Weisungen über die Einhaltung der PCI DSS Sicherheitsvorschriften für Vertragspartner

Weltweit sind alle Vertragspartner, die Kartendaten übermitteln, verarbeiten oder speichern, verpflichtet, die im Payment Card Industry Data Security Standard (PCI DSS) definierten Sicherheitsrichtlinien einzuhalten. Wenn diese missachtet werden, kann PostFinance das Vertragsverhältnis mit sofortiger Wirkung beenden und Schadenersatz für allfällige Bussen und Forderungen geltend machen.

Die folgenden Weisungen sind – als technische und organisatorische Richtlinien – bindende Bestandteile des Akzeptanzvertrags betreffend die Zahlungsarten Combo mit PostFinance.

Was beinhaltet PCI DSS?
PCI DSS umfasst zwölf verbindliche Anforderungen, die den Schutz der Kartendaten während der Verarbeitung, Speicherung und Übermittlung sicherstellen sollen. Die Umsetzung von PCI DSS wird durch die Sicherheitsprogramme der Kartenorganisationen gesteuert. Dazu zählen AIS von Visa, SDP von Mastercard® sowie die entsprechenden Programme von American Express, Discover (Diners Club) und JCB.

Wieso wurde PCI DSS eingeführt?
Der Diebstahl von Kartendaten hat in den vergangenen Jahren kontinuierlich zugenommen. Durch den missbräuchlichen Einsatz der gestohlenen Kartendaten entstanden bei allen Beteiligten erhebliche Schäden.

Was bezweckt PCI DSS?
Die Kartenorganisationen wollen mit PCI DSS die Sicherheit von Kartenzahlungen weiter erhöhen und dadurch Händler, Karteninhaber sowie die gesamte Branche noch effektiver vor Kartendatendiebstahl und -missbrauch schützen.

Wer ist zur Einhaltung von PCI DSS verpflichtet?
PCI DSS verpflichtet weltweit alle Vertragspartner, die Kartendaten übermitteln, verarbeiten oder speichern, wirkungsvolle Sicherheitsmassnahmen zu ergreifen und einzuhalten.

Die Vertragspartner sind zudem dafür verantwortlich, dass beauftragte Drittunternehmen wie Payment Service Provider (PSP) oder Data Storage Entities (DSE), die in ihrem Namen Daten übermitteln, verarbeiten oder speichern, diese Sicherheitsrichtlinien ebenfalls einhalten.

Wer ist dafür verantwortlich, dass PCI DSS eingehalten wird?
Grundsätzlich liegt es in der Eigenverantwortung jedes Vertragspartners, die Sicherheitsvorschriften einzuhalten. Die Kartenorganisationen verlangen jedoch, dass die Vertragspartner die von ihnen getroffenen Sicherheitsmassnahmen deklarieren (zertifizieren lassen). Der Umfang einer Deklarierung (Zertifizierung) ist abhängig von der Anzahl Transaktionen und davon, ob der Vertragspartner mit Kartendaten bei der Übermittlung, Verarbeitung und Speicherung in Berührung kommt.

Welche Arten von Zertifizierungsmassnahmen gibt es?
Unter PCI DSS gibt es die folgenden drei Arten von Zertifizierungsmassnahmen (siehe auch Tabelle auf der nächsten Seite):

- **Self-Assessment Questionnaire (SAQ)**
  Ein Selbstbeurteilungsfragebogen muss ausgefüllt werden.
- **Network Scan**
  Ein akkreditiertes Zertifizierungsunternehmen (Approved Scanning Vendor) führt vierteljährlich und nach Absprache mit dem Vertragspartner freundliche Hacking-Angriffe durch, um mögliche Schwachstellen zu ermitteln.
- **On-Site Audit**
  Vertragspartner mit grossen Transaktionsvolumen oder Vertragspartner, die Opfer eines Kartendatendiebstahls wurden, sind verpflichtet, einen ROC (Report on Compliance) zu komplettieren. Die Ergebnisse müssen durch einen QSA (Qualified Security Assessor) oder durch einen ausgebildeten Auditor (ISA – Internal Security Assessor) überprüft und bestätigt werden.

Wenn ein Vertragspartner nicht alle Zertifizierungskriterien erfüllt, ist er verpflichtet, seine Sicherheitsvorkehrungen umgehend in den entsprechenden Bereichen zu verbessern.

Wer trägt die Kosten einer Zertifizierung?
Die Kosten für die Zertifizierungsmassnahmen gehen vollumfänglich zulasten des Vertragspartners bzw. des beauftragten Dritten; ebenso der Aufwand für die Behebung der Mängel, die bei der Überprüfung festgestellt werden.

