

# Gesetzeskonformer Umgang mit Kreditkartendaten

## PCI DSS-Compliance verständlich gemacht

**Bis Ende 2007 müssen sämtliche Händler und Dienstleister, die Kreditkartendaten ihrer Kunden speichern, bearbeiten oder übermitteln, die strengen Sicherheitsvorgaben des PCI DSS (Payment Card Industry Data Security Standard) umgesetzt haben. Der verpflichtende Best-Practice-Standard zum netzwerkweiten Schutz vor Datenverlust und -diebstahl wurde von den fünf wichtigsten Kreditkartenunternehmen ins Leben gerufen, um den weltweit wachsenden Missbrauch von Kartendaten zu unterbinden.**

Bereits seit dem Jahr 2004 werden Händler und Dienstleister dazu angehalten, sich für den PCI DSS fit zu machen. Besondere Brisanz hat das Thema PCI DSS durch eine Reihe eklatanter Sicherheitsverstöße erhalten. Hierzu gehört vor allem die aufsehenerregende Meldung des US-Einzelhändlers TJX Companies Inc. zu Beginn des Jahres: Im Verlauf von 18 Monaten waren TJX unter anderem mehr als 45 Millionen Datensätze mit Kontoinformationen von Kreditkartenkunden abhanden gekommen.

### Entstehung des PCI DSS

Der PCI DSS beruht auf der Zusammenarbeit zwischen Visa und MasterCard und vereint Vorgaben aus den zuvor unabhängig voneinander aufgestellten jeweiligen Schutzprogrammen der Kartenunternehmen. Die Anforderungen des PCI DSS sind somit nicht gänzlich neu. Seit Juni 2001 hatte Visa von Händlern und Dienstleistern die Einhaltung seines CISP (Cardholder Information Security Program) zum Schutz von Karteninhaberdaten gefordert. MasterCard gab im Juni 2004 ein eigenes Paket mit Schutzmaßnahmen bekannt, das SDP (Site Data Protection Program). Auch andere große Kartenunternehmen wie American Express mit seinem DSS (Data Security Standard) und Discover Card mit Discover Information Security and Compliance (DISC) zogen mit eigenen Maßnahmen zum Datenschutz nach.

Es existierten somit verschiedene Regularien nebeneinander, die allesamt den Schutz der vertraulichen Daten von Karteninhabern zum Ziel hatten. Händlerbanken, Akzeptanzpartner und Dienstleister stellten daher die Frage nach dem Sinn gleich mehrerer Standards. Sie forderten, einen übergreifenden, weltweit gültigen Best-Practice-Standard zur Datensicherheit zu implementieren.

Im Dezember 2004 wurde diese Forderung umgesetzt, als Visa und MasterCard sich

auf ein gemeinsames Regelwerk einigten und ihre Sicherheitsprogramme CISP und SDP zusammenlegten – der PCI DSS entstand. Im Januar 2005 wurde der PCI DSS als offizieller gemeinsamer Sicherheitsstandard der Unternehmen vorgestellt; American Express, Discover Card und JCB schlossen sich ebenfalls an.

### Worum handelt es sich beim PCI-Regelwerk?

Der PCI-Standard bedeutet für Administratoren nicht etwa die Umsetzung neuer, unbekannter Sicherheitskonzepte. Ganz im Gegenteil: Er fordert lediglich die Umsetzung von Best-Practice-Richtlinien, die bereits aus allgemeinen Sicherheitsgründen in allen Firmennetzwerken gelten sollten. Im Wesentlichen umfasst der PCI DSS zwölf

grundlegende Anforderungen, die zum Ziel haben: 1) Einrichtung und Wartung eines geschützten Netzwerks, 2) Schutz von archivierten und zu übermittelnden (Karteninhaber)daten, 3) Einrichtung eines Schwachstellen-Management-Systems, 4) Umsetzung effektiver Richtlinien zur Zugriffskontrolle, 5) regelmäßige Überwachung und Überprüfung der IT-Infrastruktur und 6) Formulierung und Durchsetzung einer Richtlinie zur Informationssicherheit. Die nachfolgende Tabelle 1 liefert einen Überblick über die zwölf in Kategorien eingeteilten Anforderungen, die von Unternehmen im Rahmen der PCI-Compliance umzusetzen sind.

