Händlerservice

Hintergrund PCI DSS

Der Standard für die maximale Sicherheit Ihrer Kartenzahlungen

Der weltweite Sicherheitsstandard Payment Card Industry Data Security Standard (PCI DSS) unterstützt Sie dabei, die Sicherheit sensibler und schützenswerter Karteninhaberdaten sicherzustellen und das Vertrauen Ihrer Kunden zu erhalten.

Warum PCI DSS?

Moderne Chiptechnologien und Terminals mit Manipulationsschutz machen das bargeldlose Bezahlen noch sicherer. Doch Kartenbetrüger tüfteln laufend an neuen Tricks, um an Karteninhaberdaten zu kommen, mit denen sie dann illegale Geschäfte tätigen. Gelingt ihnen das, kann der Schaden beträchtlich sein. Denn schwerer als finanzielle Einbußen wiegen Vertrauens- und Imageverlust für Ihr Geschäft.

PCI DSS schützt die Daten Ihrer Kunden

PCI DSS (Payment Card Industry Data Security Standard) ist ein weltweiter Sicherheitsstandard für den kartengestützten Zahlungsverkehr. 2006 vom PCI Security Standards Council (PCI SSC) und den führenden Kartenorganisationen ins Leben gerufen, wird dessen Einhaltung von den führenden Kartenorganisationen bei der Akzeptanz ihrer Kartenprodukte vorausgesetzt.

Das Regelwerk sorgt produktübergreifend für einen sicheren Umgang mit den Karteninhaberdaten Ihrer Kunden. Alle Händler und Dienstleister im kartengestützten Zahlungsverkehr, die Karteninhaberdaten speichern, übermitteln oder verarbeiten, müssen diesen Standard erfüllen.

Welche Sicherheitsanforderungen enthält PCI DSS?

- Installation und Aufrechterhaltung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
- Vermeiden Sie es, die Standardeinstellungen des Lieferanten für Systemkennwörter und andere Sicherheitsparameter zu verwenden
- Schutz gespeicherter Karteninhaberdaten
- Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene bzw. öffentliche Netze
- Verwendung und regelmäßige Aktualisierung von Antivirensoftware
- Entwicklung und Wartung sicherer Systeme und Anwendungen
- Wenden Sie streng bedarfsgerechte Maßnahmen für den Datenzugriff von Karteninhaberdaten an
- Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten
- Physischen Zugriff auf Karteninhaberdaten beschränken
- Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
- Regelmäßiges Testen der Sicherheitssysteme und -prozesse
- Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal

PCI DSS-Zertifizierung leicht gemacht

So erbringen Sie Ihren PCI DSS-Nachweis

Den PCI DSS-Nachweis erbringen Sie, indem die Sicherheitsanforderungen, die auf Ihr Unternehmen zutreffen, erfüllt werden. Welche das im Einzelnen sind, ergibt sich aus der Einstufung des Händlers und der Ermittlung des Selbstbeurteilungsfragebogens. Diese werden bei der Registrierung auf der PCI DSS-Plattform ermittelt. Je nach Größe und Risikopotenzial des Händlers ergeben sich bestimmte Vorgaben für den Validierungsprozess. Nach Abschluss der Registrierung ist bekannt, welche Sicherheitsanforderungen in welcher Ausprägung ein Händler zu erfüllen hat. Welche PCI DSS-Sicherheitsanforderungen an einen Händler gestellt werden, hängt u. a. von der Anzahl der jährlich abgewickelten Kartentransaktionen, dem Vertriebskanal (Präsenz oder Fernabsatzgeschäft) und der Zugehörigkeit zu einer bestimmten Branche, z. B. Hotels und Luftfahrtgesellschaften oder Fernabsatzgeschäft (E-Commerce), ab. Die folgende Tabelle gibt Aufschluss darüber, wie und in welchem Umfang Anforderungen an das Unternehmen bestehen.

Händlerkategorie	Nachweispflicht ggü. dem Acquirer		Sicherheitsanforderungen		
	mastercard / maestro	VISA / V PAY	**Selbstbeurteilungsfragebogen**	**Sicherheitsscan des Händlernetzwerks**	**Sicherheitsüberprüfung vor Ort**
Kategorie 1: > 6.000.000 Transaktionen pro Jahr kumuliert für alle Vertriebsbereiche (POS, E-Commerce, MoTo)	Ja	Ja	AoC	erforderlich[2]	jährlich
Kategorie 2: > 1.000.000 Transaktionen pro Jahr kumuliert für alle Vertriebsbereiche (POS, E-Commerce, MoTo)	Ja	Ja	jährlich[1] + AoC	erforderlich[2]	jährlich[3]
Kategorie 3: E-Commerce-Händler > 20.000 Transaktionen pro Jahr	Ja	Ja	jährlich[1] + AoC	erforderlich[2]	optional
Kategorie 4: E-Commerce-Händler < 20.000 Transaktionen pro Jahr	Ja	Ja	jährlich[1] + AoC	erforderlich[2]	optional
Kategorie 4: alle anderen Händler < 1.000.000 Transaktionen pro Jahr	optional	optional	optional	optional	optional

