

Grundlegender PCI-DSS-Compliance -Leitfaden



Interaktiver Index



- 1. Was bedeutet PCI?**
- 2. Warum muss der PCI DSS eingehalten werden und was sind die Folgen einer Nichteinhaltung?**
- 3. Welche Maßnahmen muss ich ergreifen, um den PCI einzuhalten?**

Die Verletzung der Zahlungskartendaten Ihrer Kunden hat unmittelbare Auswirkungen auf Ihr Geschäft: Reputationsschäden, Vertrauensverlust, Sanktionen und viele weitere Folgen, die Ihrem Unternehmen schaden können. Die Anzahl der Konfigurationen und Funktionalitäten in Zahlungsmethoden nimmt zu und können bei unsachgemäßer Nutzung zu einer Schwachstelle werden, die den Zugriff auf Kundendaten erleichtert. Zum Beispiel unter anderem WLAN-Technologie, Fernzugriffsoftware oder Aufzeichnungssysteme.

Aus diesem Grund ist es wichtig, einige Konzepte zu berücksichtigen, die notwendig sind, um die verbindlichen Sicherheitsstandards für alle Unternehmen einzuhalten. Nachfolgend listen wir die oben genannten Grundkonzepte auf.

1 | Was bedeutet PCI?

PCI DSS („PCI“ steht für Payment Card Industry und „DSS“ steht für Data Security Standard) sind die Sicherheitsstandards, die alle Händler oder Dienstleister einhalten müssen, die Kartendaten verarbeiten oder speichern. Es geht um eine **Reihe von technischen und betrieblichen Anforderungen, die zum Schutz von Karteninhaberdaten geschaffen werden.**

Der PCI SSC (Security Standards Council), der von den wichtigsten internationalen Marken gegründet wurde, ist für die Festlegung der Sicherheitsstandards zuständig, die für alle Teilnehmer des Sektors gelten (Finanzinstitute, Einzelhändler, Dienstleister, Softwareunternehmen usw.).

2 | Warum muss der PCI DSS eingehalten werden und was sind die Folgen einer Nichteinhaltung?

Es ist wichtig sicherzustellen, dass die Kartendaten unserer Kunden vollständig geschützt sind. Und dazu muss man Folgendes wissen:

- **Der Schutz von Daten hilft** uns, Betrug im Zusammenhang mit Sicherheitsverletzungen, die im System auftreten können, sowie „Datenkompromittierungen“ zu verhindern. Das heißt, jede Art von unrechtmäßigem Zugriff auf die Daten der Karten unserer Kunden.
- **Der Vertrauensverlust unserer Kunden** muss vermieden werden, da sie davon ausgehen, dass ihre Kartendaten zu jeder Zeit und in jedem System sicher sind.
- **Ein unrechtmäßiger Zugriff auf Daten kann der Marke**, dem Erwerber und in noch größerem Maße dem Unternehmen schaden. Dies kann wirtschaftliche, image- oder rufschädigende Folgen haben und das Geschäft gefährden.
- **Die Techniken der kriminellen Organisationen werden im** Laufe der Zeit immer weiter verfeinert und sie verfügen zunehmend über die Mittel, sich Zugang zu den Systemen von Unternehmen zu verschaffen. Daher ist es wichtig, die technischen und Sicherheitsanforderungen einzuhalten, um Eindringlinge zu verhindern.

Und was passiert, wenn der Händler die PCI DSS-Standards nicht einhält? Dieser Verstoß kann schwerwiegende Folgen haben, darunter:



Zahlung von Bußgeldern oder Strafen, die von den Marken oder sogar von den Acquirern auferlegt werden, sowie die eventuelle Zahlung von Entschädigungen an die betroffenen Kunden, da der Karteninhaber in keinem Fall die Verantwortung für getätigte und nicht als eigene anerkannte Gebühren übernimmt. Es würde auch die Übernahme anderer Kosten wie die für forensische Untersuchungen (PFI genannt) oder Korrekturmaßnahmen (da sie höher sind als die präventiv durchgeführten) nach sich ziehen.



Unfähigkeit, mit dem Erwerber zusammenzuarbeiten, da dieser sicherstellen muss, dass alle beschafften Unternehmen diese Standards einhalten, um ein Reputations-, Finanz- oder Sanktionsrisiko zu vermeiden.




Möglichkeit der Verletzung anderer Gesetze und Vorschriften.

3 | Welche Maßnahmen muss ich ergreifen, um den PCI einzuhalten?


