AKAMAI-CHECKLISTE

JavaScript-Sicherheitscheckliste für PCI DSS v4.0 mit Akamai Client-Side Protection & Compliance

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein globaler Sicherheitsstandard, der die Datensicherheit von Zahlungskartenkonten fördern und so die weltweite Einführung einheitlicher Datensicherheitsmaßnahmen erleichtern soll. Er ist einer der wichtigsten Sicherheitsstandards. Jedes Unternehmen, das Zahlungskartendaten online verarbeitet, ist zur Compliance verpflichtet.

Die neueste Version von PCI DSS (nur in englischer Sprache verfügbar), Version 4.0, tritt 2025 in Kraft. Sie umfasst zwölf grundlegende Anforderungen an die Datensicherheit, die mit Hinweisen zur Bewältigung neuer und sich weiterentwickelnder Cybersicherheitsbedrohungen aktualisiert wurden. Zwei wichtige Anforderungen (6.4.3 und 11.6.1), die in PCI DSS v4.0 integriert wurden, beziehen sich auf JavaScript-Sicherheit und den Schutz vor clientseitigen Web-Skimming-Angriffen, bei denen vertrauliche Endnutzerinformationen über den Browser gestohlen werden. Diese Angriffe haben im Laufe der Jahre an Popularität gewonnen und ihre Erkennung ist aufgrund ausgefeilterer Techniken immer schwieriger geworden. Sie können verheerende Folgen für attackierte Unternehmen haben, darunter hohe Geldstrafen, Imageschäden, Umsatzeinbußen und schwindendes Vertrauen der Kunden.

Sehen wir uns nun eine Checkliste an, die zusammenfasst, was die Skript-Sicherheitsanforderungen für den neuen PCI DSS v4.0 bedeuten und wie Client-Side Protection & Compliance hier unterstützen kann.

Anforderungen von PCI DSS v4.0	So unterstützt Client-Side Protection & Compliance
Anforderung 6.4.3 – Öffentliche Webanwendungen sind vor Angriffen geschützt ☑ Implementierung einer Methode, um zu bestätigen, dass jedes im Browser geladene und ausgeführte Skript autorisiert ist ☑ Implementierung einer Methode, um die Integrität jedes im Browser geladenen und ausgeführten Skripts sicherzustellen ☑ Führen einer Übersicht aller im Browser geladenen und ausgeführten Skripte mit schriftlicher Begründung, warum jedes erforderlich ist	**Autorisierung mit einem Klick** ☑ Verwalten Sie einfach direkt im Tool, welche Skripte auf den Zahlungsseiten Ihrer Website ausgeführt werden dürfen **Integrität von Anfang an** ☑ Die Verhaltenserkennungstechnologie analysiert jedes im Browser ausgeführte Skript, um schädliche Aktivitäten oder Datenextraktion zu entdecken und darauf hinzuweisen **Automatisches Nachverfolgen und Inventarisieren aller Skripte** ☑ Vordefinierte Begründungen und automatisierte Regeln erleichtern es, den Zweck jedes im Browser geladenen und ausgeführten Skripts zu begründen

Anforderungen von PCI DSS v4.0	So unterstützt Client-Side Protection & Compliance

Anforderung 11.6.1 – Nicht autorisierte Änderungen auf Zahlungsseiten erkennen und darauf antworten

Ein Mechanismus zur Änderungs- und Manipulationserkennung wird wie folgt eingesetzt:

- ☑ Um Mitarbeiter auf unbefugte Änderungen (einschließlich Indicators of Compromise, Ergänzungen und Löschungen) an den HTTP-Headern und dem Inhalt der Zahlungsseiten hinzuweisen, die vom Kundenbrowser empfangen werden
- ☑ Der Mechanismus ist so konfiguriert, dass der empfangene HTTP-Header und die empfangene Zahlungsseite ausgewertet werden

Die Funktionen des Mechanismus werden mindestens einmal alle sieben Tage oder in regelmäßigen Abständen angewandt (in der Häufigkeit, die in der gemäß allen in Anforderung 12.3.1 genannten Elementen durchgeführten, gezielten Risikoanalyse des Unternehmens festgelegt ist)

Schützen Sie Ihre Zahlungsseiten

- ☑ Überwachen, analysieren und entschärfen Sie Manipulationen von Zahlungsseiten, um sicherzustellen, dass die wertvollen Daten Ihrer Endnutzer sicher bleiben

Untersuchen Sie nicht autorisierte Änderungen in Echtzeit mit sofortigen, umsetzbaren Warnmeldungen

- ☑ Dank der sofortigen Erkennung können Sicherheitsteams schnell auf unbefugte Änderungen oder Modifikationen an HTTP-Headern auf Zahlungsseiten reagieren

Sorgen Sie mit einer jederzeit aktiven Verteidigung für Schutz

- ☑ Die rund um die Uhr verfügbare Abwehr schützt die Nutzerinteraktionen auf Ihren Zahlungsseiten

Akamai Client-Side Protection & Compliance bietet zuverlässigen Schutz vor JavaScript-Bedrohungen und ermöglicht transparenten Einblick in die clientseitige Angriffsfläche, um vertrauliche Daten im Browser zu schützen. Die speziell auf PCI DSS v4.0 ausgerichteten Funktionen erleichtern Sicherheits- und Compliance-Teams den PCI DSS v4.0-Auditprozess und bieten dedizierte Workflows, um die Skript-Sicherheitsanforderungen 6.4.3 und 11.6.1 zu erfüllen.

Akamai Client-Side Protection & Compliance bietet flexible Bereitstellungsoptionen und erfordert keine aktive Akamai Connected Cloud.

Erfahren Sie mehr darüber, wie diese Funktionen Ihr Unternehmen bei der Einhaltung von PCI DSS v4.0 unterstützen können.