Der PCI DSS gilt erst dann als eingehalten, wenn Händler und Dienstleister den folgenden drei Bereichen Rechnung tragen:

#### Anforderungen des PCI DSS

PCI-Compliance wird durch Erfüllung der folgenden zwölf Anforderungen, auch als „Digitales Dutzend“ bekannt, erreicht:

##### Einrichtung und Wartung eines geschützten Netzwerks

1. Einrichtung und Wartung einer Firewall zum Schutz der Daten von Kreditkarteninhabern
2. Änderung der von Herstellern vorgegebenen Standardpasswörter und Sicherheitseinstellungen

##### Schutz der Daten von Kreditkarteninhabern

3. Schutz der gespeicherten Daten von Kreditkarteninhabern
4. Verschlüsselte Übertragung der Daten von Kreditkarteninhabern in öffentlichen Netzwerken

##### Einrichtung eines Schwachstellen-Management-Systems

5. Einsatz und regelmäßige Aktualisierung von Virenschutzlösungen
6. Entwicklung und Verwendung sicherer Systeme und Anwendungen

##### Umsetzung effektiver Richtlinien zur Zugriffskontrolle

7. Einschränkung des Zugriffs auf Kreditkartendaten nach dem Grundsatz „Kenntnis, nur wenn nötig“.
8. Zuweisung einer eindeutigen Benutzerkennung an jede Person mit Zugang zum Computersystem
9. Einschränkung des physikalischen Zugriffs auf Daten von Kreditkarteninhabern

##### Regelmäßige Überwachung und Überprüfung des Netzwerks

10. Protokollierung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen und Daten von Kreditkarteninhabern
11. Regelmäßige Überprüfung von Sicherheitssystemen und -abläufen

##### Formulierung und Durchsetzung einer Richtlinie zur Informationssicherheit

12. Einrichtung einer Unternehmensrichtlinie mit Vorgaben zur Informationssicherheit für Mitarbeiter und Vertragspartner

Tabelle 1: Anforderungen des PCI DSS

1) Alle Protokolldaten müssen geschützt erfasst werden, Informationen sind fälschungssicher zu speichern und Daten müssen für Analysen schnell zugänglich sein.

2) Unternehmen müssen bei Sicherheits-Audits anhand von sofort verfügbaren Nachweisen über implementierte Schutzmaßnahmen belegen können, dass PCI-Compliance besteht.

3) Es müssen Systeme zur kontinuierlichen Überwachung von Datenzugriff und -verwendung implementiert sein, zum Beispiel automatische Warnsysteme, die Administratoren bei kritischen Ereignissen umgehend benachrichtigen. Administratoren müssen durch diese Systeme in der Lage sein, schnelle Gegenmaßnahmen einzuleiten. Protokolldaten sind ebenfalls zu berücksichtigen – die Erfassung und Speicherung von Protokolldaten muss nachweisbar sein.

Die Anforderungen des PCI DSS für Händler und Dienstleister unterscheiden sich deutlich voneinander. Händler werden je nach Umfang ihrer jährlichen Kartentransaktionen in vier Kategorien eingestuft:

- Kategorie 1: Händler mit mehr als 6 Millionen Kartentransaktionen pro Jahr und Händler, deren kartenspezifische Kundendaten kompromittiert wurden
- Kategorie 2: Händler mit ein bis 6 Millionen Kartentransaktionen pro Jahr
- Kategorie 3: Händler mit 20.000 bis 1 Millionen Kartentransaktionen pro Jahr
- Kategorie 4: alle anderen Händler

Abhängig von ihrer Kategorie müssen Händler unterschiedliche Anforderungen erfüllen, um PCI-Compliance zu erreichen und dauerhaft aufrecht zu erhalten. Für Händler der Kategorie 1 sind eine jährliche PCI-Sicherheitsauditierung vor Ort und vierteljährliche Sicherheits-Scans des Netzwerks verpflichtend.

Die Auditierung im Unternehmen erfolgt durch einen Sicherheitsgutachter, den Qualified Security Assessor (QSA). Händler der Kategorien 2 bis 4 hingegen müssen einen jährlichen PCI-Fragebogen beantworten und vierteljährliche Sicherheits-Scans des Netzwerks durchführen.

Dienstleister, zu denen unter anderem Payment-Gateways, Hostprovider im E-Com-

merce, Auskunfteien und Datenvernichter zählen, werden in drei Kategorien eingestuft:

- Kategorie 1: alle Datenverarbeiter von Kreditkartenzahlungen und Payment-Gateways.
- Kategorie 2: jeder nicht zu Kategorie 1 zählende Dienstleister, der jährlich mehr als eine Million Kartenabrechnungen oder -transaktionen verwaltet.
- Kategorie 3: jeder nicht zu Kategorie 1 zählende Dienstleister, der jährlich weniger als 1 Million Kartenabrechnungen oder -transaktionen verwaltet.

