more security. usd

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS 4.0)

Einführung in den Standard

Klassifizierung: Öffentlich (V0)

Stand: Januar 2023

INHALTSVERZEICHNIS

REFERENZEN
DAS SAGEN UNSERE KUNDEN

equensWorldline

„In hochkomplexen Projekten wie der initialen Zertifizierung nach dem PCI-Standard ist es wichtig, einen verlässlichen Partner an seiner Seite zu wissen. usd hat uns in jeder Phase dieser Zertifizierungen kompetent unterstützt. Dabei war es besonders wichtig und angenehm zu erfahren, dass unsere Berater sehr pragmatisch und lösungsorientiert vorgingen, wodurch auch zu kniffligen Problemstellungen stets eine gute Lösung gefunden werden konnte. Auf Basis der sehr guten Erfahrungen setzen wir auch für die Re-Zertifizierungen auf usd als unseren Partner."

Thomas Maaß

Director Banking & Finance Central Europe

Eurowings

„Die Sicherheit der Daten unserer Kunden steht für uns an oberster Stelle, PCI DSS ist dabei ein strategisch wichtiges Thema. Wir sind froh, mit der usd einen starken Partner an der Seite zu haben, der uns zur Compliance Validation begleitet hat."

Mehtap Secilmis

Head of IT Governance and Information Security Officer Eurowings Group

zalando

„Ich bin vom gemeinsamen Projekt begeistert. Die Zertifizierung verlief unkompliziert und war durch die enge Zusammenarbeit zwischen den Teams von Zalando und der usd schnell umsetzbar. Für uns ist es ein wichtiger Schritt, mit dem wir zeigen, dass wir auch bei einer agilen und schnellen Produktentwicklung stets einen Fokus auf die Sicherheit der Kundendaten haben. Dies konnten wir mit diesem Projekt unter Beweis stellen."

Benjamin Pannier

Managing Director
Zalando Payments GmbH

PCI DSS
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Kreditkartendaten sind ein äußerst begehrtes Ziel für Kriminelle. Sie lassen sich mitunter leicht erbeuten und relativ unkompliziert in Geld umwandeln. Ob professionelle Hacker oder böswillige Insider am Werk sind, die Kriminellen sind meist bestens organisiert und das Geschäft mit gestohlenen Kreditkarteninformationen floriert.

Wird ein Diebstahl von Kreditkarteninformationen aufgedeckt, so zieht dies zunächst einmal kostspielige Untersuchungen nach sich, womöglich gefolgt von Schadensersatzansprüchen und Strafzahlungen. Eine Veröffentlichung des Vorfalls durch die Presse sorgt für eine Rufschädigung, die kaum zu beheben ist. Das Vertrauen der Kunden schwindet und die Geschäftstätigkeit trägt einen nachhaltigen Schaden davon.

Die Kreditkartenindustrie hat daher im Oktober 2004 das Payment Card Industry Security Standards Council (PCI SSC) gegründet. Durch die Vereinheitlichung der Sicherheitsleitlinien der einzelnen Kreditkartenorganisationen entstand so der international gültige Payment Card Industry Data Security Standard (PCI DSS).

Der PCI DSS basiert auf Best Practices und wird ständig an aktuelle Bedrohungen angepasst. Er stellt die Basis für eine einheitliche Vorgehensweise zum Schutz von Kreditkartendaten dar und umfasst dabei sowohl technische als auch organisatorische Maßnahmen. Werden die Maßnahmen umgesetzt, so sorgt deren Zusammenspiel für ein Mindestmaß an Sicherheit von Kreditkarteninformationen.

Der Nachweis der Einhaltung des PCI DSS kann im Falle von Kreditkartendiebstahl die Haftungsfrage erheblich beeinflussen. Dazu muss nachgewiesen werden, dass zum Zeitpunkt des Zwischenfalls alle notwendigen Maßnahmen des PCI DSS umgesetzt und befolgt wurden.

ÜBER DIE usd AG

Seit 2005 berät und zertifiziert die usd AG Unternehmen weltweit gemäß den Sicherheitsstandards des PCI SSC. Sie ist offiziell als Qualified Security Assessor, Approved Scanning Vendor, Payment Application Qualified Security Assessor, Point-to-Point Encryption Qualified Security Assessor, PCI 3DS Assessor, Qualified PIN Assessor, Secure Software Assessor und Software SLC Assessor akkreditiert.

