (LLM) (23,2%).

Nonostante le minacce alle API siano sempre più evidenti, dai problemi frequenti agli elevati costi legati alla mitigazione e alle sanzioni normative, dai risultati del nostro sondaggio emerge come molti team che operano nei servizi finanziari non considerano ancora la sicurezza delle API una delle loro priorità principali. Infatti, la sicurezza delle API risulta al nono posto tra le priorità in termini di cybersecurity per l'anno prossimo (18,5%).

Distinguere tra le attività legittime delle API e quelle fraudolente rimane problematico per il settore finanziario, in particolare quando si tratta di visibilità sui numerosi rischi per le API. Mentre il 73,5% dei partecipanti al nostro sondaggio ha affermato di disporre di un inventario completo delle loro API, solo il 28,5% di questo sottogruppo sa quali API restituiscono dati sensibili, incluse informazioni di identificazione personale (PII) e dati di vario tipo, dalla cronologia delle transazioni effettuate dai titolari di carte di credito ai record finanziari dei clienti di grandi banche commerciali.

L'88,7% delle società di servizi finanziari ha riscontrato un problema di sicurezza delle API negli ultimi 12 mesi

Solo il 28,5% delle società di servizi finanziari con un inventario completo delle API sa quali API restituiscono dati sensibili

832.800 dollari = l'impatto finanziario esercitato dai problemi di sicurezza delle API negli ultimi 12 mesi sulle società di servizi finanziari

Le prime 3 conseguenze

1. **Più stress e/o pressione** sui team addetti alla sicurezza
2. **Sanzioni imposte** dagli enti di controllo
3. **Perdita di fiducia** e reputazione

Fonte:
Akamai, "Studio sull'impatto della sicurezza delle API", 2024

Akamai

Considerate ciò che potrebbe succedere ad un'API ombra implementata da un reparto o una filiale di un provider di servizi finanziari senza la collaborazione o la supervisione dei team addetti alla sicurezza o del reparto IT centrale della società. In questo caso, l'API potrebbe essere stata:

- Progettata per restituire i dati relativi alle transazioni dei clienti senza appropriati controlli di autorizzazione e non adeguatamente testata per individuare eventuali errori di configurazione
- Sostituita da una nuova versione, ma non disattivata e, pertanto, resa visibile su Internet
- Nascosta al rilevamento degli strumenti tradizionali che non riescono ad individuare le API non gestite
- Sfruttata dai criminali informatici che accedono agli account dei clienti reali per rubare le loro risorse

Non si tratta meramente di un'ipotesi. Secondo lo studio LexisNexis® Risk Solutions 2023 True Cost of Fraud™, il 50% delle perdite dovute a frodi è da attribuire all'abuso dell'apertura di nuovi account, in cui i criminali violano le API per aprire account su larga scala. Inoltre, il nostro caso riflette ciò che i professionisti del settore IT e della sicurezza citano come le principali cause dei problemi delle API che hanno riscontrato.

In che modo i problemi delle API influiscono sulla conformità, sui costi aziendali e sullo stress dei team

"Dalle statistiche attuali, è emerso che una violazione delle API provoca, in media, la fuga di un numero di dati almeno 10 volte superiore a quello di una comune violazione di sicurezza", secondo la guida di settore per la protezione delle API di Gartner® pubblicata a maggio 2024*. Ecco perché, giustamente, nelle normative dello standard PCI DSS v4.0, ampiamente diffuso, sono stati aggiunti nuovi requisiti relativi alla sicurezza delle API. Questo standard ora richiede alle organizzazioni di verificare il codice delle loro API prima del rilascio, di eseguire regolarmente test sulle vulnerabilità e di utilizzare i componenti basati sulle API in modo sicuro: un approccio particolarmente importante in un settore in cui le API semplificano l'esecuzione di milioni di transazioni finanziarie ogni giorno.

La perdita di fiducia da parte degli enti di controllo può determinare un aumento delle verifiche, con nuovi carichi di lavoro per i team già sotto pressione, al fine di soddisfare le richieste di conformità ed evitare pesanti sanzioni.

È chiaro, quindi, che le società di servizi finanziari sono perfettamente consapevoli delle conseguenze causate dalle minacce alle API. Per la prima volta, abbiamo chiesto ai partecipanti al nostro sondaggio che risiedono in tre diversi paesi di condividere le loro opinioni sull'impatto finanziario esercitato dai problemi di sicurezza delle API da loro riscontrati negli ultimi 12 mesi.

	Settore dei servizi finanziari	Media di tutti i settori
Stati Uniti	$ 832.800	$ 591.404
Regno Unito	£ 297.189	£ 420.103
Germania	€ 604.405	€ 403.453

D3. Quale ritenete sia l'impatto finanziario esercitato nel complesso dai problemi di sicurezza delle API che avete riscontrato? (inclusi tutti i costi correlati, come riparazione dei sistemi, problemi di downtime, spese legali, sanzioni e altre spese associate)

* Guida di settore per la protezione delle API di Gartner, 29 maggio 2024. GARTNER è un marchio registrato e un marchio commerciale di Gartner, Inc. e/o delle sue società affiliate negli Stati Uniti e a livello internazionale, che viene usato previa autorizzazione. Tutti i diritti riservati.

Ridurre rischi e stress con una sicurezza proattiva delle API

Gli attacchi alle API sferrati contro le società di servizi finanziari sono sempre più mirati, scalabili, sofisticati e costosi, come gli attacchi di bot basati sull'AI generativa, capaci di adattarsi rapidamente in modo da bypassare i tradizionali strumenti di sicurezza delle API e altri sistemi di difesa del perimetro. Molti team addetti alla sicurezza che operano nel vostro settore subiscono queste minacce direttamente e ne risentono delle conseguenze sia da un punto di vista finanziario che umano. Tuttavia, anche se le organizzazioni capiscono l'importanza delle minacce per le API, devono comunque rispondere a questa domanda: Che fare?

Adottare le misure necessarie a proteggere le API e i loro dati può consentire alle organizzazioni di garantire il proprio fatturato e di alleggerire il carico dei team addetti alla sicurezza, preservando, al contempo, la fiducia duramente conquistata dei membri del consiglio di amministrazione e dei clienti grazie anche alle competenze sulle avanzate minacce alle API acquisite dal vostro team e alle funzionalità che vi servono per difendervi da questi attacchi.

Per leggere il rapporto completo e scoprire le best practice da adottare per migliorare la visibilità e la protezione delle API, potete scaricare lo **studio sull'impatto della sicurezza delle API 2024**.

Desiderate discutere dei vostri problemi e di come Akamai può aiutarvi?

Richiedete una demo personalizzata su Akamai API Security

Akamai offre soluzioni progettate per aiutare le organizzazioni a ridurre i rischi relativi alle minacce discusse in questo articolo:

- Akamai API Security, che individua le API, valuta il loro livello di rischio, analizza il loro comportamento e impedisce alle minacce di infiltrarsi nelle vostre attività aziendali
- Akamai Account Protector, che aiuta a prevenire gli abusi dell'apertura degli account monitorando il comportamento degli utenti in tempo reale e adattandosi ai mutevoli profili di rischio

Akamai

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 in modo che 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 e LinkedIn. Data di pubblicazione: 03/25.