more security. usd

Kreditkartensicherheit für die Reisebranche

Der Payment Card Industry Data Security Standard (PCI DSS)

So schützen Sie die Daten Ihrer Kunden vor Hackern und Kriminellen

Informationen für Mitglieder des

DRV Deutscher ReiseVerband

Vorwort

Liebe DRV-Mitglieder,

dieses Thema betrifft alle: Sowohl Reisebüros und Veranstalter als auch Anbieter von Reisedienstleistungen oder Geschäftsreisen müssen Kreditkartendaten ihrer Kunden vor Betrug oder Missbrauch schützen. Jedes Unternehmen, das für die Bezahlung von Reiseleistungen von seinen Kunden Kreditkarten akzeptiert, ist betroffen. Damit bei der Abwicklung von Zahlungen mit ‚Plastikgeld' sensible und vertrauliche Daten der Kunden geschützt sind und die Zahlungssicherheit gewährleistet ist, haben Kreditkarten-Unternehmen einen Standard entwickelt – den „Payment Card Industry Data Security Standard", abgekürzt: PCI DSS.

Dieser Standard schreibt vor, wie Unternehmen Kreditkartendaten verarbeiten, übertragen oder speichern dürfen. Handelsunternehmen und Dienstleister, die Kreditkarten-Transaktionen speichern, übermitteln oder abwickeln, müssen diese Regelungen befolgen. Die im PCI DSS festgelegten Regelungen sind mit neuen Pflichten für Händler, die Kreditkartenzahlung akzeptieren, verbunden. Sie werden Bestandteil der Verträge zwischen Merchants (Händlern) und Acquirern (Banken oder anderen Abrechnungsdienstleistern).

Wir sollten uns in unserer Branche bewusst sein, dass der sichere Umgang mit den Kreditkartendaten im Interesse aller liegen sollte, die mit diesen Daten umgehen. Nicht nur, weil ein Diebstahl von Kreditkartendaten mit hohen Schadensersatzforderungen der Kreditkartenorganisationen verbunden sein kann, sondern weil die notwendigen Untersuchungen zu zeitweisen Betriebsstilllegungen und vor allem zu einem Vertrauensverlust bei den Kunden führen können.

Um Reiseunternehmen einen Überblick über ihre aus dem PCI DSS-Standard resultierenden Pflichten zu geben, hat der Deutsche ReiseVerband (DRV) exklusiv für seine Mitglieder in dieser Informationsbroschüre alles über die Anforderungen und den korrekten Umgang mit den sensiblen Kreditkartendaten zusammengefasst. Wir danken dem PCI DSS-Zertifizierungsanbieter usd für die Ausarbeitung und Zusammenstellung und hoffen, dass diese Infobroschüre Sie im Geschäftsleben mit wertvollen Tipps und allem Wissenswerten zu PCI DSS unterstützt.

Ihr Jürgen Büchy
Präsident Deutscher ReiseVerband (DRV)

1 Warum dieser Guide?

Dieser Guide ist für die Praxis. Er ist für Unternehmen aus der Reisebranche, die sich und ihre Kunden vor Hackern und Kriminellen schützen wollen. Wir werden weder über Statistiken noch über Dunkelziffern sprechen, wir werden auch nicht darüber sprechen, wie selektive Medien die Realität verzerren. Wir sind der Überzeugung, dass die meisten Menschen verstanden haben, dass organisierte Kriminalität rund um Kreditkarten und Internet ein relevantes Thema ist. Sie verstehen die Risiken und möglichen Folgen, aber sie haben eine berechtigte Frage:

Was können wir konkret tun, um unser Unternehmen und die Daten unserer Kunden zu schützen?

Die Antwort ist einfach und komplex zugleich. Einfach, weil es bereits einen strukturierten Plan gibt, der zeigt, was man tun kann – der

Payment Card Industry Data Security Standard (PCI DSS)

Er umfasst eine Reihe von Best Practices zum Schutz Ihres Unternehmens und Ihrer Kunden. Die Schwierigkeit liegt nicht in der Theorie, sondern in der Praxis. Bei der Umsetzung des Standards gibt es wie so oft keine schnellen Ergebnisse. Die Umsetzung der Maßnahmen bedeutet mehr Sicherheit, aber eben auch Aufwand. Wie viel, hängt von der Größe und den Geschäftsprozessen Ihres Unternehmens ab.

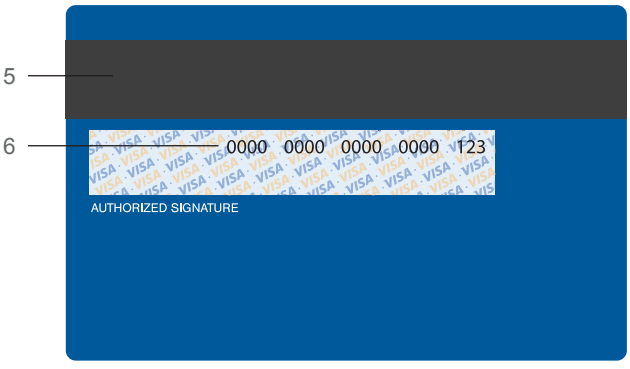
Dieser Guide ist für die Praxis. Wir werden aufzeigen, wie Sie am besten bei der Umsetzung vorgehen. Wir werden aufzeigen, wie Sie Aufwände und Kosten nachhaltig reduzieren können. Wir werden aufzeigen, wie Sie Ihr Unternehmen und Ihre Kunden vor Hackern und Kriminellen schützen.

Fangen wir an.

1.1 Kreditkartendiebe in der Reisebranche

Die Reisebranche bietet Kriminellen vielfältige Möglichkeiten. Bei Reiseveranstaltern und in (Geschäfts-) Reisebüros werden Kreditkartendaten weit verstreut und häufig in vielen Bereichen entgegengenommen, verarbeitet und gespeichert. Die Daten werden für Buchungen auf unterschiedlichsten Wegen übermittelt, z.B. per Telefon, E-Mail, Fax oder Internet. Hinzu kommen die Online-Portale mit großen Mengen an Kreditkartendaten der Kunden.

1 Chip
2 Kartennummer (Primary Account Number, PAN)
3 Gültigkeitsdatum



4 Name des Karteninhabers
5 Magnetstreifen
6 Kartenvalidierungscode, Prüfziffer

Je weiter verstreut die Daten sind, desto mehr Möglichkeiten haben Kriminelle, diese zu stehlen – und desto schwieriger ist es für Sie, die Daten angemessen zu schützen.

1.2 Wie agieren eigentlich Kreditkartendiebe?

Zunächst ein kurzer Einblick in das Vorgehen der Kartendiebe. Wie bereits angedeutet, im Zentrum des Interesses stehen nicht die physischen Karten selbst, sondern die Kreditkartendaten. Diese befinden sich auf der Karte, zum einen in Form von Beschriftung, zum anderen gespeichert auf Chip und Magnetstreifen.

Die von Kriminellen begehrten Informationen sind vor allem der Name des Karteninhabers, das Gültigkeitsdatum, die Kreditkartennummer (PAN) sowie die Prüfziffer (CVC2/CVV2/…). Ist man im Besitz dieser Informationen, kann man – z.B. im Internet – auf Kosten des eigentlichen Karteninhabers Zahlungen tätigen. In einigen wenigen Fällen reicht sogar die Kartennummer (ohne Prüfziffer). Anschließend wird die gekaufte Ware dann an Mittelsmänner ausgeliefert oder weiterverkauft.

