Whitepaper
PCI DSS

Wie können Sie sicher und verantwortungsvoll mit den Zahlungskartendaten Ihrer Kunden umgehen?

Worldline

Inhalt

Einführung

Vertrauen gewinnen

Sie wollen Ihren Kunden die Möglichkeit geben, mit Kreditkarten oder internationalen Debitkarten zu bezahlen, weil Ihre Kunden eher geneigt sind, Geld auszugeben, wenn sie das leicht und sicher tun können. Mit anderen Worten helfen Ihnen Kredit- und Debitkarten dabei, Ihren Umsatz zu erhöhen. Allerdings tragen Sie dadurch aber auch eine höhere Verantwortung, weil die Kunden davon ausgehen, dass ihre Kartendaten bei Ihnen in sicheren Händen sind.

Da Sie Zahlungen von Karteninhabern erhalten, sind Sie in gewisser Hinsicht für die Sicherheit der damit verbundenen Informationen verantwortlich.

Um Ihnen die Arbeit zu erleichtern, haben die großen Zahlungskartenanbieter – wie beispielsweise Visa und MasterCard – einen Sicherheitsstandard entwickelt, der sich „Payment Card Industry Data Security Standard" (PCI DSS) nennt. Demzufolge darf Ihr Unternehmen nur dann Kartenzahlungen entgegennehmen, wenn Sie die Anforderungen erfüllen, die der PCI DSS an Sie stellt.

Auch Ihre Anbieter (wie beispielsweise „Payment Service Providers" (PSPs) und Zahlungsterminalanbieter) müssen diese Anforderungen erfüllen. So arbeiten wir zusammen, um Ihnen zu helfen, Ihre Zahlungstransaktionen sicherer zu machen. Auch wenn Sie natürlich trotzdem noch einige Pflichten in Verbindung mit dem PCI DSS haben, besteht der Vorteil – der letztlich viel größer ist – darin, dass Ihre Kunden Ihrer Firma vertrauen und ohne Bedenken Waren von Ihnen kaufen. Außerdem schützen Sie Ihre Unternehmen vor den Gebühren und Geldbußen, die entstehen könnten, wenn Karteninformationen gestohlen und missbraucht werden.

In dieser Informationsbroschüre von PaySquare finden Sie alle wichtigen Informationen über den PCI DSS und seine Hintergründe. Sie werden erfahren, wie Sie das Vertrauen Ihrer Kunden in Sie noch erhöhen können, und was Sie tun müssen, um die Anforderungen des Standards zu erfüllen. Außerdem werden Sie Informationen darüber erhalten, wofür Sie als Unternehmen haften, und wofür nicht.

Definition

Was ist der „PCI DSS“?

Um eine transparente Rahmenstruktur zum Schutz von Zahlungskarteninformationen implementieren zu können, haben die großen Zahlungskartenanbieter eine Reihe von Richtlinien für alle Unternehmen entwickelt, die an Zahlungstransaktionen mit Zahlungskarten beteiligt sind. Diese Richtlinien wurden zum „Payment Card Industry Data Security Standard“ (PCI DSS) zusammengefasst.

Primary Account Numbers

Der PCI DSS gilt nur in Fällen, in denen „Primary Account Numbers“ (PANs), d. h. vollständige Zahlungskartennummern, gespeichert, verarbeitet, übermittelt oder entgegengenommen werden. Andere Karteninformationen (wie etwa der Name des Karteninhabers und das Ablaufdatum der Karte) müssen Sie dagegen nur dann schützen, wenn Sie sie gemeinsam mit den dazugehörigen Kartennummern aufbewahren. Authentifizierungsdaten wie etwa die Kartenprüfziffer CVC (Card Validation Code) oder CVV (Card Verification Value), die Sie auf der Rückseite jeder Kreditkarte finden, sowie die PIN dürfen jedoch unter keinen Umständen gespeichert werden.

Grundsätzlich gilt, dass Sie so wenige Kartendaten wie möglich aufbewahren sollten. Welche Daten das sind, und welche Daten Sie nicht speichern sollten, sehen Sie in der unten stehenden Abbildung, die zwar eine MasterCard zeigt, aber für alle Zahlungskarten gilt.

Welche Kartendaten müssen geschützt werden?

Sensible Authentifizierungsdaten: Folgende Informationen dürfen unter keinen Umständen gespeichert werden:

- Karten-Tracking-Informationen (= umfassende Kartendaten, die beispielsweise im Magnetstreifen 1 und/oder im Chip 2 niedergelegt worden sind)
- Die dreistellige Prüfziffer [CVC2, CVV2] auf dem Unterschriftsstreifen auf der Rückseite der Karte 3)
- Die PIN

Folgende Karteninformationen dürfen (wenn sie den PCI-DSS-Anforderungen genügen) gespeichert werden, sofern das aus geschäftlichen Zwecken notwendig ist:

- PAN (Primary Account Number = die vollständige Kartennummer 4)
- Der Name des Karteninhabers 5
- Das Ablaufdatum der Karte 6

Folgende Informationen dürfen in unverschlüsselter Form gespeichert werden, wenn sie nicht mit anderen Informationen über den Karteninhaber verbunden sind:

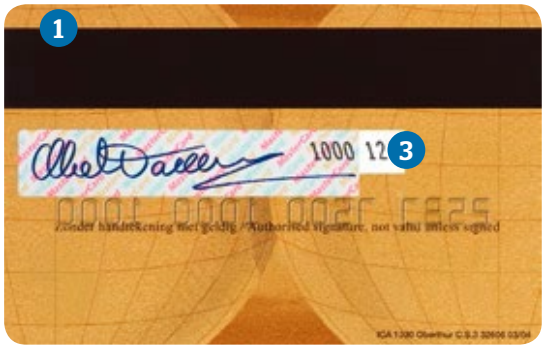
- Der Transaktionsbetrag, das Transaktionsdatum und der Transaktionsautorisierungscode

