STUDIO SULL'IMPATTO DELLA SICUREZZA DELLE API 2024

Come i problemi delle API influiscono sulla vostra azienda e sul vostro team

Akamai

Una pubblicazione affiliata dei
rapporti sullo stato di Internet (SOTI) di Akamai

Sommario

Analisi riassuntiva

Ora al suo terzo anno, il rapporto API Security Impact Study (in precedenza denominato rapporto API Security Disconnect) esamina lo stato della protezione della API sulla base di un sondaggio condotto su 1.207 dirigenti e professionisti del settore negli Stati Uniti, nel Regno Unito e (una novità introdotta nel 2024) in Germania. Lo studio esamina il modo con cui le aziende subiscono gli eventi legati alla sicurezza delle API (la loro frequenza, le cause e l'impatto esercitato) e in che modo i reparti addetti alla sicurezza affrontano il problema delle API utilizzate come vettore di attacco.

Per fornire un quadro completo della situazione, abbiamo condotto il sondaggio su un numero bilanciato di:

- CISO, CIO, CTO, esperti di sicurezza e membri dei team AppSec appartenenti ad organizzazioni con un numero di dipendenti compreso tra meno di 500 e più di 1000 unità
- Otto settori industriali: servizi finanziari, retail/e-commerce, pubblica amministrazione, settore manifatturiero, servizi energetici e di pubblica utilità e (una novità introdotta nel 2024) automotive e assicurazioni

Introduzione

Spesso, le API sono considerate un vettore di attacco *emergente*, anche considerando i relativi dati che mostrano quanto siano prevalenti e devastanti. Consideriamo questi dati:

- Sono stati registrati 108 miliardi di attacchi alle API da gennaio 2023 a giugno 2024, secondo un recente rapporto sullo stato di Internet (SOTI) di Akamai.
- "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*.
- Anche il numero di attacchi è in aumento. Secondo il rapporto SOTI, gli attacchi alle applicazioni web e alle API sono aumentati del 49% tra il 1° trimestre del 2023 e lo stesso periodo del 2024.

Queste cifre in aumento non devono sorprendere. "Dietro le quinte", le API facilitano la comunicazione e lo scambio di dati in quasi tutte le tecnologie alla base dei progetti digitali: strumenti di AI generativa, app rivolte ai clienti, servizi cloud e molto altro. Eppure, molte API non sono adeguatamente protette, sia se sono sprovviste di autenticazione, configurate in modo errato o totalmente dimenticate, il che le rende un vettore di attacco allettante e vantaggioso economicamente per i criminali informatici, che devono solo individuare un'API vulnerabile e *"bombardarla"* per ottenere un accesso diretto a tutti i dati (anche migliaia di record) restituiti dall'API quando viene chiamata.

Molte API non sono adeguatamente protette, il che le rende un vettore di attacco allettante e vantaggioso economicamente per i criminali informatici.

Ad un livello più dettagliato, la nostra ricerca ha mostrato che la sicurezza delle API deve ancora diventare un elemento fondamentale all'interno di una strategia di sicurezza completa. Le organizzazioni considerano perlopiù gli attacchi alle API come nuove minacce, poiché i relativi dati, nonché l'impatto finanziario e lo stress esercitato sui team, come emerso dal nostro studio, hanno mostrato che gli attacchi stanno crescendo di numero e stanno diventando sempre più efficaci. I risultati dello studio del 2024 offrono una panoramica su come i problemi di sicurezza delle API influiscono sui vostri colleghi e sulle loro organizzazioni. Questi dati vi saranno utili per consentire al vostro team di valutare meglio i sistemi di protezione delle API e di migliorarli in base alle specifiche esigenze.

Risultati dettagliati: come i problemi legati alle API influiscono negativamente sulle attività aziendali e sui livelli di stress dei team

Dai risultati del nostro studio del 2024, è emerso che le API sono un vettore di attacco in crescita e che stanno creando notevoli problemi di sicurezza per i team dedicati. I partecipanti al nostro sondaggio si sono mostrati estremamente d'accordo sui seguenti dati:

- I problemi di sicurezza delle API sono aumentati negli ultimi tre anni
- Il costo necessario per affrontare e ripristinare lo stato normale dopo un problema di sicurezza delle API supera, in media, il mezzo milione di dollari (precisamente, l'impatto finanziario è pari, in media, a 943.162 dollari, secondo i dirigenti di primo livello negli Stati Uniti che hanno partecipato al nostro sondaggio).
- Il prezzo pagato dalle persone che hanno subito problemi relativi alle API, con l'impatto esercitato dal livello di stress e dai danni alla reputazione per i loro team (specialmente con i controlli interni che amplificano questa pressione), è addirittura superiore rispetto ai costi necessari per risolvere questi problemi

I partecipanti al sondaggio hanno fornito diverse opinioni sulla completezza dei loro inventari delle API e questa variabilità è apparsa ancora più pronunciata quando si è passato alla suddivisione in base ai ruoli (vedere pagina 11). Sorprendentemente, il numero delle aziende con un inventario completo delle API che sanno anche quali delle loro API restituiscono dati sensibili è sceso da una percentuale già bassa pari al 40% nel 2023 al 27% nel 2024.

I partecipanti al sondaggio hanno anche indicato che gli strumenti tradizionali su cui si basano per proteggere le API non coprono completamente dai rischi. Questi strumenti, come le soluzioni WAF (Web Application Firewall), i gateway API e i firewall di rete, sono, spesso, le prime cause che favoriscono la riuscita di un attacco (vedere l'elenco completo delle cause a pagina 17 e una nota sulle soluzioni WAF e WAAP a pagina 12).

I risultati del nostro studio ci consentono anche di dedurre alcuni motivi principali che hanno portato a non dare ancora priorità alle strategie di sicurezza delle API, nonostante la presenza di prove che indicano che meritano attenzione. Un fattore fondamentale è rappresentato dalla mancanza di allineamento tra i principali ruoli aziendali sul numero, sulla posizione e sugli attributi di rischio relativi alle API che devono essere protette, probabilmente a causa della scarsa visibilità sulle API e dell'assenza di una fonte attendibile.

Inoltre, abbiamo osservato pareri discordanti tra i responsabili e gli addetti alla sicurezza sulle cause degli attacchi alle API. Questo fenomeno dipende dagli strumenti che utilizzano, dagli errori commessi dai loro sviluppatori o dagli attacchi che sfruttano le falle presenti nelle innovazioni basate sull'AI generativa? Dipende da chi risponde alla domanda.