Eine weitere Methode von Kartendieben ist die Manipulation von Bezahlterminals. Die Daten des Magnetstreifens werden beim Zahlungsvorgang ausgelesen und an den Kartendieb übermittelt. Dieser kann die erbeuteten Daten auf eine „Blanko“-Kreditkarte kopieren und mit dieser dann auch „offline“ bezahlen.

Häufig nutzen Kreditkartendiebe die erbeuteten Daten aber nicht selbst, sondern sie verkaufen sie weiter. Hierfür gibt es einen organisierten Schwarzmarkt für gestohlene Kreditkartendaten im Internet. Das Risiko für die Kriminellen ist dabei vergleichsweise gering. Sie sind meist bestens organisiert und agieren international. Eine Rückverfolgbarkeit ist so gut wie unmöglich.

2 Mehr Sicherheit durch PCI DSS

Um Kreditkartenbetrug einzudämmen und Kartentransaktionen sicherer zu machen, haben 2005 die großen Kreditkartenorganisationen Visa, MasterCard, American Express, JCB International und Discover Financial Services den **Payment Card Industry Data Security Standard (PCI DSS)** entwickelt.

PCI DSS ist ein industrieller Standard. Er wird permanent vom unabhängigen PCI Security Standards Council[1] weiterentwickelt und basiert auf einer Reihe von bewährten Best Practices. Die Umsetzung dieser Best Practices ermöglicht es Ihnen, die Kreditkartendaten Ihrer Kunden vor Kriminellen zu schützen.

2.1 Was ist „PCI DSS Compliance“?

Zunächst einmal gilt: es gibt keine gesetzliche Verpflichtung zur Einhaltung des PCI DSS. Dennoch ist PCI DSS ein verbindlicher Standard. Das heißt, alle Unternehmen, die Kreditkartendaten speichern, verarbeiten oder übertragen, müssen sich an den Standard halten. Die Vorgabe kommt nicht vom Gesetzgeber, sondern von den Kreditkartenorganisationen selbst. Diese fordern einen Nachweis über die sogenannte „PCI DSS Compliance“, also die Konformität mit dem Standard. Maßgeblich dafür, ob ein Nachweis über die PCI DSS Compliance zu erbringen ist, ist letztendlich die Vertragssituation mit den angebundenen Kreditkarten-Prozessoren, z.B. dem Acquirer (Händlerbank) oder beispielsweise dem angebundenen Reiseveranstalter oder der Airline.

Die meisten Unternehmen, die mit Kreditkartendaten in Berührung kommen, fallen in die Kategorie **„Händler“**. Sie akzeptieren Zahlungen per Kreditkarte. In der Reisebranche sind dies die **Reiseveranstalter** sowie

[1] http://de.pcisecuritystandards.org/minisite/en/

alle **Reisebüros**, sofern sie einen eigenen Kreditkartenvertrag mit einem Acquirer besitzen.

Darüber hinaus gibt es in vielfältigen Bereichen sogenannte **Service Provider**, die Dienstleistungen mit Bezug zur Kreditkartenzahlung erbringen. Einige typische Service Provider bei Bezahltransaktionen in der Kreditkartenindustrie sind in der folgenden Abbildung zu sehen: z.B. Webhosting Provider für Onlineportale oder IT-Dienstleister für den Betrieb der Unternehmens-Firewall.

2.2 Wie erbringt man den Nachweis über die PCI DSS Compliance?

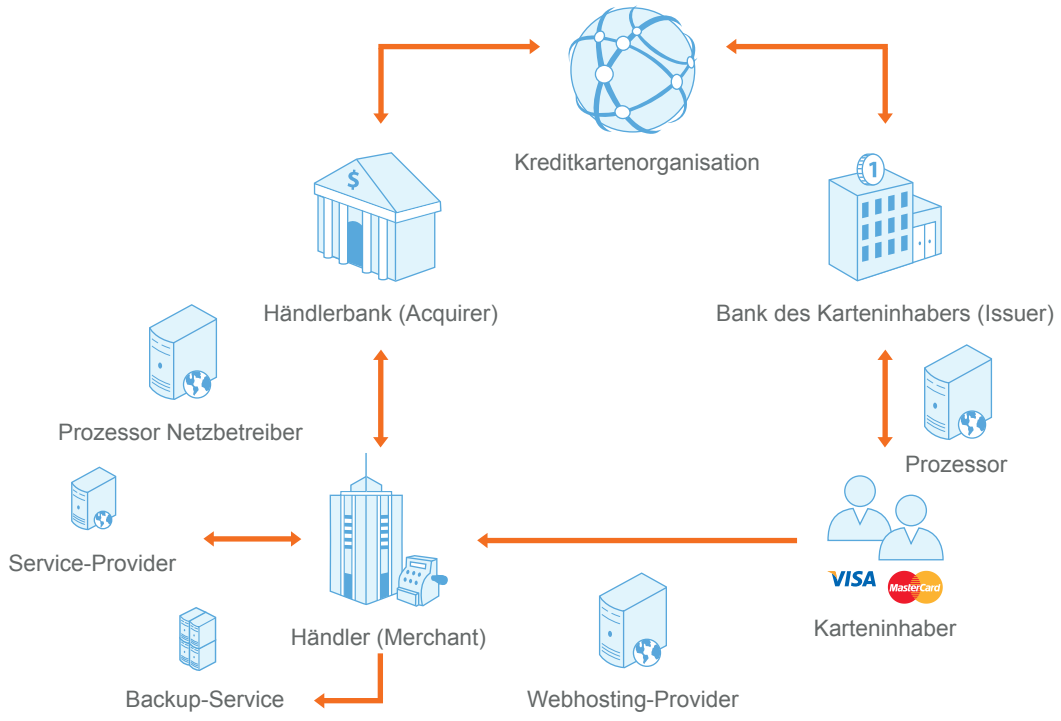
Für die meisten Unternehmen gilt: sie erbringen den Nachweis über ihre PCI DSS Compliance, indem sie einen sogenannten **Selbstauskunftsfragebogen (Englisch: Self Assessment Questionnaire, SAQ)** ausfüllen. Insgesamt gibt es fünf verschiedene Typen von SAQ, von denen der auf Ihr Unternehmen zutreffende SAQ vollständig beantwortet und zur Prüfung eingereicht werden muss. Der jeweilige SAQ ergibt sich aus den Geschäftsprozessen Ihres Unternehmens. Mehr dazu später.

Achtung: Das Reisebüro als Handelsvertreter

Falls ein Reisebüro ausschließlich als Handelsvertreter für Reiseveranstalter tätig ist und keinen Akzeptanzvertrag mit einem Acquirer besitzt, ist der Reiseveranstalter für das Thema PCI DSS verantwortlich. Das Reisebüro selbst muss sich dabei nicht um das Thema PCI DSS kümmern.

Es versteht sich von selbst, dass das reine Beantworten der Fragen nicht zur „PCI DSS Compliance“ führt.

Der Kreditkartenbezahlprozess und die beteiligten Parteien



Der SAQ ist eine Checkliste für Ihr Unternehmen. Diese können Sie Schritt für Schritt durchgehen und abarbeiten. Es geht darum, festzustellen, ob Ihre Geschäftsprozesse konform zum Standard sind. Mit jedem Punkt, den Sie konform zum Standard ausführen, minimieren Sie die Risiken für Ihr Unternehmen. Hier eine Beispielfrage:

Ist die PAN bei der Anzeige maskiert (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden)?

Hinweise

- Diese Anforderung gilt nicht für Mitarbeiter und andere Parteien, die die vollständige PAN aus betrieblichen Gründen einsehen müssen.
- Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten – z. B. für POS-Belege.

