
Akamai
Die 7 Mythen des Schutzes auf Browserebene

Es ist kein Geheimnis, dass das Internet webbasierte Anwendungen und Assets einer Vielzahl unterschiedlicher und komplexer Cyberangriffe aussetzt. Unternehmen legen großen Wert auf den Schutz ihrer unternehmenskritischen Anwendungen vor serverseitigen Angriffen. Doch viele unterschätzen den Schaden, der durch clientseitige Bedrohungen im Browser oder auf der Webseite selbst verursacht werden kann. Dieser blinde Fleck führt dazu, dass Websites gefährlichen clientseitigen Sicherheitslücken ausgesetzt sind, die zu Betrug, zur Extraktion sensibler Daten und zur Schädigung des Kundenvertrauens führen können.

Lassen Sie uns einige Irrtümer des Schutzes auf Browserebene aufklären, um genau zu verstehen, was wirklich auf dem Spiel steht.

Mythos 1

Eine Content Security Policy (CSP) ist die effektivste clientseitige Verteidigung

Eine Content Security Policy ist ein Sicherheitsstandard, mit dem Websitebetreiber präzise kontrollieren können, welche Assets im Browser ausgeführt werden können, einschließlich Skripten. Antwortheader der Content Security Policy werden verwendet, um eine Liste genehmigter Domains zu verwalten, die als legitime und sichere Quellen von ausführbarem Code gelten. Sie können ein wichtiger Teil Ihrer Abwehr von JavaScript-Bedrohungen sein, doch ihre Verwaltung erfordert eine Menge Ressourcen – und die meisten clientseitigen Angriffe erfolgen unter Einsatz vertrauenswürdiger Quellen. Deshalb ist es wichtig, das Verhalten aller Skripte zu verstehen, die auf Ihrer Website ausgeführt werden – auch das Verhalten der vertrauenswürdigen Skripte. Akamai Page Integrity Manager nutzt Verhaltenstechnologie, um das gesamte Verhalten der Skriptausführung auf einer Webseite zu überwachen und Informationen über die Aktionen von Skripten und deren Beziehungen zu anderen Skripten zu sammeln. Anschließend werden diese Daten mit einem mehrschichtigen Erkennungsansatz kombiniert, der Heuristik, Risikobewertung, künstliche Intelligenz und vieles mehr umfasst, um verdächtige Aktivitäten sofort zu identifizieren.

94 %

der Websites nutzen heute mindestens ein Skript eines Drittanbieters

Quelle: Dritte, November 2021

Mythos 2

Eine WAF schützt mein Unternehmen vor Web-Skimming-Angriffen

Eine Web Application Firewall (WAF) ist eine Sicherheitslösung, die Webanwendungen vor häufigen Angriffen schützt. Hierzu überwacht und filtert sie den Traffic, blockiert schädlichen Traffic auf dem Weg zu Webanwendungen und verhindert, dass Daten unbefugt die Anwendung verlassen. WAFs konzentrieren sich auf den Schutz der Verbindung zwischen Ihren Servern und Endnutzern. Sie sind jedoch nicht darauf ausgelegt, Ihre Webanwendungen auf Browserebene zu schützen. Da für Web-Skimming-Angriffe schädlicher Code im Browser des Endnutzers ausgeführt wird, können WAFs diese Attacken weder erkennen noch abwehren.

