hobex
PAYMENT SYSTEMS

SICHERER UMGANG MIT **KREDITKARTENDATEN** IM TOURISMUS.

INFORMATION **2019**

1. KREDITKARTENSICHERHEIT:
PCI STANDARD, DATENSCHUTZ

DER SICHERHEITSSTANDARD PCI

Kreditkartenmissbrauch ist an der Tagesordnung. Sicherheitsvorfälle, die es bis in die Medien schaffen, sind nur die Spitze des Eisberges. Alle großen Kreditkartenorganisationen (Visa, Mastercard, American Express, Diners, JCB) haben zum Schutz der Kreditkartendaten seit 2006 den verpflichtenden PCI DSS Sicherheitsstandard geschaffen. Die Grundaussage lautet:

Die **dauerhafte Speicherung von Kreditkartendaten** (Kartennummer, Name, Ablaufdatum) auf eigenen Systemen soll **vermieden** werden. Wenn unbedingt notwendig ist, dann nur unter strengen Bedingungen (u.a. Verschlüsselung, Zugriffsüberwachung) erlaubt. **Kurzfristig** notwendige **Kreditkartendaten** (z.B. für eine Reservierung oder Nachverrechnung) sind so bald als möglich, **spätestens nach 120 Tagen, zu löschen**. Die Speicherung des **Magnetstreifens** und der **Kartenprüfnummer** sind verboten.

Wer den Standard nicht einhält, riskiert bei einem Datenverlust hohe Strafen!

HOTELS BESONDERS BETROFFEN

Hotels sind durch die hohe Kundenfrequenz und die vielen Kartenzahlungen besonders interessant für Kriminelle. Zum einen bildet der starke Einsatz von Online-Buchungen und E-Mail Angriffspunkte für Kreditkartendaten, zum anderen die häufig anzutreffende Speicherung in der Hotel-Management-Software mit einem Zugang für zahlreiche Hotel-Mitarbeiter. Kommt noch eine Fernwartung über das Internet durch eine ausgelagerte IT-Betreuung dazu, wird das Risiko nochmals erhöht. Die Tourismusbranche war in den letzten Jahren diejenige mit den häufigsten Kartendiebstählen, häufiger als beim E-Commerce!

Die Kreditkartenorganisationen haben darauf reagiert und verlangen von allen Hotels jährlich einen Sicherheitsnachweis gemäß PCI. Weiters sind laut Datenschutz Kartendaten personenbezogene Daten und daher zu schützen.

HOBEX UNTERSTÜTZUNG

Kreditkartensicherheit muss nicht kompliziert und teuer sein. hobex zeigt Ihnen in diesem Folder die wichtigsten Maßnahmen für Hotels. Der PCI Nachweis kann mit einem Selbstauskunft-Fragebogen (SAQ) erbracht werden.

hobex AG • Josef-Brandstätter-Straße 2b • 5020 Salzburg
T +43 662 2255-0 • F +43 662 2255-399 • M vertrieb@hobex.at • www.hobex.at
LG Salzburg • DVR 0660868 • FN 37265b • UID-NR. ATU35185508

2. SICHERER UMGANG MITKARTENDATEN

WIE VIELE KARTENDATEN HABE ICH ÜBERHAUPT? WOZU?

Je mehr Kartendaten aufgehoben werden, je mehr Mitarbeiter Zugriff haben und je geringer die Absicherung ist, desto höher die Chance eines Datenverlusts und desto höher die Strafzahlung bei den Kreditkartenorganisationen! Am Anfang steht daher die **Erhebung** zu wissen, **wo** im Unternehmen überhaupt Kartendaten gespeichert werden, **wie viele** Daten vorhandenen sind und **wozu** diese benötigt werden.

WAS DARF ÜBERHAUPT AUFGEHOBEN WERDEN?