Wenn Sie die PAN also maskieren, dann können Sie „Ja“ ankreuzen, denn Ihr Vorgehen ist konform. Konnten Sie alle Fragen mit „Ja“ beantworten, so können Sie Ihren SAQ einreichen. Er wird geprüft und anschließend wird Ihre „PCI DSS Compliance“ offiziell bestätigt. Prüfung und Bestätigung erfolgen über ein Unternehmen, das als Prüfer für PCI DSS (QSA) akkreditiert ist.

Treffen Sie hingegen auf Fragen, bei denen Ihr Geschäftsprozess nicht dem beschriebenen Vorgehen entspricht, so ist Ihr Handeln nicht PCI DSS konform. Um Risiken zu minimieren, müssen Sie zunächst Ihren Geschäftsprozess umstellen oder eine Maßnahme zum Schutz der Daten implementieren.

Tipp: Siegel und Zertifikat

Bei einigen, aber nicht allen prüfenden Unternehmen erhalten Sie auch ein Siegel und Zertifikat, das Sie zum Beispiel auf Ihrer Website oder in Ihren Broschüren verwenden können. Wenn Sie ein Siegel und Zertifikat für Marketing und Kundenkommunikation möchten, dann sollten Sie diesen Punkt bei der Auswahl des prüfenden Unternehmens berücksichtigen.

Den richtigen SAQ auswählen

Es gibt insgesamt fünf verschiedene SAQ. Einen davon müssen Sie ausfüllen. Welchen, entscheidet sich anhand Ihrer Geschäftsprozesse. Ein maßgeblicher Einflussfaktor ist, ob Sie Kreditkartendaten in elektronischer Form speichern. Ist dies der Fall, so müssen Sie SAQ D ausfüllen. Wie Sie anhand der nachfolgenden Tabelle sehen, ist SAQ D der umfangsreichste SAQ mit den meisten Fragen.

Beispiel Szenario 1:
In einem Reisebüro werden zur Zahlung mit Kreditkarte zwei ISDN POS Terminals eingesetzt, die jeweils an den beiden Arbeitsplätzen der Mitarbeiter positioniert sind. Die Geräte speichern keine Kreditkartendaten, sie generieren nach erfolgter Zahlung lediglich einen Papierbeleg. Im Anschluss daran wird ausschließlich mit dem Papierbeleg weitergearbeitet (in Buchhaltung, etc.). Aus diesem beispielhaften Szenario resultiert, dass der SAQ der Kategorie B auszufüllen ist.

Beispiel Szenario 2:
Ein Reise-Online-Portal bietet Kreditkartenzahlung als Bezahlmethode auf der Online Buchungsplattform an. Um eine sichere Bezahlung per Kreditkarte zu ermöglichen, hat das Online-Portal einen Vertrag mit einen so genannten Internet Payment Service Provider (IPSP) geschlossen. Die Kreditkartenbezahlvorgänge

SAQ - Kategorie	Umfang	Zielpublikum/Merkmale
A	13 Fragen	Alle Kreditkartenfunktionen sind ausgelagert. Keine physische Präsenz von Kreditkarten (d.h. nur E-Commerce oder Versandhandel).
B	29 Fragen	Es werden ausschließlich Terminals mit Wählverbindung (ISDN oder analog) zur Kreditkartenzahlung eingesetzt. Keine elektronische Speicherung von Kreditkartendaten (auch nicht vom Terminal!).
C-VT	40 Fragen	Zahlungsabwicklung erfolgt ausschließlich mit webbasierten virtuellen Terminals. Der Computer, auf dem das virtuelle Terminal verwendet wird, darf mit keinem anderen System des Händlers verbunden sein. Keine elektronische Speicherung von Kreditkartendaten.
C	51 Fragen	Einsatz von Kreditkartenterminals und/oder Zahlungsanwendungssystemen, die mit dem Internet verbunden sind. Die Kreditkartenterminals und/oder Zahlungsanwendungssysteme dürfen **nur** mit dem Internet und mit **keinem** anderen System des Händlers verbunden sein. Keine elektronische Speicherung von Kreditkartendaten.
D	288 Fragen	Alle, die nicht in den Beschreibungen für SAQ A bis C oben enthalten. Alle Dienstanbieter.

werden nicht über das Online-Portal des Reisedienstleisters durchgeführt, sondern mit Hilfe des IPSPs über ein in die Webseite eingebettetes iFrame. Damit verarbeitet das Online-Portal selber keine Kreditkartendaten. Aus diesem beispielhaften Szenario resultiert, dass alle Kreditkartenfunktionen ausgelagert sind und damit der SAQ der Kategorie A ausgefüllt wird. Hinweis: Würden die Kreditkartendaten vom Online-Portal verarbeitet, müsste der SAQ D ausgefüllt werden, was die PCI DSS Umsetzung deutlich erschweren würde.

Achtung: E-Mails mit Kartendaten

Falls Ihnen jemand einmal fälschlicherweise eine E-Mail schickt, die Kreditkarteninformationen (insbesondere die Kreditkartennummer) enthält, sollten Sie diese E-Mail sofort nach Erhalt aus dem Posteingang und aus dem Papierkorb bzw. „Gelöschte Objekte“ Ordner löschen.

Wie und wo kann man den SAQ ausfüllen?

Grundsätzlich erhalten Sie den SAQ von Ihrer Händlerbank oder als Download von den Webseiten des PCI SSC unter:

http://de.pcisecuritystandards.org/minisite/en/saq-v2.0-documentation.php

Alternativ können Sie Ihr Unternehmen auf unserer PCI DSS Plattform anmelden (https://pci.usd.de). Wir unterstützen Sie bei der Auswahl des richtigen SAQ. Bei Fragen erreichen Sie einen Experten aus unserem Competence Center, der Ihnen weiterhilft.

2.3 Das Onsite-Audit: die Prüfung vor Ort

Bei einigen Unternehmen reicht das Ausfüllen des SAQ nicht aus. Sie müssen zusätzlich ein sogenanntes Onsite-Audit durchführen. Dabei handelt es sich um eine Prüfung Ihres Unternehmens vor Ort. Diese betrifft alle **Service Provider** mit mehr als 300.000 Transaktionen im Jahr sowie **Händler** mit mehr als 6 Millionen MasterCard oder Visa Transaktionen im Jahr. Das Onsite-Audit wird von einem akkreditierten PCI Prüfer durchgeführt. Das Ergebnis ist ein ca. 100 Seiten langer Bericht mit allen geprüften PCI Anforderungen und einer Gesamteinschätzung des Prüfers.

In der Reisebranche sind klassischerweise **Betreiber** von **Online-Portalen** als Service Provider anzusehen, wenn das Online-Portal als Dienstleistung für einen Dritten (zum Beispiel einen Reiseveranstalter) betrieben wird.

Service Provider mit (potentiellem) Zugriff auf Kreditkartendaten

Wie bereits erläutert, gibt es im Kreditkartenumfeld eine Vielzahl von Service Providern, die an den Prozessen der Kreditkartenzahlung beteiligt sind. Wenn ein solcher Service Provider, zum Beispiel als Web-Hosting Provider bei einem Online-Portal, von einem Kreditkartenzahlungen akzeptierenden Händler genutzt wird, gibt es zwei Möglichkeiten, wie im Rahmen der PCI DSS Zertifizierung mit dem Dienstleister umzugehen ist:

1) Der Service Provider kann eine eigene PCI DSS Zertifizierung vorweisen: Damit ist eine eigene Prüfung nicht erforderlich. Es muss nur sichergestellt werden, dass die PCI Zertifizierung des Service Providers wirklich die vom Auftraggeber genutzten Dienstleistungen beinhaltet.

