PCI DSS

DIE HÄUFIGSTEN FRAGEN ZU PCI DSS

Schutz vor Kartenmissbrauch

Mit dem Payment Card Industry DataSecurity Standard (PCI DSS) schützen Sie die Kreditkarten-Daten Ihrer Kunden. Sie beugen Datenmissbrauch und Datendiebstahl vor.

Inhalt

I. Allgemeine Erklärungen

Was ist PCI DSS?

PCI DSS (Payment Card Industry Data Security Standard, (kurz PCI) ist der Sicherheitsstandard der Kreditkartenorganisationen mit strengen Vorgaben, die den sorgfältigen und geschützten Umgang mit Kreditkartendaten sicherstellen sollen. Der Standard wurde von den fünf wichtigsten Kreditkartenunternehmen (American Express, JCB, MasterCard, Discover Financial Services and Visa) ins Leben gerufen und umfasst Sicherheitsanforderungen, die folgende Ziele verfolgen:

1. Einrichtung und Betrieb eines geschützten Netzwerks
2. Schutz von aufbewahrten und übermittelten Karteninhaberdaten
3. Einrichtung und Betrieb eines Schwachstellen-Management-Systems
4. Umsetzung effektiver Richtlinien zur Zugriffskontrolle
5. Regelmäßige Überwachung und Überprüfung der IT-Infrastruktur
6. Formulierung und Durchsetzung einer Richtlinie zur Informationssicherheit

Welche Anforderungen stellt PCI DSS?

PCI DSS umfasst zwölf Sicherheitsanforderungen. Als PCI-konform gelten Organisationen, die folgende Vorgaben einhalten:

1. Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
2. Änderung der von Herstellern vorgegebenen Standardpasswörter und Sicherheitseinstellungen
3. Schutz gespeicherter Kreditkarteninhaberdaten
4. Verschlüsselte Übertragung der Daten von Kreditkarteninhabern in öffentlichen Netzwerken
5. Verwendung und regelmäßige Aktualisierung von Antivirensoftware
6. Entwicklung und Verwendung sicherer Systeme und Anwendungen
7. Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf
8. Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff
9. Einschränkung des physikalischen Zugriffs auf Karteninhaberdaten

10. Protokollierung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen und Daten von Kreditkarteninhabern
11. Regelmäßige Überprüfung von Sicherheitssystemen und –abläufen
12. Einrichtung einer Unternehmensrichtlinie mit Vorgaben zur Informationssicherheit für Mitarbeiter und Vertragspartner

Wer ist an die Einhaltung des PCI DSS gebunden?

Jedes Unternehmen, welches Kreditkartenzahlung akzeptiert, muss sich an die Sicherheitsvorgaben der Kreditkartenorganisationen und somit des PCI DSS halten. Dabei sind die Größe des Unternehmens und die Anzahl der Kreditkartentransaktionen pro Jahr unerheblich für die Nachweispflicht des Unternehmens.

Welche Konsequenzen drohen bei Nichteinhaltung des PCI DSS?

Ihr Unternehmen kann seitens der Kreditkartenorganisationen bzw. vom Acquirer (Händlerbank) mit Geldstrafen belegt werden. Des Weiteren ist Ihr Unternehmen haftungspflichtig, wenn Kreditkartendaten Ihrer Kunden gestohlen oder missbraucht werden.

Welche Vorteile hat die Umsetzung des PCI DSS?

Der PCI DSS mit seinen verbindlichen Regeln für mehr IT-Sicherheit soll der Betrugskriminalität einen Riegel vorschieben. Durch verstärkte Schutzmaßnahmen bei der Verarbeitung von Zahlungskartendaten gemäß PCI entstehen Ihnen vor allem folgende Vorteile:

- Erhöhte Datensicherheit und Schutz Ihrer Kunden
- Gesteigertes Kundenvertrauen und somit ggf. Steigerung des Kreditkarteneinsatzes und –umsatzes
- Größere Absicherung vor finanziellen Schäden und Schadenersatz aufgrund von Sicherheitsverletzungen
- Schutz des Unternehmensimage
- Bewertung des Sicherheitsschutzes von Systemen zur Speicherung, Verarbeitung und/oder Übermittlung von Karteninhaberdaten
- Datenminimierung und –vermeidung führen zur Reduzierung des Unternehmensrisikos
- Netzwerkstrukturierung reduziert die Kosten der Aufrechterhaltung der PCI Compliance

Was bedeutet „compliant"?