Grundlegender Standard

PCI DSS ist zum grundlegenden Standard zum Schutz von Karteninhaberinformationen geworden. Er soll Unternehmen dabei helfen, eine wirksame Sicherheitsrichtlinie zu entwickeln und einzuführen. Deshalb müssen Sie, um Zahlungskarten annehmen zu können, die Anforderungen des PCI DSS erfüllen. Wenn Sie das tun, schützen Sie Ihre Kunden und stärken die Fundamente Ihres Unternehmens.

Haftpflichten

Wenn Sie die Karteninformationen Ihrer Kunden nicht ordentlich schützen, machen Sie es Betrügern leichter, sie zu entwenden, zu missbrauchen und eventuell erheblichen Schaden anzurichten. Sie haften für alle direkten Verluste, die sich aus der Verwendung von gefälschten Zahlungskarten und/oder gestohlenen Karteninformationen ergeben könnten. Darüber hinaus haften Sie für alle Rechtskosten sowie alle Kosten, die mit der Ersetzung von Zahlungskarten, mit der Untersuchung von Straftaten und mit Rufschäden verbunden sind. Außerdem kann Ihnen das kartenausgebende Unternehmen eine Geldbuße auferlegen und Sie vom Zahlungskartenverkehr ausschließen. Schon allein aus Gründen der Haftpflicht ist es also ratsam, die Richtlinien des PCI DSS zu befolgen.



Wozu dient der PCI DSS?

Bei der Implementierung des PCI DSS haben die Zahlungskartenanbieter nicht einfach nur einige Vorschriften entwickelt – im Gegenteil. Der Sicherheitsstandard basiert auf einer ganzen Reihe klar formulierter Ziele für Ihr Unternehmen. Wenn diese Ziele erreicht werden, können Ihre Kunden internationale Zahlungskarten in Ihrer Verkaufsstelle oder in Ihrem Online-Shop verwenden, um leicht, effizient und sicher zu bezahlen.

Die Ziele des PCI DSS sind:

1. Ein Zahlungsnetz zu schaffen, das sicher ist – und bleibt;
2. Die Informationen des Karteninhabers (Ihres Kunden) zu schützen;
3. Ein Programm zu entwickeln, aufrecht zu erhalten und zu aktualisieren, dass Sie in die Lage versetzt, Schwachstellen im Zahlungssystem zu beseitigen;
4. Den Zugang zu den Kartendaten Ihrer Kunden auf das Nötigste zu beschränken;
5. Eine tragfähige und verlässliche IT-Infrastruktur aufzubauen, aufrecht zu erhalten und zu aktualisieren, und
6. Eine zweckmäßige und effiziente Informationssicherheitspolitik zu verfolgen.

Wie erreichen Sie die Ziele des PCI DSS?

Jede Anforderung des PCI DSS ist mit einer Reihe von praktischen Maßnahmen verbunden, mit deren Hilfe die Ziele erreicht werden können. Welche Maßnahmen Sie ergreifen müssen, hängt davon ab, welche Methode zur Annahme von Zahlungen Sie verwenden. Gegebenenfalls können Sie auch Ihre Anbieter (wie etwa Ihren PSP, den Zahlungsterminalanbieter, den Softwarelieferanten etc.) darum bitten, die notwendigen Maßnahmen zu ergreifen.

Die Anforderungen des PCI DSS:

Ein sicheres Zahlungsnetz gewährleisten

1. Maßnahme: Sie installieren eine Firewall und sorgen für ihre lückenlose Funktionstüchtigkeit.

2. Maßnahme: Sie verwenden nicht die Standard-Passwörter, die Ihnen Ihr Systemanbieter gegeben hat.

Die Karteninformationen der Kunden schützen

1. Maßnahme: Speichern Sie Kartendaten nur, wenn es unbedingt notwendig ist. Wenn Sie Daten aus geschäftlichen Zwecken speichern müssen, müssen Sie dafür sorgen, dass die Daten gut geschützt sind.

2. Maßnahme: Wenn Sie öffentliche Netzwerke verwenden, um Kartendaten Ihrer Kunden zu übermitteln, müssen Sie für eine ausreichende Verschlüsselung sorgen.

Schwächen erkennen und beseitigen

1. Maßnahme: Verwenden Sie Antiviren-Software, und nehmen Sie regelmäßig Aktualisierungen vor.

2. Maßnahme: Schützen Sie Ihre Systeme und Anwendungen, und aktualisieren Sie regelmäßig das Sicherheitssystem.

Den Zugang beschränken

1. Maßnahme: Gewähren Sie nur den Angestellten Zugang zu Karteninformationen, die sie wirklich kennen müssen.

2. Maßnahme: Geben Sie jedem Angestellten, der Zugang zu Kartendaten hat, einen eigenen Benutzernamen und ein persönliches Passwort.

3. Maßnahme: Beschränken Sie den physischen Zugang zu Kartendaten.

Ihre IT-Infrastruktur überwachen

1. Maßnahme: Kontrollieren Sie den Zugang zu allen wichtigen IT-Komponenten und Karteninhaberdaten, und vergewissern Sie sich regelmäßig, dass sie richtig überwacht werden.