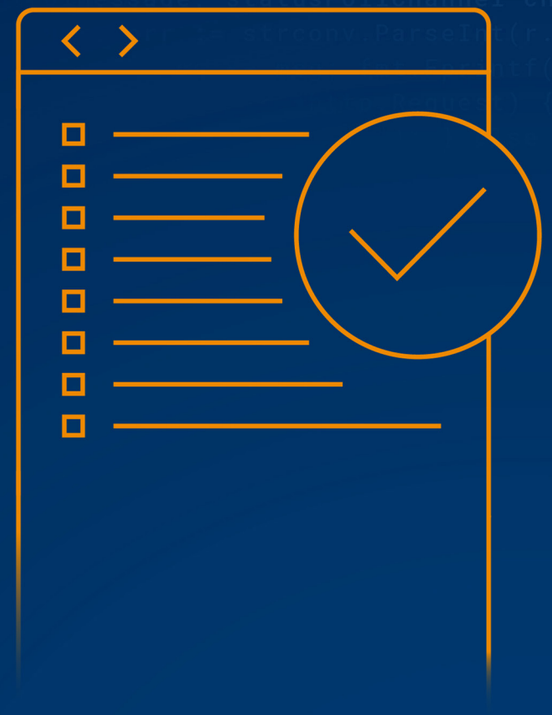
Mythos 3

Magecart-Angriffe passieren heute nicht mehr so häufig wie in der Vergangenheit

Magecart-Angriffe sind aktiver denn je – sie lassen sich nur immer schwieriger erkennen. Vor Kurzem hat unser Akamai Threat Research Team eine globale Magecart-Kampagne entdeckt, die auf mehrere E-Commerce-Websites abzielt. Dabei wurden ausgeklügelte Techniken eingesetzt, wie z. B. die Imitation eines bekannten Drittanbieters wie Google Tag Manager oder Base64-Codierung, um schädlichen Code zu tarnen. Es ist ein Katz-und-Maus-Spiel, bei dem Cyberkriminelle versuchen, Sicherheitsmaßnahmen zu umgehen, und bei ihren Web-Skimming-Angriffen immer intelligenter vorgehen, um unentdeckt zu bleiben. Akamai Page Integrity Manager überwacht alle Verhaltensweisen von Skripten, einschließlich der Interaktion mit anderen Skripten, um verdächtige Aktivitäten aufzudecken, und schützt so schnell vor den fortschrittlichsten Angriffen. Erfahren Sie mehr in unserem aktuellen Blogbeitrag.

Mythos 4

Ich kann noch damit warten, die neuen Skriptanforderungen für PCI DSS 4.0 zu erfüllen



Im März 2022 wurde die neueste Version von PCI DSS (4.0) veröffentlicht, um den immer neuen Bedrohungen für Zahlungskartendaten und kritischen Marktveränderungen zu begegnen, die seit der letzten Veröffentlichung von PCI DSS 3.2.1 im Jahr 2018 aufgetreten sind. Im Rahmen der neuen Anforderungen 6.4.3 und 11.6 muss jedes Unternehmen, das Zahlungskarten online verarbeitet, nun wissen, welche Skripte auf seiner Website ausgeführt werden, wann sich diese Skripte ändern und wann jedes dieser Skripte nicht mehr ausgeführt wird, um sich vor Angriffen durch browserinterne Skripte zu schützen. Obwohl PCI DSS 4.0 erst 2025 in Kraft tritt, können Sie es sich nicht leisten, bis dahin zu warten, um sensible Zahlungskartendaten davor zu schützen, dass sie von den Zahlungsseiten Ihrer Website gestohlen werden. Akamai Page Integrity Manager kann noch heute die PCI-Compliance beschleunigen.

Mythos 5

Audience Hijacking stellt für Online-Einzelhändler keine große Herausforderung dar

Der Begriff „Audience Hijacking“ beschreibt unerwünschte und manchmal schädliche Browseraktivitäten, die durch clientseitige Browsererweiterungen oder Plug-ins auftreten. Zu diesen unerwünschten Aktivitäten gehören Affiliate-Betrug, unbefugte Umleitungen zu konkurrierenden oder schädlichen Websites, unbeabsichtigte Rabatte und ablenkende Werbeinjektionen, die Besucher daran hindern können, einen Kauf abzuschließen. Unternehmen schätzen, dass 15–24 % aller Besuche ihrer Website von einer Audience-Hijacking-Taktik gestört werden.

Was bedeutet das? Geringere Konversionsraten, eine geringere Markentreue und millionenschwere Verluste potenzieller Umsätze. Akamai Audience Hijacking Protector bietet Nutzern Einblicke in die Auswirkungen gängiger Browsererweiterungen auf Websitesitzungen und verrät ihnen, welche schädlichen Aktivitäten Erweiterungsbetreiber durchführen können. Sie können entscheiden, welche Erweiterungen mit Ihrer Site interagieren dürfen, indem Sie detaillierte Richtlinieneinstellungen auf individuelle Erweiterungen anwenden, um Aktivitäten zu blockieren oder zuzulassen.