Ovviamente, l'altro motivo per cui la sicurezza delle API non ha ancora assunto un posto di maggior rilievo da un punto di vista strategico è il fatto che i team devono già occuparsi della protezione da altre minacce urgenti, che stanno prosciugando la maggior parte dei budget, dell'attenzione dei team e degli sforzi aziendali. Analizziamo ora i risultati più in dettaglio.

I professionisti della sicurezza ritengono che il prezzo pagato dalle persone che hanno subito problemi relativi alle API, con l'impatto esercitato dal livello di stress e dai danni alla reputazione per i loro team, sia addirittura superiore rispetto ai costi necessari per risolvere questi problemi.

API Security Impact Study - 2024
Panoramica sui risultati principali

84% Percentuale di intervistati che ha riscontrato un problema di sicurezza delle API negli ultimi 12 mesi

Costo medio richiesto per risolvere i problemi di sicurezza delle API riscontrati negli ultimi 12 mesi

Stati Uniti	REGNO UNITO	Germania
$591.404	£420.103	€403.453

Scarsa visibilità

Solo il 27% delle aziende con un inventario completo delle API sa quali API restituiscono dati sensibili, una percentuale scesa dal 40% registrato nel 2023.

Stress elevato

Il principale impatto esercito dai problemi delle API *CISO*: danni alla reputazione del reparto, nonché di dirigenti/membri del consiglio di amministrazione. *CIO*: più stress e/o pressione sui team o sui reparti.

Frequenza dei test inadeguata

Solo il 13% e il 18% dei partecipanti al sondaggio sottopone a test le proprie API in tempo reale e ogni giorno, rispettivamente, a partire dallo sviluppo fino alla produzione delle API.

I costi finanziari necessari per risolvere i problemi di sicurezza delle API inaspriscono l'impatto esercitato sui team e sui responsabili aziendali. Le costose violazioni di dati attirano i controlli aziendali e le principali parti interessate, come i membri del consiglio di amministrazione, potrebbero dedurre che i team non stiano svolgendo bene il proprio lavoro. Tutto ciò genera molto stress e, in effetti, i partecipanti al sondaggio di varie aree geografiche hanno citato lo stress dei loro team come la principale conseguenza dei problemi di sicurezza delle API.

Lo stato corrente della sicurezza delle API

Negli ultimi tre anni, il numero delle organizzazioni che riferiscono di aver riscontrato problemi di sicurezza delle API è salito costantemente, arrivando al 84% nel 2024 (vedere qui sotto). In che modo gli attacchi alle API influiscono sulle organizzazioni? Cosa stanno facendo (o non stanno facendo) le organizzazioni per ridurre i loro rischi? Abbiamo organizzato i risultati emersi dal nostro studio in base alle risposte ricevute alle domande riportate di seguito.

Gli attacchi alle API stanno influendo in modo significativo sulle organizzazioni e sui loro team addetti alla sicurezza?

Sicuramente sì. Questo è stato il primo anno in cui abbiamo raccolto dati sull'impatto finanziario esercitato dai problemi di sicurezza delle API e i risultati si sono rivelati significativi: in media, i costi necessari per mitigare i problemi relativi alle API (inclusi problemi di downtime, riparazione dei sistemi, spese legali, sanzioni e altri costi associati) riscontrati negli ultimi 12 mesi dall'84% dei partecipanti al sondaggio sono stati pari a:

- **$591.404** negli Stati Uniti
- **£420.103** nel Regno Unito
- **€403.453** in Germania

Alcuni ruoli aziendali hanno riferito di aver sostenuto costi molto più elevati, in particolar modo i dirigenti di primo livello negli Stati Uniti, che hanno riferito di aver speso 943.162 dollari (quasi il 60% in più rispetto alla media riferita da tutti i partecipanti al sondaggio negli Stati Uniti).

Avete riscontrato un problema di sicurezza delle API negli ultimi 12 mesi?

Anno	Totale	Stati Uniti	Regno Unito	Germania
2022	76%	75%	77%	-
2023	78%	85%	69%	-
2024	84%	83%	83%	84%

Indipendentemente dal numero esatto, i costi finanziari legati ai problemi di sicurezza delle API inaspriscono l'impatto esercitato sulle persone. Le costose violazioni di dati attirano i controlli aziendali e le principali parti interessate, come i membri del consiglio di amministrazione, potrebbero dedurre che i team non stiano svolgendo bene il proprio lavoro. Tutto ciò genera molto stress e, in effetti, i partecipanti al sondaggio di varie aree geografiche hanno citato lo stress (nello specifico, quello dei loro team) come la principale conseguenza dei problemi di sicurezza delle API, seguito dai danni alla reputazione del reparto, nonché di dirigenti e/o membri del consiglio di amministrazione, come seconda conseguenza e, infine, in terza posizione, i costi necessari per risolvere questi problemi. È da notare che l'impatto interno che influisce maggiormente sul morale ricompare e domina le ultime tre conseguenze, che sono strettamente correlate tra loro (vedere qui sotto).

I risultati sono stati simili quando si è passato alla suddivisione per settore: i maggiori livelli di stress e/o pressione per il team dopo una violazione di API sono stati la principale conseguenza per quattro degli otto settori su cui si è incentrato il sondaggio (vedere la sezione laterale a pagina 9), tra cui i servizi finanziari, che, in particolare, hanno segnalato come il costo maggiore affrontato da tutti i settori è stato pari a 832.801 dollari.

Le principali conseguenze dei problemi di sicurezza delle API

1. Più stress e/o pressione sui team o sui reparti: **27%**
2. Danni alla reputazione del reparto, nonché di dirigenti e/o membri del consiglio di amministrazione: **26,6%**
3. Costi sostenuti per risolvere il problema: **25,8%**
4. Sanzioni imposte dagli enti di controllo: **25,4%**
5. Perdita di fiducia ed elevato tasso di abbandono da parte dei clienti: **25%**
6. Perdita di produttività: **24,1%**
7. Perdita di fiducia e reputazione: **23,8%**
8. Perdita di impegno da parte dei dipendenti: **23,8%**
9. Incremento dei controlli interni del team/reparto da parte dell'azienda: **23,5%**

Sulla base di questa domanda: Quali costi e/o conseguenze ha subito la vostra azienda a causa dei problemi di sicurezza delle API? (massimo 3 risposte); n=1.207

La relazione tra i costi finanziari e i danni alle persone causati dagli attacchi alle API è anche emerso in modo netto e chiaro nelle risposte dei responsabili dell'IT e della sicurezza sull'impatto esercitato da questi problemi (ogni partecipante poteva scegliere fino a tre risposte). Tutti i ruoli di tutte le aree geografiche hanno concordato nel riconoscere che il personale ha subito maggiormente l'impatto dei problemi di sicurezza delle API.

