STUDIO SULL'IMPATTO DELLA SICUREZZA DELLE API 2024

il settore sanitario

In un periodo in cui si registra un aumento degli attacchi alle API, scoprite come il settore sanitario sta affrontando le sfide legate alla sicurezza delle API e cosa potete fare per difendervi dalle minacce in continua evoluzione.

In un settore in cui la fiducia dei pazienti e dei membri del consiglio di amministrazione è fondamentale, le aziende sanitarie devono affrontare una sfida crescente per la sicurezza: le vulnerabilità delle API.

Le cartelle cliniche elettroniche, la telemedicina e i dispositivi medicali connessi sono diventati bersagli privilegiati dei criminali informatici e la visibilità delle informazioni sanitarie protette (PHI) consentita da API non protette può condurre ad una mancata conformità all'HIPAA, alla violazione della privacy dei pazienti e alla perdita della fiducia faticosamente conquistata negli anni.

L'ambito di questa sfida è notevole. In un approfondito sondaggio condotto da Akamai, un allarmante 84,7% di professionisti sanitari ha riscontrato problemi di sicurezza delle API l'anno scorso: una percentuale leggermente più alta rispetto alla media dell'84% registrata in diversi settori.

Tuttavia, forse l'aspetto più preoccupante è rappresentato dall'impatto esercitato sulla fiducia: gli intervistati che operano nel settore sanitario hanno segnalato "la perdita di fiducia e reputazione" come una delle loro principali preoccupazioni riguardo ai problemi di sicurezza delle API (28,7%). In un mondo in cui i pazienti possono cambiare facilmente le loro strutture sanitarie, 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 2024.

Con l'aumento degli attacchi, la visibilità diventa sempre più preoccupante

I costi finanziari legati agli attacchi alle API sono notevoli: le aziende sanitarie spendono, in media, 510.600 dollari per risolvere i problemi di questo tipo.

Nonostante questi rischi, dai dati raccolti emerge una preoccupante lacuna nelle priorità. Quando è stato chiesto di descrivere le loro principali priorità in termini di cybersecurity per i successivi 12 mesi, gli intervistati che operano nel settore sanitario hanno inserito "la protezione delle API dai criminali" all'11° posto (16,7%) in una scala con 12 opzioni perché, invece, si stanno focalizzando sulla sicurezza dell'autenticazione per i sistemi a cui accede il personale (24,7%) e sulla gestione dei segreti degli sviluppatori (22,7%).

Distinguere le attività delle API legittime da quelle dannose rimane una sfida per le aziende sanitarie. Mentre il 65% delle aziende sanitarie riferisce di disporre di inventari completi delle API, solo il 24% di questo sottogruppo sa quali API gestiscono dati sensibili: una percentuale in calo dal 40% registrato nel 2023. Per il settore sanitario, in cui la privacy dei dati non è solo una buona pratica, ma è stabilita dalle normative vigenti, questa lacuna nella visibilità crea notevoli rischi.

Considerate ciò che potrebbe succedere ad un'API implementata da un reparto ospedaliero senza un'adeguata supervisione dei team addetti alla sicurezza o del reparto IT centrale. L'API rischierebbe di essere:

- Progettata in modo da condividere i record dei pazienti senza adeguati controlli conformi all'HIPAA
- Lasciata attiva dopo gli aggiornamenti di sistema, creando punti di accesso sconosciuti
- Non rilevata dai tradizionali strumenti di sicurezza, che non sono progettati per rilevare le API non gestite
- Sfruttata dai criminali allo scopo di accedere alle informazioni sanitarie protette (PHI)
- Violata da un partner autentico, che utilizza l'endpoint per casi di utilizzo non previsti

L'84,7% delle aziende sanitarie ha riscontrato problemi di sicurezza delle API negli ultimi 12 mesi

Il 65% delle aziende sanitarie dispone di inventari completi delle API, ma, tra di esse, solo il 24% sa quali API restituiscono dati sensibili

510.600 dollari = l'impatto finanziario esercitato dai problemi di sicurezza delle API sulle aziende sanitarie negli ultimi 12 mesi

Le prime 3 conseguenze

1. **Perdita di fiducia e reputazione** (28,7%)
2. **Perdita di produttività** (28,7%)
3. **Incremento dei controlli interni** (27,3%)

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

Akamai

E non si tratta di semplici ipotesi: considerando il fatto che le violazioni di dati sanitari raggiungono cifre da record e che i costi legati ad una violazione di dati si aggirano, in media, sui 4,88 milioni di dollari[1], le vulnerabilità delle API rappresentano un rischio sempre maggiore in termini di conformità e sicurezza. Per non citare il fatto che un caso come quello sopra menzionato riflette uno scenario che le aziende del settore citano come una delle cause principali dei loro problemi con le API.

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[2].

Ecco perché, giustamente, la conformità all'HIPAA richiede di focalizzarsi sempre più sulla sicurezza delle API. Anche se l'HIPAA non cita esplicitamente le API, richiede la restrizione dell'accesso alle PHI in base ai ruoli della forza lavoro, nonché l'applicazione di controlli di autenticazione e accesso nelle API che trasmettono i dati dei pazienti. Le aziende sanitarie e le compagnie di assicurazioni (insieme ai 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 causati da terzi nel settore sanitario.

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 aziende sanitarie sono perfettamente consapevoli delle conseguenze finanziarie 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 sui costi stimati dei problemi di sicurezza delle API da loro riscontrati negli ultimi 12 mesi.

	Settore sanitario	Media di tutti i settori
Stati Uniti	$ 510.600	$ 591.404
Regno Unito	£ 363.885	£ 420.103
Germania	€ 643.884	€ 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)

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. Come già detto, i partecipanti al nostro sondaggio hanno messo in evidenza la "perdita di fiducia e reputazione" (28,7%) e la "perdita di produttività" (28,7%) come conseguenze dagli effetti duraturi perché la perdita di fiducia da parte dei pazienti può influire negativamente sui ricavi futuri dell'azienda, mentre la perdita di produttività da parte degli operatori sanitari già sottoposti a notevoli pressioni può aumentare lo stress e diminuire il coinvolgimento del personale.

[1] Rapporto IBM sul costo di una violazione di dati, 2024

[2] 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 aziende sanitarie 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 settore sanitario 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 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 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 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 API 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.