



Informationsblatt zur PCI Zertifizierung

Neue Sicherheitsmaßnahmen im Fernabsatzgeschäft zum 01.07.2005

Allgemeines

„Verified by Visa“ und „MasterCard SecureCode“ authentifizieren den Karteninhaber persönlich.

Neue Standards sichern nun auch die Datenhaltung beim Fernabsatz-Händler und im Ladengeschäft. Sie betreffen auch PSP (Payment Service Provider wie z.B. Netzbetreiber und Internet Payment Service Provider) und Drittparteien (Inkasso-, Buchungs- und Bonussysteme), die nicht in den klassischen Transaktions-Ablauf unserer Vertragspartner involviert sind.

Risiken führen zu Verunsicherung

- Sicherheitslücken und zunehmender Kreditkarten-Missbrauch verunsichern viele Verbraucher, insbesondere im E-Commerce Geschäft.
- Viele Verbraucher meiden online-Geschäfte per Kreditkarte.

Konsequenz: Umsatz- und Gewinnverlust beim Händler

Neue Standards führen zu neuem Verbrauchervertrauen

- Neue Sicherheitsprogramme für Internet und stationären Handel sind unumgänglich.
- Anfang 2005 wurden nun AIS (Account Information Security) von Visa und SDP (Site Data Protection) von MasterCard zum einheitlichen Standard PCI (Payment Card Industry Data Security Standard) zusammengefasst.
- Händler und Service Provider sind aufgefordert, den PCI Data Security Standard bei der Verarbeitung von Kartendaten einzuhalten. Der Nachweis erfolgt über eine Auditierung und Zertifizierung des Händlers bzw. Service Providers durch einen Auditor
- Ziel der Zertifizierung ist die Aufdeckung und Beseitigung von Sicherheitslücken, über welche Hacker oder gar eigene Mitarbeiter an fremde Daten gelangen.
- Auch wird die interne Sicherheitspolitik des Unternehmens auf Herz und Nieren geprüft – in Bezug auf Kreditkarten-Daten.
- Die Einhaltung des Standards PCI ist **verbindlich**. Nichteinhaltung führt zu Strafgeldern, die der Händler („VP“ im Sinne der AGB) zu tragen hat.

Händler und PSP durchlaufen bis zu vier Schritte zur PCI Zertifizierung

1. Registrierung
2. Self-Assessment Questionnaire (Fragebogen)
3. Security Scan (u.a. Prüfung der IP-Adressen/extern relevanten URL's)
4. Security Audit (vor Ort Besuch)

Über den Umfang der Prüfungen entscheidet unter anderem die monatliche Anzahl der Kreditkarten-Transaktionen oder auch ein zurückliegender Hacker-Angriff. Schwachstellen, die im Rahmen der Prüfungen aufgedeckt werden, sind zeitnah zu beheben. Die Registrierung ist kostenlos. Kosten im Rahmen der Zertifizierung trägt der Vertragspartner.



Was können Sie als Händler im Vorfeld tun?

Beschleunigen Sie den Prozess und prüfen Sie vor der Registrierung folgende Punkte:

- Analysieren Sie Ihre Systeme auf Speicherung sensibler Kartendaten und stellen Sie die Speicherung gegebenenfalls ein.
- Verschaffen Sie sich einen Überblick über alle externen Partner/Dienstleister, die Kartendaten in Ihrem Auftrag speichern. Diese sind später an B+S zu melden (z.B. Hotelbuchungs-Systeme oder Finanzdienstleister, an welche Sie Daten übermitteln).
- Fernabsatz-Händler, die Kartendaten noch speichern, verarbeiten oder weiterleiten, sollten auf die Zahlungsmasken eines Payment Service Providers (PSP) umstellen.
- Fragen Sie Ihren PSP nach seinem Zertifizierungsstatus. Setzen Sie ausschließlich auf PSP, welche bis **30.06.2005** nach PCI zertifiziert sind.
- Bei wiederkehrenden Leistungen u.Ä. sollte der Fernabsatz-Händler mit seinem PSP besprechen, ob dieser die Kartendaten speichern und dem Händler für weitere Transaktionen zugänglich machen kann. Einige PSP bieten diesen Service an.

Unsere Abteilung Vertrieb Fernabsätze berät Sie gerne, ob Ihr PSP zertifiziert ist. Rufen Sie uns an unter +49(0)69 – 66 30-5701. Weiteres zu PCI erfahren Sie über info-tvp@bs-card-service.com oder über www.bs-card-service.com *.

B+S unterstützt Sie mit einem akkreditierten Dienstleister

Für die Registrierung empfehlen wir:

SRC Security Research & Consulting GmbH
Graurheindorfer Straße 149a
53117 Bonn

Telefax +49(0)721 – 15 14 08 862
E-Mail sdpais@src-gmbh.de

Ihre Registrierung über SRC nehmen Sie bitte unter **www.src-gmbh.de/bs-card-service** vor. Sie benötigen hierfür Ihre B+S Vertragspartnernummer.

Sollten Fragen bei der Registrierung oder zum Zertifizierungsprozess auftreten, kontaktieren Sie bitte SRC.

Durch die Registrierung schließen Sie mit SRC eine eigene direkte Vereinbarung. B+S haftet dem VP gegenüber nicht für die Leistungen von SRC.

Bitte bedenken Sie auch...

Jeder bemerkte Missbrauch und Verlust von Kartendaten muss sofort gemeldet werden! Wird PCI nicht umgesetzt, behält sich B+S die Kündigung vor und entstandene Kosten können Ihnen weiterbelastet werden! Siehe dazu das Merkblatt zur AGB Neufassung.

*www.bs-card-service.com/deutsch/vertragspartner/sicherheit/fernabsatzgeschaefte/sicherheitspruefung/index.html