- Come riferito dai CISO, le prime due conseguenze di questo impatto (danni alla reputazione del reparto, nonché di dirigenti/membri del consiglio di amministrazione, e perdita di fiducia ed elevato tasso di abbandono da parte dei clienti) hanno rivelato un perfetto legame tra l'impatto finanziario e i danni alle persone (31%).
- Analogamente, le principali conseguenze riferito dai CIO hanno rivelato un legame tra i maggiori livelli di stress e/o pressione sui team/reparti e i costi necessari per risolvere i problemi (34%).

Questi risultati hanno senso per i CISO e i CIO: cosa succederebbe se i team da loro diretti continuassero a riscontrare problemi di sicurezza che causano scarse condizioni di lavoro, prosciugano i loro budget e minano la soddisfazione dei clienti? Questi responsabili aziendali non vogliono vedere andar via i loro migliori talenti né vogliono far precipitare la reputazione del loro reparto. Se a tutto ciò si aggiungono le pressioni finanziarie, come i costi necessari per la mitigazione dei problemi e/o un elevato tasso abbandono dei clienti, il livello di stress di CISO e CIO inizia a salire notevolmente. In effetti, la perdita di fiducia e l'elevato tasso di abbandono da parte dei clienti sono stati riconosciuti come le principali conseguenze dei problemi di sicurezza delle API dai partecipanti al sondaggio che operano nel campo assicurativo e nel settore dell'automotive (vedere la sezione laterale alla pagina successiva per altri risultati di settore).

Le principali risposte fornite dai ruoli rimanenti sono state:

- CTO (30%): perdita di impegno da parte dei dipendenti
- Professionisti della sicurezza (27%): danni alla reputazione del reparto, nonché di dirigenti/membri del consiglio di amministrazione
- Team AppSec (31%): più stress e/o pressione sui team/reparti

Le principali conseguenze dei problemi di sicurezza delle API per settore	
Automotive	Perdita di fiducia ed elevato tasso di abbandono da parte dei clienti: **33%**
Servizi energetici e di pubblica utilità	Danni alla reputazione del reparto, nonché di dirigenti e/o membri del consiglio di amministrazione: **36%**
Servizi finanziari	I ncremento del livello di stress/pressione sui team/reparti + sanzioni normative: (entrambi) **29%**
Pubblica amministrazione	Incremento del livello di stress/pressione sui team/reparti: **29%**
Settore sanitario	P erdita di fiducia e reputazione + perdita di produttività: (entrambi) **29%**
Assicurazioni	Perdita di fiducia ed elevato tasso di abbandono da parte dei clienti: **28%**
Settore manifatturiero	Incremento del livello di stress e/o pressione sui team/reparti: **34%**
Retail/E-commerce	Incremento del livello di stress e/o pressione sui team/reparti: **29%**

Sulla base di questa domanda: Quali costi e/o conseguenze ha subito la vostra azienda a causa dei problemi di sicurezza delle API? (massimo 3 risposte); n=1.207

La visibilità sulle API e sui potenziali rischi è adeguata?

No, anzi più nello specifico, è effettivamente peggiorata. Quest'anno, la percentuale dei partecipanti al sondaggio con un inventario completo delle API che sanno anche quali delle loro API scambiano dati sensibili è scesa da un valore già basso del 40% nel 2023 al 27% nel 2024. Questo dato potrebbe risultare positivo se consideriamo il fatto che un maggior numero di organizzazioni sta tentando di compilare un inventario completo, ma non dispone degli strumenti necessari per individuare tutte le API e identificare le attività di ciascuna di esse.

La percentuale dei partecipanti al sondaggio con un inventario completo delle API che sanno anche quali delle loro API scambiano dati sensibili è scesa da un valore già basso del **40% nel 2023** al **27% nel 2024**.

Lo stato corrente dell'inventario e della consapevolezza delle API da parte di tutti i partecipanti al sondaggio

	2024	2023
Sì **e sappiamo** quali restituiscono dati sensibili	27%	40%
Sì, **ma non sappiamo** quali restituiscono dati sensibili	43%	32%
Disponiamo di un inventario parziale delle API **e sappiamo** quali restituiscono dati sensibili	23%	24%
Disponiamo di un inventario parziale delle API, **ma non sappiamo** quali restituiscono dati sensibili	6%	4%
No, **non disponiamo** di alcun inventario	1%	-

Sulla base di questa domanda: Disponete di un inventario completo delle API e sapete quali di esse restituiscono dati sensibili? (Scegliete una delle cinque risposte disponibili); n=1.207

Esaminando i responsabili di tutti i tre paesi e degli otto settori oggetto del sondaggio, i CIO tendono a ritenere (con un margine notevolmente superiore rispetto ai CISO) che le loro organizzazioni dispongano di un inventario completo delle API. I professionisti della sicurezza e i membri dei team AppSec sono ampiamente allineati con l'opinione media dei CIO che ritengono di conoscere tutte le loro API.

Ma come si differenziano i cinque ruoli considerati quando è stato chiesto se sanno o meno quali delle loro API restituiscono dati sensibili quando vengono chiamate? La risposta è importante perché molte di queste chiamate provengono da origini dannose, che cercano di sfruttare le comuni vulnerabilità delle API.

Quattro tipi di API non gestite che i criminali prendono di mira per accedere ai dati desiderati

1. Le **API nascoste** (dette anche API non documentate) esistono e operano all'esterno dei canali ufficialmente monitorati in un'organizzazione.
2. Le **API non autorizzate** sono create per scopi dannosi e, quindi, rappresentano un rischio per la sicurezza di un sistema o di una rete.
3. Le **API zombie** includono tutte le API che vengono eseguite anche dopo essere state sostituite completamente da nuove versioni o da altre API.
4. Le **API obsolete** non sono più consigliate per l'uso a causa delle modifiche apportate alle API.

Questi risultati evidenziano alcuni interessanti aspetti relativi alla visibilità sui rischi per le API. La maggior parte dei CISO e dei CTO ha risposto di disporre di un inventario completo delle API, ma di *non sapere* quali API restituiscono informazioni sensibili (che possiamo definire "conoscenza dei dati sensibili") o di disporre di un inventario parziale delle API *e di una conoscenza dei dati sensibili*.