2.1. WORAUF HABEN ES KRIMINELLE ABGESEHEN?

Im Zentrum des Interesses stehen nicht die physischen Karten selbst, sondern die Kreditkartendaten.

Die von Kriminellen begehrten Informationen sind vor allem:

- Name des Karteninhabers
- Gültigkeitsdatum
- Kreditkartennummer (PAN)
- Prüfziffer (CVC2/CVV2/…)

Diese befinden sich auf der Karte, zum einen in Form von Beschriftung, zum anderen gespeichert auf Chip und Magnetstreifen. Gelangen diese Informationen in den Besitz von Kriminellen, so können diese – z. B. im Internet – auf Kosten des eigentlichen Karteninhabers Zahlungen tätigen. In einigen wenigen Fällen reicht dafür sogar die Kartennummer (ohne Prüfziffer) bereits aus. Häufig verkaufen Kreditkartendiebe die erbeuteten Daten weiter. Für gestohlene Kreditkartendaten gibt es einen organisierten Schwarzmarkt im Internet. Das Risiko für die Kriminellen ist dabei vergleichsweise gering. Sie sind meist bestens organisiert und agieren international. Eine Rückverfolgbarkeit ist so gut wie unmöglich. Die vom PCI DSS vorgegebenen Maßnahmen gehen gezielt auf mögliche Angriffswege ein und verbessern dadurch den Schutz der Kreditkarteninformationen signifikant.

2.2. WAS IST PCI DSS COMPLIANCE?

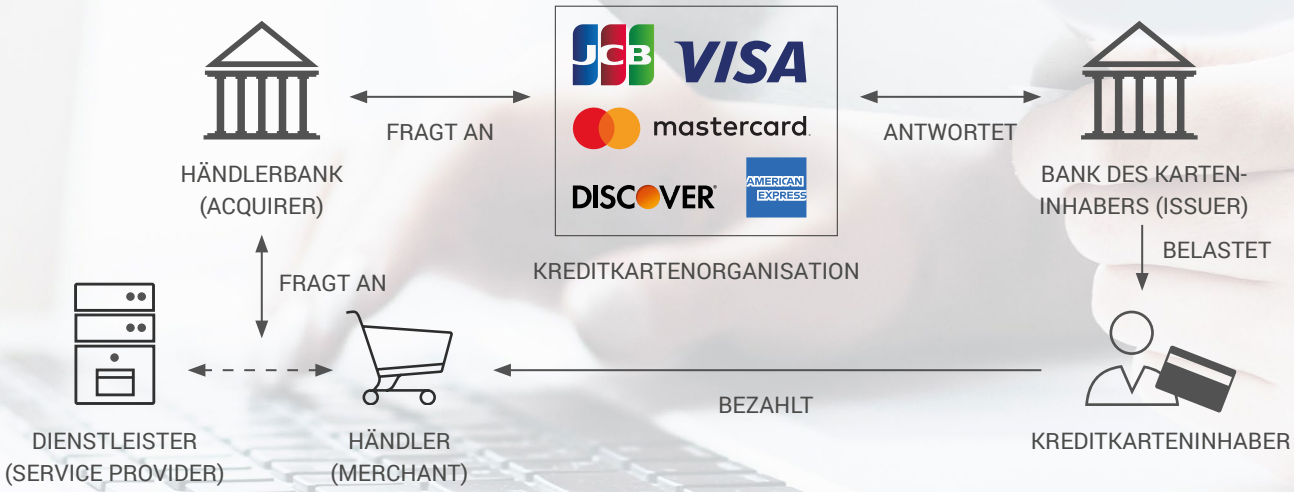
Es gibt keine gesetzliche Verpflichtung zur Einhaltung des PCI DSS. Dennoch müssen sich alle Unternehmen, die Kreditkartendaten speichern, verarbeiten oder übertragen, an den Standard halten. Diese Vorgabe kommt jedoch nicht vom Gesetzgeber, sondern von den Kreditkartenorganisationen selbst. Diese fordern einen Nachweis über die sogenannte PCI DSS Compliance, also die Einhaltung der Vorgaben des Standards.

