

Il settore del retail e dell'e-commerce

Strategie adottate dai vostri colleghi nell'affrontare le crescenti minacce per le API

Le API su cui si basano i progetti digitali delle aziende che operano nel settore del retail e dell'e-commerce sono ormai diventate un bersaglio privilegiato degli attacchi. Tramite metodi sempre più innovativi, i criminali riescono ad accedere alle informazioni presenti nelle API non protette allo scopo di rubare i dati delle carte di credito, depredate i programmi fedeltà, sferrare attacchi di credential stuffing e molto altro. I team addetti alla sicurezza sono consapevoli dell'impatto che ne consegue e cercano nuovi modi per migliorare le proprie contromisure. Tuttavia, affrontare l'ennesimo vettore di attacco può essere scoraggiante, specialmente quando viene sferrato contro le API, i cui errori di configurazione o le cui falle nella logica aziendale restano una vulnerabilità.

Come facciamo a saperlo? Akamai ha condotto un sondaggio su oltre 1.200 professionisti del settore IT e della sicurezza, dai CISO al personale AppSec, per sapere come affrontano le minacce correlate alle API.

Questa panoramica esamina i risultati emersi dal nostro sondaggio, in cui il 68% dei partecipanti ha riferito di aver riscontrato problemi di sicurezza delle API negli ultimi 12 mesi. Quali sono state le conseguenze di questi problemi? Dalle risposte fornite dai vostri colleghi, risulta che le principali conseguenze siano i crescenti livelli di stress dei team e i danni alla credibilità di dirigenti e membri del consiglio di amministrazione. Sono dati che non stupiscono, considerando che, a detta dei professionisti del settore del retail e dell'e-commerce, i costi legati ai problemi alle API ammontano a 526.531 dollari.

Per informazioni approfondite sul settore, potete consultare il rapporto [Studio sull'impatto della sicurezza delle API 2024](#).

Gli attacchi aumentano, ma la visibilità cala

Mentre la stragrande maggioranza dei partecipanti al sondaggio che operano nel settore del retail e dell'e-commerce ha riscontrato problemi di sicurezza delle API, la loro media del 68% resta inferiore all'84% riportato negli otto settori esaminati. Nel contempo, le priorità in termini di sicurezza citate dai vostri colleghi per i prossimi 12 mesi sono la difesa dagli attacchi basati sull'AI generativa e la protezione delle API dai criminali.

Si possono prevenire gli attacchi assegnando la priorità alle API? I team addetti alla sicurezza delle società che operano nel settore dell'e-commerce e del retail sono probabilmente consapevoli dell'importanza della protezione delle API e della necessità di ridurre gli incidenti che le coinvolgono. Tuttavia, dai nostri risultati, emerge anche come questi team non abbiano una visibilità completa sui casi di abuso delle API.

Distinguere tra le attività delle API legittime e quelle dannose o fraudolente rimane una sfida per le società che operano nel settore dell'e-commerce e del retail. Anche riconoscere i rischi è complicato. Mentre il 67% dei vostri colleghi riferisce di disporre di un inventario completo delle API, *solo il 29%* di questo sottogruppo sa quali tra le loro innumerevoli API restituiscono dati sensibili, tra cui informazioni di identificazione personale (PII) o dati delle carte di credito.

Considerate ciò che potrebbe succedere ad un'API implementata da una business unit senza la collaborazione o la supervisione dei team addetti alla sicurezza o del reparto IT centrale di un retailer. L'API rischierebbe di essere:

- Progettata per restituire i dati 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 per accedere agli account di fidelizzazione e per riscattare i premi di clienti reali

Il **68%** delle società che operano nel settore del retail/e-commerce ha riscontrato un problema di sicurezza delle API negli ultimi 12 mesi¹

Solo il 29% delle società che operano nel settore del retail/e-commerce con un inventario completo delle API sa quali API restituiscono dati sensibili¹

526.531 dollari = l'impatto finanziario esercitato dai problemi di sicurezza delle API negli ultimi 12 mesi sulle società che operano nel settore del retail/e-commerce¹

Le 3 conseguenze principali¹

1. **Più stress** e/o pressione sui team
2. **Costi sostenuti** per risolvere il problema
3. **Danni alla reputazione del reparto**, nonché di dirigenti e/o membri del consiglio di amministrazione

Il **44%** degli attacchi web sferrati contro le organizzazioni commerciali ha preso di mira le API²

Fonti:

1. Akamai, "Studio sull'impatto della sicurezza delle API", 2024
2. Rapporto sullo stato di Internet (SOTI) di Akamai, dal titolo "Minacce in agguato: le tendenze degli attacchi fanno luce sulle minacce delle API", 2024



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 di apertura di nuovi account, per cui i criminali violano le API per aprire account su larga scala. Per non citare il fatto che un caso come quello sopra menzionato riflette uno scenario osservato di continuo nella vita reale dai professionisti del settore IT e della sicurezza.