La maggior parte dei CIO ha riferito di disporre di un inventario completo delle API e il 42,9% di essi ha dichiarato di disporre anche di una piena conoscenza dei dati sensibili, mentre il 36,3% di essi ha riferito di non disporre di tale conoscenza. I professionisti della sicurezza si sono mostrati allineati ai CIO (il 75% di essi ha riferito di disporre di un inventario completo), ma hanno risposto *in modo contrario* per quanto riguarda la conoscenza dei dati sensibili: il 32,5% dei professionisti della sicurezza ha affermato di disporre di una conoscenza dei dati sensibili, mentre il 42,5% ha risposto di non disporre di tale conoscenza.

Infine, i membri del personale AppSec, probabilmente i più pratici di tutti i partecipanti al sondaggio, hanno rappresentato la maggioranza in tutti e cinque i ruoli aziendali. Quasi la metà di essi ha riferito di disporre di un inventario completo senza una conoscenza dei dati sensibili, mentre l'altra metà si è divisa approssimativamente rispondendo di disporre di:

- Un inventario completo delle API con una piena conoscenza dei dati sensibili
- Un inventario parziale delle API con una piena conoscenza dei dati sensibili

Possiamo notare che il livello degli inventari non è stato ancora standardizzato tanto da produrre un numero di API provenienti da una sola origine. Considerando questa variabilità, un maggior numero di aziende con inventari completi delle API potrebbe *non disporre* di una piena conoscenza dei dati sensibili. Sapere quali API restituiscono dati sensibili è sempre importante. Tuttavia, un inventario parziale può essere più pericoloso perché le API nascoste, non autorizzate, zombie e obsolete sono maggiormente prese di mira, sono scarsamente protette e, di solito, risultano invisibili agli strumenti di sicurezza tradizionali.

Lo stato corrente dell'inventario e della consapevolezza delle API in base al ruolo

	CISO	CIO	CTO	Professionisti della sicurezza	AppSec
Disponiamo di un inventario completo delle API **e sappiamo** quali restituiscono dati sensibili	17,2%	42,9%	16,5%	32,5%	26,4%
Disponiamo di un inventario completo delle API, **ma non sappiamo** quali restituiscono dati sensibili	41,4%	36,3%	34,8%	42,5%	47,4%
Disponiamo di un inventario parziale delle API **e sappiamo** quali restituiscono dati sensibili	32,5%	15,4%	39,9%	18,3%	20,4%
Disponiamo di un inventario parziale delle API, **ma non sappiamo** quali restituiscono dati sensibili	8,3%	5,5%	8,2%	5,8%	5,2%

Sulla base di questa domanda: Disponete di un inventario completo delle API e sapete quali di esse restituiscono dati sensibili? (Scegliete una delle cinque risposte disponibili); n=1.207

In un momento in cui le API non gestite proliferano e dimostrano di riuscire ad eludere i tradizionali strumenti di sicurezza, questi risultati rivelano una comune falla nei sistemi di sicurezza che rende le API un vettore di attacco più allettante per i criminali.

Ovviamente, le API non gestite sono solo uno dei cinque attributi delle API che un team addetto alla sicurezza deve considerare e valutare, tra cui:

- **API con vulnerabilità note**, che non sono state corrette con patch
- **API non gestite o dimenticate** (nascoste non autorizzate, zombie, obsolete)
- **API con vulnerabilità esterne** (come credenziali, chiavi e altre variabili che esulano dal vostro controllo)
- **API con errori dell'operatore** (errori di configurazione della sicurezza nell'infrastruttura e nei servizi)
- **API con vulnerabilità non rilevate** e bug che possono essere identificati e sfruttati dai criminali

Dalle risposte fornite dai vari ruoli aziendali relativamente agli inventari e alla visibilità sulle vulnerabilità delle API, è emerso che:

- Le aziende si basano ancora su prodotti di sicurezza non progettati specificamente per individuare e proteggere le API, specialmente quelle non gestite, che presentano un rischio elevato.
- I reparti addetti alla sicurezza devono ancora definire gli attributi di rischio delle API che vanno identificate e valutate o mettere d'accordo i vari team di sviluppo, le business unit e i vendor coinvolti nella loro strategia volta ad individuare e creare un inventario delle API.

Orchestrare tutti gli elementi coinvolti in questo processo può risultare un primo passo notevole verso una strategia che tende ad investire in funzionalità più efficaci per proteggere tutte le API (vedere la sezione "Come migliorare il sistema di sicurezza delle API" a pagina 18). Attualmente, la focalizzazione e la consulenza necessarie per allocare i budget, spesso, non vengono considerate per la sicurezza delle API, il che rende difficile dare priorità e finanziare i progetti che potrebbero migliorare non solo i sistemi di difesa di API e app web, ma anche il sistema di difesa complessivo di un'organizzazione.

Migliori insieme: i sistemi di protezione delle API e le soluzioni WAAP

Progettate per identificare e mitigare rapidamente le minacce provenienti da più vettori di attacco, le soluzioni WAAP (Web Application and API Protection) superano i tradizionali sistemi di protezione della tecnologia WAF. **Una soluzione per la sicurezza delle API deve includere strumenti tali da estendere la protezione oltre il firewall per creare la migliore difesa possibile**.

Le API vengono controllate ad una frequenza tale da ridurre il rischio di subire abusi o violazioni?

No, non vengono controllate abbastanza spesso. Le API pubbliche che presentano errori di configurazione, mancano di controlli di autenticazione, sono incorporate con errori di codifica o nascondono altri rischi che si possono prevenire sono esattamente ciò che cercano i criminali, che diventano sempre più bravi nella loro individuazione.

Ogni volta che un team di sviluppo sposta le API di questo tipo in fase di produzione (senza aver prima eseguito test completi), inconsciamente crea un carico di lavoro futuro per i team addetti alla sicurezza, che è indubbiamente urgente e che contribuisce ad aumentare il livello di stress, come è emerso dai nostri risultati).

Abbiamo, tuttavia, parlato prima di rischi che *si possono prevenire*.

Se le API vengono sottoposte a test in fase di sviluppo, con procedure automatizzate in modo frequente ed efficiente, *prima* di spostarle in fase di produzione, l'azienda, gli sviluppatori e i team addetti alla sicurezza si troveranno in una posizione di vantaggio, che è immediato in termini di riduzione del livello di stress causato da vulnerabilità sconosciute e per il fatto di sapere che non verranno trovati errori durante la produzione, quando sono molto più difficili e costosi da risolvere.