Maßgeblich dafür, ob ein Nachweis über die PCI DSS Compliance zu erbringen ist, ist letztendlich die Vertragssituation mit den angebundenen Kreditkarten-Prozessoren, z. B. dem *„Acquirer“ (Händlerbank)* oder *„Payment Service Provider“*.

Die meisten Unternehmen, die mit Kreditkartendaten in Berührung kommen, fallen in die Kategorie *„Händler“ (Merchant)*. Sie akzeptieren Zahlungen per Kreditkarte im Austausch für Waren oder Dienstleistungen. Das Vorhandensein eines Kreditkartenakzeptanzvertrags deutet zumeist auf die Einstufung als Händler hin.

Darüber hinaus gibt es in vielfältigen Bereichen sogenannte *„Service Provider“,* die beispielsweise Dienstleistungen für Händler oder Banken erbringen und hierbei Kreditkartendaten selbst verarbeiten oder Zugriff auf diese Daten haben. Hierzu gehören beispielsweise Netzbetreiber, Acquiring und Issuing Prozessoren, Webhosting-Provider für Onlineportale oder IT-Dienstleister für den Betrieb der Server-Infrastruktur und der Unternehmens-Firewall.

BETEILIGTE BEI BEZAHLTRANSAKTIONEN IN DER KREDITKARTENINDUSTRIE



2.3. COMPLIANCE-MANDATE

Die Kreditkartenorganisationen verpflichten Acquirer vertraglich dazu, dafür zu sorgen, dass ein vereinbarter Mindestprozentsatz ihrer Händler die PCI DSS Compliance erreicht. Diese Verpflichtung zur PCI DSS Compliance und zur Nachweiserbringung geben die Acquirer über den Kartenakzeptanzvertrag an ihre Händler weiter. Die Händler verpflichten wiederum ihre Service Provider vertraglich dazu, PCI DSS compliant zu sein und ihnen dies durch einen entsprechenden Nachweis zu belegen.

2.4. EINSTUFUNGEN & PRÜFMETHODEN

In Abhängigkeit von der Einstufung (Level) werden bei Händlern und Dienstleistern unterschiedlich starke Prüfmethoden im Rahmen der PCI DSS Zertifizierung vorgegeben. Ausschlaggebend für die Einstufung des zu zertifizierenden Unternehmens ist die Anzahl der pro Jahr und Kreditkartenorganisation verarbeiteten Kreditkartentransaktionen.

Die folgenden Einstufungen gelten für Händler:

Level	American Express	MasterCard & Visa Europe
1	> 2,5 Millionen Transaktionen pro Jahr	> 6 Millionen Transaktionen pro Jahr
2	50.000 bis 2,5 Millionen Transaktionen pro Jahr	1 Millionen bis 6 Millionen Transaktionen pro Jahr
3	< 50.000 Transaktionen pro Jahr	20.000 bis 1 Millionen E-Commerce-Transaktionen pro Jahr
4	–	E-Commerce-Händler mit weniger als 20.000 Transaktionen pro Jahr
	–	Nicht-E-Commerce-Händler mit bis zu 1 Millionen Transaktionen pro Jahr

Die folgenden Einstufungen gelten für Dienstleister:

Level	American Express	MasterCard & Visa Europe
1	>= 2,5 MillionenTransaktionen pro Jahr	>= 300.000 Transaktionen pro Jahr
2	50.000 bis 2,5 Millionen Transaktionen pro Jahr	< 300.000 Transaktionen pro Jahr

Die folgenden Prüfmethoden leiten sich aus den vorgenannten Einstufungen für Händler und Dienstleister ab.

Einstufung	Selbstauskunfts-fragebogen (SAQ)	PCI DSS Security Scans	PCI DSS Audit
Level 1 Händler	–	Vierteljährlich	Jährlich
Level 2 Händler	Jährlich[1]	Vierteljährlich	Jährlich[2]
Level 3 Händler	Jährlich	Vierteljährlich	–
Level 4 Händler	Jährlich	Vierteljährlich	–
Level 1 Dienstleister	–	Vierteljährlich	Jährlich
Level 2 Dienstleister	Jährlich	Vierteljährlich	–

Als akkreditierter Assessor in der Kreditkartenindustrie unterstützen wir Sie bei dem Nachweis der PCI DSS Compliance. Eine detaillierte Beschreibung der vorgenannten Prüfmethoden finden Sie in den nachfolgenden Kapiteln.

