STUDIO SULL'IMPATTO DELLA SICUREZZA DELLE API NEL 2024:

la pubblica amministrazione

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

Gli enti governativi di tutto il mondo sono sempre più sottoposti alla pressione di dover proteggere i loro servizi digitali in un'epoca incentrata sulle API. Nel 2024, l'86,1% delle organizzazioni del settore pubblico ha segnalato di aver subito un problema di sicurezza delle API, con una percentuale in netto balzo rispetto al 76,8% registrato l'anno precedente. Questo incremento pone il settore pubblico al di sopra della media dell'84% registrata in tutti i settori, a sottolineare l'intensificarsi di questo problema. Dalla necessità di soddisfare i requisiti del regolamento generale per la protezione dei dati (GDPR) all'applicazione della residenza dei dati nei sistemi multicloud e al confronto con le minacce per la sicurezza della sovranità dei dati, gli enti governativi devono affrontare un'esigenza a livello universale: disporre di una maggiore visibilità, una governance più solida e una resilienza integrata.

I costi reali dei problemi di sicurezza delle API nella pubblica amministrazione

Gli enti governativi stanno adottando sempre più le API per gestire i servizi digitali, facilitare la condivisione dei dati tra un ente e l'altro e modernizzare le loro infrastrutture. Tuttavia, questa tendenza ha introdotto una serie di nuove vulnerabilità che i criminali cercano di sfruttare. Deboli meccanismi di autenticazione, errori di configurazione delle API e una scarsa consapevolezza dei principali indicatori di rischio hanno reso gli enti governativi particolarmente vulnerabili alle violazioni dei sistemi di sicurezza delle API. Le conseguenze di questi incidenti si estendono oltre il furto dei dati ponendo rischi per la continuità operativa, la conformità alle normative e la fiducia da parte del pubblico.

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.

Abbiamo filtrato qui i nostri risultati relativi ai partecipanti al sondaggio appartenenti al settore pubblico, che hanno affermato di aver subito principalmente le seguenti conseguenze causate dai problemi di sicurezza delle API da loro riscontrati:

- "Più stress e/o pressione sui team o sui reparti" (28,5%)
- "Danni alla reputazione del reparto, nonché di dirigenti e/o membri del consiglio di amministrazione" (27,2%)
- "Sanzioni imposte dagli enti di controllo" (25,2%)

Queste conseguenze intercorrelate sono semplici da comprendere se si considera che i partecipanti al sondaggio hanno riferito di aver speso 717.500 dollari per risolvere i problemi legati alle API: una percentuale del 21,3% superiore alla media di tutti gli otto settori oggetto del sondaggio.

Continuate a leggere per ulteriori approfondimenti specifici di settore, che sono stati ricavati dallo studio sull'impatto della sicurezza delle API nel 2024.

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

Quando è stato chiesto di citare le cause principali alla base dei problemi di sicurezza delle API da loro riscontrati, i partecipanti al sondaggio hanno identificato le seguenti due vulnerabilità principali:

- Mancanza di controlli di autenticazione delle API (16%)
- Utilizzo di strumenti tradizionali per la protezione delle API (25,2%)

Nonostante le conseguenze delle minacce alle API siano sempre più evidenti, dagli elevati costi legati alla mitigazione alla perdita di fiducia da parte dei clienti, dai risultati del nostro sondaggio emerge come molti team che operano negli enti governativi non considerano ancora la sicurezza delle API una delle loro priorità principali. Infatti, la sicurezza delle API risulta al sesto posto tra le priorità in termini di cybersecurity per l'anno prossimo (17,9%).

L'86,1% degli enti governativi ha segnalato di aver subito un problema di sicurezza delle API nel 2024: una percentuale in notevole aumento rispetto al 76,8% registrato nel 2023

Il costo medio di una violazione della sicurezza delle API per gli enti governativi negli Stati Uniti è pari a 717.500 dollari: una cifra che supera la media di tutti i settori (591.404 dollari)

Il 66,9% degli enti governativi ha stilato un inventario delle API. Tuttavia, solo il 18,5% di essi dispone di una visibilità completa sulle API che gestiscono dati sensibili, il che mette a rischio le informazioni di importanza critica

Le prime 3 conseguenze

1. **Più stress e/o pressione sui team addetti alla sicurezza**
2. **Danni alla reputazione dei team, nonché di dirigenti e membri del consiglio di amministrazione**
3. **Sanzioni normative per mancata conformità**

Fonte:
Studio sull'impatto della sicurezza delle API nel 2024

Per gli enti governativi, i costi degli attacchi alle API sono elevati, incluso l'impatto sugli aspetti finanziari e sulle risorse umane. La perdita di fiducia da parte dei dirigenti a causa delle violazioni può implicare un maggior numero di controlli minuziosi, l'interruzione delle attività e un aumento del lavoro per i team che sono già sottoposti a pressione e che faticano per soddisfare i requisiti di conformità.

Akamai

Proprio come nel settore privato, per gli enti governativi non è facile distinguere le attività delle API legittime da quelle dannose, in parte a causa della ridotta visibilità sulle aree precise in cui le API sono vulnerabili. Mentre il 66,9% dei partecipanti al nostro sondaggio ha affermato di disporre di un inventario completo delle loro API, solo il 18,5% di questo sottogruppo sa quali API restituiscono dati sensibili, incluse informazioni di identificazione personale (PII), come numeri di carte di identità, dati biometrici e informazioni di contatto.

