

Settore assicurativo

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

Quando si verificano eventi catastrofici, come un incidente automobilistico o danni alle apparecchiature aziendali, i titolari delle polizze assicurative si affidano ai servizi digitali per inviare le richieste di rimborso e ricevere assistenza da parte delle loro compagnie di assicurazioni, le cui API devono gestire, nell'ambito di questi servizi, le informazioni sensibili che rappresentano la storia degli assicurati sotto forma di dati.

In un settore in cui la fiducia dei clienti è fondamentale, le aziende del settore assicurativo devono affrontare una sfida crescente per la sicurezza: le vulnerabilità delle API.

Secondo un esaustivo sondaggio condotto da Akamai, il 76,7% dei professionisti del settore assicurativo ha riferito di aver riscontrato problemi di sicurezza delle API negli ultimi 12 mesi, il cui impatto finanziario è stato notevole, dovendo affrontare, in media, una spesa di 625.634 dollari per risolvere questi problemi solo negli Stati Uniti.

Tuttavia, forse ciò che preoccupa maggiormente è l'impatto sulle aziende: la perdita di fiducia e l'elevato tasso di abbandono da parte dei clienti (28%) sono stati riconosciuti come le principali conseguenze dei problemi di sicurezza delle API dalle compagnie di assicurazioni. In un mercato competitivo in cui i clienti possono cambiare facilmente le loro compagnie di assicurazioni, questi danni alla reputazione possono avere effetti duraturi oltre ai costi immediati.

Continuate a leggere per ulteriori approfondimenti di settore tratti dallo [Studio sull'impatto della sicurezza delle API nel 2024](#).

Con l'aumento degli attacchi, la visibilità rimane una delle sfide principali

I costi finanziari legati agli attacchi alle API sono notevoli per le compagnie di assicurazioni: le spese, solo negli Stati Uniti (625.634 dollari), hanno superato la media registrata in diversi settori (591.404 dollari). Ma cosa sta favorendo questi problemi?

Secondo i team addetti alla sicurezza nel settore assicurativo, tra le cause principali, figurano le seguenti:

1. API non gestite, come API inattive o "zombie" (22%)
2. API visibili in modo imprevisto su Internet (21,3%)
3. Utilizzo di strumenti tradizionali per la protezione delle API che non riescono ad individuare le minacce (20%)
4. Vulnerabilità di autorizzazione (19,3%)
5. Errori di configurazione delle API (18,7%)

Molte organizzazioni sono consapevoli delle cause che favoriscono gli attacchi alle loro API, ma non dispongono della visibilità su un indicatore cruciale dei rischi correlati: la capacità delle API di restituire dati sensibili quando vengono chiamate. Mentre il 56,7% delle compagnie di assicurazioni riferisce di disporre di un inventario completo delle loro API (inferiore alla media registrata in diversi settori, pari al 69,7%), solo il 20,7% sa quali API restituiscono dati sensibili.

Questa lacuna nella visibilità influisce notevolmente sulla conformità e sulla sicurezza in un settore altamente regolamentato per il trattamento dei dati personali e finanziari.

Il 76,7% delle compagnie di assicurazioni ha riscontrato problemi di sicurezza delle API negli ultimi 12 mesi

Solo il 20,7% delle compagnie di assicurazioni con un inventario completo delle API sa quali API restituiscono dati sensibili

625.634 dollari = l'impatto finanziario esercitato dai problemi di sicurezza delle API sulle compagnie di assicurazioni negli ultimi 12 mesi

Le prime 3 conseguenze

1. **Perdita di fiducia ed elevato tasso di abbandono da parte dei clienti (28%)**
2. **Danni alla reputazione dei reparti, nonché dei dirigenti (25,3%)**
3. **Costi sostenuti per risolvere i problemi riscontrati (24,7%)**

Fonte:
Akamai, [Studio sull'impatto della sicurezza delle API, 2024](#)

Abbiamo osservato **varie tendenze** che rendono complicato proteggere le API:

- **Continua proliferazione delle API:** in ogni iniziativa digitale, le API si moltiplicano e si evolvono costantemente, rendendo difficile mantenere un inventario accurato.
- **Standard non coerenti:** molti assicuratori dispongono di più team addetti allo sviluppo che operano separatamente uno dall'altro nelle varie business unit senza una strategia centralizzata in grado di garantire una progettazione sicura.
- **Rischi invisibili:** le API trasmettono i dati sensibili degli assicurati, ma la maggior parte delle organizzazioni non riesce ad identificare quali API nello specifico restituiscono informazioni sensibili.

Considerate ciò che potrebbe succedere ad un'API implementata da un reparto senza un'adeguata supervisione del team addetto alla sicurezza. L'API in questione potrebbe essere stata progettata in modo da condividere i dati senza adeguati controlli o lasciata attiva dopo gli aggiornamenti di sistema, creando potenziali punti di esposizione per i dati sensibili dei clienti.

In che modo i problemi delle API influiscono sulla conformità, sulla fiducia dei clienti e sullo stress dei team

Non sorprende il fatto che le compagnie di assicurazioni siano perfettamente consapevoli delle conseguenze finanziarie causate dalle minacce alle API. Abbiamo chiesto ai partecipanti al nostro sondaggio di condividere le loro opinioni sui costi stimati dei problemi di sicurezza delle API da loro riscontrati negli ultimi 12 mesi:

	Settore assicurativo	Media di tutti i settori
 Stati Uniti	\$ 625.633,70	\$ 591.404,01
 Regno Unito	£ 493.000,50	£ 420.103,18
 Germania	€ 373.918,72	€ 403.453,26

Con un impatto finanziario notevole, i partecipanti al nostro sondaggio hanno affermato chiaramente che i costi sono stati determinati sia dai ricavi che dalle preoccupazioni relative alla reputazione. Quando abbiamo chiesto di elencare le principali conseguenze causate dai problemi di sicurezza delle API:

- Il 28% ha risposto: "La perdita di fiducia e l'elevato tasso di abbandono da parte dei clienti"
- Il 25,3% ha risposto: "I danni alla reputazione dei team, nonché di dirigenti e membri del consiglio di amministrazione"
- Il 24,7% ha risposto: "I costi sostenuti per risolvere i problemi riscontrati"

Ridurre rischi e stress con una sicurezza proattiva delle API

Gli attacchi alle API sferrati contro le compagnie di assicurazioni 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 in questo settore subiscono queste minacce direttamente e risentono delle conseguenze sia da un punto di vista finanziario che umano. Tuttavia, anche se le organizzazioni capiscono l'importanza delle minacce alle 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 salvaguardare 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 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 nel 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:** 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:** 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 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: 05/25.