Was passiert, wenn sich ein Vertragspartner nicht zertifizieren lässt?
Lässt sich ein Vertragspartner, der dazu verpflichtet ist, nicht zertifizieren, ist PostFinance berechtigt, das Vertragsverhältnis mit sofortiger Wirkung zu beenden und für allfällige Bussen der Kartenorganisationen und Forderungen der Kartenherausgeber Schadenersatz zu verlangen.

Wer hat Einsicht in die Zertifizierungsdaten?
Einsicht in die Daten, die im Rahmen einer Zertifizierung erhoben werden, haben nur der Vertragspartner und das beauftragte Zertifizierungsunternehmen. Der Vertragspartner ist jedoch verpflichtet, die Zusammenfassung der Zertifizierungsergebnisse an PostFinance zu senden. Ebenfalls haben PostFinance und der Acquirer Worldline Einsicht in die Self-Assessment Questionnaires. Die Kartenorganisationen erhalten hingegen nur statistische Auswertungen.

Wie oft muss eine Zertifizierung erneuert werden?
Die Zertifizierungsmassnahmen müssen periodisch gemäss der Tabelle auf der nächsten Seite wiederholt werden.

Änderungen beim Vertragspartner wie die Installation einer neuen Hard- oder Software, eine neue Website oder ein Wechsel des Service Providers, die einen Zusammenhang mit der Akzeptanz der Kartenzahlungen haben, müssen zudem umgehend PostFinance gemeldet werden. Unter Umständen wird dadurch eine neue Zertifizierung notwendig.

Von welchen Unternehmen müssen die Zertifizierungsmassnahmen durchgeführt werden?
Ein Verzeichnis sämtlicher akkreditierter Zertifizierungsunternehmen finden Sie im Internet.

- Für die Durchführung von On-Site Audits:
  pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- Für die Durchführung von Network Scans:
  listings.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.0.pdf

Wo finde ich noch mehr Informationen über PCI DSS?
Weitere Informationen über PCI DSS finden Sie auf den folgenden Websites:

- Worldline:
  worldline.com/merchant-services/pci
- PCI Security Standards Council:
  pcisecuritystandards.org

Wer muss welche Zertifizierungsmassnahmen ergreifen?

Level	Bezeichnung	Visa, Mastercard®/ Maestro, Diners/ Discover	JCB	American Express
1	Händler mit mehr als 6 Mio. Transaktionen pro Jahr	Jährlicher On-Site Audit [1] ¼-jährlicher Network Scan		
	Händler, die Opfer eines Kartendatendiebstahls wurden			
	Händler mit mehr als 2,5 Mio. Transaktionen pro Jahr			Jährlicher On-Site Audit ¼-jährlicher Network Scan
	Händler mit mehr als 1 Mio. Transaktionen pro Jahr		Jährlicher On-Site Audit ¼-jährlicher Network Scan	
2	Händler mit 1 – 6 Mio. Transaktionen pro Jahr	Jährlicher Self-Assessment Questionnaire [2] ¼-jährlicher Network Scan		
	Händler mit 50 000 – 2,5 Mio. Transaktionen pro Jahr			¼-jährlicher Network Scan
3	E-Commerce-Händler mit 20 000 – 1 Mio. Transaktionen pro Jahr	Jährlicher Self-Assessment Questionnaire ¼-jährlicher Network Scan		
	Händler mit weniger als 50 000 Transaktionen pro Jahr			¼-jährlicher Network Scan
4	E-Commerce-Händler mit weniger als 20 000 Transaktionen pro Jahr	Jährlicher Self-Assessment Questionnaire ¼-jährlicher Network Scan	Jährlicher Self-Assessment Questionnaire ¼-jährlicher Network Scan	
	Händler (ausgenommen E-Commerce) mit weniger als 1 Mio. Transaktionen pro Jahr			

[1] Der Händler kann entscheiden, ob er den On-Site Audit mit der Unterstützung eines QSA (Qualified Security Assessor) oder durch einen ISA (Internal Security Assessor) durchführen möchte.
[2] Die für das Komplettieren des SAQ verantwortlichen Personen müssen als ISA (Internal Security Assessor) zertifiziert sein.

On-Site Audit und/oder Network Scan sind nur für diejenigen Vertragspartner verpflichtend, die Kartendaten elektronisch verarbeiten, übermitteln oder speichern. Unabhängig davon empfehlen wir jedoch – speziell Vertragspartnern mit komplexen Infrastrukturen – diese Validierungsmassnahmen trotzdem durchzuführen. Die Richtlinien von PCI DSS sind durch den Vertragspartner immer einzuhalten. Den Nachweis über deren Einhaltung muss der Vertragspartner jedoch erst nach schriftlicher Aufforderung durch PostFinance erbringen.

PostFinance AG
Mingerstrasse 20
3030 Bern

www.postfinance.ch

460.349 de (dok.pf/pf.ch) 02.2025