Handel - Oberösterreich

PCI-DSS Compliance für Händler

Antworten auf häufig gestellte Fragen

Was ist die „PCI DSS" Compliance?

Das PCI Security Standards Council ist eine Dachorganisation der Kredit- und Debitkartengesellschaften (z.B. MasterCard, VISA, etc) und hat die Aufgabe Sicherheitsstandards zu entwickeln. Der „Payment Card Industry Data Security Standard" (PCI-DSS) wurde entwickelt, um die Karteninformationen während und nach einer Finanztransaktion zu schützen und ist ein weltweit gültiger Standard.

Der Standard ist daher ein Regelwerk für Sicherheitsanforderungen, die Händler dabei helfen können, die Kartendaten ihrer Kunden besser zu schützen.

Ist die Einhaltung der PCI DSS verpflichtend?

Alle Unternehmen, die Kartendaten entgegennehmen, übermitteln, verarbeiten und speichern sind gemäß den Richtlinien der internationalen Kartenorganisationen (VISA, MasterCard, etc.) verpflichtet den PCI DSS (Payment Card Industry Data Security Standard) einzuhalten.

Daher müssen Unternehmen, die Kartentransaktionen abwickeln, sich zwingend an die Datenschutzrichtlinien der Kreditkartenindustrie (z.B. VISA, MasterCard, etc) halten.

Die Pflicht zur Einhaltung der PCI-DSS Sicherheitsstandards trifft alle Handelsunternehmen mit Kartentransaktionen (unabhängig von ihrer Größe, Transaktionsvolume oder von der Anzahl der Kartentransaktionen).

Was sind die Konsequenzen der Nichteinhaltung der PCI Sicherheitsstandards?

- Wenn das Unternehmen keine ausreichenden Sicherheitsvorkehrungen trifft und Kreditkartendaten gestohlen werden, kann es zu Reputationsschaden kommen.
- Kunden wechseln zu der Konkurrenz, weil ihre Kundendaten dort besser geschützt sind.
- Es drohen Strafgebühren durch Kartenorganisationen und Gerichtsverfahren – die Höhe ist nicht genau definiert.
- Unternehmen können die Berechtigung verlieren, Bezahlverfahren mit Zahlungskarten anzubieten. Dies könnte auch inkludieren, dass Acquirer dem Händler keine Terminals anbieten.

Ist die Durchführung der PCI-DSS kostenpflichtig?

Manche Zahlungsanbieter verlangen für die PCI-Zertifizierung eine Gebühr, andere wiederum (z.B. Six Payment) stellen ein kostenloses Zertifizierungsportal zur Verfügung.

Muss die PCI-Zertifizierung über den Zahlungsanbieter erfolgen?

Grundsätzlich besteht die Möglichkeit einer Selbsteinschätzung. Danach sind je nach Umsatzhöhe und Art der Kartendaten-Verwendung entsprechende Fragebögen auszufüllen und ggf. je nach Risiko Maßnahmen zu treffen (z.B. Schwachstellenscans, Auditbericht durch ein befugtes Unternehmen, ...).

In diesem Dokument finden Sie einen Leitfaden zur Klassifizierung Ihres Unternehmens. Sie erfahren, in welches LEVEL Ihr Unternehmen fällt und welcher Fragebogen/welche Fragebögen für Ihre Selbstauskunft (SBF) bearbeitet werden müssen.
» "SBF"-Fragebögen

Wir empfehlen Ihnen sich bei Ihrem Zahlungsanbieter zu erkundigen, ob eine Selbsteinschätzung akzeptiert wird.

Tipp: Die Broschüre „Gängige Zahlungssysteme" gibt Ihnen einen Überblick, wie Zahlungen im bargeldlosen Zahlungsverkehr in der Praxis technisch abgewickelt werden. Mit Fallbeispielen werden Szenarien aufgezeigt, wie Kriminelle Ihre Zahlungsterminals, Websites, PCs manipulieren können und welche Schutzmaßnahmen dafür erforderlich sind.

Kreditkartendaten können nur geschützt werden, wenn Sie wissen, wo sich diese Daten befinden. Der Leitfaden für „sichere Zahlungsverfahren" gibt Ihnen zahlreiche Sicherheitstipps.

Stand: 13.11.2018