ERLAUBT	EINGESCHRÄNKT	VERBOTEN
Karteninhaber	Kartennummer	Magnetstreifen
Ablaufdatum	nur maskiert (max. die ersten 6 und letzten 4 Ziffern sichtbar) oder verschlüsselt	Kartenprüfnummer (CVC, CVV)
		PIN Code

MASSNAHMEN FÜR DEN SICHEREN UMGANG

Für die Umsetzung in Ihrem Unternehmen gilt der zentrale Grundsatz:

So wenige Kartendaten wie möglich, Aufbewahrung so kurz wie möglich!

Kartennummern werden von hobex weder für Reklamation noch für Korrekturbuchungen benötigt.
In diesen Fällen genügt die Transaktionsnummer vom Beleg. Auch Hotel-Stammkunden schätzen Sicherheit!
Die Speicherung der Kartendaten ist eine oft gut gemeinte, aber **gefährliche Dienstleistung.**
Nur vertrauenswürdige (z.B. Strafregisterauszug) und geschulte Mitarbeiter sollten Zugriff zu Kreditkartendaten erhalten. Dies erfordert auch das Datenschutzgesetz.

CHECKLISTE

- ○ Dokumentation ob und wie viele Kartendaten gespeichert werden
- ○ betroffene Mitarbeiter geschult
- ○ Regelung für künftige Speicherung (wo, wie lange)
- ○ Kartennummer nur maskiert oder verschlüsselt gespeichert

hobex AG • Josef-Brandstätter-Straße 2b • 5020 Salzburg
T +43 662 2255-0 • F +43 662 2255-399 • M vertrieb@hobex.at • www.hobex.at
LG Salzburg • DVR 0660868 • FN 37265b • UID-NR. ATU35185508

hobex

3. RESERVIERUNGEN:
ÜBER BUCHUNGSPLATTFORMEN, E-MAIL, FAX

RESERVIERUNGEN

Reservierungen, die direkt beim Hotel mit der Kreditkartennummer (über Telefon, Fax oder E-Mail) für eine manuelle Buchung am POS-Terminal verwendet werden, verursachen die hohen Datenschutzanforderungen des PCI-Standards. Wenn Sie dieses Verfahren anwenden, beachten Sie bitte folgende Punkte:

1. **Übertragung** von E-Mails mit Kreditkartendaten aus dem Posteingang so rasch als möglich in eine **sichere Aufbewahrung** (z.B. passwortgeschütztes PDF, verschlüsseltes ZIP-Archiv). Anschließend löschen Sie das E-Mail im **Posteingang** und im Papierkorb.
2. Ablage von Papierausdrucken mit Kreditkartennummern (Fax, E-Mail-Ausdruck) in einem versperrten Schrank mit Zugriff für wenige Mitarbeiter. Reservierungsmappen an der Rezeption gelten als unsicher!
3. Sobald eine Reservierung nicht mehr benötigt wird – längstens vier Monate nach Leistung – sind die **Dateien/Datensätze mit Kreditkartendaten zu löschen** und die Ausdrucke zu **shreddern/vernichten.**
4. **Einschulung der Mitarbeiter auf diese Vorgangsweise:**
   hobex bietet für Reservierungen Online-Lösungen, wo keine Speicherung der Kartendaten im Hotel und keine manuelle Buchung mehr notwendig sind.

HOMEPAGE UND BUCHUNGSPLATTFORMEN: DAS HOTEL BLEIBT VERANTWORTLICH

Wer eine Buchungsplattform oder eigene Homepage nutzt, muss sich vergewissern, dass diese entweder PCI-zertifiziert ist oder nur sichere Arten des Kartenumgangs bietet (keine oder verschlüsselte Speicherung, maskierte Anzeige von Kartennummern). Die **Übertragung der Kreditkartendaten** im Klartext per **E-Mail** von der Buchungsplattform/Homepage an das Hotel wird zwar häufig eingesetzt, ist aber **nicht erlaubt!**