2) Der Service Provider hat keine eigene PCI Zertifizierung: Ist dies der Fall, muss der Auftraggeber die vom Dienstleister zur Verfügung gestellten PCI relevanten Services mit im Rahmen seiner eigenen PCI DSS Zertifizierung prüfen. Konkret heißt das, beim Ausfüllen des Selbstauskunftsfragebogens (oder bei der Durchführung des Onsite-Audits) müssen die für den Service Provider relevanten Teile des PCI DSS mit beantwortet werden. Falls beispielsweise ein Dienstleister die Unternehmens-Firewall betreibt, muss der Dienstleister die im PCI DSS definierten Anforderungen zum Thema Firewall (Kapitel 1) für den Auftraggeber beantworten.

Tipp: Nutzen Sie zertifizierte Dienstleister

Wenn ein Dienstleister im Rahmen der Kreditkartenverarbeitung eingesetzt wird, sollte darauf geachtet werden, dass der Dienstleister eine PCI DSS Zertifizierung vorweisen kann. Dies vereinfacht Ihre PCI DSS Zertifizierung, da Sie beim Ausfüllen des SAQ auf die Zertifizierung des Dienstleisters verweisen können.

2.4 Wie starten?

Bevor Sie sich um detaillierte Maßnahmen Gedanken machen, sollten Sie zunächst überprüfen, wo und wie Kreditkartendaten in Ihrem Unternehmen verarbeitet werden. Um Ihre Daten vor Kreditkartendieben zu schützen, benötigen Sie zunächst einen Überblick, wo diese generell gestohlen werden können.

Als nächstes sollten Sie mit den beteiligten Personen diskutieren, ob am bestehenden Prozess etwas geändert werden kann. Ziel ist es, möglichst auf die Speicherung und Aufbewahrung von Kreditkartendaten zu verzichten. Daten, die Sie nicht benötigen, sollten Sie nicht aufbewahren, denn offensichtlich können diese dann auch nicht gestohlen werden.

Erstellen Sie am besten eine sogenannte **„Cardholder Data Matrix“**. Diese könnte beispielsweise so aussehen:

Hinweis: Maskierte Kartennummern

Maskierte Kartennummern der Form 512345XXXXXX1234 sind aus Sicherheitssicht nicht schützenswert, weil sie für den Angreifer keinerlei Wert haben. Nach Möglichkeit sollten ausschließlich maskierte Kartennummern gespeichert werden (zum Beispiel auf dem Händlerpapierbeleg).

Ein besonderes Augenmerk sollten Sie auf jene Stellen legen, wo Kreditkartendaten in elektronischer (digitaler) Form vorhanden sind. Auf Rechnern gespeicherte Informationen stellen für Hacker eine leichte Beute dar. Wenn sie sich Zugang zum internen Netzwerk verschafft haben, können Kreditkartendaten in großen Mengen entwendet werden. Da sie dabei nicht physisch vor Ort sein müssen, ist das Risiko entdeckt zu werden für sie relativ gering.

Geschäftsprozess	Bereich	Medium, das die Kreditkartendaten enthält	Weiterverarbeitung der Kreditkartendaten
Kunde bezahlt eine gebuchte Reise mit seiner Kreditkarte	Reisebüro POS Terminal	Händlerbeleg (Papier) aus dem POS Terminal	Der Reisebüromitarbeiter zieht die Karte durch das Terminal, gibt sie anschließend dem Kunden zurück und behält einen Papierbeleg, welcher in einem verschließbaren Schrank/ Schublade aufbewahrt wird.
Buchung einer Reise auf dem Online-Portal	E-Commerce	Kreditkartendaten werden kurzzeitig in der Web-Datenbank gespeichert.	Die Kreditkartendaten werden vom Online-Portal entgegengenommen und temporär in der Datenbank gespeichert. Nach erfolgreicher Transaktion werden die Daten aus der Datenbank gelöscht.

Tipp: Verzichten Sie auf die Speicherung von Daten

Der Aufwand, um diese angemessen zu schützen, ist enorm und bedarf einer Vielzahl an Maßnahmen. Konkret bedeutet dies das Ausfüllen des umfangreichsten SAQ D. Klären Sie daher, ob Kreditkarteninformationen wirklich in elektronischer Form gespeichert werden müssen.

Nachdem Sie die Matrix erstellt und Ihre Geschäftsprozesse hinterfragt haben, können Sie die Umsetzung des PCI DSS in Angriff nehmen. Springen Sie zum entsprechenden Kapitel, je nachdem in welchem Bereich Sie tätig sind: (Geschäfts-)Reisebüro, Online-Portal oder Reiseveranstalter. Dort haben wir weitere Hinweise und Tipps für Sie.

3 PCI DSS in der Praxis für (Geschäfts-) Reisebüros

Generell gibt es verschiedene Varianten, wie mit Kreditkarten in (Geschäfts-)Reisebüros umgegangen wird. Vergleichen Sie zunächst Ihren Geschäftsprozess mit den Beispielen.

3.1 Das Reisebüro als Handelsvertreter

Für den PCI DSS ist die vertragliche Situation Ihres Unternehmens im Prinzip irrelevant. Alle Kreditkartenprozesse sollten sicher betrieben werden. Hierzu bietet der vorliegende Guide viele Vorschläge und Anregungen.

Allerdings bedeutet die Sondersituation bei Reisebüros mit Handelsvertreter-Status, dass die Entscheidung über die PCI DSS Umsetzung letztendlich bei den vertretenden Firmen liegt. Von daher sollte die PCI DSS Umsetzung mit den vertretenden Unterneh-

1	Bezahlung erfolgt mittels Kreditkarte vor Ort im Reisebüro mit Hilfe eines POS Terminals durch Stecken oder Durchziehen der Karte durch das Terminal.	Wir empfehlen diese Variante, weil sie die Umsetzung des PCI DSS und den Schutz der Daten vereinfacht.
2	Bezahlung erfolgt über eine Payment Anwendung (z.B. Amadeus) mit Direkteingabe der Kreditkartendaten in die Applikation.	Diese Variante ist möglich, doch ist der Schutz der Daten hier aufwendiger als in Variante 1.
3	Kreditkarteninformationen werden per E-Mail empfangen oder in Excel-Tabellen aufbewahrt.	Auf diese Art der Kreditkartenverarbeitung sollten Sie auf jeden Fall verzichten, weil sie leicht von Kriminellen ausgenutzt wird und vor allem unnötig ist. Normalerweise können mit den Varianten 1 oder 2 alle Geschäftsprozesse rund um Kreditkarten abgedeckt werden.

men abgestimmt werden. Fordert beispielsweise keines der Unternehmen eine offizielle PCI DSS Zertifizierung, so ist das Ausfüllen eines Selbstauskunftsfragebogens nicht notwendig.

3.2 Zugriff auf Kreditkarteninformationen

In der Einleitung haben wir bereits darüber gesprochen, dass Sie keine Kartendaten speichern sollten, die Sie nicht wirklich benötigen. Der nächste Schritt ist: überlegen Sie, wer im Unternehmen Zugang zu den Kartendaten hat und wer ihn wirklich benötigt.

Grundsätzlich gilt, der Zugriff auf Kreditkartendaten (zum Beispiel auf Papierbelege) sollte nur denjenigen Mitarbeitern möglich sein, die den Zugriff für ihre Tätigkeit auch benötigen. Mit steigender Anzahl von Personen, die Zugriff auf sensible Daten haben, vergrößert sich natürlich auch das Risiko, dass diese abhandenkommen. Dies muss nicht zwangsläufig durch einen böswilligen Insider geschehen, sondern kann schlichtweg auf Unwissenheit zurückzuführen sein, wie mit sensiblen Informationen umzugehen ist.

