
Akamai
I 7 miti sulla protezione interna al browser

Non è un segreto che Internet esponga le applicazioni e le risorse rivolte al web a una serie diversificata e complessa di attacchi informatici. Sebbene le organizzazioni si concentrino in modo significativo sulla protezione delle proprie applicazioni mission-critical dagli attacchi lato server, molte sottovalutano il danno che può essere inflitto dalle minacce lato client all'interno del browser o all'interno della pagina web stessa. Questo punto cieco lascia i siti web esposti a pericolose vulnerabilità lato client che possono causare frodi, sottrazione di dati sensibili e danni alla fiducia dei clienti.

Analizziamo alcuni dei frequenti falsi miti sulla protezione interna al browser per avere un quadro più chiaro di qual è realmente la posta in gioco.

Mito numero 1

Una CSP (Content Security Policy) è la difesa lato client più efficace

Una policy di sicurezza dei contenuti è uno standard di sicurezza che consente agli operatori di siti web di controllare in modo granulare quali risorse possono essere eseguite all'interno del browser, inclusi gli script. Le intestazioni di risposta della policy di sicurezza dei contenuti vengono utilizzate per mantenere un elenco di domini approvati considerati fonti legittime e sicure di codice eseguibile. Possono essere una parte fondamentale del vostro sistema di difesa contro le minacce JavaScript, ma richiedono un'elevata quantità di risorse per essere gestite e la maggior parte degli attacchi lato client si verificano sfruttando fonti attendibili. Ecco perché è importante comprendere il comportamento di tutti gli script in esecuzione sul vostro sito, anche quelli attendibili. Akamai Page Integrity Manager sfrutta la tecnologia comportamentale per monitorare il comportamento di esecuzione di tutti gli script su una pagina web, acquisendo informazioni sulle azioni degli script e sulle loro relazioni con altri script. Quindi abbina questi dati a un approccio di rilevamento a più livelli che include euristica, valutazione del rischio, intelligenza artificiale e molto altro, per identificare immediatamente l'attività sospetta.

Il **94%**
dei siti web oggi sfrutta almeno uno script di terze parti

Fonte: Terze parti, novembre 2021

Mito numero 2

Un WAF protegge la mia organizzazione dagli attacchi di web-skimming

Un WAF (Web Application Firewall) è una soluzione per la sicurezza che protegge le applicazioni web dagli attacchi comuni, monitorando e filtrando il traffico, bloccando il traffico dannoso in ingresso in un'applicazione web o i dati in uscita dall'app. I WAF sono incentrati sulla protezione della connessione tra i server e gli utenti finali, ma non sono progettati per proteggere la vostra applicazione web a livello di browser. Poiché gli attacchi di web skimming si verificano all'interno del browser dell'utente finale tramite l'esecuzione di codice dannoso, i WAF non sono in grado né di rilevare né di mitigare.

Mito numero 3

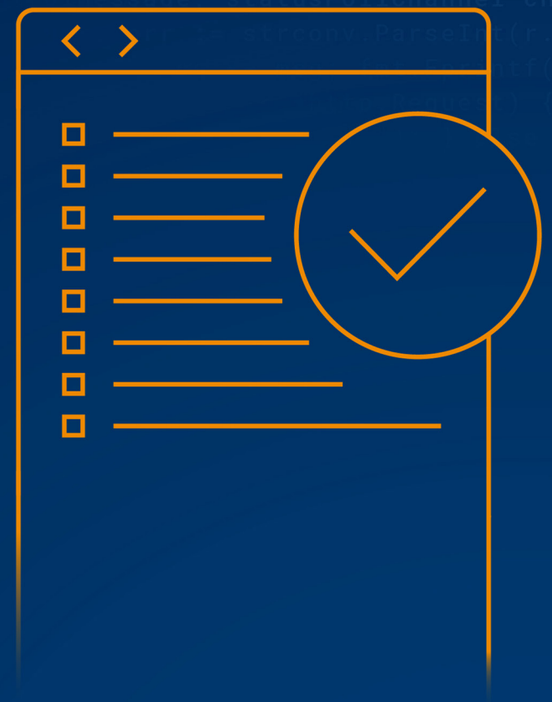
Gli attacchi Magecart non si verificano così frequentemente oggi come in passato

Gli attacchi Magecart sono più attivi che mai: stanno diventando sempre più difficili da rilevare. Di recente, il nostro team Akamai per la ricerca sulle minacce ha scoperto una campagna globale Magecart che ha preso di mira diversi siti di e-commerce utilizzando tecniche sofisticate, come impersonare un noto fornitore di terze parti come Google Tag Manager o utilizzare la codifica Base64 per mascherare il codice dannoso. È un gioco tra gatto e topo, in cui gli autori delle minacce cercano di aggirare le misure di sicurezza ed attacchi di web-skimming in modi più intelligenti per non essere rilevati. Akamai Page Integrity Manager monitora tutti i comportamenti degli script, incluso il modo in cui interagiscono con altri script per esporre qualsiasi attività sospetta e difende rapidamente anche dagli attacchi più avanzati. Per ulteriori informazioni, leggete il nostro recente post del blog.

