CLOUDFLARE

WHITEPAPER

Ein strategischer Ansatz zur PCI DSS 4.0-Konformität

Inhalt

Übersicht

Alle Unternehmen, die Transaktionen mit Kredit-, Debit- oder Prepaid-Karten verarbeiten, müssen den Payment Card Industry Data Security Standard (PCI DSS) einhalten. Dazu gehören kleine Händler, Einzelhandelsfirmen, E-Commerce-Websites, Banken und Großkonzerne. Die Verlagerung in die Cloud und die Umstellung auf hybride Arbeitsmodelle in Verbindung mit der Einführung von PCI DSS 4.0 machen eine effiziente Einhaltung der Standards jedoch schwierig.

In der heutigen digital-modernisierten Welt benötigen wir einen neuen Ansatz, um den Compliance-Prozess zu optimieren und skalierbar zu machen. Nur dann können Unternehmen mit dem dynamischen regulatorischen Umfeld Schritt halten, das sich im Zuge der digitalen Modernisierung rasant verändert.

Herausforderungen der PCI DSS-Konformität für moderne Unternehmen

Die Einhaltung der PCI-Richtlinien ist unerlässlich, denn wer dagegen verstößt, muss mit Geldstrafen, Klagen und behördlichen Ermittlungen rechnen. Doch die Befolgung der Vorschriften stellt unter anderem Finanzinstitute und den Online-Handel vor einige Herausforderungen.

Dass IT-Teams aufgrund der zunehmenden Verbreitung von Cloud Computing und Remote-Arbeit die Kontrolle über ihre digitalen Umgebungen verloren haben, macht es nicht leichter.

Zeit- und Ressourcenzuweisung: 53 % der Unternehmen geben an, dass sie im technischen Datenschutz unterbesetzt sind, was die Einhaltung der Vorschriften erschwert.[1]

Komplexität bei der Integration des Tech-Stacks: Die Integration und Wartung der notwendigen Technologien zur Einhaltung von Compliance-Standards, wie Verschlüsselung und Firewall-Konfigurationen, ist oft komplex. In Unternehmen mit Altsystemen oder solchen, die eine digitale Transformation durchlaufen, ist dieses Problem noch größer.

Konformität der Anbieter: Zusätzlich verkompliziert wird die Aufgabe durch die Notwendigkeit, sich zu vergewissern, dass auch externe Dienstleister und Anbieter die PCI-Standards einhalten.

Datensicherheit in unterschiedlichen Umgebungen: Durch das Aufkommen von Cloud Computing und mobilem Bezahlen wird es immer schwieriger, die Compliance in unterschiedlichen und oft weniger gut kontrollierten Umgebungen sicherzustellen.

Auditing: IT-Teams müssen einen aktuellen Prüfpfad für die gesamte Infrastruktur und alle Systeme vorweisen können, um die Einhaltung der Vorschriften zu gewährleisten.

Dank PCI DSS 4.0 mit raffinierten Cyberbedrohungen Schritt halten

PCI DSS 4.0 wurde am 31. März 2022 veröffentlicht und tritt am 31. März 2024 in Kraft. Zusätzliche Anforderungen werden am 31. März 2025 eingeführt. PCI DSS 4.0 hat folgende Ziele:[2]

1. Weiterhin die Sicherheitsanforderungen der Zahlungsbranche erfüllen

- **Erhöhte Authentifizierungsanforderungen:** Es wird mehr Wert auf die Authentifizierung gelegt, insbesondere auf die Multi-Faktor-Authentifizierung für alle Zugriffe auf die Cardholder Data Environment (CDE). Die Anforderungen an Passwörter sind ebenfalls strenger geworden, so wurde etwa die Mindestzeichenzahl von acht auf zwölf erhöht.
- **Strengere Verschlüsselungsanforderungen:** PCI DSS 4.0 schreibt die Verwendung einer „starken" Verschlüsselung für die Speicherung und Übertragung von Karteninhaberdaten vor. Ein Beispiel dafür wäre die TLS-Verschlüsselung, bei der bisher keine Schwachstellen bekannt sind.
- **Neue E-Commerce- und Phishing-Bestimmungen, um aktuellen Bedrohungen zu begegnen:** PCI 4.0 enthält zusätzliche Anforderungen für die clientseitige Sicherheit und für den Schutz vor Phishing und Social Engineering.