Se le API vengono sottoposte a test in fase di sviluppo, con procedure automatizzate in modo frequente ed efficiente, *prima* di spostarle in fase di produzione, l'azienda, gli sviluppatori e i team addetti alla sicurezza si troveranno in una posizione di vantaggio,

Finora, tuttavia, l'esecuzione dei test non sta prendendo piede, secondo quanto riferiscono i partecipanti al nostro sondaggio. Il numero dei test delle API eseguiti frequentemente (in tempo reale e ogni giorno) si è ridotto dall'anno scorso durante il ciclo di vita delle API, inclusa la fase di produzione.

- Nel 2023, il 18% dei partecipanti al sondaggio negli Stati Uniti e nel Regno Unito ha affermato di aver eseguito i test delle API in tempo reale. Per lo stesso gruppo di persone **nel 2024, questa percentuale è scesa al 13%**.
- Nel 2023, il 37% dei partecipanti al sondaggio negli Stati Uniti e nel Regno Unito ha affermato di aver eseguito i test delle API almeno una volta al giorno. **Nel 2024, solo il 13% dei partecipanti al sondaggio ha affermato di aver eseguito i test a questa frequenza**, anche se il 26% dei partecipanti al sondaggio in Germania ha affermato di averli eseguiti una volta al giorno.

L'esecuzione dei test delle API con cadenza settimanale è più comune per i partecipanti in varie aree geografiche, ma in nessuna area geografica è stata raggiunta una percentuale del 50%. Inoltre, la frequenza dei test delle API è stata molto variabile nelle diverse aree geografiche, a volte eseguiti *in tempo reale* , a volte*non eseguiti affatto*. Soprattutto, è da notare che solo il 6% dei partecipanti al sondaggio ha risposto di eseguire i test sulla sicurezza delle API solo prima di passarle alla fase di produzione. Teoricamente, si osserverà una tendenza da parte dei team addetti alla sicurezza ad eseguire test continui nell'intero ciclo di vita delle API.

Cosa significa eseguire continuamente i test delle API?

Le vulnerabilità possono essere introdotte nelle API in qualsiasi punto nel loro ciclo di vita, dagli errori di codifica apportati in fase di sviluppo alle falle di sicurezza che sono emerse una volta iniziata l'interazione tra gli utenti e le API. Ecco perché, idealmente, i test delle API vengono eseguiti in fase di sviluppo (Shift-Left) e in modo continuato durante la produzione (Shift-Right).

Esempi di test delle API in fase di sviluppo:

- Esecuzione di test automatizzati che simulano il traffico dannoso
- Verifica delle specifiche delle API sulla base delle policy di governance stabilite
- Esecuzione di test sulla sicurezza delle API on-demand o come parte di una pipeline CI/CD

Esempi di test delle API in fase di produzione:

- Monitoraggio continuo del traffico delle API e valutazione dei relativi metadati.
- Identificazione delle modifiche apportate alle API esistenti tramite analisi automatizzate.
- Individuazione dei problemi in tempo reale e relativa mitigazione prima che i criminali se ne rendano conto.

I vostri protocolli di sicurezza delle API soddisfano gli obblighi in materia di conformità?

Molti regolamenti sulla protezione delle API non fanno esplicito riferimento alle API, ma le normative si focalizzano chiaramente sulla protezione di applicazioni e infrastrutture all'interno della quali operano le API, Gli obblighi di conformità sono sempre in continua evoluzione e sono in fase di attuazione ulteriori regolamenti con riferimenti alle API, incluso il Privacy Rights Act negli Stati Uniti (attualmente in progetto di legge) e il Cyber Resilience Act dell'UE.

Tra i regolamenti e i quadri normativi con implicazioni correnti e dirette per la sicurezza delle API, figurano i seguenti:

- PCI DSS (attualmente v4.0.1)
- Regolamento generale sulla protezione dei dati (GDPR)
- DORA (Digital Operational Resilience Act)
- HIPAA (Health Insurance and Portability and Accountability Act)
- Direttiva NIS2 (Network and Information Security)

La sicurezza delle API richiede attenzione, ma rimane in secondo piano

Se gli attacchi alle API impongono sanzioni e costi elevati, se contribuiscono alla perdita della fiducia dei clienti, se causano livelli crescenti di stress sul personale e perdita di credibilità con i membri del consiglio di amministrazione, perché i team non stanno prendendo azioni più decisive? Le risposte alle seguenti domande ci aiutano a comprendere la situazione.

In che modo i vari ruoli aziendali stanno dando priorità alla sicurezza delle API?

Abbiamo chiesto ai partecipanti al nostro sondaggio di identificare le loro principali priorità in termini di cybersicurezza per i prossimi 12 mesi, scegliendo fino a tre risposte da un elenco esaustivo (vedere a lato). Le principali sei priorità sono diverse solo per il 2%, mentre le ultime sei solo per l'1%, il che suggerisce che le priorità sono simili nei vari settori e aree geografiche e che, spesso, i team sono costretti a gestirle tutte.

In alcuni settori, tuttavia, le differenze di priorità relative alle API raccontano tutta un'altra storia. Ad esempio, nei servizi di pubblica utilità la sicurezza delle API è considerata come la priorità minima, mentre la percentuale che indica la sua priorità per tutti gli altri settori è pari al 13,2% (inferiore alla media del 18% che caratterizza tutti i partecipanti al sondaggio). Nello stesso tempo, per quanto riguarda la segnalazione dei problemi di sicurezza delle API i servizi di pubblica utilità si sono distinti con un 91%, che è la percentuale più alta rispetto a tutti gli otto settori esaminati e superiore alla media dell'84%. Tutto ciò a cosa contribuisce? A riscontrare la bassa priorità attribuita alla sicurezza delle API e l'elevato numero di attacchi.

