PCI DSS...
DER SICHERHEITSSTANDARD FÜR SIE UND IHRE KUNDEN

Der Missbrauch von gestohlenen Kreditkartendaten ist allgegenwärtig. Verunsicherung der Kunden und finanzielle Verluste der Händler sind vorprogrammiert.

Die Lösung: PCI DSS (Payment Card Industry Data Security Standard, kurz PCI). PCI ist ein Sicherheitsstandard für den Umgang mit Zahlungskartendaten. Das Ziel ist eine verbesserte Datensicherheit, um Diebstahl und Missbrauch mit Kreditkarten zu reduzieren.

Ins Leben gerufen wurde dieses Sicherheitssystem von den fünf wichtigsten Kreditkartenunternehmen (American Express, JBC, MasterCard, Discover Financial Services und Visa). PCI soll den sorgfältigen und geschützten Umgang von Zahlungskartendaten sicherstellen. Das System gilt für die gesamte Kartenzahlungsbranche und fordert eine organisatorische und technische Sicherheitszertifizierung. Jeder Händler, der Karten speichert, verarbeitet oder auch nur übermittelt, ist verpflichtet die zwölf umfangreichen Sicherheitsvorgaben einzuhalten. Details finden Sie unter dem Punkt „PCI-Anforderungen im Überblick". Nicht zertifizierte Unternehmen können bei einem Datendiebstahl für den entstandenen Schaden haftbar gemacht werden.

Datenspeicherung

Der PCI DSS legt fest, welche Karteninhaberdaten im Einzelnen gespeichert werden dürfen und wie sie zu schützen sind. Die Speicherung der Kartennummer, Karteninhabername und Ablaufdatum sind unter der Voraussetzung erlaubt, dass kein unbefugter Zugriff darauf erfolgen kann. Die vertraulichen Identifizierungsdaten wie zum Beispiel die Kartenprüfnummer dürfen keinesfalls gespeichert werden. Auch alle in Schriftform vorliegenden Daten von Zahlungskarten müssen unwiderruflich vernichtet werden. Die Nichteinhaltung der Vorgaben kann im Missbrauchsfall hohe Geldstrafen zur Folge haben.

Level-Einstufung:

Händler werden nach Umfang ihrer jährlichen Kartentransaktionen in vier Kategorien eingestuft. Je nach Level müssen Händler unterschiedliche externe und interne Prüfungen bestehen, um die PCI-Zertifizierung zu erreichen und dauerhaft aufrecht zu erhalten:

Händlerkategorie	Self Assessment	Security Scan	Onsite Security Audit
Level 1: Händler mit mehr als 6 Millionen Kartentransaktionen pro Jahr mit MasterCard bzw. Visa über alle Vertriebskanäle (POS, E-Commerce, MOTO)	-	4 x pro Jahr Visa und MasterCard	Visa und MasterCard
Level 2: Händler mit 1 bis 6 Millionen Kartentransaktionen pro Jahr mit MasterCard bzw. Visa über alle Vertriebskanäle (POS, E-Commerce, MOTO)	Visa	4 x pro Jahr Visa und MasterCard	MasterCard
Level 3: Händler mit 20.000 bis 1 Million Kartentransaktionen pro Jahr mit MasterCard bzw. Visa	Visa und MasterCard	4 x pro Jahr Visa und MasterCard	-
Level 4: alle anderen Händler	Visa und MasterCard	4 x pro Jahr Visa und MasterCard	-

Anforderungen am Beispiel von Visa und MasterCard, Stand Juni 2010

PCI-Anforderungen im Überblick

Die folgenden zwölf Sicherheitsvorgaben bilden die Überpunkte für die im PCI DSS festgelegten sehr umfangreichen Anforderungen:

- Einrichtung und Instandhaltung einer Firewall zum Schutz der Daten von Kreditkarteninhabern
- Änderung der von Herstellern vorgegebenen Standardpasswörter und Sicherheitseinstellungen
- Schutz der gespeicherten Daten von Kreditkarteninhabern
- Verschlüsselte Übertragung der Karteninhaberdaten in öffentlichen Netzwerken
- Einsatz und regelmäßige Aktualisierung von Anti-Viren-Programmen
- Entwicklung und Verwendung sicherer Systeme und Anwendungen
- Beschränkung des Zugriffs auf die Daten nach dem Grundsatz „Kenntnis nur wenn notwendig“
- Zuweisung von eindeutigen Benutzerkennungen an alle Personen mit Computer-Zugriff
- Einschränkung des physischen Zugangs zu Karteninhaberdaten
- Verfolgung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen sowie Karteninhaberdaten
- Regelmäßige Prüfungen der Sicherheitssysteme und -prozesse
- Einrichtung einer Unternehmensrichtlinie mit Vorgaben zur Informationssicherheit für Mitarbeiter und Vertragspartner.

Ihre Vorteile bei ExperCash

Vertrauen Sie bei Ihren Kartendaten auf einen professionellen Partner: Händler, die die ExperCash iFrame- oder Popup-Technologie nutzen, müssen nicht aufwendig nach PCI zertifiziert werden und durchlaufen nur einen Prozess mit elf Fragen (SAQ Typ A). So sparen Sie je nach Händler-Level 2.000 Euro oder mehr pro Jahr. Außerdem entfallen so die umfangreichen externen und internen PCI Implementierungs-Aufwendungen sowie die regelmäßigen Einhaltungskontrollen. Voraussetzung hierfür ist, dass alle Kartentransaktionen ausschließlich über den ExperCash iFrame abgewickelt werden. Sie als Händler dürfen selbst keine Kartendaten verarbeiten. Auch über die schwerwiegenden Konsequenzen bei Nichteinhaltung der Vorgaben müssen Sie sich bei einer Abwicklung über den ExperCash iFrame keine Gedanken machen.

Das Handling ist einfach: Klassifizieren und validieren Sie sich einfach auf www.compliance.expercash.com und beantworten Sie die elf Fragen bezüglich Ihres Unternehmens, um die PCI Registrierung in Verbindung mit ExperCash abzuschließen. Ihre PCI-Zertifizierung in Verbindung mit ExperCash – einfach, sicher, schnell und kostenlos.

Weitere Vorteile für Sie als Händler:

- **Erhöhte Datensicherheit und Schutz für Ihre Kunden**
  PCI macht es Betrügern schwerer, Kartendaten zu stehlen und zu missbrauchen. Für die Kunden bedeutet dies erhöhte Datensicherheit und für Sie eine positive Assoziation mit Ihrem Online Shop.

- **Gesteigertes Kundenvertrauen**
  Die erhöhte Datensicherheit führt zu mehr Vertrauen der Kunden in die Kartensicherheit und in Ihr Unternehmen. Ihr Image wird geschützt und verbessert. Eine Steigerung der Kreditkarteneinsätze ist möglich. Starkes Vertrauen in Ihr Unternehmen und Ihren Online-Shop kann den Umsatz Ihres Unternehmens langfristig steigern.

- **Absicherung vor finanziellen Schäden**
  Bei Einhaltung der PCI-Anforderungen sind Sie stärker vor finanziellen Schäden und Schadenersatzansprüchen aufgrund von Sicherheitsverletzungen abgesichert. Durch die sogenannte Safe-Harbour-Lösung können PCI-zertifizierten Opfern eines Datenmissbrauchs die Strafgebühren reduziert oder ganz erlassen werden.

Für weitergehende Fragen steht Ihnen Ihr persönlicher Ansprechpartner gerne zur Verfügung.

EXPERCASH GmbH | Augustaanlage 59 | 68165 Mannheim | Germany
Phone +49.621.72 49 38 – 0 | Fax +49.621.72 49 38 29 – 00 | info@expercash.com | **www.expercash.com**

EXPERCASH