2. Sicherheit als kontinuierlichen Prozess fördern

- **Zusätzlicher Fokus auf Risikoanalyse und -management:** Unternehmen werden ermutigt, kontinuierliche Risikoanalyse- und Managementprozesse zu implementieren, um Schwachstellen umgehend zu erkennen und zu beheben.
- **Stärkerer Fokus auf Verantwortlichkeit und Kontrolle:** Die neue Version legt einen stärkeren Schwerpunkt auf die Verwaltung von Karteninhaberdaten und die Verantwortung, regelmäßig Sicherheitskontrollen durchzuführen.
- **Nähere Anweisungen für die Umsetzung und Erfüllung der Sicherheitsanforderungen:** PCI 4.0 präzisiert die Ziele des Standards und die dafür vorgesehenen Zeitrahmen.

3. Mehr Flexibilität für verschiedene Methoden

- **Integration neuer Technologien:** PCI DSS 4.0 befasst sich mit der Sicherheit von neuen Technologien wie cloudbasierten und mobilen Zahlungssystemen.
- **Mehr Flexibilität bei der Art und Weise, in der Unternehmen ihre Sicherheitsziele erreichen können:** Unternehmen können zur Erfüllung der Anforderungen einen „maßgeschneiderten Ansatz" verfolgen, d. h. eine breitere Palette von Methoden nutzen. Zudem bietet PCI 4.0 mehr Flexibilität bei der Häufigkeit, mit der Maßnahmen angewandt werden, die auf gezielten Risikoanalysen basieren.

4. Validierungsmethoden verbessern

- **Kontinuierliche Überwachung und Tests:** Der neue Standard empfiehlt statt einer jährlichen Überprüfung der Vorschriftenkonformität eine kontinuierliche Überwachung von Sicherheit und Compliance.
- **Bessere Abstimmung von Selbstbewertungen und Compliance-Bescheinigungen:** Die Informationen in den Selbstbewertungsbögen oder Compliance-Berichten stimmen besser mit den in den Compliance-Bescheinigungen zusammengefassten Informationen überein.

Die Lösung: Ein neuer Ansatz für die PCI-Anforderungen mittels der Connectivity Cloud von Cloudflare

Sicherheits- und IT-Teams müssen die PCI-Anforderungen auf eine einfache und programmierbare Weise erfüllen, die sich problemlos in ihre aktuelle Sicherheits- und Technologielösung integrieren lässt – auch dann, wenn sich ihre Infrastruktur und der PCI DSS weiterentwickeln.

Die Antwort liegt nicht in einem Mosaik aus veralteten und isolierten Sicherheitslösungen. Benötigt wird eine einzige Plattform mit cloudnativen Sicherheits- und Netzwerkdiensten, mit deren Hilfe Unternehmen die Kontrolle über ihre IT-Umgebungen wiedererlangen und verschiedene Compliance-Anforderungen, einschließlich PCI, erfüllen können. Eine solche Plattform wird als Connectivity Cloud bezeichnet.

Das bietet die Connectivity Cloud von Cloudflare:

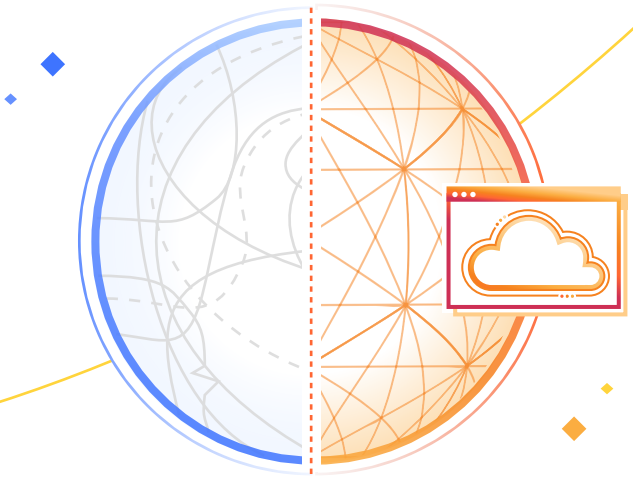
- Eine für Datenkonformität ausgelegte Plattform
- Eine gemeinsame Richtlinien-Engine
- Datenhoheit ohne Kompromisse
- Smarte Berichterstattung für erfolgreiche Audits

Cloudflare ermöglicht IT-Teams standortübergreifend einheitliche Kontrollen, die über eine einzige Steuerungsebene überall aktiviert werden können.