Le principali priorità della sicurezza nei prossimi 12 mesi

1. Difesa dagli attacchi basati sull'AI generativa: **21,2%**
2. Difesa dai ransomware: **20,5%**
3. Protezione dell'autenticazione per la forza lavoro: **19,7%**
4. Gestione e protezione dei segreti degli sviluppatori: **19,6%**
5. Protezione degli endpoint: **19,2%**
6. Soluzioni per la sicurezza nel cloud: **19,1%**
7. Protezione dell'accesso basato sui privilegi: **18,6%**
8. Prevenzione della perdita di dati: **18,6%**
9. Protezione delle API dai criminali: **17,9%**
10. Protezione delle applicazioni: **17,7%**
11. SIEM (Security Information and Event Management): **17,6%**
12. Gestione e risposta agli incidenti: **17,6%**

Sulla base di questa domanda: Quali saranno le principali priorità della cybersicurezza per la vostra azienda nei prossimi 12 mesi? (massimo 3 risposte); n=1.207

Dalle risposte suddivise in base al ruolo, è emerso un maggior numero di dati indicativi:

- I CISO hanno citato la protezione delle API e dagli attacchi basati sull'AI generativa come le massime priorità, rispettivamente con percentuali del **25,5%** e del **24,8%**.
- Il personale del team AppSec si è allineato con i CISO citando la protezione dagli attacchi basati sull'AI generativa come la massime priorità, con una percentuale del **22,5%**.
- I ruoli dei CIO e dei CTO si sono entrambi focalizzati sugli accessi con privilegi, a cui i CTO hanno aggiunto anche la risposta agli incidenti.
- I professionisti della sicurezza hanno citato soltanto i ransomware come loro massima priorità.

Queste differenze ci conducono nuovamente a farci alcune domande, come: Perché i vari livelli dei team addetti alla sicurezza IT sembrano operare sulla base di diverse strategie? Perché i principali responsabili della sicurezza e i team dedicati sembrano tutti allineati nel considerare come gravoso il ruolo che le API (e i rischi correlati) svolgono negli attacchi basati sull'AI generativa, a differenza di altri ruoli?

Forse perché i CISO vedono che le loro business unit implementano frettolosamente innovazioni come le app basate sull'AI generativa per soddisfare le richieste dei clienti, mentre *solo* i membri del team AppSec conoscono l'entità delle incognite relative alle vulnerabilità dei componenti AI (come i modelli LLM) che trattano dati sensibili. Inoltre, questo team può accorgersi immediatamente dei molti segni che indicano come i criminali stiano implementando l'AI generativa nei loro metodi di attacco.

Tuttavia, la ragione principale potrebbe essere la più semplice: Le comunicazioni gerarchiche e verticistiche non si verificano abbastanza frequentemente (soprattutto, nelle grandi aziende), il che conduce ad una disparità tra le priorità citate a livello dirigenziale rispetto a ciò che i team dedicati *devono* gestire giorno per giorno.

Infine, passiamo a confrontare le principali priorità della cybersicurezza citate dai partecipanti al sondaggio con le causa da loro attribuite ai problemi di sicurezza delle API. Come mostrato a pagina 17, tre delle principali cause citati si riferiscono ai tradizionali strumenti per la sicurezza delle applicazioni che non sono stati in grado di rilevare i problemi relativi alle API. Il confronto offre una buona opportunità per aprire una discussione su come le soluzioni di individuazione e test delle API potrebbero migliorare non solo la sicurezza delle API, ma soddisfare anche quasi tutte le altre priorità principali in materia di sicurezza.

In altre parole, se gli appropriati strumenti di sicurezza delle API possono proteggere non solo le API, ma migliorare anche la sicurezza in altri campi, come per i dati, il cloud e le applicazioni, la sicurezza delle API si rivela sempre meno un settore di nicchia e isolato per tutte le parti coinvolte. Considerare il quadro generale può semplificare il processo di approvazione della necessità di porre la sicurezza delle API in cima alla lista delle priorità.

Se gli appropriati strumenti di sicurezza delle API possono proteggere non solo le API, ma migliorare anche la sicurezza in altri campi, come per i dati, il cloud e le applicazioni, la sicurezza delle API si rivela sempre meno un settore di nicchia e isolato per tutte le parti coinvolte.

La mancanza di allineamento sui problemi legati alla sicurezza delle API indica che non esiste una fonte attendibile?

Abbiamo evidenziato le differenze tra i dirigenti di primo livello e il personale dedicato relativamente alle priorità complessive in termini di sicurezza e queste discordanze si ritrovano in problemi più specifici che riguardano le minacce alle API. Ad esempio, i CIO concordano con il team AppSec sul fatto di essere consapevoli degli attacchi alle API (circa l'88% dei partecipanti al sondaggio che operano in tutti i ruoli ha segnalato di aver subito problemi di questo tipo). Nel contempo, i CISO, i CTO e i professionisti della sicurezza hanno tutti fatto registrare circa otto punti percentuali in meno, ossia circa l'80% di essi ha segnalato di aver subito problemi di questo tipo.

Anche la principale causa dei problemi di sicurezza delle API si è rivelata diversa in base al ruolo aziendale: la maggior parte dei CISO e dei professionisti della sicurezza hanno riferito che il gateway API non è riuscito a rilevarli, mentre gli altri tre ruoli esaminati hanno tutti individuato un diverso colpevole:

- CISO: il gateway API non è riuscito ad individuarli - **26,8%**
- CIO: visibilità imprevista su Internet - **28,6%**
- CTO: la soluzione WAF non è riuscita ad individuarli - **25,9%**
- Professionisti della sicurezza: il gateway API non è riuscito ad individuarli - **23,3%**
- Team AppSec: Errori di configurazione delle API - **23,2%**

Le principali cause dei problemi di sicurezza delle API (tutti i partecipanti al sondaggio)

1. Le API sono state rese visibili in modo imprevisto su Internet - 21,8%
2. La soluzione WAF (Web Application Firewall) non è riuscita ad individuarli - 21,8%
3. Il gateway API non è riuscito ad individuarli - 20,2%
4. API presenti negli strumenti/tecnologie basati sull'AI generativa, ad es., i modelli LLM – 20%
5. Errori di configurazione delle API - 19,9%
6. Il firewall di rete non è riuscito ad individuarli - 19,6%
7. Strumenti/Servizi tecnologici ben noti, ad es., Microsoft - 19,2%
8. Vulnerabilità dovuta agli errori di codifica delle API - 19,1%
9. API non gestite, ad es., API inattive o zombie - 18,9%
10. Mancanza di controlli di autenticazione delle API - 18,8%
11. Vulnerabilità di autorizzazione - 18,7%
12. Soluzioni software scaricate da Internet - 17,6%
13. Soluzioni software di livello medio, ad es., Slack - 16.3%

Sulla base di questa domanda: Quali ritenete siano le cause dei problemi di sicurezza delle API riscontrati dalla vostra organizzazione? (massimo 3 risposte); n=1.207

Anche i costi associati ai problemi di sicurezza delle API hanno mostrato una mancanza di allineamento dai ruoli dirigenziali verso il basso, anche se è importante notare che la suddivisione dei dati in base al ruolo *e* all'area geografica ha ovviamente ridotto le dimensioni del campione esaminato. Anche in questo caso, vale la pena notare le differenze presenti in questi sottogruppi, specialmente negli Stati Uniti, in cui i costi associati ai problemi di questo tipo sono stati calcolati da CIO e CTO come pari a circa 1 milione di dollari, dai CISO come pari a circa 737.000 dollari e dai professionisti della sicurezza e team AppSec come pari, rispettivamente, a circa 375000 e 444.000 dollari.

