



# Schutz vor Kartenbetrug und Cyberkriminalität

Verpflichtende Datensicherheitsstandards bei Kartenzahlungen einhalten

## PCI-Datensicherheitsstandards verstehen

Als kartenakzeptierendes Unternehmen bieten Sie Ihren Kunden durch die Akzeptanz bargeldloser Zahlungen ein Höchstmaß an Service und Bequemlichkeit. Aber wissen Sie, wie Sie die Kartendaten Ihrer Kunden vor der sogenannten Cyberkriminalität schützen können?

Immer wieder berichten die Medien darüber, dass bekannte Unternehmen Opfer von Hackerangriffen oder Datendiebstählen geworden sind. In vielen Fällen sind davon auch die vertraulichen Daten von Millionen von Kunden betroffen.

## Kleinere Unternehmen im Visier von Cyberkriminellen

Den Wenigsten ist jedoch bewusst, dass Hacker häufig auch kleinere Betriebe im Visier haben, da es diese Angriffe selten in die Schlagzeilen schaffen. Der Grund dafür liegt auf der Hand: Kleinere Firmen verfügen oftmals nicht über die internen Ressourcen, Sicherheitsstrategien zum Schutz von Kundendaten gegen Hackerangriffe zu entwickeln.

## Wie man Kartendaten schützen kann

Hinzukommt, dass vielen Unternehmen nicht bekannt ist, welche konkreten Maßnahmen zu ergreifen sind, um die vertraulichen Kartendaten ihrer Kunden zu schützen. Daher haben die Kartenorganisationen Visa®, MasterCard®, JCB®, Discover® und American Express® die PCI-Datensicherheitsstandards eingeführt. Dabei wurden 12 Anforderungen definiert, die helfen, die Speicherung, die Verarbeitung sowie die Übertragung von Kartendaten sicherer zu gestalten.

**Es liegt in Ihrer Verantwortung, die Daten Ihrer kartenzahlenden Kunden bestmöglich zu schützen.**

Wenn Sie Kartenzahlungen akzeptieren müssen Sie sicherstellen, dass Ihre kartenzahlenden Kunden nicht Opfer einer Sicherheitslücke werden. Und dass nicht nur, weil Ihnen der Schutz Ihrer Kunden am Herzen liegen sollte, sondern auch um Ihr eigenes finanzielles Risiko zu minimieren. Selbst kleinere Betriebe müssen im Falle eines Abgriffs von vertraulichen Kartendaten mit Kosten von 23.000 € bis 46.000 € und mehr rechnen, abhängig vom Umfang der kompromittierten Daten.

Um Ihre Kunden UND sich selbst zu schützen, ist es daher unerlässlich, dass Sie die Vorgaben der PCI-Datensicherheitsstandards (PCI DSS) einhalten und sich dies jährlich zertifizieren lassen.

**Die Erfüllung der PCI-Datensicherheitsstandards ist für kartenakzeptierende Unternehmen verpflichtend. Bei Nichterfüllung der verbindlichen Vorgaben innerhalb von 90 Tagen muss eine Gebühr in Rechnung gestellt werden.**



## PCI-Vorteile auf einen Blick

92 % aller kompromittierenden Vorfälle mit Kartendaten werden in kleineren Betrieben verzeichnet. Leider unterschätzen viele Unternehmen die finanziellen Auswirkungen und den Imageverlust als Folge einer Sicherheitslücke.

Vorteile des PCI-Zertifizierungsprogram Elavon:

### 1 Sicherheit

Die vertraulichen Kartendaten Ihrer Kunden werden geschützt, da Transaktionen sicher abgewickelt und verarbeitet werden.

### 2 Überzeugung

Ihre kartenzahlenden Kunden sind dank der erhöhten Datensicherheit von Ihrem Angebot überzeugt.

### 3 Finanzielle Absicherung

Sichern Sie sich gegen finanzielle Verluste und zusätzliche Kosten ab, die im Falle einer Sicherheitslücke entstehen können.

### 4 Vertrauen

Bewahren Sie sich das Vertrauen Ihrer kartenzahlenden Kunden und schützen Sie Ihren guten Ruf.



## Unterstützung beim Kampf gegen Hacker

Als Anbieter für die Abrechnung bargeldloser Zahlungen liegt Elavon nicht nur Ihr Geschäftserfolg am Herzen, sondern auch die sichere Abwicklung Ihrer Transaktionen. Aus diesem Grunde haben wir uns mit Trustwave®, einem führenden PCI-DSS-Sicherheitsgutachter zusammengesgeschlossen, um Ihnen Zugang zu Trustwaves TrustKeeper®-Portal zu geben.

Der PCI-Wizard von TrustKeeper führt Sie durch das Portal und hilft, etwaige Sicherheitslücken innerhalb Ihrer IT-Infrastruktur aufzufindig zu machen, diese zu beheben, den Nachweis über die Einhaltung der PCI-Anforderungen zu erbringen und Ihr Unternehmen vor Datenabgriffen zu schützen.

Elavon setzt mit seinem PCI-Zertifizierungsprogramm Maßstäbe, da wir Unternehmen aktiv dabei unterstützen, Kartendaten sicher zu verwalten und die verbindlichen PCI-Datensicherheitsstandards zu erfüllen. So schützen Sie nicht nur Ihren guten Namen, sondern auch Ihre finanziellen Erträge.

