AKAMAI-PRODUKTBESCHREIBUNG

Client-Side Protection & Compliance

Schützen Sie sich vor clientseitigen JavaScript-Schwachstellen und optimieren Sie Ihre Compliance

JavaScript ist ein unverzichtbares Tool für moderne Webanwendungen. Von der Optimierung des Nutzererlebnisses bis hin zur Verbesserung von Funktionalität und Performance ist die Verwendung von JavaScript bei Erst- und Drittanbietern im Laufe der Zeit exponentiell gestiegen. Trotz zahlreicher Vorteile, die die Verwendung von JavaScript mit sich bringt, kann eine digitale Lieferkette mit JavaScript Websites auch anfällig für clientseitige Angriffe machen, die darauf abzielen, schädlichen Code zu injizieren, um vertrauliche Informationen des Nutzers über den Browser zu stehlen, einschließlich Zahlungskartendaten.

Da diese Angriffe serverseitig nicht sichtbar sind und herkömmliche Sicherheitsmaßnahmen umgehen, können Unternehmen leicht zu Opfern werden – mit der Folge, dass das Vertrauen der Kunden schwindet, Geldbußen und Strafen für die Nichteinhaltung gesetzlicher Vorschriften drohen und der Ruf der Marke Schaden nimmt.

Akamai Client-Side Protection & Compliance

Akamai Client-Side Protection & Compliance verhindert die Extraktion von Endnutzerdaten und schützt Websites vor JavaScript-Bedrohungen. Es wurde entwickelt, um schädliches Skriptverhalten zu erkennen und verwertbare Warnmeldungen für Sicherheitsteams bereitzustellen, damit schädliche Aktivitäten in Echtzeit entschärft werden können.

Mit speziell entwickelten Funktionen zur Einhaltung von PCI DSS v4.0 unterstützt Client-Side Protection & Compliance Unternehmen bei der Erfüllung der neuen Skriptsicherheitsanforderungen und schützt Zahlungskartendaten vor clientseitigen Angriffen. So können Sie das Inventar an Skripten auf Ihrer Zahlungsseite einfach verwalten, den Auditprozess über ein einziges, umfassendes Dashboard rationalisieren und spezielle PCI-Warnmeldungen erhalten, um schnell auf Compliance-bezogene Ereignisse zu reagieren.

Wichtige Funktionen

Schutz vor Exfiltration sensibler Daten auf Clientseite

Cyberkriminelle sind auf der Jagd nach den sensiblen Daten Ihrer Endnutzer. Indem sie Schwachstellen in JavaScript-Lieferketten ausnutzen, sind schädliche Akteure in der Lage, Code in Websites einzuschleusen, um vertrauliche Informationen abzugreifen und zu betrügerischen Zwecken zu extrahieren. Client-Side Protection & Compliance verbindet maschinelles Lernen und heuristische Risikobewertung, um das Skriptverhalten in Echtzeit zu analysieren und schädliche Aktivitäten und anfällige Ressourcen zu erkennen. Es bietet Sicherheitsteams sofortige, umsetzbare Warnmeldungen, um sich schnell gegen clientseitige Angriffe zu schützen, einschließlich Web Skimming, Magecart und Formjacking.

VORTEILE FÜR IHR UNTERNEHMEN

Erkennung und Schutz
Überwachung des Skriptverhaltens in Sitzungen echter Nutzer zur Erkennung verdächtiger Aktivitäten

PCI DSS v4.0-Workflows
Erfüllung der JavaScript-Sicherheitsanforderungen 6.4.3 und 11.6.1

Priorisierte Echtzeit-Warnmeldungen
Sofortige Abwehr risikoreicher Ereignisse durch umsetzbare Warnmeldungen

Clientseitige Transparenz
Umfassender Einblick in Ihre clientseitige Angriffsfläche

Verwaltung von Richtlinien
Steuerung des Skriptverhaltens und Kontrolle der JavaScript-Ausführung zur Laufzeit

Schwachstellenerkennung
Identifizierung gängiger Schwachstellen und Risiken (CVEs) mit Unterstützung von Akamai Threat Intelligence

Flexible Bereitstellungsoptionen
Einfache Bereitstellung über die Akamai Connected Cloud oder direkt auf dem Ursprungsserver