Wenn wir die Daten unserer Kunden schützen wollen, ist Folgendes notwendig:

1. Entwickeln und pflegen Sie ein sicheres Netzwerk.
2. Schützen Sie die gespeicherten Daten der Karteninhaber, verschlüsseln Sie Daten und andere sensible Informationen, die über offene öffentliche Netzwerke übertragen werden.
3. Pflegen Sie ein Programm zur **Verwaltung von Sicherheitslücken** (Verwendung und Pflege von Virenschutz und sicheren Anwendungen).
4. Implementieren Sie strenge **Zugangskontrollmaßnahmen** (Zugangsbeschränkungen, eindeutige IDs).
5. **Regelmäßige Überwachung und Prüfung der Netzwerke.**
6. **Pflegen Sie eine Informationssicherheitsrichtlinie.**


Und deshalb ist die gute Nachricht, dass Sie Ihr Unternehmen mit diesen Sicherheitsgrundlagen schon heute schützen können:

 **Verwenden Sie starke Passwörter und ändern Sie die Standardpasswörter.**


Kosten	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 100%;"><div style="background-color: red; height: 10px;"></div></div>

 **Schützen Sie Kartendaten und speichern Sie nur das, was Sie brauchen**

Kosten	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 80%;"><div style="background-color: red; height: 10px;"></div></div>

 **Untersuchen Sie Zahlungsterminals auf Manipulationen**

Custo	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Facilidade	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Mitigação dos riscos	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>

 **Nutzen Sie vertrauenswürdige Geschäftspartner und erfahren Sie, wie Sie sie kontaktieren können**


Kosten	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>

 **Installieren Sie Patches von Ihren Anbietern**


Kosten	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 100%;"><div style="background-color: red; height: 10px;"></div></div>

 **Schützen Sie den internen Zugriff auf Kartendaten**


Kosten	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>

 **Lassen Sie Hacker nicht einfach auf Ihre Systeme zugreifen**


Kosten	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 100%;"><div style="background-color: red; height: 10px;"></div></div>

 **Verwenden Sie Antivirensoftware**


Kosten	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>

 **Suchen Sie nach Schwachstellen und beheben Sie Probleme**


Kosten	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 100%;"><div style="background-color: red; height: 10px;"></div></div>

 **Verwenden Sie sichere Zahlungsterminals und -lösungen**

Kosten	<div style="width: 100%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 100%;"><div style="background-color: red; height: 10px;"></div></div>

 **Schützen Sie Ihr Unternehmen im Internet**

Kosten	<div style="width: 50%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 100%;"><div style="background-color: red; height: 10px;"></div></div>

 **Für optimalen Schutz machen Sie Ihre Daten für Kriminelle unbrauchbar**

Kosten	<div style="width: 100%;"><div style="background-color: red; height: 10px;"></div></div>
Leichtigkeit	<div style="width: 20%;"><div style="background-color: red; height: 10px;"></div></div>
Risikominderung	<div style="width: 100%;"><div style="background-color: red; height: 10px;"></div></div>

Neben diesen Hinweisen leiten sich je nach PCI-Level des Unternehmens weitere Pflichten ab, wie z. B. Die Vorlage verschiedener Dokumente und die Durchführung von Audits. Hier sind sie auf einfache Weise erklärt:

Welches PCI-Level hat mein Unternehmen?

Um alle Sicherheitsanforderungen zu erfüllen, gibt es für Händler PCI-Stufen, auf deren Grundlage ihnen eine Reihe von Dokumenten zugewiesen wird, die von den Marken benötigt werden, um den Grad der Konformität zu bestätigen.

Stufe 1: Händler, die jährlich mehr als 6 Millionen Transaktionen abwickeln (Dokumente: ROC, AOC und ASV).

Stufe 2: Händler, die zwischen 1 und 6 Millionen Transaktionen pro Jahr abwickeln (Dokumente: SAQ, AOC und AV).

Stufe 3: Händler, die jährlich zwischen 20.000 und 1 Million E-Commerce-Transaktionen abwickeln (Dokumente: SAQ und AOQ)

Stufe 4: E-Commerce, der weniger als 20.000 Transaktionen verarbeitet und der Rest der Unternehmen, die weniger als 1 Million Transaktionen durchführen (Dokument: SAC)

Woraus besteht jedes Dokument?

- **ROC** (Report on Compliance): Ein Bericht, in dem die Einhaltung der PCI-Standards akkreditiert wird. Das PCI-DSS-Audit eines Stufe-1-Unternehmens kann mit einem qualifizierten externen (QSA) oder internen (ISA) Assessor durchgeführt werden. Bei Dienstleistern kann der Audit nur durch einen externen Berater erfolgen.
- **SAQ** (self-assessment questionnaire): Es ist ein Selbstbewertungsdokument für Unternehmen und Dienstleister, in dem der Grad der PCI-DSS-Konformität festgehalten wird. Abhängig von der Art des Geschäfts werden einige oder andere Kontrollen angewendet.
- **AOC** (Attestation of Compliance): Eine Konformitätserklärung, die eine vereinfachte Version des SAQ oder des ROC enthält.
- **Scannt von einem ASV** (Approved Scanning Vendor/Zugelassener Scanning-Anbieter): Hierbei handelt es sich um interne und externe Analysen von Netzwerkschwachstellen auf vierteljährlicher Basis, die von einem vom PCI SSC als ASV zugelassenen Unternehmen durchgeführt werden.