2. Maßnahme: Testen Sie regelmäßig alle Sicherheitsfunktionen und -verfahren.

Informationssicherheit

1. Maßnahme: Entwickeln Sie eine Richtlinie auf der Basis der Informationssicherheit, und kontrollieren Sie regelmäßig, ob diese Richtlinie im Alltag auch wirklich befolgt wird.

Vier Kategorien

In welcher Branche sind Sie tätig?

Bei der Entwicklung der Anforderungen des PCI DSS wurde berücksichtigt, dass sich die Unternehmen in vielerlei Hinsicht unterscheiden. Um dieser Tatsache Rechnung zu tragen, wurden für den Standard vier Unternehmenskategorien entwickelt. Welcher Kategorie Ihr Unternehmen zuzuordnen ist, hängt davon ab, wie viele Kartenzahlungen Sie entgegennehmen, und mit welcher Methode Sie das tun. Wenn Sie die für Ihre Kategorie geltenden Anforderungen erfüllen, dürfen Sie sich als „PCI-DSS-konform" bezeichnen.

Kategorie	Merkmale	Notwendige PCI-DSS-Maßnahmen
Level 1 Verkaufsstellen und Fernkaufoptionen (E-Commerce, MO/TO, d. h. Bestellung per Post oder Telefon)	Alle Unternehmen, die Zahlungskarten akzeptieren und schon mehr als 6 Millionen Visa-Transaktionen abgewickelt haben, oder Alle Unternehmen, die Zahlungskarten akzeptieren und (zusammengenommen) schon mehr als 6 Millionen MasterCard- und Maestro-Transaktionen abgewickelt haben, oder Alle Unternehmen, die Zahlungskarten akzeptieren, die schon von einer Verletzung oder Beeinträchtigung des Datenschutzes betroffen waren	Jährliche PCI-DSS-Konformitätsprüfung vor Ort seitens des PCI SSC (Security Standards Council), befugter Firmenangestellter oder eines externen „Qualified Security Assessor" (QSA), der vom PCI SSC zugelassen wurde, und Vierteljährliche Netzwerk-Scans seitens eines „Approved Scanning Vendor" (ASV)
Level 2 Verkaufsstellen und Fernkaufoptionen (E-Commerce, MO/TO)	Alle Unternehmen, die Zahlungskarten akzeptieren und schon mehr als 1 Million, aber weniger als 6 Millionen Visa-Transaktionen abgewickelt haben, oder Alle Unternehmen, die Zahlungskarten akzeptieren und schon (zusammengenommen) mehr als 1 Million, aber weniger als 6 Millionen MasterCard- und Maestro-Transaktionen abgewickelt haben	Jährliche Selbsteinschätzung seitens des PCI SSC (Security Standards Council), befugter Firmenangestellter oder eines externen „Qualified Security Assessor" (QSA), der vom PCI SSC zugelassen wurde, und Vierteljährliche Network-Scans seitens eines ASV
Level 3 (nur E-Commerce)	Alle Unternehmen, die Zahlungskarten akzeptieren und schon mehr als 20.000, aber weniger als 1 Million Visa-E-Commerce-Transaktionen abgewickelt haben, oder Alle Unternehmen, die Zahlungskarten akzeptieren und (zusammengenommen) schon mehr als 20.000, aber weniger als 1 Million MasterCard- und Maestro-Transaktionen abgewickelt haben	Jährliches Ausfüllen eines Selbsteinschätzungsbogens („Annual Self Assessment Questionnaire", kurz SAQ), und Vierteljährliche Netzwerk-Scans seitens eines ASV
Level 4	Alle anderen Unternehmen, die Zahlungskarten akzeptieren	(Die Sicherheitspolitik kann sich von Erwerber zu Erwerber unterscheiden.) Jährliches Ausfüllen eines Selbsteinschätzungsbogens („Annual Self Assessment Questionnaire", kurz SAQ), und Vierteljährliche Netzwerk-Scans seitens eines ASV

Wie erfüllen Sie die Anforderungen des PCI DSS?

Wenn Sie anfangen, den PCI DSS zu verwenden, sollten Sie sich zuerst einmal von Ihrem gesunden Menschenverstand leiten lassen. Bevor Sie die Vorschriften lesen, sollten Sie sich darüber Gedanken machen, welchen Zwecken der Sicherheitsstandard dient. Ihre Antworten auf diese Frage sind oft schon ein solides Fundament für Ihr PCI-DSS-Projekt.

Fangen Sie am besten mit dem Selbsteinschätzungsbogen (SAQ) an.

Der Selbsteinschätzungsbogen („Self Assessment Questionnaire", kurz SAQ) ist hervorragend dazu geeignet, mit einem PCI-DSS-Verfahren zu beginnen. Es gibt 5 verschiedene Fragebögen. Welchen Fragebogen Sie verwenden sollten, hängt davon ab, mit welcher Methode Sie Kartenzahlungen akzeptieren. Nachdem Sie sich die Fragen durchgelesen haben, werden Sie eine klare Vorstellung davon gewonnen haben, wie Sie auf dem Weg zu einer sicheren Abwicklung von Kartenzahlungstransaktionen vorgehen sollten. Wenn Sie die Anforderungen bereits erfüllen, müssen Sie den SAQ vollständig ausfüllen und Ihrem Erwerber übergeben.

Wenn Sie gleich mit PCI DSS anfangen möchten und PaySquare-Kunde sind, können Sie sich direkt an die Kundenserviceabteilung wenden, um ein Passwort zu bekommen, mit dem Sie auf die PCI-DSS-Seite von PaySquare zugreifen können.

