Reisebüros - Oberösterreich

Kreditkartendatensicherheit: PCI-DSS Compliance für Reisebüros

Sicherheit bei Kreditkartenzahlungen

Der Payment Card Industry Data Security Standard (PCI bzw. PCI-DSS) ist ein Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht und von allen wichtigen Kreditkartenorganisationen unterstützt wird.

Der PCI DSS Standard wurde entwickelt, um die Sicherheit von Karteninhaberdaten zu verbessern und die umfassende Akzeptanz einheitlicher Datensicherheitsmaßnahmen auf der ganzen Welt zu vereinfachen. Er liefert grundlegende technische und betriebliche Anforderungen zum Schutz von Kontodaten. Der PCI-DSS gilt für **alle Einrichtungen, die mit Zahlungskarten arbeiten** (einschließlich Vertragsunternehmen, EDV-Dienstleistern, abrechnenden Stellen, Kartenemittenten und Dienstleistern) und **die Karteninhaberdaten und/oder vertrauliche Authentifizierungsdaten speichern, verarbeiten oder übertragen.**

Grundsätzlich ist jedes Unternehmen verpflichtet, eine Selbsteinschätzung gemäß den Vorgaben des Kreditkartenanbieters vorzunehmen. Danach sind je nach Umsatzhöhe und Art der Kreditkartendaten-Verwendung entsprechende Fragebögen auszufüllen und ggf. je nach Risiko Maßnahmen zu treffen (z.B. Schwachstellenscans, Auditbericht durch ein befugtes Unternehmen, ...).

Wie vielen bereits bekannt ist, fordert die IATA ab 1. März 2018 die Einhaltung der Vorschriften aktiv ein. **Wir möchten aber darauf hinweisen, dass auch Nicht-IATA Reisebüros den Anforderungen entsprechen müssen, wenn Kreditkartenzahlungen akzeptiert werden.** Bitte prüfen Sie diesbezüglich Ihren Vertrag mit dem Kreditkarteninstitut.

Hier finden Sie die Unterlage des Vortrags von Ralph Wörn (www.adsigno.com) vom 21.7.2017 . In Kapitel 3 der Unterlagen PCI DSS 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. Die "SBF"-Fragebögen finden Sie hier.

Achtung!

- In nicht zertifizierten Midoffice Systemen keine Kreditkartendaten speichern!
- Wenn möglich keine Kreditkartendaten am eigenen PC oder Server speichern (Datenbanken, Excel Listen, Buchhaltung,...). Falls doch, müssen entsprechende Sicherheitsvorkehrungen getroffen werden
- Aufpassen bei der Übertragung der Kreditkartendaten bei Direktinkasso (Lösung: Lediglich Übertragung eines Tokens)
- Firewall + Virenscanner installieren, ggf. Sicherheitsüberprüfung durch geplanten Hackerangriff!