Payment Services

Merkblatt zum Sicherheitsstandard PA-DSS

Der weltweit gültige Sicherheitsstandard Payment Application Data Security Standard (PA-DSS) enthält verschiedene Sicherheitsrichtlinien für die Entwicklung von Zahlungsapplikationen, die beim Zahlungsvorgang Kartendaten speichern, verarbeiten oder weiterleiten.

Durch den Einsatz PA-DSS-zertifizierter Zahlungsapplikationen kann das Risiko von Kartendatendiebstahl erheblich reduziert werden. Zudem vereinfacht PA-DSS Unternehmen die Erreichung und die Einhaltung des Sicherheitsstandards nach PCI DSS (Payment Card Industry Data Security Standard).

Wir haben für Sie die wichtigsten Informationen zu diesem Programm PA-DSS zusammengestellt.

Wieso wurde PA-DSS eingeführt?

Die Untersuchung verschiedener Fälle von Kartendatendiebstahl hat gezeigt, dass solche immer wieder auf unzureichend geschützte Zahlungsapplikationen zurückzuführen waren. Aus diesem Grund wurde 2008 der einheitliche und weltweit gültige Sicherheitsstandard PA-DSS eingeführt.

Was bezweckt PA-DSS?

Der Einsatz zertifizierter Zahlungsapplikationen trägt mit dazu bei, das Risiko von Kartendatendiebstahl zu reduzieren. PA-DSS unterstützt Lösungsanbieter bei der Entwicklung neuer Zahlungsapplikationen und unterstützt Händler die Compliance nach PCI DSS (Payment Card Industry Data Security Standard) zu erreichen.

Was beinhaltet PA-DSS?

Der Standard beinhaltet 14 Haupt- und rund 90 Detailanforderungen – sie stellen für Lösungsanbieter einen Leitfaden für die Entwicklung sicherer Zahlungsapplikationen dar. Die Anforderungen konzentrieren sich im Wesentlichen auf die folgenden Bereiche: Entwicklung, Prozesse, Implementierung, Verschlüsselung und Zugriffe.

Wer muss PA-DSS umsetzen?

Die Umsetzung obliegt den Lösungsanbietern von Zahlungsapplikationen, die Kartendaten speichern, verarbeiten oder weiterleiten. Voraussetzung ist, dass diese Applikationen Bestandteil des Autorisierungsprozesses und/oder der Zahlungsabwicklung sind und an Dritte verkauft werden.

Wer ist dafür verantwortlich, dass PA-DSS eingehalten wird?

In erster Linie müssen die Lösungsanbieter die Konformität der Zahlungsapplikationen mit PA-DSS sicherstellen. Vertriebspartner, Integratoren und Vertragspartner, die Zahlungsapplikationen kaufen, verkaufen oder installieren, müssen ihrerseits sicherstellen, dass die von ihnen eingesetzten Zahlungsapplikationen nach PA-DSS zertifiziert sind.

Welche Applikationstypen unterliegen PA-DSS?

- Serienmässige Zahlungsapplikationen, die an Dritte verkauft und installiert werden
- Modulare Zahlungsapplikationen (nur die Module mit Zahlungsfunktionen)
- Autonome Zahlterminals, die
  1. mit dem System oder Netzwerk des Händlers verbunden sind
  2. nicht nur mit dem Zahlungsverarbeiter (Acquirer) verbunden sind
  3. eine sichere Fernwartung der Zahlungsapplikation nicht gewährleisten
  4. nach dem Autorisierungsprozess sensitive Kartendaten (Magnetstreifendaten, CVV2, CVC2, CAV2, CID oder PIN) speichern

Welche Applikationstypen unterliegen nicht PA-DSS?

1. Kundenspezifische Einzellösungen (kein Vertrieb)
2. Eigens vom Händler entwickelte Applikationen, die nur intern verwendet werden
3. Betriebssysteme (Windows, Unix usw.), Datenbanken, Verwaltungssysteme (Backoffice) und ähnliches

Diese Applikationen werden im Rahmen der PCI DSS Zertifizierung des Händlers überprüft.

Wer darf eine PA-DSS-Zertifizierung durchführen?

Zahlungsapplikationen müssen zwingend durch qualifizierte Sicherheitsprüfer (PA-QSA – Payment Application Qualified Security Assessor) abgenommen und zertifiziert werden. Diese Sicherheitsprüfer werden vom PCI Council akkreditiert. Eine Liste aller zugelassenen PA-QSA findet sich online unter: https://www.pcisecuritystandards.org/security_standards/vpa/

Wie lange ist das PA-DSS-Zertifikat gültig?

Alle drei Jahre wird der Standard überarbeitet und in einer neuen Version veröffentlicht. Die Gültigkeit einer Zertifizierung verfällt drei Jahre nach der Veröffentlichung der neuen Standardversion. Eine Konformität von mindestens drei Jahren ist dadurch gewährleistet.

Zahlungsapplikationen müssen jedoch jährlich beglaubigt werden. Bei Änderungen an der Zahlungsapplikation ist je nach Art der Änderungen eine Revalidierung durch einen PA-QSA notwendig.

Was kostet eine Zertifizierung, und wer zahlt?

Die Kosten für die Zertifizierung einer Zahlungsapplikation variiert. Nebst dem Umfang und der Komplexität einer Zahlungsapplikation spielt zudem auch immer die Wahl des Sicherheitsprüfers (PA-QSA) eine Rolle.

Die Aufnahme einer Zahlungsapplikation nach erfolgreicher Zertifizierung im Verzeichnis des PCI Council kostet USD 1250 pro Zahlungsapplikation. Danach wird jährlich eine Verwaltungsgebühr von USD 500 pro Zahlungsapplikation erhoben.

Wo finde ich mehr Informationen zu PA-DSS?

Weitere Informationen zu PA-DSS sind auf der Website des PCI Council verfügbar: https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

Auch zu empfehlen ist deren Webinar zum Thema PA-DSS: http://www.webcastgroup.com/client/start.asp?wid=0800522084108

Die aktuelle Liste aller zertifizierten Zahlungsapplikationen: https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html

110.0115.01 CHE_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