Das PCI-Zertifizierungsprogramm setzt drei Schwerpunkte:

**Aufklärung:** Wir stellen Ihnen Material zur Verfügung, damit Sie sich mit den Vorgaben von PCI DSS vertraut machen können.

**Zertifizierung:** Wir helfen Ihnen, den Nachweis über die Erfüllung der PCI-Datensicherheitsstandards zu erbringen.

**Finanzielle Absicherung:** Wir reduzieren Ihr finanzielles Risiko, falls Ihnen trotz gültiger PCI-Zertifizierung ein Schaden durch eine Datensicherheitslücke entstehen sollte.

Wir empfehlen unseren neuen Kunden, die bereitgestellten Materialien gut durchzulesen, denn Information ist der erste Schritt auf dem Weg zu mehr Sicherheit bei Kartenzahlungen.

*HINWEIS: Die PCI-Zertifizierung muss jährlich erneuert werden.*

## Sichern Sie Ihr Unternehmen ab

Die Erfüllung der PCI-Datensicherheitsstandards ist für alle kartenakzeptierende Unternehmen verpflichtend. Neukunden müssen innerhalb von neunzig (90) Tagen ab Unterzeichnung der Servicevereinbarung den Nachweis über die Erfüllung der PCI-Datensicherheitsstandards erbringen. Je früher Sie sich darum kümmern, desto schneller sind Sie und Ihre Kunden geschützt. Bestandskunden werden jährlich über die Erneuerung der Zertifizierung informiert.

- Besuchen Sie unsere PCI-Internetseite [www.elavon.de/PCI](http://www.elavon.de/PCI). Dort finden Sie nähere Informationen über die PCI-Datensicherheitsstandards, eine Liste mit Antworten auf häufig gestellte Fragen (FAQs) und weiterführende Links. Über diese Internetseite können Sie auch auf das Portal unseres von Visa® und MasterCard® zertifizierten Sicherheitsgutachters (QSA, Qualified Security Assessor) und Anbieter von Netzwerkskans.
- Wählen Sie auf dem Portal des Sicherheitsgutachters aus, wie Sie Kartenzahlungen entgegennehmen und vervollständigen Sie anschließend den Selbstbewertungsfragebogen (SAQ).

- Während und nach der Vervollständigung des Fragebogens werden Sie online von unserem Sicherheitsgutachter unterstützt. Auf dem Portal werden Ihnen auch die Software zum Scannen Ihrer Systeme sowie andere Hilfsmittel zur Verfügung gestellt, die erforderlich für die Erstellung des Analyseberichts und damit auch für Ihre PCI-Zertifizierung sind.

*HINWEIS: Sollten Sie bereits über eine gültige PCI-Zertifizierung verfügen, die Sie nicht im Rahmen des Elavon-Programms erworben haben, stellen Sie uns bitte Ihre vollständigen PCI-Unterlagen innerhalb von 90 Tagen zur Verfügung. Ansonsten müssen wir Ihnen eine Gebühr wegen Nichterfüllung der PCI-Datensicherheitsstandards in Rechnung stellen.*

## Sichern Sie Ihre Erträge ab

Trotz gültiger PCI-Zertifizierung können Kartendaten kompromittiert werden - was erhebliche Kosten zur Folge haben kann, wie die Bußgeldforderungen der Kartenorganisationen oder etwaige Ermittlungen und Sicherheitsüberprüfungen vor Ort.

Da die Erfüllung der PCI-Datensicherheitsstandards aufwändig sein kann, geht Elavon im Rahmen des PCI-Zertifizierungsprogramms einen Schritt weiter und bietet eine Kostenübernahme im Falle einer Datensicherheitslücke, um Ihr finanzielles Risiko so gering wie möglich zu halten.

Die Höhe der übernommenen Kosten im Rahmen des Elavon-Programms richtet sich nach der Art der PCI-Zertifizierung.

- Elavon-Kunden, die eine gültige PCI-Zertifizierung von dem im Elavon-Programm ausgewiesenen Sicherheitsgutachter erhalten haben, können von einer Kostenübernahme von bis zu € 70.000 pro Schadensfall profitieren.
- Elavon-Kunden, die eine gültige PCI-Zertifizierung von einem anderen - als den im Elavon-Programm ausgewiesenen - Sicherheitsgutachter erhalten haben, können von einer Kostenübernahme von bis zu € 35.000 pro Schadensfall profitieren.

*HINWEIS: Das Elavon-Programm für die Einhaltung der PCI-Datensicherheitsstandards deckt bestimmte Gebühren der Kartenorganisationen sowie die Kosten für Untersuchungen bzw. Sicherheitsüberprüfungen vor Ort im Rahmen der jeweiligen Deckungssumme ab. Andere Kosten wie Gerichts- oder Anwaltskosten, Rückbelastungsgebühren, Kostenaufwand durch Kundeninformationen und Systemerneuerungen etc. variieren in der Regel und sind nicht durch das Elavon-Programm abgedeckt.*

## Im Falle einer Sicherheitslücke

Sollten Kartendaten in Ihrem Unternehmen kompromittiert werden, wird Elavon von den beteiligten Zahlungsnetzwerken entsprechend informiert. Wir werden Sie daraufhin kontaktieren und Ihnen Details über den Umfang der Kompromittierung mitteilen. Selbstverständlich unterstützen wir Sie, die Sicherheitslücke schnellstmöglich zu beheben und helfen Ihnen, die notwendigen Schritte einzuleiten, damit Sie künftig die Kartendaten Ihrer Kunden besser schützen können.