Die meisten Unternehmen erfüllen nicht schon von Anfang an alle Anforderungen des PCI DSS. Wenn das auch für Sie gilt, können Sie damit anfangen, die notwendigen Maßnahmen in Ihrem Unternehmen zu ergreifen oder einen externen Anbieter mit den Aufgaben Ihres PCI-DSS-Projekts zu betrauen. Auf der Webseite des PCI Security Standards Council finden Sie ein Verzeichnis aller Unternehmen und Zahlungssoftwaretools, die vom SCC zur Unterstützung Ihrer PCI-DSS-Projekte zugelassen worden sind.

Praktische Tipps für einen erfolgreichen Ablauf des PCI-DSS-Projekts

Warten Sie nicht länger – fangen Sie noch heute damit an!

Je eher Sie anfangen, desto weiter werden Sie Ihren Konkurrenten später voraus sein, und desto mehr Kosten werden Sie sich sparen.

Speichern Sie Daten nur, wenn es wirklich notwendig ist.

PCI DSS ist zwar der Sicherheitsstandard für die Speicherung, Verarbeitung und Übertragung von Zahlungskartendaten, aber manchmal ist die Speicherung von Kartendaten gar nicht notwendig. Wir empfehlen Ihnen deshalb, eine Liste von Daten anzufertigen, die Sie speichern wollen und/ oder müssen, und herauszufinden, ob das auch ohne Ihr Wissen geschehen könnte. Dabei sollten Sie folgende Faustegel beachten: „Was wir nicht brauchen, sollten wir nicht speichern."

Formulieren Sie klare Richtlinien.

Eine klare Richtlinie für den Umgang mit Zahlungskarteninformationen gibt Ihnen eine solide Arbeitsgrundlage. Berücksichtigen Sie dabei alle Aufgabenfelder: die Speicherung, die Verarbeitung und die Übertragung von Karteninformationen.

Vergleichen Sie die Vorschriften.

Schon bei der Speicherung von Karteninformationen müssen Sie unter Umständen bestimmte gesetzliche Anforderungen erfüllen, die Ihnen das niederländische Datenschutzgesetz [Wet Bescherming Persoonsgegevens] auferlegt. Sie können jedoch schon sehr früh feststellen, ob diese Vorschriften den Anforderungen des PCI DSS entsprechen.

Nehmen Sie eine Abweichungsanalyse (Gap Analysis) vor.

Für Ihr PCI-DSS-Projekt benötigen Sie spezielle Kenntnisse. Das heißt, dass Sie prüfen müssen, ob Sie in Ihrem Unternehmen über das Wissen verfügen, das Sie brauchen, um jede einzelne Vorschrift zu erfüllen. Wenn das nicht der Fall ist, empfehlen wir Ihnen, die Dienste externer Experten auf diesem Gebiet in Anspruch zu nehmen.

Sprechen Sie mit Ihren Anbietern, und vereinbaren Sie schriftlich die Bedingungen.

Wenn Sie die Anforderungen des PCI DSS erfüllen wollen, müssen auch die Anbieter von Hard- und Software, die in Ihrem Auftrag Kartendaten verarbeiten oder übertragen, die Vorschriften des PCI DSS erfüllen. Da Sie nicht davon ausgehen können, dass Ihre Anbieter ebenfalls PCI-DSS-konform sind, sollten Sie die Bedingungen dafür schriftlich fixieren.

Sie sollten Beweise für die PCI-DSS-Konformität verlangen und die getroffenen Vereinbarungen vertraglich verankern. Auf der Webseite des PCI Security Standards Council (PCI SSC) können Sie ebenfalls prüfen, ob Ihre Anbieter und/oder die Hard- und Software, die auf ihren Systemen installiert ist, vom SSC zugelassen worden sind.

Nehmen Sie Kontakt mit Ihren Lieferanten auf.

Sie sollten unter keinen Umständen Tracking-Daten aufheben (d. h. die vollständigen Kartendaten, die auf dem Magnetstreifen oder dem Chip einer Zahlungskarte enthalten sind), da diese Daten relativ leicht dazu verwendet werden können, widerrechtlich Kopien der Karte anzufertigen. Außerdem sollten Sie niemals Autorisierungs- und Authentifizierungsdaten speichern, da einige Hardwareprodukte diese Daten sogar dann speichern, wenn es nicht beabsichtigt ist. Wir empfehlen Ihnen, sich bei Ihrem/Ihren Hard- und Softwarelieferanten zu erkundigen, ob das bei Ihrem Zahlungsterminalsystem oder Ihrer Zahlungsinfrastruktur der Fall ist.

Suchen Sie alle relevanten Daten.

Suchen Sie alle Daten, die für PCI DSS relevant sein könnten. Finden Sie alle Zahlungskanäle und Datenströme, und fertigen Sie eine Liste aller Orte an, an denen Karteninformationen eventuell landen könnten.

Verschlüsseln Sie alle Kartendaten.

Vergessen Sie nie, alle Kartendaten zu verschlüsseln, die Sie weiterleiten.

Nutzen Sie nur geschützte Wi-Fi-Netze.

Nicht geschützte drahtlose Netze sind nicht für die Übertragung von Karteninformationen geeignet.

Schulen Sie Ihre Angestellten.

Auch wenn nicht all Ihre Angestellten PCI Qualified Security Assessors (QSA) ein müssen, müssen sie wissen, was dazu gehört, die Anforderungen des PCI DSS zu erfüllen.

Überprüfen Sie Ihre POS-Systeme.