Für Dienstleister der Kategorien 1 und 2 sind eine jährliche PCI-Sicherheitsauditierung vor Ort und vierteljährliche Sicherheits-Scans des Netzwerks obligatorisch. Kategorie 3-Dienstleister sind hingegen nur zur Beantwortung eines jährlichen PCI-Fragebogens und zu vierteljährlichen Netzwerk-Scans verpflichtet.

Händler der Kategorie 1 müssen die PCI-Sicherheitsmaßnahmen bis zum 30. September 2007 implementiert haben. Für Händler der Kategorie 2 endet die Frist am 31. Dezember 2007. Werden die Vorgaben nicht befolgt, drohen empfindliche Geldstrafen in bis zu sechsstelliger Höhe, Rechtsstreite sowie Umsatz- und Ansehensverlust. Im schlimmsten Fall kann Händlern sogar die Akzeptanz von Kreditkarten untersagt werden.

### Herausforderungen bei der Einhaltung des PCI DSS

Durch die in Kürze ablaufenden Fristen sind Händler und Dienstleister in Zugzwang. Der überwiegende Teil der Anforderungen kann ohne großen Aufwand umgesetzt werden, doch einige Vorgaben werden nur schwierig zu erfüllen sein. Beispielsweise stellt Anforderung 5, „Einsatz und regelmäßige Aktualisierung von Virenschutzlösungen“, kein Problem dar, da die Handlungsanweisung eindeutig ist. Andere Anforderungen sind wiederum sehr viel weiter gefasst und somit möglicherweise schwerer einzuhalten. Dies gilt unter anderem für Anforderung 3, „Schutz der gespeicherten Daten von Kreditkarteninhabern“: Unternehmen müssen sämtliche Speicherorte von Karteninhaberdaten ermitteln und jeweils überprüfen, ob Geschäftsprozesse die Speiche-

rung an all diesen Orten tatsächlich erforderlich machen. Nicht zuletzt müssen die Informationen verschlüsselt werden, um sie angemessen zu schützen.

VeriSign Global Security Consulting hat als Anbieter von PCI-Assessments und unterstützenden Sicherheits-Services herausgefunden, dass die meisten Unternehmen Anforderung 3 des PCI DSS nicht erfüllen. Bei einer von VeriSign durchgeführten Stichprobe von 112 Vor-Ort-Audits traf dies auf ganze 79 Prozent der Unternehmen zu. Ein weiteres Ergebnis der Untersuchung: Die unverschlüsselte Speicherung von Daten in Microsoft Excel-Tabellen war der Hauptgrund für das Nichtbestehen der PCI-Audits. Darüber hinaus wurde festgestellt, dass Mitarbeiter Kartendaten in Flat-Files oder anderen Formaten gesichert hatten, deren Zugriff nur schwer zu kontrollieren ist, da sie mühelos auf Laptops, Desktops und kabellose Geräte übertragbar sind.

### Schlussfolgerungen

Die Einhaltung der PCI-Compliance ist erst der Anfang eines fortlaufenden Prozesses, der Händler zur regelmäßigen Überwachung des Sicherheitsstatus ihres Netzwerks verpflichtet. Das Prinzip einer einmaligen, dauerhaften Zertifizierung ist in diesem Zusammenhang überholt: Allein die Bestätigung des Qualified Security Assessors (QSA), dass die Einhaltung des Sicherheitsstandards zu einem bestimmten Zeitpunkt gegeben ist, reicht nicht aus. Ebenso wichtig, wenn nicht gar noch wichtiger, ist es für Organisationen, PCI-Compliance auf Dauer aufrecht zu erhalten.

Der PCI DSS wird Händler und Dienstleister auch noch in mittelbarer Zukunft begleiten, denn es gilt: „Der Weg ist das Ziel.“ Auch wenn Unternehmen durch den PCI DSS hohe Kosten tragen müssen – diese sind vergleichsweise niedriger als Geldbußen oder Ansehensverlust im Fall einer Sicherheitsverletzung.

-----  
 Andre Muscat,  
 Director of Network Security Products bei GFI Software, einem Hersteller von Netzwerksicherheits-, Inhaltssicherheits- und Messaging-Lösungen. ([www.gfisoftware.de/](http://www.gfisoftware.de/))