Nel Regno Unito, i costi sono stati generalmente più allineati nei vari sottogruppi appartenenti a diversi ruoli aziendali, anche se i membri del AppSec, in questo caso, hanno segnalato la cifra più alta, pari a 749.000 sterline e i CISO la più bassa, pari a 190.000 sterline (i ruoli intermedi hanno calcolato i costi associati come compresi tra 374.000 e 222.000 sterline). La differenza di costi segnalata in Germania è stata simile a quella riscontrata nel Regno Unito, in cui i costi più elevati sono derivati dalla posizione più bassa, ossia dal personale tecnico che ha riferito costi pari a 345.000 di euro, mentre i CISO che ricoprono il ruolo aziendale più alto hanno riferito i costi più bassi, pari a 197.000 sterline (al contrario dei risultati riscontrati negli Stati Uniti). Tutti i ruoli di tutte le aree geografiche hanno concordato nel riconoscere che il personale ha subito maggiormente l'impatto dei problemi di sicurezza delle API (vedere la sezione sull'impatto a pagina 7).

Come migliorare il sistema di sicurezza delle API

Come già detto, i nostri risultati hanno chiarito la situazione: i membri dei team addetti alla sicurezza che ricoprono vari livelli all'interno delle organizzazioni non considerano, attualmente, la sicurezza delle API allo stesso modo. Tuttavia, d'altro canto, è risultato chiaro che si riferiscono ad una base comune: Questi ruoli sono consapevoli dei costi (in termini finanziari e di risorse umane) e riconoscono che gli strumenti su cui si basano non sono adeguati.

Mentre la sicurezza delle API influisce notevolmente sulle organizzazioni, successivamente si potrebbe decidere su cosa basarsi e cosa cambiare, mostrando ai responsabili come la protezione delle API sia in grado di contribuire a migliorare il fatturato. Mettere d'accordo i reparti addetti alla sicurezza, dai CISO al team AppSec, su come dare priorità alla sicurezza delle API è un buon punto di partenza, a cui deve seguire la promozione di una comunicazione aperta tra i dirigenti e i membri del team AppSec dedicati, nonché ai livelli manageriali intermedi.

Procedure da adottare

A conclusione del nostro studio, abbiamo messo insieme una serie di procedure progressive che i team addetti alla sicurezza possono adottare per iniziare, o per migliorare, la propria strategia di sicurezza delle API e passare ad un livello superiore di protezione delle API.

1 Iniziare con l'individuazione e la visibilità delle API

Per stilare un inventario completo dell'intero patrimonio delle API, vi servono strumenti che dispongono di un approccio automatizzato all'individuazione delle API e dei microservizi supportati. L'ampiezza della copertura è fondamentale perché le API non gestite (vedere la sezione laterale a pagina 10) sono un obiettivo di primo piano per i criminali.

2 Investire nell'esecuzione dei test

Scegliere una soluzione per la sicurezza delle API in grado di eseguire facilmente i test delle API per garantirne la corretta codifica e il funzionamento previsto. Teoricamente, i test vanno eseguiti prima dell'implementazione, ma è anche importante eseguire i test di tutte le API che si trovano già in fase di produzione con analisi in tempo reale del traffico e delle potenziali vulnerabilità.

3 Stilare una documentazione completa delle API

È fondamentale controllare l'intero ambiente delle API allo scopo di identificare le API configurate in modo errato o altri tipi di errori. Le funzionalità di controllo dovrebbero anche garantire un'adeguata documentazione di tutte le API e stabilire se le API contengono dati sensibili o non sono sottoposte agli appropriati controlli di sicurezza per aiutarvi così a soddisfare gli obblighi di conformità relativi alla sicurezza delle API in modo implicito o esplicito (vedere a pagina 14).

4 Utilizzare il rilevamento del runtime

Una soluzione per la sicurezza delle API con una funzionalità di rilevamento del runtime automatizzata riesce a distinguere le attività delle API normali da quelle anomale. Monitorando in tal modo le interazioni delle API, è possibile rilevare i comportamenti che indicano una minaccia in tempo reale e intraprendere le azioni appropriate.

5 Rispondere ai comportamenti sospetti

Integrando una soluzione per la sicurezza delle API con i sistemi di sicurezza esistenti (ad es., le soluzioni WAF o WAAP), è possibile individuare un comportamento molto rischioso e bloccare il traffico sospetto prima che possa accedere alle risorse critiche.

6 Effettuare indagini e ricerche sulle minacce

Nel caso di un sistema di sicurezza delle API più avanzato, vengono eseguite analisi approfondite sui dati relativi alle minacce precedenti per scoprire se gli avvisi hanno identificato correttamente le minacce e se sono emersi modelli che attivano una ricerca proattiva delle minacce con una combinazione di strumenti sofisticati e intelligenza umana.