Sicherheitsmaßnahmen zum Minimieren des Zugriffs auf Kreditkarteninformationen

Zugriffsrechte sollten so vergeben werden, dass jeder Mitarbeiter ausschließlich die zur Ausführung seiner Tätigkeit notwendigen Rechte hat. Dies schließt sowohl den Zugang zu Rechnern, als auch den Zugang zu Schränken, Schubladen oder Räumlichkeiten ein. Ein Passwort sollte nur demjenigen Mitarbeiter bekannt sein, der den Rechnerzugang auch benötigt. Genauso sollten nur diejenigen Mitarbeiter einen Schlüssel für die Aufbewahrungsorte von Kreditkarteninformationen erhalten, die diesen für ihre Tätigkeit brauchen. Dabei sollten Sie sämtliche Aufbewahrungsorte berücksichtigen, also beispielsweise auch den Schrank im Back-Office oder die Buchhaltung. Scheidet ein Mitarbeiter aus dem Reisebüro aus, dann überprüfen Sie, ob dieser mit speziellen Zugriffsrechten ausgestattet war. Hatte er Zugang zu einem Rechner, dann ändern Sie das Passwort. Stellen Sie sicher, dass Sie alle ausgehändigten Schlüssel zurückbekommen.

Checkliste für den Zugang zu Daten

- ☐ Überprüft, wer Zugang zu Kartendaten hat
- ☐ Standardvorgehen etabliert, wenn ein Mitarbeiter mit Zugang zu den Daten das Unternehmen verlässt

3.3 Umgang mit Kartendaten auf Papier

Wenn Sie Kreditkarteninformationen im Reisebüro auf Papier aufbewahren – z.B. als Ausdrucke, Faxe und Belege aus den Bezahlterminals – dann sollten Sie auf folgendes achten:

Bewahren Sie Kreditkarteninformationen auf Papier immer in verschließbaren Schränken oder Schubladen auf. Ausdrucke und Belege sollten beispielsweise niemals sichtbar auf einem Schreibtisch gestapelt werden. Solche Dokumente sollten generell als vertraulich eingestuft werden und die Mitarbeiter, die mit ihnen in Berührung kommen, sollten hinsichtlich der Sensibilität der Informationen, die sie enthalten, geschult sein (siehe Kapitel 3.5).

Auf keinen Fall dürfen Sie die sogenannten sensiblen Authentisierungsdaten speichern, also Prüfziffer oder die PIN. Auf die PIN hat ein Reiseunternehmen in der Regel zwar keinen Zugriff, enthält aber beispielsweise eine fälschlicherweise empfangene E-Mail (siehe Hinweis zum Umgang mit E-Mails in Kapitel 2.2) eines Kunden auch seine Prüfziffer, so muss diese auf einem Ausdruck unkenntlich gemacht (geschwärzt) werden.

Achten Sie bei der Entsorgung von Ausdrucken, Belegen und sonstigen Dokumenten mit Kreditkartendaten darauf, dass diese auch wirklich vernichtet werden und nicht wieder herstellbar sind. Sie gehören in den Aktenvernichter und nicht einfach nur in den Papierkorb. Durch einen Kreuzschnitt/Partikelschnitt (cross-cut) werden Dokumente in einer Weise zerkleinert, so dass eine Verwertbarkeit der Informationen auf den Einzelteilen nicht mehr möglich ist.

Tipp: Verlässliche Aktenvernichter

Wenn Sie die Aktenvernichtung selbst vornehmen, dann achten Sie bei der Anschaffung eines Aktenvernichters darauf, dass er über einen Cross-Cut verfügt. In der Norm DIN 32757-1 sind fünf Sicherheitsstufen definiert. Für die sichere Vernichtung von sensiblen Informationen wird hierzu mindestens ein Aktenvernichter der Sicherheitsstufe 3 empfohlen.

Wenn Sie einen Dienstleister mit der Entsorgung beauftragt haben, dann achten Sie darauf, dass dieser die Verantwortung für die ordnungsgemäße Vernichtung der Dokumente übernimmt. Dieser Aspekt sollte Bestandteil des schriftlichen Vertrags mit dem jeweiligen Dienstleister sein. Häufig werden in solch einer Situation die Dokumente nicht sofort vernichtet, sondern erst gesammelt. Dann muss der Container, in dem diese aufbewahrt werden, vor Zugriff durch Unbefugte geschützt werden. Wenn diese beispielsweise in einem Schrank aufbewahrt werden, sollte dieser mindestens mit einem Schloss gesichert werden.

3.4 Dokumentation und Prozesse

Wichtig ist auch eine saubere Dokumentation Ihrer Prozesse, um den Überblick über die verschiedenen Maßnahmen zu behalten. Abgesehen davon ist die schriftliche Dokumentation der beste Weg, um im Zweifelsfall gegenüber Dritten Ihre PCI DSS Compliance nachweisen zu können. Wir empfehlen, für die folgenden Bereiche eine knappe und pragmatische Dokumentation zu pflegen.

Informationssicherheitsrichtlinie

Hierbei handelt es sich um ein Dokument, dass vor allem zur Information für Ihre Mitarbeiter dient. Dabei geht es nicht um die Anfertigung eines komplexen Nachschlagewerks, sondern darum, alle sicherheitsrelevanten Themen kurz abzubilden. Dies betrifft in erster Linie den sicheren Umgang mit Kreditkarteninformationen, aber auch den Umgang mit Computern und

Checkliste für den Umgang mit Kreditkartendaten auf Papier

- Ausdrucke, Faxe und Belege mit Kreditkarteninformationen werden unter Verschluss aufbewahrt ☐
- Hochgradig sensible Informationen (insbesondere die Prüfziffer) werden auf Ausdrucken geschwärzt ☐
- Sichergestellt, dass Kreditkartendaten bei Entsorgung unwiederbringlich vernichtet werden ☐
- Überprüft, ob der beauftragte Dienstleister (falls vorhanden) die Dokumente ordnungsgemäß entsorgt und auch die Verantwortung dafür übernimmt (Vertragsregelung) ☐

der auf ihnen installierten Software. Insbesondere sollten Mitarbeiter darauf hingewiesen werden, dass Kreditkarteninformationen niemals ungeschützt per E-Mail versendet werden dürfen.

Zur Kommunikation werden häufig sogenannte Messaging-Technologien für Endanwender verwendet, die allerdings keine Möglichkeit bieten, die zu übertragenden Daten angemessen zu schützen. Deshalb dürfen diese keinesfalls zum Versand von Kreditkartendaten verwendet werden. Unter den Begriff der Endbenutzer-Technologien fallen generell unverschlüsselte E-Mails, Instant Messenger und Chat Programme, wie beispielsweise WhatsApp oder Skype. Durch im Internet frei verfügbare Software können die Nachrichten leicht abgefangen und ausgelesen werden, da die meisten dieser Programme keinerlei Möglichkeiten zur Verschlüsselung der Nachrichten bieten. Aufgrund des verstärkten Risikos bei der Kommunikation über Software, die Nachrichten unverschlüsselt übertragen, sollte gänzlich auf deren Nutzung verzichtet werden. Am besten ist dies in einer Arbeitsanweisung festzuhalten, die die Nutzung von riskanten Technologien verbietet. Damit Mitarbeiter verstehen, warum sie darauf verzichten sollen, weist man sie am besten auf die damit verbundenen Gefahren hin.

Geben Sie die Informationssicherheitsleitlinie an jeden Mitarbeiter aus und lassen Sie sich per Unterschrift auf einem Formular bestätigen, dass die Richtlinie gelesen und verstanden wurde.