Teams können Protokolle zu Audit-Zwecken direkt von der Cloudflare-Edge an ein bevorzugtes SIEM- oder Cloud-Ziel senden. Der umfassende Überblick über den Internet-Traffic bedeutet auch, dass Cloudflare neue Bedrohungen automatisch erkennen und abwehren kann.

Cloudflare selbst ist PCI-konform und unterstützt von Haus aus die Anforderungen von PCI DSS 4.0. Mit Cloudflare kann zum Beispiel problemlos eine Multi-Faktor-Authentifizierung durchgesetzt werden, ein wichtiger Schwerpunkt von PCI DSS 4.0. Cloudflare unterstützt auch die neuesten Verschlüsselungsstandards bzw. wirkt oft aktiv bei deren Entwicklung mit, sodass Kunden die PCI DSS 4.0-Anforderungen für die Verschlüsselung sensibler Daten erfüllen können.

Eine zusammenfassende Zuordnung der PCI DSS-Anforderungen zu den Funktionen der Connectivity Cloud von Cloudflare finden Sie auf der nächsten Seite:



Wichtige Bereiche, in denen Cloudflare bei der Erfüllung der PCI-Anforderungen helfen kann*

PCI-Anforderung	Die Lösung von Cloudflare
1. Installation und Pflege von Netzwerksicherheitskontrollen (früher „Installation und Wartung einer Firewall“)	Cloudflare schützt Netzwerke, Anwendungen und Cloud-Implementierungen gleichermaßen vor bösartigem Netzwerk-Traffic. Mithilfe von Daten zu Hunderten Milliarden täglich registrierter Bedrohungen werden Websites und Webanwendungen vor Gefahren aus dem Internet wie den OWASP Top 10 und Zero-Day-Angriffen geschützt. Die Sicherheitsplattform von Cloudflare ist cloudnativ, lässt sich innerhalb weniger Minuten einrichten und ermöglicht es Nutzern, globale Richtlinienänderungen in Sekundenschnelle umzusetzen.
2. Anwendung sicherer Konfigurationen bei allen Systemkomponenten	Nutzer, Geräte und Anwendungen hinter Cloudflare sind stark verschlüsselt und werden vor potenziellen Angreifern aus dem Internet verborgen. Mit API Shield von Cloudflare können Nutzer Sicherheitsvorkehrungen gegen Schwachstellen in ihren API treffen, indem sie Sequenzen identifizieren und Richtlinien für API-Transaktionen durchsetzen.
3. Schutz gespeicherter Kontodaten durch starke Verschlüsselung oder andere Datenschutzmethoden	Cloudflare kann gespeicherte personenbezogene Informationen identifizieren und erfüllt die Anforderungen an die Aufbewahrungszeit für Karteninhaberprotokolle.
4. Schutz von Karteninhaberdaten mit starker Kryptographie während der Übertragung über offene, öffentliche Netzwerke	Der über das globale Netzwerk von Cloudflare gesendete Traffic erfüllt die in dieser Anforderung festgelegten Verschlüsselungsstandards und Cloudflare kann die Übertragung von personenbezogenen Informationen blockieren, die der Nutzer identifizieren muss.
5. Schutz aller Systeme und Netzwerke vor Schadsoftware	Cloudflare verarbeitet mehr als 55 Millionen HTTP-Anfragen pro Sekunde, wodurch wir einen einzigartigen Überblick über die neuesten Angriffe im Internet haben. Wir bieten Nutzern eine Reihe von Schutzmaßnahmen gegen Malware, darunter Virenschutz, cloudbasierte E-Mail-Sicherheit und Remote-Browserisolierung.
6. Entwicklung und Wartung sicherer Systeme und Software	Cloudflare kann Sicherheitsverstöße von Nutzern sowie Fehlkonfigurationen, die in SaaS-Anwendungen entdeckt werden, bewerten und gewichten. Die Sicherheitsdienste von Cloudflare sind in der Lage, alle öffentlichen Webanwendungen vor bekannten Angriffen und Exploits zu schützen.
7. Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten nach dem „Need to know“-Prinzip	Cloudflare kann präzise Zugriffskontrollen mit geringsten Zugriffsrechten durchsetzen, unabhängig davon, wo sich die Nutzer befinden oder die Daten gespeichert sind.
8. Identifizierung von Nutzern und Authentisierung beim Zugriff auf Systemkomponenten	Cloudflare kann für den gesamten Traffic, der unser globales Netzwerk durchläuft, identitätsbasierte Richtlinien und Sicherheitsprüfungen durchsetzen (und beispielsweise prüfen, ob MFA verwendet wurde).
10. Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten	Wir bieten detaillierte Audit-Protokolle für alle Produkte der Cloudflare-Plattform und können in die meisten großen SIEM integriert werden.
11. Regelmäßige Prüfung der Sicherheit von Systemen und Netzwerken	Wir bieten eine eingeschränkte Testfunktion für Zugriffsrichtlinien und Funktionen zur Angriffserkennung sowie ausführliche Protokolle für alle Cloudflare-Hauptprodukte.