Unternehmen, die nachweislich den PCI DSS einhalten, erhalten eine Konformitätsbescheinigung. Diese Unternehmen haben erfolgreich dokumentiert, dass sie die Sicherheitsanforderungen der Kreditkartenorganisationen im Umgang mit Kreditkartendaten kennen und einhalten. Damit hat das Unternehmen den Status PCI DSS „compliant" erlangt und befindet sich im Schutz der so genannten „Safe-Harbour Rule". Somit kann im Falle eines Datendiebstahls- bzw. missbrauchs nach Analyse durch einen Forensiker das Unternehmen mit einer teilweisen oder vollständigen Befreiung von Geldstrafen seitens der Kreditkartenorganisationen bzw. des Acquirers rechnen.

Warum muss ich den Nachweis der Kreditkartensicherheit (PCI DSS) einhalten?

Ihr Unternehmen bietet Kreditkartenzahlung an und muss deshalb den PCI DSS nachweislich erfüllen. Daher hat Ihr Acquirer Sie kontaktiert, den Compliance Nachweis zu erbringen.

Wie oft muss ich den PCI DSS Nachweis erbringen?

Der PCI DSS Nachweis muss mindestens einmal im Jahr erbracht werden. Da durch den PCI DSS Nachweis der aktuelle Stand der Kreditkartenabwicklung in Ihrem Unternehmen dokumentiert wird, ist es notwendig, auf Änderungen der Kreditkartenakzeptanz bzw. Zahlungsabwicklungen auch außerhalb des vorgegebenen Turnus von einem Jahr durch die Aktualisierung Ihres PCI DSS Nachweises zu reagieren. Sie sind verpflichtet jederzeit die PCI DSS Konformität aufrecht zu erhalten.

Ich habe die Abwicklung von Kreditkartenzahlungen an einen externen Dienstleister vergeben. Warum müssen wir trotzdem den PCI DSS Nachweis erbringen?

Der PCI DSS Nachweis muss im Falle einer Auslagerung der Speicherung, Verarbeitung oder Übertragung von Kreditkartendaten an einen Drittdienstleister dennoch erbracht werden, um zu dokumentieren, dass der gewählte Dienstleister PCI compliant ist und dass sie regelmäßig den PCI Status des Dienstleisters überprüfen. Ihr Acquirer benötigt generell eine Selbstauskunft Ihres Unternehmens gemäß dem PCI DSS, indem die Art und Weise der Kreditkartenabwicklung

dokumentiert und die Konformität mit dem Datensicherheitsstandard der Kreditkartenorganisationen nachgewiesen wird.

Wie kann ich prüfen, ob mein Dienstleister PCI DSS compliant ist?

Die Kreditkartenorganisationen MasterCard und Visa haben, unter den folgenden Links, eine Liste mit PCI DSS konformen Dienstleistern im Internet veröffentlicht:
Visa
http://www.visaeurope.com/en/businesses__retailers/payment_security/downloads__resources.aspx

MasterCard
http://www.mastercard.com/us/company/en/whatwedo/compliant_providers.html

Oder Sie sprechen den Dienstleister direkt an und fragen diesen nach seinem PCI-Zertifikat.

Mein Dienstleister gibt mir die Auskunft, dass ich mich nicht nach dem PCI DSS zertifizieren muss.

