InterCard
powered by Verifone

Mehr Datensicherheit im Kartengeschäft mit PCI DSS!

Zum Schutz vor Missbrauch und Diebstahl von Kartendaten haben die führenden Kreditkartenorganisationen den Sicherheitsstandard PCI DSS (Payment Card Industry Data Security Standard) ins Leben gerufen. Das Regelwerk ist für alle Unternehmen verpflichtend, die mit Kartendaten in Berührung kommen.

Was ist PCI DSS?

PCI DSS (Payment Card Industry Data Security Standard) ist ein Sicherheitsstandard der international führenden Kreditkartenorganisationen zum Schutz vor Datenmissbrauch und -diebstahl im bargeldlosen, elektronischen Zahlungsverkehr. Das weltweit gültige Regelwerk umfasst Sicherheitsvorschriften zur Einhaltung technischer und betrieblicher Anforderungen an den Umgang mit Kartendaten. Alle Unternehmen, die mit Kartendaten in Berührung kommen, sind zur Einhaltung der definierten Standards verpflichtet.

Welche Vorteile bringt Ihnen PCI DSS?

- Schützen Sie sich und Ihre Kunden durch eine erhöhte Datensicherheit
- Stärken Sie das Vertrauen und die Kundenbindung durch sicheren Zahlungsverkehr
- Weniger Zahlungsausfälle wegen Kartenmissbrauchs
- Schutz vor Imageschäden durch Vermeidung von Datendiebstahl
- Geringeres Risiko durch Reduzierung der Datenhaltung

Wer muss die Sicherheitsstandards einhalten?

PCI DSS ist verpflichtend für alle Unternehmen, die mit sensiblen Kartendaten in Berührung kommen – weltweit. Grundsätzlich gilt für jedes Unternehmen, das Kreditkarten akzeptiert, verarbeitet, speichert oder übermittelt, dass die Sicherheitsstandards eingehalten werden müssen. Je nach Einstufung bzw. Kategorisierung des Händlers müssen unterschiedliche Maßnahmen ergriffen werden, um den Status „PCI-compliant“ nachzuweisen.

Der Händler ist zudem dafür verantwortlich, dass die von ihm beauftragten Dienstleister, wie Internet Payment Service Provider (PSP) oder Data Storage Entities (DSE), die im Namen des Händlers Daten übermitteln, verarbeiten oder speichern, die Sicherheitsanforderungen ebenfalls erfüllen und einhalten.

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

Immer dann, wenn Sie Kreditkarten in Ihrem Geschäft oder Online-Shop akzeptieren, kommen Sie mit sensiblen Kartendaten in Berührung. Dabei ist es irrelevant, ob Sie nur kurzfristig oder dauerhaft mit den Daten in Kontakt kommen oder die Daten an einen Dienstleister weiterleiten. In jedem Fall akzeptieren, verarbeiten, speichern oder übermitteln Sie sensible Kartendaten.

Wer ist für die Einhaltung von PCI DSS verantwortlich?

Es obliegt Ihnen als Händler, für die Einhaltung der Sicherheitsstandards Sorge zu tragen. Die Kreditkartenorganisationen verlangen jedoch unter Umständen, dass die von Ihnen getroffenen Sicherheitsmaßnahmen überprüft werden. Der Umfang der Überprüfung ist abhängig von der Anzahl der Transaktionen, die Sie verarbeiten, und ob Sie bei der Verarbeitung mit den sensiblen Daten in Berührung kommen. Kreditkartenverarbeitende Händler sind verpflichtet, gegenüber Ihrem Kreditkartenverarbeiter (Acquirer) die Erfüllung der PCI DSS Anforderungen nachzuweisen.

Welche Anforderungen müssen erfüllt werden?

1. Einrichtung und regelmäßige Aktualisierung einer Firewall zum Schutz von Kartendaten
2. Keine Verwendung von gelieferten Standardwerten für System-Passwörter oder anderer sicherheitsrelevanter Parameter
3. Schutz der gespeicherten Kartendaten
4. Verschlüsselte Übertragung von Kartendaten und sensiblen Informationen in öffentlichen Netzen
5. Verwendung und regelmäßige Aktualisierung einer Anti-Viren-Software
6. Entwicklung, Verwendung und Aufrechterhaltung sicherer Systeme und Anwendungen
7. Zugriffsbeschränkung auf Kartendaten nach dem Need-to-know-Prinzip
8. Zuteilung einer eindeutigen, persönlichen Kennung für jede Person mit Zugang zum System
9. Beschränkung des physischen Zugriffs auf sensible Kartendaten
10. Verfolgung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen und Karteninhaberdaten
11. Regelmäßige Überprüfung der Sicherheitssysteme und -prozesse
12. Einhaltung einer Informationssicherheits-Richtlinie im Unternehmen

Welche Einstufungen bzw. Kategorien gibt es?

	Selbstauskunft (SAQ)	Schwachstellen-Test (Network Scan)	Sicherheitsprüfung vor Ort (On-Site Audit)
Level 1			
> 6 Mio. Transaktionen pro Jahr und Marke über alle Vertriebskanäle (POS, E-Commerce und MoTo)	/	4 x pro Jahr	1 x pro Jahr
Level 2			
1 Mio. bis 6 Mio. Transaktionen pro Jahr und Marke über alle Vertriebskanäle (POS, E-Commerce und MoTo)	1 x pro Jahr	4 x pro Jahr	1 x pro Jahr
Level 3			
20.000 bis 1 Mio. Transaktionen pro Jahr und Marke im E-Commerce	1 x pro Jahr	4 x pro Jahr*	/
Level 4			
Alle Händler (nicht E-Commerce) mit < 1 Mio. Transaktionen pro Jahr und E-Commerce Händler mit < 20.000 Transaktionen pro Jahr	1 x pro Jahr	4 x pro Jahr*	/

* Nur notwendig, wenn Kreditkartendaten gespeichert, elektronisch verarbeitet oder übermittelt werden und Sie keinen PCI DSS-zertifizierten Internet Payment Service Provider nutzen. Die InterCard AG ist nach den erfordlichen PCI Security Standards zertifiziert.

Weitere Informationen rund um das Thema PCI DSS finden Sie auf der Website des PCI Security Standards Council:
de.pcisecuritystandards.org

Was passiert, wenn ich mich nicht zertifizieren lasse?

Lässt ein kreditkartenverarbeitender Händler sich nicht nach PCI DSS zertifizieren, ist InterCard berechtigt, das Vertragsverhältnis mit sofortiger Wirkung zu kündigen und mögliche Strafzahlungen der Kreditkartenorganisationen und Forderungen der Kartenherausgeber (Issuer) in Form von Schadensersatz an den Händler weiterzureichen.

InterCard AG

Mehlbeerenstraße 4
82024 Taufkirchen b. München

T: +49 89 61445-494
F: +49 89 61445-760

E: kreditkarten@intercard.de
www.intercard.de

55.154.006 (0817)