Unternehmen schätzen, dass

15–24 %

aller Besuche ihrer Website von einer Audience-Hijacking-Taktik gestört werden

Quelle: Awareness of Audience Hijacking among Online Retailers, Retail Dive, Februar 2023

Mythos 6

Digital Experience Platforms bieten Einblicke in Browseraktivitäten und die Auswirkungen von Browsererweiterungen

Eine Digital Experience Platform besteht aus einer Reihe von Technologien, die zusammenarbeiten, um inhaltsgesteuerte Erlebnisse bereitzustellen und zu optimieren. Die aktuellen Analysen, die von diesen Plattformen bereitgestellt werden, liefern zu Websitesitzungen lediglich Einblicke in die Vorgänge aufseiten der Organisation, nicht aufseiten des Endnutzers. Das heißt, dass Sie zwar nachverfolgen können, wie ein Websitebesucher mit Ihrer Website und deren Verhalten interagiert, aber keine Einsicht in die Interaktion zwischen Endnutzer und Browser haben. Wenn Sie verstehen, wie sich Browsererweiterungen und unerwünschte Browseraktivitäten auf Ihre Websitesitzungen auswirken können, erhalten Sie einen umfassenden Überblick über Ihre gesamte Customer Journey und können die Gründe für abgebrochene Käufe besser definieren.

Mythos 7

Erweiterungen für Coupons und Preisvergleiche sind für mein Unternehmen nicht schädlich

Wir wissen, dass dieser Punkt etwas knifflig ist. Jeder liebt ein gutes Angebot und Erweiterungen wie Honey, Rakuten und Amazon Assistant können Online-Einzelhändlern dabei helfen, die Konversionsraten zu steigern. Doch diese Erweiterungen können auch Nachteile mit sich bringen. Nehmen wir als Beispiel eine Couponerweiterung, die bei Nutzern außerhalb Ihrer Zielgruppe automatisch einen exklusiven Angebotscode zum Warenkorb hinzufügt, was zu Massenrabatten führt. Oder Amazon Assistant fügt automatisch eine Anzeige auf Ihrer Website ein, die Ihr exaktes Produkt oder Ihre exakte Dienstleistung zu einem niedrigeren Preis von einem Wettbewerber anbietet. Diese Erweiterungen können zu erheblichen potenziellen Umsatzverlusten führen und Ihre treuesten Kunden in die Irre führen. Akamai Audience Hijacking Protector unterstützt Dutzende der weltweit beliebtesten Browsererweiterungen und unser erweitertes Dashboard bietet Einblicke auf Ebene der einzelnen Erweiterungen. So können Nutzer analysieren, welche Erweiterungen tatsächlich für das Unternehmen von Vorteil sind und welche sie lieber nicht zulassen sollten.

Im gesamten globalen Traffic der Akamai-Kunden stieg die Anzahl der Websitesitzungen, die von Erweiterungen für Coupons und Preisvergleiche betroffen waren, zwischen Black Friday und Cyber Monday um

25 %

Quelle: Akamai Threat Research, 2022

Wie Akamai Sie unterstützen kann

Das Risiko, von einem clientseitigen Angriff getroffen zu werden, wird immer größer. Deshalb ist es entscheidend, Einblicke in das Verhalten innerhalb des Browsers sowie in unerwünschte Aktivitäten zu gewinnen, um das Risiko zu verringern. Der Page Integrity Manager von Akamai schützt Websites vor JavaScript-Bedrohungen wie Web Skimming, Formjacking und Magecart-Angriffen, indem er anfällige Ressourcen identifiziert, verdächtiges Verhalten erkennt und schädliche Aktivitäten blockiert. Und um unerwünschtes Verhalten im Browser zu verhindern, bietet Audience Hijacking Protector Echtzeiteinblicke in Browseraktivitäten, die auf Ihrer E-Commerce-Website stattfinden, sowie umfassende Optionen zur Analyse und Abwehr.

Erfahren Sie, wie Sie mithilfe der Akamai-Lösungen für Anwendungs- und API-Schutz sowie für Schutz auf Browserebene die clientseitige Sicherheit verbessern können.