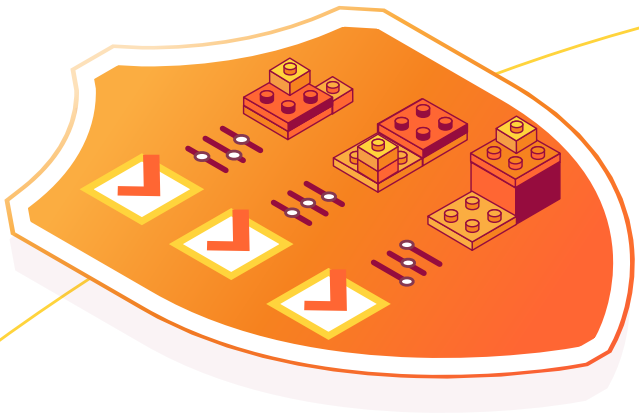
* Cloudflare bietet keine Unterstützung bei der Erfüllung der PCI DSS 4.0-Anforderungen Nr. 9 und Nr. 12, da sich diese auf die physische Sicherheit und die Firmenstruktur beziehen.

Fazit: Setzen Sie zur Einhaltung der PCI-Anforderungen auf Cloudflare

Cloudflare ist PCI-konform und verfügt über Funktionen, mit denen Kunden die Compliance-Anforderungen selbst erfüllen können – unabhängig vom Aufbau ihrer Infrastruktur.

Tatsächlich kann der Einsatz von Cloudflare die Wahrscheinlichkeit eines Datenverstoßes um 65 %[3] verringern, die jährlichen Cyber-Versicherungsprämien um 24 %[4] senken und den Zeitaufwand für die Verwaltung von Systemen und Prozessen um 59 %[4] reduzieren.

> **Unsere Enterprise-Kunden verlangen vertraglich, dass Stax ganz bestimmte Compliance-Standards einhält. Das hat uns dazu veranlasst, Sicherheitskontrollen wie Zero Trust in unserer gesamten Infrastruktur durchzusetzen. [...] Cloudflare hat genau das getan, was wir brauchten: unsere Endpunkte geschützt und unsere Sicherheit gewährleistet."** [5]
>
> **Troy Ridgewell**
> Head of Security, Stax
>
> STAX



Entdecken Sie noch heute die Cloudflare-Lösungen für Datenkonformität. Sprechen Sie mit unseren Fachleuten, um loszulegen.

Quellen

1. https://www.isaca.org/about-us/newsroom/press-releases/2023/privacy-staff-shortages-continue-amid-increasing-demand-for-these-roles
2. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf
3. IBM-Bericht: „Cost of Breach 2022."
4. Cloudflare TechValidate-Umfrage 2023 unter Kunden des Cloudflare-Anwendungsdienstes
5. https://www.cloudflare.com/de-de/case-studies/stax/

CLOUDFLARE

+49 89 2555 2276 | enterprise@cloudflare.com | cloudflare.com/de-de/

REV:BDES-5776.2024APR09