Vergessen Sie nicht, einmal pro Jahr die Richtlinie hinsichtlich ihrer Aktualität zu prüfen und gegebenenfalls anzupassen, sofern Veränderungen stattgefunden haben.

Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten

Mitarbeiter, die Umgang mit Kreditkartendaten haben, sollte Sie darauf hinweisen, dass sie es mit sensiblen Informationen zu tun haben und wie mit diesen korrekt umzugehen ist. Dies umfasst die Inhalte aus den Abschnitten *Umgang mit E-Mails sowie Umgang mit Ausdrucken und Papierbelegen*.

Liste mit Zugriffs- und Zugangsberechtigungen

Legen Sie eine Liste an, in der Sie vermerken, welche Mitarbeiter Zugang zu Kartendaten haben. Unterscheiden Sie zwischen Zugang zu digitalen Daten (also Computer und E-Mails) sowie Zugang zu Daten auf Papier (Schlüssel für die Aufbewahrungsorte von Ausdrucken und Papierbelegen). Im Zusammenhang mit dem Dienstplan können Sie so nachverfolgen, wer zu welchem Zeitpunkt Zugang auf Kartendaten hat. Außerdem hilft Ihnen die Liste, wenn ein Mitarbeiter Ihr Unternehmen verlässt und Sie überprüfen müssen, ob Passwörter geändert und/oder Schlüssel eingesammelt werden müssen.

Liste externer Dienstleister

Bestehen Verträge mit externen Dienstleistern, die mit Kreditkartendaten in Berührung kommen, so sollten diese hinsichtlich der Sensibilität der Daten aufgeklärt werden. Es sollte vertraglich berücksichtigt werden, dass diese für die Sicherheit von Kreditkartendaten mitverantwortlich sind, sobald sie mit diesen zu tun haben. Beispielsweise muss einem Dienstleister, der mit der Vernichtung von Kreditkartendaten beauftragt wird, klar sein, dass er für eine ordnungsgemäße Entsorgung verantwortlich ist.

Die großen Kreditkartengesellschaften führen eigene Listen, in denen die PCI DSS Compliance von Dienstleistern und Herstellern rund um das Kreditkartengeschäft nachvollziehbar ist. Diese werden auf den jeweiligen Webseiten zur Verfügung gestellt und können von jedem eingesehen werden.

Liste von MasterCard

www.mastercard.com/us/company/en/whatwedo/compliant_providers.html

Liste von Visa Europe

www.visaeurope.com/en/businesses__retailers/payment_security/service_providers.aspx

Ob das von Ihnen eingesetzte Kartenterminal zertifiziert ist, können Sie ebenfalls auf den Webseiten des PCI Council, unter folgendem Link herausfinden:

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Den Status der PCI DSS Compliance von Dienstleistern sollten Sie einmal jährlich überprüfen.

Checkliste Sicherheitsrichtlinien und Prozesse

- Informationssicherheitsrichtlinie existiert und wird an Mitarbeiter ausgehändigt ☐
- Arbeitsanweisung für Mitarbeiter mit Zugriff auf Kreditkartendaten angefertigt ☐
- Liste mit Zugriffs- und Zugangsberechtigungen angefertigt ☐
- Liste externer Dienstleister angefertigt ☐
- Den Status der Dienstleister zur PCI DSS Konformität überprüft ☐

Insbesondere, wenn Sie Kreditkartendaten mit Zahlungsanwendungen verarbeiten und damit in den Anwendungsbereich des SAQ C fallen, können Sie auf den Webseiten des PCI Councils nachverfolgen, ob die von Ihnen eingesetzte Software dem PCI Payment Application Data Security Standard (PCI PA-DSS) genügt. Die Verwendung von zertifizierter Software erleichtert die Umsetzung der Maßnahmen zur eigenen PCI DSS Compliance. Ob und welche Version einer Zahlungsanwendung nach PCI PA-DSS zertifiziert ist, können Sie unter folgendem Link auf den Webseiten des PCI Councils überprüfen:

https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

3.5 Sensibilisierung der Mitarbeiter

Besonders wichtig ist, dass Sie Ihre Mitarbeiter „sensibilisieren“ und ein sogenanntes **Security Awareness Training** absolvieren lassen. Hier werden wichtige Hinweise für eine Vielzahl von Situationen vermittelt. Wie merke ich mir Passwörter? Worauf muss ich beim Umgang mit E-Mails achten? Wie verhalte ich mich im Notfall richtig? Eine Sensibilisierung kann aber auch schon erreicht werden, indem beispielsweise Poster oder Bildschirmschoner mit einem Sicherheitshinweis am Arbeitsplatz darauf hinweisen.

3.6 Kreditkartenbezahlung mit Bezahlterminal

Die sicherste Variante zur Verarbeitung von Kreditkartenzahlungen ist die Nutzung eines modernen POS Terminals, das mit Hilfe von ISDN Technologie kommuniziert. Bei der ISDN Technologie werden die Kartendaten nicht über das Internet versendet und sind daher für einen Angreifer besonders schwierig abgreifbar. Außerdem sind diese Geräte normalerweise speziell gegen Manipulationen gesichert (beispielsweise durch den Einsatz eines Sicherheitssiegels) und machen es für Angreifer sehr schwierig, sensible Kreditkarteninformationen zu stehlen. Wir empfehlen daher die Nutzung eines POS Terminals.

Wenn Sie absolut sicher sein wollen, dass Ihr POS tatsächlich manipulationssicher ist und keine Kartendaten speichert, sollten Sie sich von Ihrem Dienstleister, der Ihnen das Terminal zur Verfügung gestellt hat, bestätigen lassen, dass das Bezahlterminal die Kreditkartensicherheitsstandards erfüllt.

Auf folgender Website des PCI Council können Sie herausfinden, ob das von Ihnen eingesetzte Kartenterminal eine gültige Zertifizierung nach PCI PTS (PIN Transaction Security) aufweist. Ist dies der Fall, dann können Sie davon ausgehen, dass das Gerät mit den Anforderungen des PCI DSS vereinbar ist.

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

3.7 Transaktionen per Payment Application

Neben der klassischen Nutzung eines Bezahlterminals bieten moderne Buchungsanwendungen (Amadeus, Sabre, etc.) ebenfalls ein Bezahlmodul, in das die Kreditkartendaten des Kunden eingegeben werden. Hierbei sind aus PCI DSS Sicht jedoch einige zusätzliche Sicherheitsmaßnahmen erforderlich, um die IT-Infrastruktur im Reisebüro angemessen vor Angreifern zu schützen.

Hinweis: POS Terminal oder Payment Application?

Durch den Einsatz einer Payment Application wird die PCI DSS Zertifizierung komplizierter, d.h. es muss, im Vergleich zum Bezahlterminal, ein umfangreicherer Fragebogen beantwortet werden (mindestens SAQ C oder C-VT).

Checkliste POS Terminals

Optional: Dienstleister oder Hersteller des eingesetzten Kartenterminals kontaktiert und geklärt, ob

- das Kartenterminal gegen Manipulationen besonders geschützt ist ☐
- das eigene Kartenterminal Kreditkartendaten speichert* ☐

*Falls ja, klären, ob diese sicher gelöscht werden können. Wenn nicht, dann spätestens bei der Anschaffung eines neuen Terminals auf diese Punkte achten.