CHECKLISTE

- ◯ Vorgangsweise für E-Mails, Ausdrucke und Faxe mit Kreditkartennummern definiert
- ◯ Gäste über Risiko bei E-Mail-Versand der Kartennummer informiert
- ◯ Sicherheitsstatus der eigenen Homepage und verwendeten Buchungsplattformen gecheckt
- ◯ Mitarbeiterschulung erfolgt

hobex AG • Josef-Brandstätter-Straße 2b • 5020 Salzburg
T +43 662 2255-0 • F +43 662 2255-399 • M vertrieb@hobex.at • www.hobex.at
LG Salzburg • DVR 0660868 • FN 37265b • UID-NR. ATU35185508

4. NETZWERKE, FIREWALL, GÄSTEZUGANG

FIREWALL IST SELBSTVERSTÄNDLICH

Eine Firewall muss Ihr Hotel-Netzwerk vom Internet schützen und zwar in beide Richtungen:

1. eingehend, damit Unbefugte keinen Zugriff auf Ihre Daten, insb. Kreditkartendaten erlangen können
2. ausgehend, damit Trojaner, Angreifer oder Mitarbeiter keine Daten unbeschränkt ins Internet übertragen können

FERNWARTUNG NUR MIT KONTROLLE

Die Fernwartung von IT-Programmen oder Haustechnik sollte nicht ständig und unbeaufsichtigt verfügbar sein, sondern nur nach Bedarf des Hotels. Das vermindert die Gefahr von unerlaubten Angriffen oder der Ausnutzung von Sicherheitslücken. Fernwartungsprogramme wie z.B. Teamviewer verwenden dazu eine Freigabe für die Fernwartung mittels Sitzungspasswort.

GÄSTE BITTE DRAUSSEN BLEIBEN

Wenn Ihr Hotel den Gästen einen Internetzugang zur Verfügung stellt, dann muss dieser abgetrennt vom Büronetzwerk erfolgen. Gäste dürfen niemals Zugriff auf das hobex-Zahlungsterminal, ihre Hotel-Management-Software oder eventuell gespeicherte Kreditkartendaten erlangen. Die Trennung kann durch eine eigene Internetanbindung für Gäste oder besondere Netzwerktechnik (VLAN) erfolgen.
Wenn das Hotel für sich selbst WLAN einsetzt, so ist darauf zu achten, dass durch die Absicherung (WPA2) weder für Gäste noch Unbekannte ein unerlaubter Zugriff möglich ist.

CHECKLISTE

- ○ aktuelle und wirkungsvolle Firewall für die Anbindung an das Internet
- ○ Fernwartungszugänge nur nach Bedarf aktiviert
- ○ Trennung des Internetzugangs für Gäste vom Hotel-Netzwerk
- ○ WLAN-Verschlüsselung nach aktuellem Standard (WPA2)

5. SOFTWARE

SICHERE SOFTWARE ALLGEMEIN

Sobald Sicherheitslücken zeitnah geschlossen werden, sinken die Chancen für Angreifer. Daher gilt besonders für alle IT-Systeme und Webseiten, auf denen Sie Kreditkartendaten verarbeiten oder speichern:

1. Einspielung aller notwendigen **Sicherheitsaktualisierungen** (z.B. Microsoft-Updates, Adobe Updates,...) zumindest **1x im Monat**
2. aktuelles und ständig laufendes **Antivirenprogramm**
3. Aktivierung der **Ereignisprotokollierung**, um die Spuren von Angriffsversuchen oder unerlaubten Zugriffen aufzuzeichnen

BESONDERHEITEN HOTEL-SOFTWARE

Eine Hotel-Management-Software steuert die Prozesse von der Buchung bis zur Abrechnung. In vielen Fällen können bei den Abrechnungsdaten oder Zahlungsschnittstellen Kreditkarten eingegeben und gespeichert werden. Wenn Sie eine derartige Software einsetzen und Kreditkartendaten erfassen, dann muss folgendes gewährleistet sein:

1. Die Software sollte eine Zertifizierung nach PCI (Payment Application) haben. Damit erbringt der Softwarehersteller den Nachweis, dass sein Programm in der Lage ist alle Sicherheitsanforderungen einzuhalten.
2. Sie müssen bei der Konfiguration Ihrer Software alle Einstellungen, wie vom Hersteller vorgegeben („Implementation Guide"), so getroffen haben, dass Sie den PCI Sicherheitsstandard erfüllen.