Jedes Unternehmen, das Kreditkartenzahlung anbietet, ist verpflichtet den PCI DSS einzuhalten und diesen nachzuweisen. Haben Sie Kreditkartenzahlungen an einen PCI DSS konformen Dienstleister übergeben und speichern, verarbeiten oder übertragen Sie keine Kreditkartendaten auf Ihren eigenen IT-Systemen, steht Ihnen ein verkürzter Weg zum Nachweis der PCI-Compliance zur Verfügung.

Warum muss ich auch die Kreditkartenzahlungen über einen anderen Acquirer in meinem PCI DSS Nachweis berücksichtigen?

Der Nachweis der Kreditkartensicherheit wird für das eigene Unternehmen durchgeführt und gilt unabhängig davon, bei welchem Acquirer der Kreditkartenakzeptanzvertrag abgeschlossen wurde. Entsprechend handelt es sich bei der Konformitätsbescheinigung um ein Dokument, welches universell einsetzbar als Nachweis der Kreditkartensicherheit für das Unternehmen vorgelegt werden kann.

II. Registrierung

Ich habe das Passwort geändert und kann mich damit jetzt nicht mehr einloggen?

Bitte prüfen Sie Ihre Zugangsdaten: - Haben Sie Ihre als Benutzername hinterlegte E-Mail Adresse genutzt? - Haben Sie beim Passwort auf Groß- und Kleinschreibung geachtet? - Haben Sie darauf geachtet, dass kein Leerzeichen eingegeben wurde? Sind die genutzten Zugangsdaten korrekt und ein Login weiterhin nicht möglich, nutzen Sie bitte die Funktion „Neues Passwort anfordern".

Ich kann mich mit den von Ihnen geschickten Daten (Initialdaten) nicht einloggen?

Haben Sie sich bereits auf der PCI DSS Plattform registriert? In diesem Fall sind die Initialdaten nicht mehr gültig. Bitte nutzen Sie als Benutzername die hinterlegte E-Mail Adresse (an die Sie ebenfalls die Erinnerungsemails versendet bekommen) und das von Ihnen angelegte, persönliche Passwort. Sind die Zugangsdaten bisher noch nicht genutzt worden, ein Login jedoch mit den vorliegenden Daten nicht möglich, kontaktieren Sie bitte das PCI Competence Center.

Ich habe mein Passwort vergessen. Was kann ich tun?

Bitte fordern Sie sich über die PCI DSS Plattform ein neues Passwort an. Klicken Sie auf die Funktion „Neues Passwort anfordern". Dort geben Sie bitte die hinterlegte E-Mail Adresse ein. Das neue Passwort wird Ihnen per E-Mail zugeschickt.

Wie viele Ansprechpartner können auf der Plattform gelistet sein?

Im Rahmen des Registrierungsprozesses können Sie einen speziellen Ansprechpartner für PCI angeben. Sollte zu einem späteren Zeitpunkt ein oder mehrere Ansprechpartner notwendig sein, wenden Sie sich bitte an das PCI Competence Center.

III. Stammdaten:

Welche Standorte muss ich angeben?

Bitte geben Sie den oder die Orte an, an denen sich die Niederlassung Ihres Unternehmens befindet, für die die Nachweis über die Einhaltung des PCI DSS erbracht wird.

Was ist eine Zahlungssoftware?

Die Zahlungssoftware ist ein Programm, das auf Ihren eigenen IT Systemen installiert ist und die Kreditkartenzahlung Ihrer Kunden verarbeitet. Nicht zu verwechseln mit einer Payment-Page, ein Zahlungsmodul Ihres Zahlungsdienstleisters, in die der Kunde bei der Zahlung mit Kreditkarte seine Kartendaten eingibt. In diesem Fall kommen die Kreditkartendaten nicht mit Ihren eigenen IT Systemen in Berührung (keine Weiterleitung, Verarbeitung oder Speicherung).

Was ist ein Drittdienstanbieter?

