WORLDLINE

Payments to grow your world

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 Worldline 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 jedes Vertrages mit Worldline.

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.

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 für die 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 Web-Hosting-Anbieter oder Payment Service Provider (PSP), die Einfluss auf die Sicherheit von Daten der Karteninhaber haben können oder in ihrem Namen Tätigkeiten ausführen, diese Sicherheitsrichtlinien ebenfalls einhalten.
Vergleichen Sie dazu die in den für die Kartenakzeptanz anwendbaren Allgemeinen Geschäftsbedingungen enthaltenen Bestimmungen bezüglich «Datenschutz» und «Haftung».

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.

Welche Arten von Zertifizierungsmassnahmen gibt es?

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

Wenn ein Vertragspartner nicht alle Zertifizierungskriterien erfüllt, ist er verpflichtet, seine Sicherheitsvorkehrungen umgehend in den entsprechenden Bereichen zu verbessern, und kann bis zur Erfüllung der Kriterien finanziellen Bussen unterliegen.

Wer trägt die Kosten einer Zertifizierung?

Die Kosten für die Zertifizierungsmassnahmen gehen vollumfänglich zulasten des Vertragspartners; 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 Worldline 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, hat nur der Vertragspartner und das beauftragte Zertifizierungsunternehmen. Der Vertragspartner ist jedoch verpflichtet, die Zusammenfassung der Zertifizierungsergebnisse an Worldline zu senden. Ebenfalls hat Worldline Einsicht in die Self-Assessment Questionnaires.
Die Kartenorganisationen erhalten hingegen nur statistische Auswertungen.

Wie oft muss eine Zertifizierung erneuert werden?

Alle Unternehmen müssen sich einem jährlichen Assessment unterziehen und Unternehmen mit dem Internet zugewandten IP-Adressen (E-Commerce usw.) müssen darüber hinaus vierteljährliche ASV (Schwachstellen) Scans unternehmen. Erhebliche Änderungen an der Händlerumgebung müssen umgehend Worldline gemeldet werden, damit beurteilt werden kann, ob sich diese Änderungen auf die wirtschaftlichen oder die Compliance-Anforderungen auswirken.

Durch welche 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:
  pcisecuritystandards.org/pdfs/asv_report.html

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

Ihren lokalen Ansprechpartner finden Sie unter: worldline.com/merchant-services/contacts

110.00110.01 INT_DE/08.2023