! **Kreditkartendaten in einer Software ohne Zertifizierung ist das Risiko des Hotels!**

CHECKLISTE

- ◯ Sicherheits-Updates eingespielt, Antivirus laufend aktualisiert
- ◯ Ereignisprotokollierung aktiviert
- ◯ Prüfung der eingesetzten Hotel-Software auf PCI Zertifizierung
- ◯ Konfiguration Hotel-Software entsprechend „Implementation Guide"

6. BENUTZER UND PASSWÖRTER

PASSWÖRTER

Wirkungsvolle Passwörter dürfen nur dem **Besitzer bekannt** sein, **schwer zu erraten** sein und sollten **regelmäßig** gewechselt werden. Nutzen Sie zur Erzeugung oder Ablage der Passwörter beispielsweise einen Passwortmanager auf einem Smartphone. Damit gehören aufgeschriebene Passwörter auf Post-IT's oder schwache Passwörter die in sekundenschnelle zu knacken sind („1234", „hans") der Vergangenheit an.

PROBLEMFALL STANDARDPASSWÖRTER, STANDARDBENUTZER

Zahlreiche Software- und Hardwareprodukte (z.B. Router, WLAN) werden mit Standardbenutzern/-passwörter ausgeliefert, damit sie sofort funktionieren. Diese vom Hersteller vergebenen Standardkennungen sind natürlich auch Angreifern bekannt und werden automatisiert durchprobiert.

> **Gemäß PCI Standard sind alle Standardpasswörter zu ändern oder die Standardbenutzer zu deaktivieren.**

PROBLEMFALL GRUPPENBENUTZER

Hotels neigen in Bereichen mit vielen Mitarbeitern, Schichtdienst oder Personalwechsel dazu, allgemeine Gruppenbenutzer wie z. B: „rezeption" zu vergeben. Der Benutzer und das Passwort sind weitläufig bekannt, oft sogar bei externen IT-Betreuern oder ausgeschiedenen Mitarbeitern. Im Ernstfall gibt es keine Möglichkeit nachzuvollziehen, wie und durch wen ein Datenzugriff stattgefunden hat.

> **Gruppenbenutzer für Systeme und Programme wo Kreditkartendaten verarbeitet oder gespeichert werden, sind nach dem PCI Standard nicht zulässig.**

CHECKLISTE

- ◯ Mitarbeiter zu sicheren Passwörtern verpflichtet und Passwortregeln in Programmen aktiviert (Länge, Aufbau, Wechsel)
- ◯ Standardpasswörter gewechselt
- ◯ Gruppenbenutzer abgeschafft und durch Individualbenutzer ersetzt

7. HARDWARE

MANIPULIERTE TERMINALS

Selten aber doch scheuen Betrüger nicht den Aufwand die POS-Terminals zu manipulieren. Mit kleinen Einschüben (Skimming) werden Kartendaten mitgelesen.

> **Wer solche Manipulationen rasch erkennt ist den Betrügern voraus!**

CHECKLISTE

- ○ regelmäßige Sichtkontrolle der Kartenlesegeräte auf Manipulationen
- ○ Liste der Kartenlesegeräte führen (Seriennummer)
- ○ kein Terminalzugriff für Unbekannte außerhalb der Geschäftszeiten
- ○ Reparaturen nur durch hobex; bei unbekannten Technikern im Zweifel hobex zum Gegencheck fragen