Akamai

Dedizierte Unterstützung für PCI DSS v4.0-Compliance

Die Skript-Sicherheitsanforderungen 6.4.3 und 11.6.1 der PCI DSS v4.0 erfordern, dass Unternehmen Zahlungskartendaten vor clientseitigen Angriffen schützen und die Skriptverwaltung auf Zahlungsseiten gewährleisten. Client-Side Protection & Compliance verfolgt und inventarisiert alle Skripte auf Zahlungsseiten, um deren Integrität und Autorisierung sicherzustellen. Es bietet vordefinierte Begründungen und automatisierte Regeln, um alle geladenen Skripte einfach zu legitimieren. Die Lösung überwacht außerdem Änderungen an HTTP-Headern und den Schutz von Zahlungsseiten, um vor Seitenmanipulationen zu schützen. Ein umfassendes Dashboard und spezielle PCI-Warnmeldungen ermöglichen es Unternehmen, schnell auf Compliance-bezogene Ereignisse zu reagieren und den Schutz von Zahlungskartendaten im Browser sicherzustellen. Mit diesen Funktionen können Sicherheits- und Compliance-Teams die Arbeit durch den PCI-Prüfungsprozess reduzieren und Workflows schnell optimieren.

Umfassender Einblick in JavaScript-Bedrohungen

Herkömmliche Schutzmechanismen für Webanwendungen wie z. B. Web Application Firewalls überwachen nur den serverseitigen Traffic und bieten keinen Einblick in clientseitige Aktivitäten. Auf Standards basierende Ansätze zum Schutz vor solchen Bedrohungen, wie z. B. Richtlinien zur Inhaltssicherheit, sind schwer zu verwalten und bieten nur begrenzten Schutz vor schädlichen Payloads, die in der Lieferkette von Skripten außerhalb der Kontrolle der Webseitenbetreiber eingeschleust werden. Dies erzeugt einen blinden Fleck für Unternehmen, sodass schädlicher Code für Tage, Wochen oder sogar Monate unentdeckt bleiben kann, während er ungehindert sensible Daten stiehlt. Client-Side Protection & Compliance bietet einen beispiellosen Einblick in die clientseitige Angriffsfläche Ihrer Website wie das Verhalten, die Schwachstellen, die Reichweite und die Auswirkungen jedes Skripts sowie der Daten, auf die zugegriffen wird oder die von ihm ausgehende Gefahr.

So funktioniert es

Client-Side Protection & Compliance wird im Browser des Endnutzers ausgeführt, um clientseitige Skriptausführungen auf einer geschützten Webseite zu überwachen. Wenn sich das Verhalten von Skripten ändert, werden Techniken des maschinellen Lernens eingesetzt, mit denen das Risiko nicht autorisierter oder unangemessener Aktionen bewertet wird. Die Lösung gibt Warnmeldungen über risikoreiche Ereignisse aus und ermöglicht so die sofortige Untersuchung und Abwehr potenzieller Bedrohungen.

Einrichtung Einfache Skripte werden ohne nennenswerte Auswirkungen auf die Performance in jede überwachte Seite eingefügt.

Überwachung und Bewertung JavaScript-Aktivitätsdaten werden vom Webbrowser des Nutzers gesammelt und überwacht. Dazu werden Techniken des maschinellen Lernens eingesetzt, um das Risiko unautorisierter oder unangemessener Handlungen zu bewerten, falls diese festgestellt werden.

Warnung Wird eine aktive Bedrohung oder ein Angriff entdeckt, werden in Echtzeit Warnmeldungen mit detaillierten Informationen zur Bedrohungsabwehr gesendet.

Abwehr Schädliches JavaScript wird mit einem einzigen Klick sofort daran gehindert, auf geschützte Seiten zuzugreifen und sensible Daten zu extrahieren.

Beschleunigen Sie die Compliance mit den Skript-Sicherheitsanforderungen PCI DSS v4.0

Skript-Integrität und -Autorisierung (6.4.3)

Stellen Sie die Integrität und Autorisierung aller auf geschützten Zahlungsseiten geladenen Skripte sicher.

Skript-Inventar und -Begründung (6.4.3)

Verfolgen und inventarisieren Sie Skripte, die auf geschützten Zahlungsseiten geladen werden. Belegen Sie alle Skripte schnell mit vordefinierten Begründungen und automatisierten Regeln.

Schutz von Zahlungsseiten (11.6.1)

Erkennen und reagieren Sie umgehend auf unbefugte Änderungen auf geschützten Zahlungsseiten.

Intuitives Dashboard

Vereinfachen Sie die Compliance mit PCI DSS v4.0 und den Auditprozess über ein spezielles Dashboard mit detaillierten Informationen zu den entsprechenden Aufgaben und Warnmeldungen für die Skript-Sicherheitsanforderungen 6.4.3 und 11.6.1.

Umsetzbare PCI-Warnungen

Sie erhalten detaillierte Warnmeldungen zu PCI-Compliance-bezogenen Ereignissen, z. B. nicht autorisierte Skripte, Extraktion von Zahlungsdaten und Manipulation von Zahlungsseiten, und können diese protokollieren.

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

 | Support | Veröffentlicht: 09/23