Drittdienstanbieter sind zum Beispiel Anwendungsdienstleister (Payment Gateways), Webhosting-Unternehmen (Dienstleister, die Ihnen über deren Server, Netzanbindung und Internetbereitstellung und Betrieb anbieten.) sowie Internet Zahlungsdienstleister (Payment Service Provider).

Was ist ein Acquirer?

Der Acquirer, auch Händlerbank genannt, ist Ihr Partner zur Akzeptanz und Abrechnung von Kreditkarten und Debitkarten, mit dem Sie den Kreditkarten-Akzeptanzvertrag abgeschlossen haben.

Was ist ein Point of Sale (POS)?

Point of Sale ist ein Zahlungssystem, in dessen Rahmen der Kunde Vorort beim Händler mit seiner Kreditkarte bezahlt. Die Legitimation des Kunden erfolgt dabei durch Unterschrift. Der Point of Sale kann ein eigenständiges Terminal sein, welches über Telefonleitung mit einem Zahlungsdienstleister verbunden ist, oder es kann ein Zahlungssystem sein, welches mit der Ladenkasse und/oder dem Internet verbunden ist.

Was ist JCB, CUP und Discover?

JCB (Japan Credit Bureau) und CUP (China Union Pay) sind Kreditkarten, die im asiatischen Raum weit verbreitet sind. Die Discover Card ist eine amerikanische Kreditkarte.

Ich kenne meine jährlichen Transaktionszahlen mit Kreditkarten nicht. Was soll ich angeben?

Bitte schätzen Sie die Anzahl der Transaktionen, wenn Ihnen die genauen Zahlen nicht vorliegen.

IV. SAQ (Self-Assessment Questionnaire = Selbstbeurteilungsbogen)

Welcher SAQ ist der richtige für mich?

Bei der Wahl des für Ihr Unternehmen zutreffenden SAQs unterstützt Sie der SAQ-Auswahl-Assistent. Mit Hilfe von gezielten Fragen zur Akzeptanz und Abwicklung von Kreditkartendaten wird der für Ihr Unternehmen passende SAQ ermittelt. Sollten Sie den passenden SAQ-Typ bereits kennen, finden Sie im SAQ-Auswahl-Assistenten einen Link, der Sie direkt in die Übersicht der SAQs führt und Sie den passenden SAQ auswählen können. Im Zweifelsfall ist es aber immer zu empfehlen, den Weg über den SAQ-Auswahl-Assistent zu wählen, damit Sie auch wirklich den für Ihr Unternehmen aktuellen SAQ ermitteln.

Warum muss ich einen SAQ ausfüllen?

Mit dem Selbstbeurteilungsbogen (SAQ) wird die Einhaltung der Sicherheitsanforderungen des PCI DSS nachgewiesen.

Die Fragen des SAQ A treffen auf mich nicht zu, da ich alle Kreditkartenfunktionen extern vergeben habe. Wie soll ich antworten?

Auf Ihr Unternehmen nicht zutreffende Fragen können Sie mit „N/A" (nicht anwendbar) beantworten. Anschließend geben Sie eine Erklärung an, warum diese Frage auf ihr Unternehmen nicht anwendbar ist. Bei SAQ A liegt für Ihr Unternehmen der Schwerpunkt auf der PCI Compliance Ihres Zahlungsdienstleisters. Diese gilt es regelmäßig zu prüfen und im SAQ nachzuweisen.

Ich habe SAQ A ausgewählt bzw. über den SAQ Auswahl Assistent wurde SAQ A ermittelt. Warum habe ich keinen Zugriff auf die Fragen im SAQ?

Da die Auswahl des SAQ A immer die Verwendung eines Dienstleisters zur Verarbeitung, Speicherung oder Weiterleitung der Daten impliziert, prüfen Sie bitte in den Stammdaten („Administration", „Händlerdaten bearbeiten"), ob dort die Frage „Nehmen Sie Dienstleister in Anspruch, um Kreditkartendaten zu speichern, zu verarbeiten oder zu übertragen?" positiv beantwortet wurde.

Was bedeutet N/A?