Considerate ciò che potrebbe succedere ad un'API non autorizzata che viene implementata da un reparto o una filiale di un ente governativo senza la collaborazione o la supervisione dei team addetti alla sicurezza o del reparto IT centrale.

In questo caso, l'API potrebbe essere stata:

- Progettata per fornire accesso ai dati personali o finanziari dei cittadini senza appropriati controlli di autorizzazione, esponendo potenzialmente informazioni sensibili
- Sostituita da una nuova versione, ma non correttamente rimossa, lasciando un endpoint obsoleto che può essere facilmente sfruttato
- Resa operativa senza la visibilità dei team addetti alla sicurezza e del reparto IT centrale, eludendo i controlli di conformità e gli strumenti di monitoraggio tradizionali
- Sfruttata dai criminali per ottenere un accesso autorizzato ai sistemi degli enti governativi, causando potenzialmente violazioni di dati, furto di identità o frodi finanziarie

Non si tratta di semplici teorie: lo scenario della cybersecurity per gli enti governativi statunitensi presenta notevoli sfide. Secondo il Cybernews Business Digital Index, molti enti e reparti governativi faticano a mantenere solidi livelli di sicurezza: di essi, quasi 4 su 10 (38,8%) vengono classificati come a "rischio critico", mentre il 75% ha subito una violazione di dati.

Questi dati riflettono la realtà complessa dei team addetti alla sicurezza degli enti governativi, che devono bilanciare obiettivi aziendali, sistemi tradizionali e minacce in continua evoluzione, operando, al contempo, sotto la pressione di vincoli specifici e controlli minuziosi. Con l'intensificarsi di questi problemi, specialmente nel campo della sicurezza delle API, gli enti governativi hanno bisogno di partner in grado di comprendere i loro specifici requisiti e di fornire soluzioni personalizzate in base ai loro ambienti.

In che modo i problemi delle API influiscono sulla fiducia da parte dei clienti, sui costi e sullo stress dei team

Considerando la frequenza e i costi degli attacchi alle API, non sorprende che la protezione delle API sia una priorità crescente per gli enti governativi a livello globale. Negli Stati Uniti, il progetto Data.gov, gestito dalla General Services Administration, standardizza le API utilizzate nei vari enti governativi per migliorare la coerenza, la sicurezza e l'interoperabilità di cui dispongono. Simili attività vengono intraprese in tutto il mondo, dai sistemi di dati aperti nell'Unione europea e nel Regno Unito alle iniziative di trasformazione digitale avviate nell'area Asia-Pacifico e nel Medio Oriente, in cui gli enti governativi adottano API standardizzate per semplificare e proteggere gli scambi di dati.

Molte di queste iniziative sono in linea con le normative vigenti a livello locale, come il GDPR nell'UE, lo schema NDB (Notifiable Data Breaches) in Australia e il My Number Act in Giappone. Applicando standard e sistemi comuni, gli enti governativi si stanno impegnando nell'intento di garantire la protezione degli scambi di dati, riducendo, al contempo, i rischi da parte delle integrazioni di terze parti e gli accessi non autorizzati.

	Pubblica amministrazione	Media di tutti i settori
Stati Uniti	**717.500,50 dollari**	**591.404,01 dollari**
Regno Unito	**378.140,69 sterline**	**420.103,18 sterline**
Germania	**296.975,79 euro**	**403.453,26 euro**

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)

È chiaro che gli enti governativi 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.

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 abbiamo detto in precedenza, i partecipanti al nostro sondaggio hanno indicato come le due principali conseguenze di questi problemi "l'aumento dello stress e/o pressione per il team/reparto" e "i danni alla reputazione del reparto, nonché di dirigenti e/o membri del consiglio di amministrazione".

Queste conseguenze hanno un impatto di lunga durata. Le violazioni minano la fiducia da parte dei clienti, che può mettere a rischio i ricavi futuri e indebolire la reputazione dell'organizzazione. Nello stesso tempo, la perdita di produttività per gli enti governativi già sottoposti a notevoli pressioni può aumentare lo stress e ridurre l'engagement dei dipendenti.

Tuttavia, non solo alcune aree geografiche sono sotto pressione. Anche se questo rapporto si focalizza su specifici mercati, la sicurezza delle API è diventata un problema critico per le organizzazioni del settore pubblico a livello mondiale, perché anche gli enti governativi che operano nell'area Asia-Pacifico, nell'America Latina e oltre devono affrontare simili sfide per salvaguardare le infrastrutture digitali, soddisfare gli standard di conformità e proteggere i dati sensibili dalle minacce in continua evoluzione.

Ridurre rischi e stress con una sicurezza proattiva delle API

Gli attacchi alle API sferrati contro gli enti governativi 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 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 proteggere il proprio fatturato e i dati sensibili, nonché alleggerire il carico di lavoro dei team addetti alla sicurezza, preservando, al contempo, la fiducia duramente conquistata dei membri del consiglio di amministrazione e dei responsabili degli enti governativi. Nell'ambito di queste misure, 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 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: 05/25.