Netzwerksegmentierung per Firewall

Trennen Sie jene Systeme, die Kreditkartendaten verarbeiten, von denen, die keinen Zugriff auf diese Informationen benötigen. Insbesondere für die Anwendbarkeit des SAQ C ist die Isolierung der kreditkartendatenverarbeitenden Systeme zwingende Voraussetzung. Konkret bedeutet diese Anforderung, dass die Reisebüro-PCs mit der Bezahlanwendung in diesem Fall nur mit dem Internet und mit keinem anderen System im Reisebüro verbunden sein dürfen. Damit soll das Risiko eines Diebstahls von Kreditkarteninformationen gesenkt werden.

Der Einsatz und die geeignete Konfiguration von Firewalls und / oder Routern mit strikten Access Control Listen (ACLs)[2] kann die Kommunikation zwischen denjenigen Systemen, welche Kreditkartendaten verarbeiten, und den anderen sich im Reisebüro befindlichen Systemen unterbinden, so dass die gewünschte Segmentierung erreicht wird. Kreditkartendatenverarbeitende Systeme dürfen keinen direkten Zugriff auf Systeme haben, die mit Kreditkartendaten arbeiten. Sprechen Sie mit Ihrem IT-Dienstleister. Er kann Sie bei der Umsetzung unterstützen.

Hinweis: Warum ist die Trennung so wichtig?

Wenn die kreditkartendatenverarbeitenden Systeme nicht isoliert werden, dann müssen Sie für das gesamte Netzwerk umfangreiche Maßnahmen zu dessen Schutz treffen. Sie fallen in die Kategorie SAQ D mit 288 Fragen und haben einen erheblichen höheren Aufwand bei der Umsetzung.

Sichere Konfiguration der Firewall und der PCs mit der Bezahlanwendung

Für den sicheren Betrieb des PCs mit der Bezahlanwendung muss eine Firewall oder ein Router mit strikten Access Control Lists (ACLs) implementiert werden. Die Konfiguration der Firewall-Regeln darf unter keinen Umständen den Datenverkehr zwischen den normalen Büro-PCs und dem PC mit der Bezahlanwendung zulassen und muss darüber hinaus dokumentiert werden. Der PC mit der Bezahlanwendung darf über die Firewall ausschließlich eine Verbindung zum Internet bekommen. Alle anderen Verbindungen müssen deaktiviert werden („deny-all“).

Auch der für die Bezahlvorgänge eingesetzte PC muss laut Vorgabe der PCI Anforderungen besonders geschützt werden. Falls ein mobiler PC (Laptop) eingesetzt wird, muss dort eine Desktop Firewall genutzt werden, die von den Mitarbeitern im laufenden Betrieb nicht deaktiviert oder umkonfiguriert werden darf.

Standardkennwörter und Einstellungen

Ändern Sie die Standardkennwörter und Einstellungen aller eingesetzten Geräte, über die Kreditkartendaten übertragen werden (z.B. Firewall und andere Netzwerkgeräte wie Router oder Switches), um eine sichere Konfiguration der Geräte und PCs sicherzustellen. Hierzu gehört auch das Abschalten von nicht benötigten Diensten und Funktionen. In der Regel finden sich entsprechende Anweisungen in den Handbüchern und es gibt für sehr viele Betriebssysteme sogenannte Härtungsrichtlinien, mit deren Hilfe das Betriebssystem besonders sicher konfiguriert werden kann. Eine umfassende Ressourcen-Quelle für Härtungsrichtlinien aller Art ist beispielsweise das „Center for Internet Security (CIS)“. Dort finden Sie im Bereich „Security Benchmarks“ Konfigurationshinweise für nahezu alle Betriebssystem-Typen und Anwendungen:

[2] http://de.wikipedia.org/wiki/Access_Control_List

http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks

Achtung: Updates nicht vergessen

Es gibt immer wieder Sicherheitsschwachstellen in Produkten und Geräten. Aktualisieren Sie mindestens einmal monatlich Ihre Geräte mit den Sicherheitsupdates der Hersteller.

Falls Sie Windows Systeme verwenden, benötigen Sie einen Virenscanner zu deren Schutz. Der Virenscanner sollte seine Viren- Signaturen täglich aktualisieren. Wichtig ist auch, darauf zu achten, dass die Anti-Virus-Lösung mindestens folgende Arten von Malware erkennen kann: Viren, Trojaner, Würmer, Spyware, Adware und Rootkits. Überwachen Sie die Systeme nicht nur im „on-access“ Scan Modus (Live-Überwachung), sondern führen Sie auch regelmäßig (einmal pro Woche) einen kompletten Scan des Systems durch.

Checkliste Firewall und PC mit Bezahlanwendung

- Einsatz und Konfiguration einer Firewall oder eines Routers mit strengen Access Control Lists ☐
- Firewall Regelsatz minimiert und dokumentiert, PCs mit der Bezahlanwendung isoliert, der PC mit der Bezahlanwendung kommuniziert ausschließlich über die Firewall mit dem Internet ☐
- Alle anderen Verbindungen eingestellt auf „deny-all“ ☐
- Bei der Verbindung zum Internet wird eine sogenannte „Stateful Inspection“ (zustandsorientierte Firewall) genutzt ☐
- Bei Einsatz von mobilen PCs gilt: Es wird eine aktivierte Desktop-Firewall genutzt, die Firewall kann nicht von unautorisierten Mitarbeitern deaktiviert oder umkonfiguriert werden ☐
- Standardkennwörter auf allen Geräten (Firewalls, Router, Switches, PCs, usw.) geändert ☐
- Nicht benötigte Funktionen und Dienste deaktiviert ☐
- Alle eingesetzten Komponenten werden mindestens einmal monatlich mit allen aktuellen Hersteller-Sicherheitsupdates versorgt ☐
- **Falls Windows Systeme eingesetzt werden:** Die Systeme werden geschützt durch eine Anti-Virus-Lösung, bei der die Viren-Signaturen täglich aktualisiert werden und die in der Lage ist, mindestens folgende Arten von Malware zu erkennen: Viren, Trojaner, Würmer, Spyware, Adware und Rootkits. Regelmäßige Komplett-Scans (einmal pro Woche) des Systems werden durchgeführt. ☐

Sicherheit der Bezahlanwendung gewährleisten

Für den Einsatz von Bezahlanwendungen gibt es einen besonderen Sicherheitsstandard, genannt „Payment Application Data Security Standard“ (PA-DSS). Verwenden Sie eine Bezahlanwendung, die die Anforderungen von PA-DSS erfüllt, damit Sie sicher sein können, dass diese sicher ist. Lassen Sie sich vom Hersteller oder dem Reseller der Software bestätigen, dass die Bezahlanwendung die Anforderungen des PA-DSS erfüllt.

Beim Einsatz einer Bezahlanwendung gibt es für den Hersteller oder einen IT-Dienstleister häufig die Möglichkeit eines Fernzugriffs auf die Systeme. Dieser Fernzugriff aus dem Internet heraus muss immer über eine so genannte Zwei-Faktor-Authentisierung erfolgen. Bitte sprechen Sie hierzu mit Ihrem IT-Dienstleister oder Software-Hersteller, falls es einen Fernzugriff in Ihr Netzwerk gibt.

Auch für die Bezahlanwendung gilt: Standardkennwörter sollten geändert und die Einstellung der Software nach Herstellervorgabe sicher konfiguriert werden. Hierzu sollte Ihnen der Hersteller eine entsprechende Konfigurations-Vorgabe zur Verfügung stellen. Falls die Bezahlanwendung offiziell PA-DSS zertifiziert ist, liefert der Hersteller Ihnen einen so genannten Implementation Guide, in dem alle PCI relevanten Einstellungen im Detail dokumentiert sind.