Conclusione

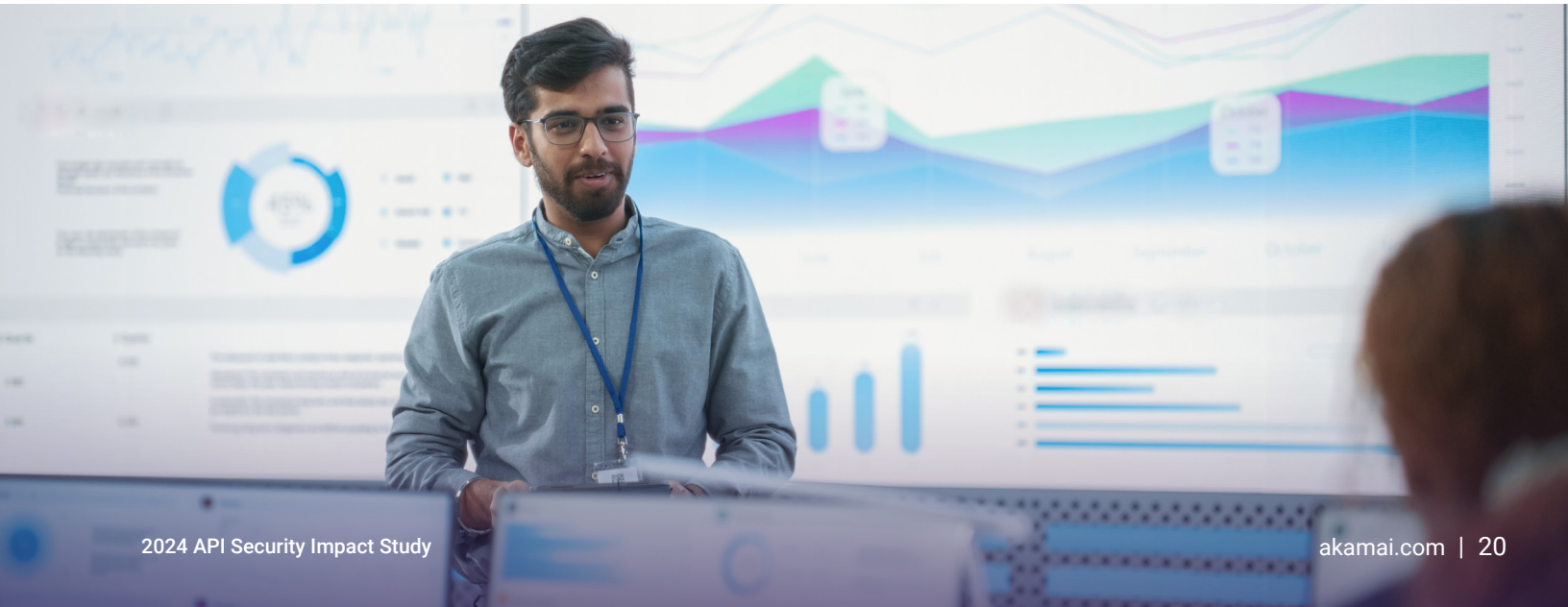
Nel rapporto di quest'anno, è risultato evidente che la sicurezza (in questo caso, la sicurezza delle API) non si esaurisce solo in un elenco di minacce o di strumenti, ma riguarda anche le persone coinvolte.

Il nostro studio conferma che i team addetti alla sicurezza sono oberati di lavoro e che l'aggiunta di un vettore di attacco totalmente nuovo al loro carico di lavoro potrebbe sembrare scoraggiante. Tuttavia, la proliferazione delle API non è destinata a diminuire, pertanto intraprendere le azioni appropriate per proteggere le API provoca una reazione a catena su molti altri aspetti altamente prioritari, come le vulnerabilità basate sull'AI generativa (per proteggere le API che scambiano dati con i modelli LLM) e la sicurezza nel cloud (per ridurre i rischi presenti in tutte le API incluse nei carichi di lavoro che vengono migrati).

Siamo fermamente convinti che adottando un approccio proattivo alla sicurezza delle API, non solo riuscirete a proteggere le vostre attività aziendali, ma anche a fornire al vostro team gli strumenti giusti per migliorare i suoi livelli di credibilità e affidabilità nei confronti di questo importante vettore di attacco tra colleghi, dirigenti e membri del consiglio di amministrazione. Questo approccio avrà l'enorme vantaggio di ridurre i livelli di stress del vostro team, che, secondo il nostro studio, si è rivelato altamente influenzato dai problemi di sicurezza delle API, nonché dai controlli e della perdita di fiducia che generano, sia da parte dei dipendenti che dei clienti.

Intraprendere le azioni appropriate ora facilita anche preventivamente la pianificazione e la creazione di rapporti sulla conformità, per non parlare della prevenzione tempestiva delle sanzioni normative. Allora perché non iniziamo subito?

- Se la vostra azienda è pronta a compiere i passi successivi nel suo percorso volto a migliorare il suo sistema di sicurezza delle API, vi consigliamo di iniziare a consultare il nostro white paper dal titolo Nozioni fondamentali sulla sicurezza delle API.
- Se preferite discutere dei vostri problemi e di come possiamo aiutarvi, potete richiedere facilmente una demo personalizzata su Akamai API Security.



Informazioni sul rapporto API Security Impact Study

Il rapporto 2024 API Security Impact Study è stato stilato sulla base di un sondaggio condotto da Opinion Matters tra il 24 giugno 2023 e il 7 luglio 2024. Il team dedicato al sondaggio ha esaminato un totale di 1.207 partecipanti suddivisi in base alla sede delle loro aziende nel modo seguente: 404 nel Regno Unito, 402 negli Stati Uniti e 401 in Germania. Un terzo dei partecipanti al sondaggio è stato rappresentato da CIO o CISO, un terzo da professionisti della sicurezza e un terzo da team addetti alla sicurezza delle applicazioni appartenenti ad aziende con un numero di dipendenti compreso tra meno di 500 e più di 1000 unità, che operavano in otto settori principali: automotive, servizi finanziari, retail/e-commerce, settore sanitario, assicurazioni, pubblica amministrazione, settore manifatturiero e servizi di pubblica utilità

Opinion Matters è vincolata al codice di condotta e ai requisiti stabiliti da Market Research Society, a cui appartengono i suoi dipendenti, e si attiene ai principi di ESOMAR. Opinion Matters fa anche parte del British Polling Council.

Riconoscimenti

Redattore
Annie Brunholzl

Caporedattore
John Natale

Direttore della ricerca
Mitch Mayne

Revisore di testi
Randi Kravitz

Promozioni
Barney Beal

Marketing ed editoria
Georgina Morales Hampe

Revisione e contributi di esperti del settore
Pam Cobb
Jim Lubinskas
Kimberly Gomez
Stas Neyman

Stato di Internet - Security

Leggete i numeri precedenti e consultate le prossime pubblicazioni degli acclamati rapporti sullo stato di Internet - Security di Akamai sul sito **akamai.com/soti**

Ricerca sulle minacce di Akamai

Restate aggiornati con le ultime novità in materia di intelligence sulle minacce, rapporti sulla sicurezza e ricerche sulla cybersicurezza consultando il sito **akamai.com/security-research**

dopo aver implementato la soluzione Akamai API Security

Scoprite come Akamai sia in grado di proteggere le API per tutto il loro ciclo di vita, dallo sviluppo alla produzione, con importanti funzionalità di individuazione delle API, gestione dei sistemi, protezione del runtime ed esecuzione di test sulla sicurezza delle API. **https://www.akamai.com/products/api-security**