[1] Der PCI DSS-Nachweis ist jährlich zu erbringen
[2] Erforderlich, wenn Karteninhaberdaten über vom Internet erreichbares System verarbeitet, gespeichert oder weitergeleitet werden
[3] Ausfüllen eines SAQ durch einen akkreditierten ISA (Internal Security Auditor) des Unternehmens oder Durchführung eines Vorort-Audits durch einen akkreditierten QSA

Maximale Sicherheit mit PCI DSS

Die Vorteile für Sie und Ihre Kunden

- → Sicherung der Karteninhaberdaten gegen Diebstahl
- → Schutz vor technischen Manipulationen
- → Mehr Schutz vor Datenspionage im Internet
- → Erschwernis von Identitätsdiebstahl
- → Absicherung gegen finanzielle Schäden und Schadensersatzforderungen
- → Schutz vor Reputationsschäden
- → Erhöhung der Kundenbindung durch Vertrauen

Diese Kartenprodukte orientieren sich am PCI DSS-Standard

Geprüfte Sicherheit

Die usd AG, ein vom PCI Security Standards Council (PCI SSC) akkreditierter Qualified Security Assessor (QSA) und Approved Scanning Vendor (ASV) ist unser leistungsstarker Partner für Kartendatensicherheit. Zeigen Sie Ihren Kunden, wie wichtig Ihnen Datensicherheit ist und laden Sie sich nach Erreichen der PCI DSS-Konformität das PCI DSS-Siegel herunter.

Registrieren und anmelden:

Besuchen Sie das von uns bereitgestellte Zertifizierungs-Portal für den Nachweis der PCI DSS-Compliance unter:
https://pci.s-haendlerservice.de

Schutz von Karteninhaberdaten

Das müssen Sie beachten

In der folgenden Tabelle sind häufig verwendete Karteninhaberdaten und vertrauliche Authentifizierungsdaten aufgeführt. Für jedes Datenelement wurde im PCI DSS-Standard definiert, ob eine Speicherung des Datenelements zulässig oder verboten ist und ob dieses geschützt werden muss.

Zu den Karteninhaberdaten[1] zählen:		
Datenelemente	Speichern zulässig	Schutzbedarf
Kartennummer/Primary Account Number (PAN)	Ja	Ja[3]
Name des Karteninhabers	Ja	Nein
Ablaufdatum	Ja	Nein
Servicecode	Ja	Nein
Zu den vertraulichen Authentifizierungsdaten[2] zählen:		
Vollständige Spurdaten[4]	Nein	Ja
CVC2/CVV2[5]	Nein	Ja
PINs/PIN-Blöcke[6]	Nein	Ja

Bitte beachten Sie Folgendes:

- → Die PCI DSS-Richtlinien betreffen alle Karteninhaberdaten: egal, ob sie digital oder in Papierform vorliegen.
- → Unternehmen, die für die Bezahlabwicklung externe Dienstleister mit der Transaktionsabwicklung beauftragen, müssen sicherstellen, dass diese die PCI DSS-Anforderungen vollumfänglich erfüllen.
- → Unternehmen, die Zahlungsanwendungen von Drittanbietern einsetzen, müssen sicherstellen, dass diese die Kartendatensicherheitsstandards erfüllen.

[1] Karteninhaberdaten können auch nach Abschluss einer Transaktion vom Händler gespeichert und verwendet werden
[2] Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung (auch im verschlüsselten Zustand) nicht gespeichert werden
[3] Datenverschlüsselung notwendig, sofern eine Speicherung erfolgt
[4] Vollständige Verfolgungsdaten vom Magnetstreifen, gleichwertige Daten auf dem Chip oder einem anderen Speicherort
[5] Die drei- bzw. vierstellige Zahl auf der Vorder- bzw. Rückseite der Zahlungskarte
[6] Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht

Glossar

POS	Point of Sale	E-Commerce	Begriff aus dem Fernabsatzhandel, Kauf per Karte auf Basis einer im Internet platzierten Order	SAQ	(Self-Assessment Questionnaire) Fragenkatalog
MoTo	Begriff aus dem Fernabsatzhandel, Kauf per Karte auf Basis einer telefonischen oder postalischen Order			QSA	(Qualified Security Assessor) PCI DSS-Auditor

Sie benötigen Unterstützung?

Gern können Sie Fragen oder weiterführende Informationen zum Thema PCI DSS-Zertifizierung an das Competence Center richten. Es ist von Montag bis Freitag in der Zeit von 08.00 bis 18.00 Uhr für Sie erreichbar.

E-Mail:
support@pci.s-haendlerservice.de
oder
Telefon: 069 6630-5531