4 PCI DSS in der Praxis für Online-Portale

Die Anforderungen und Sicherheitsmaßnahmen zum Schutz der Kartendaten auf Online-Portalen sind äußerst umfangreich. Wir empfehlen daher: überprüfen Sie, ob Sie die Bezahlfunktion per Online-Portal unbedingt benötigen oder ob Sie diese nicht an einen Payment-Dienstleister auslagern können. Durch die Auslagerung hat Ihr Online-Portal keinen Kontakt mit Kreditkartendaten mehr, denn diese werden nur durch den Payment-Dienstleister verarbeitet. Natürlich müssen Sie bei der Auswahl eines Dienstleister darauf achten, dass dieser PCI DSS zertifiziert ist.

Die Erfahrung hat gezeigt, dass das Auslagern der Bezahlfunktion an einen PCI zertifizierten Dienstleister gerade für kleinere Online-Portale (zum Beispiel für Reisebüros mit eigenem Online-Portal) in jedem Fall mittelfristig die kostengünstigere Lösung ist, auch wenn im ersten Moment Kosten für die Migration auf die neue Bezahlschnittstelle entstehen. Weil die Kreditkartendaten nicht länger im Unternehmen verarbeitet werden, bleibt letztlich nur noch das Ausfüllen von SAQ A, in dem bestätigt wird, dass ein Bezahldienstleister eingesetzt wird.

Checkliste Bezahlanwendung

- ☐ Sichergestellt, dass die Anwendung die Anforderungen des PCI PA-DSS erfüllt (Anfrage an den Hersteller der Software)
- ☐ Fernzugriff mit einer Zwei-Faktor Authentisierung abgesichert
- ☐ Standardkennwörter der Anwendung geändert und die Bezahlanwendung nach Vorgabe des Herstellers sicher konfiguriert

Falls aus Geschäftsgründen eine Auslagerung des Bezahlvorgangs nicht möglich ist, müssen Sie zum Schutz der Kartendaten umfangreiche Sicherheitsanforderungen umsetzen. Hierbei können Sie sich zunächst an den im Kapitel „PCI DSS in der Praxis für (Geschäfts-) Reisebüros“ beschriebenen Maßnahmen orientieren. Sie müssen aber davon ausgehen, dass darüber hinaus weitere Maßnahmen auf Sie zukommen. Welche genau, darüber lässt sich nur schwer eine generelle Aussage treffen, da sich Online-Portale in den Details ihrer Geschäftsprozesse häufig unterscheiden.

Der wichtigste Hinweis, den wir geben können: lassen Sie sich von einem autorisierten PCI Auditor (QSA) beraten. Wenn Sie sich für die Auslagerung der Bezahlfunktion entschieden haben, kann er Sie bei der Auswahl eines zertifizierten Dienstleisters unterstützen. Wenn Sie die Bezahlfunktion nicht auslagern können, dann sollten Sie eine Statusanalyse machen lassen, um eine verlässliche Aussage darüber zu erhalten, welche Maßnahmen für den Schutz Ihrer Daten notwendig sind.

Wie finde ich einen autorisierten PCI Auditor (QSA)?

Unter diesem Link finden Sie eine Liste der akkreditierten Prüfer.

https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

4.1 Sondersituation Reisevermittlerportale (Online Travel Agents)

Bei Reisevermittlerportalen, die Kreditkartendaten ausschließlich an das Zielunternehmen weiterleiten, selber aber niemals Kreditkartenbezahltransaktionen durchführen, besteht eine vertragliche Sondersituation. Von daher gibt es sehr häufig keinen Vertragspartner, der die PCI Compliance einfordert. Es existiert also weder eine Vertragsbeziehung mit einem Acquirer, noch mit den Kreditkartengesellschaften selbst. Im Prinzip gelten aber die gleichen Anforderungen wie für jedes andere Online-Portal auch, d.h. die Kreditkartendaten müssen ebenso PCI DSS konform verarbeitet und übermittelt werden.

Checkliste Online-Portale

Geprüft, ob der Bezahlvorgang auf dem Online-Portal an einen Bezahldienstleister ausgelagert werden kann.

- Wenn ja: einen zertifizierte Dienstleister ausgewählt ☐
- Wenn nein: Statusanalyse über einen autorisierten PCI Auditor (QSA) durchgeführt ☐

5. PCI DSS in der Praxis für Reiseveranstalter

Reiseveranstalter können an vielfältigen Stellen in Kontakt mit Kreditkartendaten von Endverbrauchern kommen. Sei es als Betreiber von Reisebüros oder auch bei der Akzeptanz von Kreditkartenzahlung über externe Online-Portale. Außerdem betreiben Reiseveranstalter fast immer eigene Online-Plattformen zur Reisebuchung. In der Regel wird ein Reiseveranstalter **als Händler zertifiziert** und muss damit einen Selbstauskunftsfragebogen ausfüllen.

Für die vom Reiseveranstalter betriebenen Online-Portale gelten die im Kapitel „PCI DSS in der Praxis für Online-Portale“ beschriebenen Empfehlungen.

Auch für Reiseveranstalter ist es aus PCI DSS Sicht sehr wichtig, alle relevanten Service Provider zu identifizieren und deren PCI DSS Status zu ermitteln. Eine Erläuterung zum Umgang mit Service Providern finden Sie in Kapitel 2.3.

Ähnlich wie bei den Online-Portalen gilt: lassen Sie sich von einem autorisierten PCI Auditor (QSA) beraten. Um eine verlässliche Aussage zu erhalten, welche Schritte in Ihrer individuellen Situation notwendig sind, sollten Sie eine Statusanalyse machen lassen.

Wie finde ich einen autorisierten PCI Auditor (QSA)?

Unter diesem Link finden Sie eine Liste der akkreditierten Prüfer.

https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

Checkliste PCI DSS für Reiseveranstalter

- Cardholder Data Matrix erstellt, um die kreditkartenrelevanten Prozesse und Systeme zu identifizieren ☐
- Online-Portale: geprüft, ob der Bezahlvorgang auf dem Online-Portal an einen Bezahldienstleister ausgelagert werden kann (falls ja, reduziert sich der Aufwand für die PCI DSS Zertifizierung dramatisch) ☐
- Alle im Bezahlprozess eingesetzten Dienstleister identifiziert ☐
- Beratung bei einem autorisierten PCI Auditor (QSA), Status-Analyse der Bezahlprozesse mit Blick auf PCI DSS ☐

6. Kontakt und Feedback

Zunächst einmal hoffen wir, dass dieser Guide die meisten Ihrer Fragen beantworten konnte und Ihnen dabei hilft, das Thema Kreditkartensicherheit effizient umzusetzen. Wenn Sie noch weitere Fragen zu PCI DSS und zur Sicherheit Ihres Unternehmens haben, dann erreichen Sie uns hier:

usd PCI DSS Competence Center
Telefon: +49 6103 9034-90
E-Mail: pci@usd.de

usd PCI DSS Plattform
https://pci.usd.de

Über uns
www.usd.de
Wir schützen Unternehmen und ihre Kunden vor Hackern und Kriminellen. Wir prüfen IT-Systeme, Applikationen und Prozesse auf sicherheitsrelevante Schwachstellen. Als akkreditierter Auditor beraten und zertifizieren wir europaweit nach dem internationalen Sicherheitsstandard der Kreditkartenindustrie (PCI DSS). Mehr als 1.600 Webshops, Portale und Unternehmen haben bereits ihr PCI DSS Siegel von uns erhalten.

DRV Deutscher ReiseVerband e.V.
Schicklerstraße 5-7
10179 Berlin
Telefon: +49 30 28406-0
Fax: +49 30 28406-30
E-Mail: info@drv.de
www.drv.de