Mehr clientseitiger Einblick

JavaScript ist für die Bereitstellung eines leistungsstarken Nutzererlebnisses unerlässlich. Leider macht es Ihre Website zugleich anfällig für clientseitige Bedrohungen und den Diebstahl von Endnutzerdaten.

Web-Skimming-, Magecart- und Formjacking-Angriffe können schädliche Folgen für Marken haben – von Bußgeldern bis hin zu Vertrauensverlusten und Umsatzausfällen.

Wo die Infektion beginnt

Ausnutzen der Schwachstellen von Erstanbietern

Fehlerhafte Sicherheitskonfiguration, Framework-Sicherheitslücken usw.

Angriffe auf die Lieferkette von Drittanbietern

Einfügen von schädlichem Code über einen autorisierten Drittanbieter

Wie Web-Skimming-Angriffe Endnutzerdaten stehlen

Endnutzer, der online surft

Webanwendung

Endnutzer gibt **vertrauliche Informationen** auf einer Checkout-Seite ein

Daten werden durch schädliches Skript gestohlen

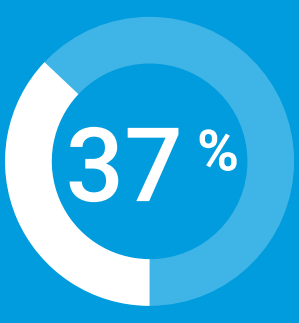
Kompromittiertes JavaScript

Daten werden gestohlen und **extrahiert** (über eine vom Angreifer kontrollierte Domain)

JavaScript von Drittanbietern macht Marken anfällig

Prozentsatz von JavaScript auf Websites, das von Drittanbietern stammt

Einzelhandel und Handel[1]



Finanzdienstleistungen[2]

Eine Bedrohung für Unternehmen jeder Größe

81 % der großen Onlineeinzelhändler geben an, dass ihr Unternehmen im Jahr 2022 von verdächtigem Skriptverhalten betroffen war[3]

Die verheerenden Auswirkungen

4,45 Mio. $	Durchschnittliche Gesamtkosten eines Datenschutzvorfalls weltweit im Jahr 2023[4]
9,48 Mio. $	Durchschnittliche Gesamtkosten eines US-Datenschutzvorfalls im Jahr 2023[4]

PCI-Compliance bedarf jetzt clientseitiger Sicherheit

PCI Security Standards Council

Unternehmen, die Zahlungskartendaten verarbeiten, müssen **bis 2025 die neuen JavaScript-Sicherheitsanforderungen für PCI DSS v4.0 erfüllen**, andernfalls drohen Strafen[5]

Anforderung 6.4.3 | **Anforderung 11.6.1**

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance schützt vor JavaScript-Bedrohungen, optimiert PCI DSS v4.0-Workflows und sorgt für die Sicherheit von Endnutzerdaten. Es bietet Einblick in JavaScript-Sicherheitslücken und analysiert Skriptverhalten, um bösartige und schädliche Skriptaktivitäten zu erkennen. Außerdem werden umsetzbare Warnmeldungen bereitgestellt, mit denen Sicherheitsteams clientseitige Angriffe schnell verhindern und abwehren können.

Weitere Informationen finden Sie auf unserer Produktseite oder beim Vertriebsteam von Akamai.

1. Eine Analyse der Bedrohungstrends im Handelssektor | SOTI-Bericht von Akamai 2023
2. Der hohe Einsatz von Innovationen? Angriffstrends in der Finanzdienstleistungsbranche | SOTI-Bericht von Akamai 2023
3. Von schlechten Bots zu schädlichen Skripten: Die Wirksamkeit spezialisierter Abwehrmechanismen | 2023
4. IBM-Bericht „Cost of a Data Breach“ (Kosten durch Datendiebstahl) | 2023
5. PCI DSS v4.0 | 2022

©2023 Akamai Technologies | Support | | Veröffentlicht: Dezember 2023