Payment Services

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 SIX Payment Services das Vertragsverhältnis fristlos kündigen und Schadenersatz für mögliche Strafen und Forderungen geltend machen.

Die folgenden Weisungen sind als technische und organisatorische Richtlinien bindende Bestandteile jedes Vertrages mit SIX Payment Services.

Wieso wurde PCI DSS eingeführt?

Der Diebstahl von Kartendaten hat in den vergangenen Jahren massiv 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 wirkungsvoller vor Kartendatendiebstahl und -missbrauch schützen.

Was beinhaltet PCI DSS?

PCI DSS umfasst 12 verbindliche Anforderungen, welche 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.

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. Vergleichen Sie dazu:

– Ziffer 13 der «Allgemeinen Geschäftsbedingungen für das bargeldlose Zahlen»

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 Rückseite):

– **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, welche Opfer eines Kartendatendiebstahls wurden, sowie alle Payment Service Provider und andere Dienstleister, die im Auftrag Kartendaten übermitteln, speichern oder verarbeiten, werden vor Ort überprüft. Während Vertragspartner einen solchen On-Site Audit selbst durch einen ausgebildeten Auditor durchführen und von einem Geschäftsverantwortlichen quittieren lassen können, müssen sich Service Provider zwingend durch ein akkreditiertes Zertifizierungsunternehmen (QSA – Qualified Security Assessor) zertifizieren lassen.

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 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 SIX Payment Services berechtigt, das Vertragsverhältnis fristlos zu kündigen und für mögliche Strafen 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, hat nur der Vertragspartner und das beauftragte Zertifizierungsunternehmen. Der Vertragspartner ist jedoch verpflichtet, die Zusammenfassung der Zertifizierungsergebnisse an SIX Payment Services zu senden. Ebenfalls hat SIX Payment Services 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 unten stehenden Tabelle wiederholt werden. Änderungen beim Vertragspartner wie die Installation einer neuen Hard- oder Software, eine neue Website oder ein Wechsel des Service Providers müssen zudem umgehend SIX Payment Services gemeldet werden. Unter Umständen wird dadurch eine neue Zertifizierung notwendig.

Durch welche Unternehmen müssen die Zertifizierungsmassnahmen durchgeführt werden?

Ein Verzeichnis sämtlicher akkreditierter Zertifizierungsunternehmen finden Sie im Internet.

- Für die Durchführung von On-Site Audits: www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- Für die Durchführung von Network Scans: www.pcisecuritystandards.org/pdfs/asv_report.html

Wo finde ich noch mehr Informationen über PCI DSS?

Weitere Informationen über PCI DSS finden Sie auf der Website des PCI Security Standards Council: www.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 – ¼-jährlicher Network Scan				
	Händler, welche 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	– ¼-jährlicher Network Scan – jährlicher Self Assessment Questionnaire				
	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	– ¼-jährlicher Network Scan – jährlicher Self Assessment Questionnaire				
	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	– ¼-jährlicher Network Scan – jährlicher Self Assessment Questionnaire			– ¼-jährlicher Network Scan – jährlicher Self Assessment Questionnaire	
	Händler (ausgenommen E-Commerce) mit weniger als 1 Mio. Transaktionen pro Jahr					

On-Site Audit und/oder Network Scan sind nur für diejenigen Vertragspartner Pflicht, welche Kartendaten elektronisch verarbeiten, übermitteln oder speichern. Wir empfehlen jedoch, speziell Vertragspartnern mit komplexen Infrastrukturen, diese Validierungsmassnahmen trotzdem durchzuführen.

110.0157.01 INT_DE/04.2012

Ihr persönlicher Kontakt: www.six-payment-services.com/kontakt

SIX Payment Services AG
Hardturmstrasse 201
8005 Zürich
Schweiz

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luxemburg