Le principali cause alla base dei problemi delle API citate dai team addetti alla sicurezza nel settore del retail/e-commerce

1. API presenti negli strumenti basati sull'AI generativa, ad es., nei modelli LLM - **24,7%**
2. API con una visibilità imprevista su Internet - **24%**
3. Errori di configurazione delle API - **22%**
4. La soluzione WAF (Web Application Firewall) non è riuscita ad individuarli - **21,3%**
5. Il gateway API non è riuscito ad individuarli - **20,7%**
6. Vulnerabilità dovuta agli errori di codifica delle API - **20%**
7. Strumenti/Servizi tecnologici noti - **20%**
8. Il firewall di rete non è riuscito ad individuarli - **18,7%**
9. Vulnerabilità di autorizzazione - **17,3%**
10. Soluzioni software scaricate da Internet - **16,7%**
11. Mancanza di controlli di autenticazione delle API - **16%**
12. Soluzioni software di livello medio - **14,7%**
13. API non gestite, ad es., API zombie - **13,3%**




D. Quali ritenete siano le cause dei problemi di sicurezza delle API riscontrati dalla vostra organizzazione? (massimo 3 risposte) n=1.207

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 sicurezza³, secondo la guida di settore per la protezione delle API di Gartner® pubblicata a maggio 2024³. Ecco perché, giustamente, nelle normative dello standard PCI DSS v4.0, ampiamente diffuso, sono stati aggiunti nuovi requisiti relativi alla sicurezza delle API. Le aziende (e i relativi enti di controllo) devono sapere quali tipi di dati transitano non solo tramite le loro API, ma anche tramite quelle dei propri partner e fornitori, il che accresce le sfide relative alla gestione dei rischi di terzi nel settore dell'e-commerce.

La perdita di fiducia da parte degli enti di controllo può determinare un aumento delle verifiche, con nuovi carichi di lavoro per team già sotto pressione, al fine di soddisfare le richieste di conformità ed evitare pesanti sanzioni. Le società che operano nel settore del retail e dell'e-commerce sono quindi perfettamente consapevoli delle conseguenze finanziarie causate dalle minacce per le 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.

³ 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.

	Retail/E-commerce	Media di tutti i settori
 Stati Uniti	526.531 dollari	591.404 dollari
 Regno Unito	258.815 sterline	420.103 sterline
 Germania	348.467 euro	403.453 euro

D. 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, n=1.207)

Con un impatto finanziario notevole, i partecipanti al nostro sondaggio hanno affermato chiaramente che i costi hanno superato abbondantemente i ricavi ma, quando abbiamo chiesto di elencare le principali conseguenze causate dai problemi di sicurezza delle API, sono stati concordi nell'escludere i costi. I partecipanti al sondaggio che operano nel settore del retail e dell'e-commerce hanno sottolineato il prezzo pagato dalle persone: l'aumento dello stress e della pressione sui loro team.

Le 5 principali conseguenze dei problemi di sicurezza delle API per le società che operano nel settore del retail e dell'e-commerce

1. Incremento del livello di stress e/o pressione sui team/reparti - **28,7%**
2. Costi sostenuti per risolvere il problema - **28%**
3. Danni alla reputazione del reparto, nonché di dirigenti e/o membri del consiglio di amministrazione - **25,3%**
4. Incremento dei controlli interni del team/reparto da parte dell'azienda - **23,3%**
5. Sanzioni imposte dagli enti di controllo - **25,3%**

D. Quali costi e/o conseguenze ha subito la vostra azienda a causa dei problemi di sicurezza delle API? (massimo 3 risposte) n=1.207

Obiettivi futuri: ridurre rischi e stress con una sicurezza proattiva delle API

Gli attacchi alle API sferrati contro le società che operano nel settore del retail e dell'e-commerce sono sempre più mirati, scalabili e sofisticati, 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 sia da un punto di vista finanziario che umano. Tuttavia, anche se le organizzazioni capiscono l'importanza delle minacce per le API, restano di fronte a un quesito fondamentale. 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. Nell'ambito di queste operazioni, è necessario formare i team in merito alle avanzate minacce per le API e alle funzionalità con cui potete difendervi.



Per scoprire le best practice sulla visibilità e sulla protezione delle API, potete scaricare il rapporto **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 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 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](https://twitter.com) (in precedenza Twitter) e [LinkedIn](https://www.linkedin.com/company/akamai). Data di pubblicazione: 11/24.