Point-of-Sales-Systeme (wie z. B. die Verbindung zwischen Ihrer Kasse, einem Zahlungsterminal und Ihrer Verwaltungssoftware) können im Hinblick auf Ihre Kartendaten Sicherheitslücken aufweisen. Vergewissern Sie sich deshalb bitte, dass Ihr POS-System keine vollständigen Kartendaten speichert, vor allem nicht den Card Verification Value/Code. Außerdem darf nie die ganze 16-stellige Kreditkartennummer auf Verkaufsquittungen angegeben werden.

Gewährleisten Sie die physische Sicherheit Ihrer Systeme.

Sorgen Sie dafür, dass nur Ihre eigenen befugten Angestellten Zugang zu Ihren Zahlungssystemen haben.

Dokumentieren Sie das Verfahren.

Führen Sie Buch über die Maßnahmen, die Sie ergreifen, um die PCI-DSS-Vorschriften zu erfüllen.

Praxis (2)

Wie können Sie die Anforderungen des PCI DSS dauerhaft erfüllen?

Wenn Ihre Zahlungstransaktionen den Anforderungen genügen, können Sie sich sicher sein, dass alle Transaktionen für Sie und Ihre Kunden sicher und verantwortungsvoll abgewickelt werden. Dann besteht der nächste Schritt darin, zu gewährleisten, dass die Methode, die Sie im Hinblick auf Ihre Zahlungskartendaten verwenden, auch in Zukunft noch die Standardanforderungen erfüllen wird.

Praktische Tipps für die Aufrechterhaltung Ihrer PCI-DSS-Konformität

Erinnern Sie Ihre Angestellten immer wieder daran.

Sprechen Sie regelmäßig mit Ihren Mitarbeitern über das Thema PCI DSS. Formulieren Sie einige eindeutige und zielführende Richtlinien, die sie befolgen können.

Beschränken Sie den Zugang.

Beschränken Sie weiterhin den Zugang zu Ihren Kartendaten. Nur Angestellte, die wirklich einen Zugang zu ihnen haben müssen, um ihre Aufgaben erledigen zu können, sollten einen Benutzernamen und ein Passwort bekommen.

Löschen Sie regelmäßig überflüssige Daten.

Prüfen Sie regelmäßig, welche Kundendaten Sie nicht mehr brauchen, und löschen Sie diese Daten sofort.

Bereiten Sie sich auf den schlimmsten Fall vor.

Sorgen Sie dafür, dass Ihre Kundenkartendaten keinen Schaden erleiden, und seien Sie darauf vorbereitet, dass das doch einmal geschieht. Überlegen Sie sich, was Sie und Ihre Angestellten tun müssen, wenn ein solcher Fall eintritt, und entwickeln Sie Krisenszenarien.

Nehmen Sie regelmäßig Kontrollen vor.

Kontrollieren Sie regelmäßig die Systemsicherheit und die Prüfprotokolle.

Wo fängt Ihre Verantwortung an, und wo hört sie auf?

Die Verwendung von Zahlungskarten ist leicht, sicher und effizient. Ihre Kunden verlassen sich darauf, dass Sie geschützte technische Systeme und Anlagen einsetzen und mit zuverlässigen Partnern und Anbietern zusammenarbeiten, um Ihre Zahlungstransaktionen abzuwickeln.

Die Kartenanbieter nutzen den PCI DSS, um Sie dabei zu unterstützen, die Kartendaten Ihrer Kunden so gut wie möglich zu schützen. Ihre Verantwortung für die Sicherheit dieser Daten bezieht sich auf folgende Aspekte von Zahlungstransaktionen:

- Die Hardware, die Sie verwenden, um Kreditkarten und andere Zahlungskarten, die Ihre Kunden verwenden, zu scannen;
- Die Zahlungsterminals, die Sie in Ihrer/ Ihren Verkaufsstätte(n) (oder Ihren POS-Systemen) verwenden;
- Die Netzwerke und Hardware, die bei Ihren Zahlungstransaktionen verwendet werden (z. B. Server, drahtlose Router, Modems usw.);
- Die Speicherung, Verarbeitung und Übertragung von Zahlungskarteninformationen;
- Der Schutz der Hardware und der Software aller Parteien, die Sie an Ihren Zahlungstransaktionen beteiligen, und
- Der physische Zugang zu wichtigen IT-Komponenten und Karteninhaberdaten.

Ihre Lieferanten haben ihre eigenen Sicherheitsstandards.

Natürlich sind Sie nicht das einzige Unternehmen, das für den Schutz von Zahlungstransaktionen verantwortlich ist. Andere daran beteiligte Unternehmen spielen ebenfalls eine Rolle und müssen PCI-DSS-konform sein. So brauchen Sie zum Beispiel einen Zahlungsterminal oder eine Online-Kasse und eine Zahlungssoftware. Nun wurden für die Hersteller und Anbieter von Zahlungsterminals sowie für die Anbieter von Zahlungssoftware aber unterschiedliche Sicherheitsstandards entwickelt. Laut den Anforderungen des PCI DSS müssen Sie stets einen Zahlungsterminal oder eine Anwendung verwenden, der oder die diese Standards erfüllt, und einen Softwarelieferanten wählen, der dies ebenfalls tut. Eine Liste von Anbietern zugelassener Zahlungsapplikationen und Lieferanten finden Sie unter pcisecuritystandards.org.

PCI DSS – Was kommt als nächstes?