N/A bedeutet „nicht anwendbar (englisch: not applicable") und kann als Antwort auf Fragen im SAQ genutzt werden, wenn die gestellte Frage nicht auf Ihr Unternehmen passt. Nutzen Sie diese Antwortmöglichkeit, werden Sie aufgefordert die Auswahl zu begründen.

Was bedeutet Compensating Controls?

Compensating Controls bedeutet „ausgleichende Maßnahmen". Wenn Sie die technische Spezifikation einer Anforderung nicht erfüllen können, Sie das damit verbundene Risiko aber auf andere Weise ausreichend gemindert haben, wählen Sie bitte "Compensating Control" (ausgleichende Maßnahme) als Antwort aus. In diesem Fall werden Sie nach Abschluss des SAQ aufgefordert, genauere Angaben zu den getroffenen Maßnahmen zu machen.

V. Durchführung von Schwachstellenscans

Wann bin ich verpflichtet Schwachstellenscans durchzuführen, um meinen PCI Nachweis zu erbringen?

Kommen Ihre eigenen IT-Systeme mit den Kreditkartendaten Ihrer Kunden in Berührung (Speicherung, Weiterleitung, Verarbeitung) und sind diese IT-Systeme oder angeschlossene IT-Systeme extern aus dem öffentlichen Internet erreichbar, sind Sie verpflichtet durch einen zertifizierten Anbieter (Approved Scanning Vendor (ASV)) alle 90 Tage mittels Schwachstellenscans die Sicherheit dieser IT-Systeme überprüfen zu lassen.

Obwohl ich SAQ C oder D mit dem Status PCI compliant ausgefüllt habe, teilt mir die Plattform immer noch mit, dass ich noch nicht im Status PCI compliant bin. Was muss ich denn noch tun?

Die Auswahl der SAQ C und D signalisieren eine Berührung Ihrer eigenen IT-Systeme mit den Kreditkartendaten Ihrer Kunden. Entsprechend muss geprüft werden, ob in dem Fall die Durchführung von Schwachstellenscans notwendig ist, um den PCI Nachweis mit dem Status PCI compliant abzuschließen. Bei dieser Prüfung steht Ihnen gerne das PCI Competence Center zur Verfügung.

Ich habe Schwachstellenscans bei einem ASV durchführen lassen. Warum werde ich immer noch informiert, dass wir den Status PCI compliant nicht erreicht haben?

Auch wenn Ihnen ein ASV mittels eines PCI compliant abgeschlossenen Schwachstellenscans mitteilt, dass Sie den Compliance-Status erreicht haben, muss diese Information noch in Ihrem Datensatz auf der PCI Plattform hinterlegt werden. Sollten Sie den Schwachstellenscan nicht beim Kooperationspartner usd AG durchgeführt haben, ist es notwendig, den Schwachstellenscan manuell auf die PCI Plattform in Ihrem Datensatz hochzuladen. Dafür melden Sie sich bitte auf der PCI Plattform an und laden Sie im Bereich „Ihre Scans" den Executive Summary Report bestehend aus den Dokumenten „Attestation of Scan Compliance" und „Executive Summary" hoch.

Kostenloses Siegel für den Webshop oder die Webseite

Wenn Sie den Selbstauskunftsbogen A, B oder C-VT mit dem Status PCI compliant abgeschlossen haben, können Sie ein kostenloses Compliant-Siegel in Ihrem Webshop implementieren. Dieses Siegel wird Ihnen von dem Kooperationspartner Ihres Acquirers, der usd AG, zur Verfügung gestellt. Bitte nutzen Sie die Verlinkung auf der PCI Plattform im Bereich „PCI DSS Schwachstellenscans" in Ihrem Datensatz, um die Registrierung bei der usd AG durchzuführen. Bei Fragen hierzu steht Ihnen das PCI Competence Center usd AG unter der Telefonnummer 06103/903490 (E-Mail: pci@usd.de) gerne zur Verfügung.