Mito numero 4

Non vedo l'ora di rispettare i nuovi requisiti di script per PCI DSS v4.0

Nel marzo 2022, è stata rilasciata l'ultima versione di PCI DSS (v4.0) per affrontare le minacce in evoluzione ai dati delle carte di pagamento e i cambiamenti critici del mercato che si sono verificati dalla versione precedente di PCI DSS v3.2.1 nel 2018. Come parte dei nuovi requisiti 6.4.3 e 11.6, qualsiasi organizzazione che elabora le carte di pagamento online deve ora sapere quali script vengono eseguiti sul proprio sito, quando tali script cambiano e quando ciascuno di essi smette di funzionare, per difendersi dagli attacchi di script interni al browser. Sebbene PCI DSS v4.0 non entrerà in vigore fino al 2025, non potete permettervi di ritardare la protezione dal furto e dall'esfiltrazione dei dati sensibili delle carte di pagamento dalle pagine di pagamento del vostro sito web. Akamai Page Integrity Manager può contribuire ad accelerare la conformità PCI oggi stesso.



Mito numero 5

Il dirottamento degli utenti non è una grande sfida per i retailer online

Dirottamento degli utenti ("audience hijacking") è il termine utilizzato per descrivere attività del browser indesiderate e talvolta dannose che si verificano a seguito di estensioni del browser o plug-in installati sul lato client. Queste attività indesiderate possono includere frodi di affiliazione, reindirizzamenti non autorizzati a siti concorrenti o dannosi, sconti non intenzionali e annunci pubblicitari che distraggono e possono impedire a un visitatore di completare un acquisto. Le organizzazioni stimano che il 15%-24% delle visite totali al proprio sito web venga interrotto da tattiche di dirottamento degli utenti.

Cosa può comportare? Tassi di conversione inferiori, diminuzione della fedeltà al brand e milioni di potenziali profitti persi. Akamai Audience Hijacking Protector consente agli utenti di ottenere visibilità sull'impatto delle comuni estensioni del browser sulle sessioni del sito e sul modo in cui gli operatori delle estensioni potrebbero condurre attività dannose. Vi consente di decidere quali estensioni sono autorizzate a interagire con il vostro sito, utilizzando l'impostazione di policy granulari a livello di singola estensione per bloccare o consentire l'attività.

Le organizzazioni stimano che il

15%-24%

delle visite totali al proprio sito web venga interrotto da tattiche di dirottamento degli utenti

Fonte: Awareness of Audience Hijacking Among Online Retailers, Retail Dive, Febbraio 2023

Mito numero 6

Le piattaforme di experience digitali possono fornire visibilità sulle attività all'interno del browser e sull'impatto delle estensioni del browser

Una piattaforma di experience digitale è un insieme di tecnologie che lavorano insieme per ottimizzare e fornire experience basate sui contenuti. Le attuali analisi fornite da queste piattaforme offrono solo informazioni su ciò che sta accadendo sul lato dell'organizzazione di una sessione del sito e non su quello dell'utente finale. Ciò significa che mentre è possibile monitorare come un visitatore del sito interagisce con il vostro sito e i suoi comportamenti, non disponete della visibilità sulle possibili interazioni del browser con l'utente finale. Comprendendo in che modo le estensioni del browser e le attività indesiderate del browser possono influire sulle sessioni del vostro sito, ottenete una visibilità completa dell'intero percorso del cliente per definire meglio i motivi dell'abbandono del carrello.

Mito numero 7

Le estensioni relative a coupon e confronto dei prezzi non sono dannose per la mia attività

Questo è complicato: lo capiamo. A tutti piacciono le occasioni ed estensioni come Honey, Rakuten e Amazon Assistant possono aiutare i retailer online a incrementare i tassi di conversione. Queste estensioni, tuttavia, possono avere un lato oscuro. Prendiamo, ad esempio, un'estensione relativa a un coupon che inserisce automaticamente un codice offerta esclusivo nella pagina di pagamento degli utenti al di fuori del segmento di utenti previsto, causando sconti di massa. O Amazon Assistant che inserisce automaticamente un annuncio sul vostro sito offrendo esattamente il vostro prodotto o servizio a un prezzo inferiore tramite un concorrente. Queste estensioni possono causare una significativa perdita di potenziali profitti e sviare il vostro cliente più fedele. Akamai Audience Hijacking Protector supporta decine delle estensioni del browser più popolari al mondo e la nostra dashboard avanzata fornisce informazioni a livello di singola estensione, consentendo agli utenti di analizzare quali estensioni sono effettivamente vantaggiose per l'azienda e quali semplicemente non vale la pena autorizzare.

Nel traffico globale del sito dei clienti Akamai, il numero di sessioni del sito interessate dalle estensioni relative a coupon o al confronto di prezzi è aumentato del

25%

tra il Black Friday e il CyberMonday

Fonte: Ricerca sulle minacce di Akamai, 2022

Il contributo di Akamai

È chiaro che il rischio di essere colpiti da un attacco lato client sta aumentando e ottenere visibilità sui comportamenti all'interno del browser e sulle attività indesiderate è fondamentale per ridurre il rischio. Page Integrity Manager di Akamai protegge i siti web dalle minacce Javascript, come attacchi di web skimming, form jacking e Magecart, identificando le risorse più vulnerabili, rilevando i comportamenti sospetti e bloccando le attività dannose. E per arrestare comportamenti indesiderati all'interno del browser, Audience Hijacking Protector offre visibilità in tempo reale sulle attività del browser che si verificano sul vostro sito di e-commerce con analisi granulari e opzioni di mitigazione.

Scoprite come il sistema di difesa delle applicazioni **e** delle API e le soluzioni di protezione interne al browser di Akamai possono aiutarvi a migliorare le strategie di sicurezza lato client.