Wenn Sie die Anforderungen des PCI DSS erfüllen, werden Sie einen wichtigen Beitrag zur Sicherheit der Daten leisten, die für Ihre Kunden so wichtig ist. Dass die Kartenprogramme einen Sicherheitsstandard haben, heißt aber nicht, dass es keine weiteren (gesetzlichen) Vorschriften geben muss. So müssen Sie zum Beispiel bei der Speicherung, Verarbeitung und Übertragung von Karteninformationen Ihrer Kunden auch das niederländische Datenschutzgesetz (Wet Bescherming Persoonsgegevens) befolgen. Sie sind zwar gesetzlich dazu verpflichtet, die Daten Ihrer Kunden zu verwalten, müssen sich aber zum Beispiel auch Beschränkungen des Einsatzes von Kundendaten zu geschäftlichen Zwecken auferlegen.

Welche Betrugsfälle könnten auftreten?

Betrug hat viele Gesichter, und jede Methode der Annahme von Zahlungskarten hat ihre eigenen Risiken und Maßnahmen zu deren Verringerung. Die PaySquare-Informationsbroschüre zum Thema Betrug mit Hilfe von Kreditkarten und internationalen Zahlungskarten enthält auch Informationen dazu, wie man Betrugsfälle entdecken kann, und was man tun kann, um sie zu verhindern. Im Rahmen der PCI-DSS-Informationen stellen wir Ihnen im Anschluss verschiedene mögliche Betrugsfälle vor, die eintreten könnten.

Bei einem eigenständigen Zahlungsterminal in der Verkaufsstätte

Selbst wenn Ihre Kasse und Ihr Zahlungsterminal in der Verkaufsstätte nicht miteinander verbunden sind, besteht das Risiko, dass der Zahlungsterminal selbst oder die Datenverbindung manipuliert werden. Das würde Betrügern die Möglichkeit geben, die Karten- und/ oder Transaktionsdaten Ihrer Kunden abzufangen.

Wie können Sie das verhindern?

Überprüfen Sie regelmäßig (am besten jeden Morgen) Ihren Zahlungsterminal und die Kommunikationsverbindung auf Hinweise auf Manipulationen. Wenn Sie vermuten, dass Ihr Zahlungsterminal und/ oder Ihre Verbindungen und/ oder Kabel manipuliert wurden, wenden Sie sich bitte an Ihren Lieferanten, der Sie bei der Problemlösung unterstützen wird.

Bei einem Zahlungsterminal in der Verkaufsstätte, der mit der Kasse verbunden ist

Wenn Ihre Kasse und Ihr Zahlungsterminal miteinander verbunden sind, könnte(n) die Kommunikationsverbindung und/ oder die Zahlungssoftware gehackt werden. Dadurch könnten Betrüger Zugriff auf Karteninformationen erhalten, die in Ihrem System gespeichert sind, und Schadsoftware bei Ihnen installieren.

Wie können Sie das verhindern?

Implementieren Sie ein angemessenes Sicherheitssystem, und verwenden Sie zur Datenübertragung eine effektive Verschlüsselungsmethode.

Bei einem integrierten Zahlungsterminal in der Verkaufsstätte

Die Kommunikationsverbindungen können selbst dann gehackt werden, wenn Sie Zahlungsterminal und Kasse zusammen verwenden. Da diese Geräte hauptsächlich von Unternehmen mit mehreren Niederlassungen verwendet werden, könnten auch die Verbindungen zwischen den Niederlassungen und mit dem Hauptbüro gehackt werden.

Wie können Sie das verhindern?

Vereinbaren Sie eine Reihe von klaren Regeln mit Ihrem IT-Anbieter, und vergewissern Sie sich, ob die Produkte Ihres Lieferanten wirklich die Anforderungen des PCI SSC erfüllen.

Bei einem Online-Store, der die Zahlungsseite eines PSPs nutzt

Viele E-Commerce-Firmen nutzen die Zahlungsseite eines PSPs zur Abwicklung von Kartenzahlungen. Auch PSPs müssen zwar regelmäßig ihre Methoden daraufhin überprüfen, ob sie die Anforderungen des PCI DSS erfüllen, aber letztlich liegt es in Ihrer Verantwortung

sicherzustellen, dass Ihr PSP wirklich PCI-DSS-konform ist. Wenn die Zahlungsseite Ihres PSPs noch nicht richtig konfiguriert wurde und nach wie vor Kartendaten speichert, könnte das für Ihre Kunden unangenehme Folgen haben.

Wie können Sie das verhindern?

In Ihrem Vertrag mit Ihrem PSP müssen Sie angeben, dass die Zahlungsseite zu allen Zeiten den Anforderungen des PCI DSS entsprechen muss. Sie müssen umfassende Sicherheitssysteme wie beispielsweise Antiviren-Software und Firewalls implementieren; wenn Sie das nicht tun, wird Ihr Online-Store den Angriffen der Hacker ausgeliefert sein.

Bei einem Online-Store mit eigener Zahlungsseite

E-Commerce-Firmen mit eigenen Zahlungsseiten sind einem sehr hohen Risiko ausgesetzt.

Wie können Sie das verhindern?

Viele Erwerber nehmen keine E-Commerce-Firmen mit eigenen Zahlungsseiten an (d. h. Zahlungsseiten, die nicht von einem PSP stammen). Nutzen Sie deshalb am besten die Zahlungsseite eines PSPs, die die Anforderungen des PCI DSS erfüllt, um Betrugsfälle und Sicherheitsrisiken weitestgehend zu verhindern.

Kreditkartenannahme bei Fernkaufgeschäften (MO/TO)

Wenn Sie Bestellungen telefonisch oder postalisch entgegennehmen (MO/TO), können Sie die Kreditkartendaten manuell über einen PSP empfangen, der von PaySquare gewählt wurde, aber nur unter bestimmten genau festgelegten Bedingungen. Sie setzen die Daten Ihrer Kunden einem Risiko aus, wenn Sie Kartendaten speichern oder mit Ihren Kunden per E-Mail (oder über eine Webseite) kommunizieren.