[1] Level 2 Händler erhalten ihren Audit-Bericht üblicherweise in Form eines Self-Assessment Questionnaire (SAQ). Auf Wunsch erstellen wir einen Report on Compliance (RoC) auch für Händler dieses Levels.

[2] MasterCard verpflichtet Händler mit Level 2, auf die entweder SAQ A, A-EP oder D zutrifft, ihre Selbstauskunft zusammen mit einem QSA oder ISA auszuführen oder ein Audit von einem QSA durchführen zu lassen

WARUM IST DER **PCI DSS NACHWEIS** WICHTIG?

In vielen Fällen von Kreditkartendiebstahl wird im Nachgang festgestellt, dass eine oder mehrere der PCI DSS Anforderungen nicht umgesetzt wurden. Zahlreiche Untersuchungen haben bewiesen, dass

MEHR ALS

3/4

ALLER ANGRIFFE

durch einfache Maßnahmen und geringen (finanziellen) Aufwand hätten vermieden werden können.

Die Implementierung der PCI DSS Anforderungen gewährleistet nicht nur ein spürbar höheres Sicherheitsniveau in Ihrem gesamten Unternehmen, sondern schafft auch einen wesentlichen Mehrwert, verbunden mit folgenden Vorteilen:

- Sie können Risiken bei der Verarbeitung von Kreditkarten- und sonstigen Kundendaten identifizieren
- Sie zeigen Ihren Kunden, dass Sie die Sicherheit ihrer Daten ernst nehmen
- Sie verbessern Ihren Schutz vor finanziellen Haftungsrisiken, Rechtskosten und Kosten zur Beweissicherung
- Sie vermeiden negative Presse

2.5. DIE ANFORDERUNGEN DES PCI DSS

Der PCI DSSv4.0 umfasst insgesamt 6 Kontrollziele, die sich in 12 Hauptanforderungen mit insgesamt 329 Einzelanforderungen aufgliedern. Der Standard umfasst dabei sowohl technische als auch organisatorische und dokumentarische Anforderungen.

Kontrollziel	Nr.	Kapitel
Aufbau und Betrieb eines sicheren Netzwerkes	1	Einrichtung und Pflege von Netzwerksicherheitskontrollen
	2	Anwendung von sicheren Konfigurationen auf allen Systemen
Schutz der Kreditkarten-daten	3	Schutz gespeicherter Kreditkartendaten
	4	Verschlüsselte Übermittlung von Kreditkarten- und anderen sensiblen Informationen über öffentliche Netzwerke
Management von Schwachstellen	5	Schutz aller Systeme und Netzwerke vor Schadsoftware
	6	Entwicklung und Pflege sicherer Systeme und Anwendungen
Starker Zugriffsschutz	7	Beschränkung des Zugriffs auf Daten und Systeme nach dem Need-to-know-Prinzip
	8	User-Identifikation und Zugangsauthentifizierung auf Systemen
	9	Beschränkung des physischen Zugriffs auf Kreditkarteninformationen
Regelmäßige Prüfung und Test des Netzwerkes	10	Überwachung und Nachverfolgung jeglicher Zugriffe auf Systeme und Kreditkartendaten
	11	Regelmäßige Tests der Sicherheitssysteme und -prozesse
Pflege einer Informations-sicherheitsrichtlinie	12	Unterstützung der Informationssicherheit durch organisatorische Richtlinien

Durch die Umsetzung des PCI DSS wird eine ganzheitliche Verbesserung des Sicherheitsniveaus in Ihrem Unternehmen erzielt und dadurch gleichermaßen der Schutz von Kreditkartendaten ermöglicht.

IHRE ANSPRECHPARTNER*INNEN

Sie haben Fragen zu unseren Leistungen und Produkten? Sprechen Sie uns gern persönlich an. Unser Fachvertrieb steht Ihnen zur Verfügung.

Anna-Magdalena Kohl
Technical Sales Consultant, PCI Professional

Telefon: +49 6102 8631–190 | Mail: vertrieb@usd.de
PGP oder S/MIME für verschlüsselte Kommunikation

Benedikt Krümmel
Technical Sales Consultant, PCI Professional

Telefon: +49 6102 8631–190 | Mail: vertrieb@usd.de
PGP oder S/MIME für verschlüsselte Kommunikation