

Sicherheit im bargeldlosen Zahlungsverkehr – PCI

Der PCI DSS (Payment Card Industry Data Security Standard) ist ein weltweit gültiger Sicherheitsstandard der führenden internationalen Kreditkartenorganisationen für den Umgang mit Zahlungsdaten. Er enthält verbindliche Regeln für alle Unternehmen für die Verarbeitung von Kartendaten, um diese besser vor Missbrauch und Diebstahl zu schützen. Das gesamte Netzwerk hängt von der Sicherheit seiner Teile ab.

Wer muss den PCI-Sicherheitsstandard einhalten?

Grundsätzlich ist jedes Unternehmen, das Kartendaten akzeptiert, speichert, verarbeitet oder übermittelt, verpflichtet, die Sicherheitsvorgaben des PCI DSS einzuhalten und PCI-compliant zu sein.

Was bedeutet „akzeptieren, speichern, verarbeiten oder weiterleiten von Kreditkartendaten“?

Dies trifft bereits dann auf Sie zu, wenn Sie Kreditkartendaten Ihrer Kunden auf Ihren Systemen entgegennehmen, sei es zur dauerhaften Speicherung oder nur zur kurzfristigen Verarbeitung bzw. Weiterleitung an einen Drittdienstleister.

Welche Vorteile bringt PCI DSS?

- » Erhöhte Datensicherheit und Schutz Ihrer Kunden
- » Mehr Kundenvertrauen und somit Potenzial für mehr Kreditkarteneinsätze und höhere Umsätze
- » Größere Absicherung vor finanziellen Schäden und Schadenersatzklagen aufgrund von Sicherheitsverletzungen
- » Schutz des Unternehmensimages durch Vermeidung von Kartendatenmissbrauch



- » Bewertung des Sicherheitsschutzes Ihrer Systeme zur Speicherung, Verarbeitung und/oder Übermittlung von Karteninhaberdaten (inkl. Report über Schwachstellen und Vorschläge, diese zu beseitigen).
- » Reduzierung des Unternehmensrisikos durch Datenminimierung und -vermeidung

Händlerkategorien bei MasterCard und Visa

Händlerkategorie	Self Assessment	Security Scan	Security Audit
Level 1 > 6 Mio. Transaktionen p. a. mit MasterCard bzw. Visa über alle Vertriebskanäle (POS, E-Commerce, MOTO)	–	4 x pro Jahr	1 x pro Jahr
Level 2 1 Mio. bis 6 Mio. Transaktionen p. a. mit MasterCard bzw. Visa über alle Vertriebskanäle (POS, E-Commerce, MOTO)	1 x pro Jahr	4 x pro Jahr	1 x pro Jahr ¹
Level 3 20.000 bis 1 Mio. E-Commerce-Transaktionen p. a. mit MasterCard bzw. Visa	1 x pro Jahr	4 x pro Jahr	–
Level 4 Alle anderen	1 x pro Jahr ²	4 x pro Jahr	–

¹ ab 30.06.2011 Pflicht bei MasterCard

² ab 01.10.2009 Pflicht bei Visa

Die zwölf Anforderungen von PCI

1. Einrichtung und Instandhaltung der Firewall-Konfiguration zum Schutz der Daten
2. Keine Verwendung der vom Händler ausgelieferten und voreingestellten System-Passwörter bzw. anderer Sicherheitsparameter
3. Schutz der gespeicherten Daten
4. Verschlüsselte Übertragung der Karteninhaberdaten und sensibler Informationen über öffentliche Netze
5. Gebrauch und regelmäßige Aktualisierung der Anti-Viren-Programme
6. Entwicklung und Aufrechterhaltung von sicheren Systemen und Anwendungen
7. Beschränkung des Zugriffs auf die Daten nach dem need-to-know-Prinzip
8. Zuweisung von eindeutigen Kennungen an alle Personen mit Computer-Zugriff
9. Einschränkung des physischen Zugangs zu Karteninhaberdaten
10. Verfolgung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen sowie Karteninhaberdaten
11. Regelmäßige Prüfungen der Sicherheitssysteme und -prozesse
12. Aufrechterhaltung von Informationssicherheitspolitik

Über die ConCardis PCI-Plattform bequem prüfen und zertifizieren

Ab sofort bietet ConCardis Kunden und Partnern den einzigartigen Service, sich umfassend und kostengünstig überprüfen und zertifizieren zu lassen. Kunden müssen sich lediglich registrieren und alle erforderlichen Daten eingeben – die ConCardis PCI-Plattform führt sie durch alle weiteren Schritte für die Prüfung und Zertifizierung.

Kostenlos registrieren

Registrieren Sie sich kostenlos auf der ConCardis PCI-Plattform unter <https://www.pciplatform.concardis.com/merchant/register>. Die Webseite, die auch ausführliche Informationen über die einzuhaltenden Auskunfts- und Dokumentationsprozesse enthält, wurde von ConCardis in Kooperation mit dem IT-Beratungshaus usd AG (autorisierter PCI-Zertifizierer) entwickelt.

The screenshot shows the 'Ihr Weg zum Compliance-Nachweis' (Your way to compliance proof) page. It includes a navigation menu on the left with options like 'Ihre SAQ', 'Ihre Scans', 'Beschneidung', 'PCI DSS Security Scans', and 'Ihre Audits'. The main content area features a 'So erreichen Sie PCI DSS Compliance' section with a table showing the current compliance status (Compliant, Level 3, dated 17.05.2012). Below this is a table of action items (SAQ, Scan, Audit) with their respective statuses and due dates.

Compliance-Status Ihres Unternehmens	PCI Level	Ablaufdatum
Compliant	3	17.05.2012

Status	Maßnahme	Fälligkeit
SAQ-Status	Ihr SAQ ist gültig. Momentan müssen Sie keinen neuen SAQ ausfüllen.	17.05.2012
Scan-Status	Sie müssen keinen Scan durchführen.	
Audit-Status	Sie müssen kein Audit durchführen.	

Hinweise: Den Händlern können zusätzliche Pflichten auferlegt werden. Für Händler, die Karten von American Express® akzeptieren, gelten andere Kategorien (siehe www.americanexpress.com).



Haben Sie noch Fragen? Sie können das PCI Communication Center montags bis freitags von 8 Uhr bis 18 Uhr erreichen: Telefonisch unter +49 69 7922 2231 (Deutschland), +43 12 65 6001 (Österreich), +41 44 5801 690 (Schweiz), +31 20 71 68 244 (Niederlande) +32 2400 1901 (Belgien) Per E-Mail: support@pciplatform.concardis.com **Weitere Informationen finden Sie unter www.concardis.com/pci (Deutschland), www.concardis.at/pci (Österreich), www.concardis.ch/pci (Schweiz)**