Wie können Sie das verhindern?

Speichern Sie nicht die Kreditkartendaten Ihrer Kunden, und verschlüsseln Sie ordnungsgemäß die gesendeten Daten, wenn Sie sich mit Ihren Kunden über ihre Bestellungen austauschen.

Erläuterung

Irrtümer im Hinblick auf PCI DSS

Es gibt eine Reihe von weit verbreiteten Irrtümern in Bezug auf die Sicherheit von Kartendaten und auf PCI DSS. Einige dieser Irrtümer möchten wir an dieser Stelle beseitigen.

1. Irrtum

PCI DSS ist eine Empfehlung und keine Anforderung.

Zahlungskartenanbieter dürfen entscheiden, wie Sie als Unternehmen die Kartendaten behandeln müssen. Das heißt, dass Sie die Anforderungen des PCI DSS erfüllen müssen, um Kartenzahlungen entgegennehmen zu können.

2. Irrtum

Ein Scan seitens eines ASV ist alles, was ich brauche, um PCI-DSS-konform zu sein.

Der Sicherheitsscan, der von einem Approved Scanning Vendor vorgenommen wird, ist nur EIN Bestandteil des PCI-DSS-Verfahrens; als Unternehmen müssen Sie aber in der Regel zusätzlich jährlich einen Selbsteinschätzungsfragebogen („Self Assessment Questionnaire") ausfüllen. Auf der Webseite pci.paysquare.nl erfahren Sie, welche Bedingungen PaySquare den Händlern auferlegt.

3. Irrtum

Ich nehme so wenige Kartenzahlungen entgegen, dass ich die Anforderungen des PCI DSS nicht erfüllen muss.

Selbst wenn Sie nur eine einzige Kartenzahlung entgegennehmen, muss Ihr Unternehmen die PCI-DSS-Vorschriften erfüllen.

4. Irrtum

Da ich die Kartendaten meiner Kunden nicht speichere, gelten die Vorschriften des PCI-DSS nicht für mich.

PCI DSS ist der Sicherheitsstandard für die Speicherung, Verarbeitung und Übertragung von Kartendaten; das heißt, dass Sie die Mehrzahl der Anforderungen des PCI DSS erfüllen müssen. Und sind Sie wirklich ganz sicher, keine Kartendaten zu speichern?

5. Irrtum

Kleine Firmen werden nie von Zahlungskartenanbietern mit einer Geldbuße belegt.

Wenn Kartendaten aus Ihrem Unternehmen entwendet werden, müssen Sie beweisen können, dass Sie zum Zeitpunkt des Diebstahls die Anforderungen des PCI DSS erfüllt haben. Wenn Ihnen das nicht gelingt, werden Sie unabhängig von der Größe Ihres Unternehmens für die entstandenen Verluste haftbar gemacht. Außerdem können Sie von der Annahme von Kartenzahlungen ausgeschlossen und sogar einer höheren Händler-Kategorie (siehe Tabelle auf Seite 8) mit strengeren Anforderungen und höheren Prüfungsgebühren zugeordnet werden.

6. Irrtum

Der PCI DSS gilt nur für E-Commerce.

Alle Unternehmen, die Katendaten speichern, verarbeiten und/ oder übertragen, müssen die Anforderungen des PCI DSS erfüllen. Das gilt auch für Verkaufsstellen (d. h. Ladengeschäfte) und Unternehmen, die Bestellungen postalisch oder telefonisch entgegennehmen (MO/TO).

7. Irrtum

Sobald der ausgefüllte Selbsteinschätzungsfragebogen („Self Assessment Questionnaire“) ausgefüllt und eingereicht worden ist, ist das PCI-DSS-Verfahren abgeschlossen.

Da sich die Informationen, die Sie im SAQ angeben, mit der Zeit ändern können, müssen Sie die Anforderungen des PCI DSS auch nach der Einreichung des Fragebogens weiterhin erfüllen. Wenn ein Problem mit den Zahlungskartendaten aufgetreten ist, müssen Sie beweisen können, dass Sie im betreffenden Zeitraum PCI-DSS-konform gewesen sind.

8. Irrtum

Der PCI DSS lässt einen großen Auslegungsspielraum.

Der PCI DSS ist die konkreteste Sammlung von Sicherheitsanforderungen, die die Branche bislang herausgegeben hat. Im Gegensatz zu anderen sicherheitsbezogenen Standards (wie z. B. SOX, ISO und ISO 27002) ist der PCI DSS mehr als eine Rahmenstruktur, denn er enthält auch eine detaillierte Beschreibung der damit verbundenen Anforderungen und Verfahren.

9. Irrtum

Es reicht, eine PA-DSS-zertifizierte Applikation zu haben, um die Anforderungen des PCI DSS zu erfüllen.

Die Verwendung einer PA-DSS-zertifizierten Applikation ist nur der erste Schritt. Danach müssen Sie alle Vorschriften befolgen und Kontrollsysteme implementieren, die gewährleisten, dass all Ihre Netzwerke und Server die Anforderungen des PCI DSS erfüllen. Wenn Sie andere Unternehmen mit Ihrer Systemadministration betraut haben, müssen deren Administratoren die Anforderungen erfüllen.

Terminologie

PCI-DSS-Glossar

Erwerber („Acquirer“)

Erwerber sind dafür verantwortlich, die Kartenzahlungen eines Unternehmens abzurechnen. Zu diesem Zweck schließen sie eine Lizenzvereinbarung mit einem internationalen Kartenanbieter ab.

Attestation of Compliance (AoC)

Dieses Dokument ist der Beleg dafür, dass Sie den SAQ richtig und wahrheitsgemäß ausgefüllt haben.

Approved Scanning Vendor (ASV)

ASVs führen Scans in Unternehmen durch, die Zahlungskarten akzeptieren, um deren IT-Systeme und -Netzwerke zu prüfen. ASVs müssen vom PCI Security Standards Council zertifiziert werden. Eine Liste zugelassener Unternehmen finden Sie auf der Webseite des PCI Security Council unter www.pcisecuritystandards.org. Die meisten IT-Systeme und Netzwerke müssen aller drei Monate gescannt werden, was in der Regel auch aus der Ferne geschehen kann. Dieses Verfahren ähnelt einem Virenscan auf Ihrem PC.

Zertifizierung

Im Rahmen des Zertifizierungsverfahrens prüft ein Zertifizierungsgremium, ob das Unternehmen zum Zeitpunkt der Zertifizierung bestimmte Vorschriften und Anforderungen erfüllt.

Compliance

Das ist die Erfüllung und/ oder Befolgung bestimmter Gesetze und/ oder Vorschriften.

Manipulation

Das sind die Manipulation, der Diebstahl und der Verlust von Daten und/oder Systemen oder deren Beeinflussung zum Zweck ihres Missbrauchs.

Payment Service Provider (PSP)

PSPs (Anbieter von Zahlungsdienstleistungen) haben die Aufgabe, die technische Verbindung eines Unternehmens mit dem Erwerber zu erleichtern und Kartentransaktionen durchzuführen. Darüber hinaus bieten PSPs andere Produkte und Dienstleistungen zur Abrechnung einer ganzen Reihe von elektronischen Zahlungen an.

PCI DSS

Das ist eine Sammlung von Vorschriften, die die großen Zahlungskartenanbieter (darunter auch Visa und MasterCard) herausgegeben haben, und die den Missbrauch von Zahlungskarten verhindern sollen. Alle an der Zahlungskartentransaktionskette beteiligten Parteien (wie etwa Firmen, Erwerber, PSPs und IT-Anbieter) müssen die PCI-Anforderungen erfüllen.

Qualified Security Assessor (QSA)

Das ist ein IT-Sicherheitsexperte, der vom PCI SCC dazu berechtigt wurde, Sicherheitsprüfungen („OnSite Assessments“) in Unternehmen durchzuführen, die Karten annehmen und Kartendaten verarbeiten.

„Safe-Harbour“-Lösung

Wenn ein Einzelhändler einem Datendiebstahl/ -betrug zum Opfer fällt, obwohl er PCI-DSS-konform ist, kann der Zahlungskartenaussteller unter Umständen die Geldstrafe verringern, die er andernfalls erhoben hätte, oder ganz auf sie verzichten.

Sicherheitsprüfung

Das ist eine physische Sicherheitsprüfung auf dem Betriebsgelände des Unternehmens, die eine Inspektion der Serverräume und die Befragung von Angestellten beinhaltet.

Sicherheits-Scan

Das ist eine Untersuchung zur Aufdeckung von Schwächen der IT-Infrastruktur oder Systemkonfiguration. Sicherheits-Scans werden in der Regel online vorgenommen.

Self Assessment Questionnaire (SAQ)

Selbsteinschätzungsfragebögen (SAQs) sind Fragebögen, mit deren Hilfe Unternehmen ihrem Erwerber Informationen über die Implementierung der PCI-DSS-Vorschriften in ihrer Firma zukommen lassen. Dabei hat jede Unternehmenskategorie ihren eigenen Fragebogen. Die Fragebögen enthalten Informationen über die vom Unternehmen verwendete Methode der Annahme und Verarbeitung von Kartenzahlungstransaktionen sowie über die Verarbeitung allgemeiner Geschäftsinformationen, Beziehungen (einschließlich Vertragsverhältnissen) zu anderen Unternehmen sowie technische Details. Wenn sie der entsprechenden Händlerkategorie angehören (siehe Seite 9 für Informationen zu den einzelnen Kategorien), müssen Unternehmen den SAQ einmal im Jahr ausfüllen und dem Erwerber übergeben.

Weitere Informationen finden Sie unter

www.paysquare.de

oder auf einer der unten stehenden Webseiten.

www.paysquare.eu
www.visa.com
www.mastercard.com
www.pcisecuritystandards.org

Kontaktinformationen

Haben Sie Fragen zu diesem Thema? Dann wenden Sie sich bitte an unsere Customer-Service.

Tel.: (069) 8 01 09 54 30
E-Mail: customer-service@de.paysquare.eu

Als professioneller Partner in Sachen Zahlungstransaktionen möchten wir Sie mit Hilfe unserer veröffentlichten Informationsbroschüren unabhängig und objektiv über Zahlungstransaktionen informieren. In diesen Broschüren stellen wir Ihnen Lösungen für eine Reihe von Problemen vor, die mit bestimmten Anforderungen des Marktes verbunden sind. All unsere Informationsbroschüren und weiteren Materialien stehen im Bereich „Kundenservice-Downloadcenter“ von www.paysquare.de zum Download bereit.

PaySquare SE
a Worldline Company
Hahnstraße 25
60528 Frankfurt am Main

Telefon: +49 (0) 69 80 10 95-0
Fax: +49 (0) 69 80 10 95-120
www.paysquare.de