more security. usd

Payment Card Industry Data Security Standard (PCI DSS)

Beratungs- und Zertifizierungsleistungen der usd AG

Inhaltsverzeichnis

1 Payment Card Industry Data Security Standard (PCI DSS)

Der Diebstahl von Kreditkartendaten sind ein sehr begehrtes Ziel für Kriminelle. Die Daten lassen sich besonders in schlecht geschützten Unternehmen leicht erbeuten und ohne großes Risiko auf dem Schwarzmarkt in Geld umwandeln. Ob nun 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 kostspielige Untersuchungen nach sich, die vor allem für kleinere Unternehmen schwerwiegende wirtschaftliche Folgen haben können. Es folgen Schadensersatzansprüche und Strafzahlungen. Zu guter Letzt sorgt die Veröffentlichung des Vorfalls durch die Presse für eine Rufschädigung, die auch langfristig unangenehme Konsequenzen mit sich bringen kann. Das Vertrauen der Kunden schwindet und die Geschäftstätigkeit trägt einen nachhaltigen Schaden davon.

Die Kreditkartenindustrie hat sich daher im Oktober 2004 weltweit zusammengeschlossen und das Payment Card Industry Security Standards Council (PCI SSC) gegründet. Es wurde die Vereinheitlichung der bisher geltenden Sicherheitsstandards der einzelnen Kreditkartenorganisationen beschlossen, woraus schließlich der international gültige Payment Card Industry Data Security Standard (PCI DSS / Datensicherheitsstandard der Kreditkartenorganisationen) entstand.

Der PCI DSS basiert auf Best Practices und wird ständig an aktuelle technische Entwicklungen 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 eigenen PCI DSS Compliance kann bei Bekanntwerden von Kreditkartendiebstahl die Haftungsfrage erheblich beeinflussen. Dazu muss allerdings nachgewiesen werden, dass zum Zeitpunkt des Zwischenfalls alle notwendigen Maßnahmen des PCI DSS umgesetzt und befolgt wurden, sowie eine gültige Zertifizierung vorlag.

Seit 2005 berät und zertifiziert die usd AG weltweit Unternehmen als offiziell vom PCI Council akkreditierter Qualified Security Assessor, Approved Scanning Vendor und Payment Application Qualified Security Assessor gemäß den Standards PCI DSS, P2PE (Point-To-Point-Encryption), PCI 3 DS (Sicherheitsstandard für sichere Online-Kreditkartentransaktionen) und PCI PA-DSS (Payment Card Industry Payment Application Data Security Standard / Datensicherheitsstandard für Zahlungsanwendungen der Kreditkartenorganisationen).

1.1 Worauf haben es Kriminelle abgesehen?

Im Zentrum des Interesses stehen nicht die physischen Karten selbst, sondern die Kreditkartendaten. Diese sind einerseits auf der Karte aufgedruckt, zum anderen sind sie auf dem integrierten Chip und Magnetstreifen hinterlegt.

1. Chip
2. Kreditkartennummer (PAN / Primary Account Number)
3. Gültigkeitsdatum
4. Name des Karteninhabers
5. Magnetstreifen
6. Kartenvalidierungscode, Prüfziffer (CVC / Card Validation Code, CVV /Card Verification Value)

Die von Kriminellen begehrten Informationen sind vor allem der Name des Karteninhabers, das Gültigkeitsdatum, die Kreditkartennummer (PAN) sowie die Prüfziffer (CVC2/CVV2/…). Ist der Kriminelle im Besitz dieser Informationen, kann dieser - z.B. im Internet - auf Kosten des eigentlichen Karteninhabers Zahlungen tätigen. In einigen Fällen reicht sogar die Kreditkartennummer (ohne Prüfziffer). Anschließend wird die gekaufte Ware dann an Mittelsmänner ausgeliefert oder weiterverkauft.

Eine weitere Methode von Kartendieben ist die Manipulation von Bezahlterminals. Die Daten des Magnetstreifens werden beim Zahlungsvorgang ausgelesen und an den Kartendieb übermittelt. Dieser kann die erbeuteten Daten auf eine „Blanko“-Kreditkarte kopieren und mit dieser dann auch „offline“ bezahlen.

Häufig nutzen Kreditkartendiebe die erbeuteten Daten aber nicht selbst, sondern verkaufen sie im Internet weiter. Hierfür gibt es einen organisierten Schwarzmarkt für gestohlene Kreditkartendaten. Das Risiko für die Kriminellen ist dabei vergleichsweise gering. Sie sind meist bestens organisiert und agieren international. Eine Rückverfolgbarkeit ist so gut wie unmöglich und Ermittlungen über nationale Grenzen hinweg schwierig.

Die PCI DSS Maßnahmen gehen gezielt auf mögliche Angriffswege ein und verbessern dadurch den Schutz der Kreditkarteninformationen Ihrer Kunden signifikant.

1.2 Was ist PCI DSS Compliance?

PCI DSS ist ein verbindlicher Standard der Kreditkartenorganisationen. Das heißt, alle Unternehmen, die Kreditkartenzahlungen von ihren Kunden akzeptieren, müssen den vorgegebenen Standard einhalten. Die Kreditkartenorganisationen fordern den Nachweis über die sogenannte PCI DSS Compliance, also die Konformität mit dem Sicherheitsstandard. Durch die vollständige Umsetzung aller zutreffender Anforderungen des PCI DSS wird eine ganzheitliche Verbesserung des Sicherheitsniveaus in Ihrem Unternehmen erzielt und dadurch gleichermaßen der Schutz von Kreditkartendaten Ihrer Kunden ermöglicht.

1.3 Welche Einstufungen und Prüfmethoden sind vorgegeben?

In Abhängigkeit von der Einstufung (Level) werden bei Händlern 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	> 6 Millionen Transaktionen pro Jahr
2	50.000 bis 2,5 Millionen Transaktionen pro Jahr	1 Millionen bis 6 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	20.000 bis 1 Millionen E-Commerce Transaktionen pro Jahr
4	-	Alle sonstigen Händler	< 20.000 E-Commerce Transaktionen pro Jahr
	-	-	Nicht-E-Commerce Händler mit bis zu 1 Millionen Transaktionen pro Jahr

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

Einstufung	Selbstauskunftsfra-gebogen (SAQ)	PCI DSS Security Scans	PCI DSS Audit
Level 1 Händler	-	Vierteljährlich	Jährlich
Level 2 Händler		Vierteljährlich	Jährlich*
Level 3 Händler	Jährlich	Vierteljährlich	-
Level 4 Händler	Jährlich	Vierteljährlich	-

* MasterCard akzeptiert die PCI DSS Zertifizierung mittels SAQ nur, sofern diese von einem Internal Security Assessor (ISA) durchgeführt wurde. Der ISA ist ein vom PCI SSC akkreditierter Mitarbeiter Ihres Unternehmens.

Als akkreditierter Auditor in der Kreditkartenindustrie unterstützen wir Sie bei dem Nachweis der PCI DSS Compliance. Eine detaillierte Beschreibung der vorgenannten Prüfmethoden finden Sie im nachfolgenden Kapitel.

Warum ist der PCI DSS Nachweis so wichtig?

In vielen Fällen von Kreditkartendiebstahl wird im Nachgang festgestellt, dass eine oder mehrere der PCI DSS Maßnahmen nicht umgesetzt wurden. Die Lösungen müssen dabei nicht immer komplex und teuer sein. Zahlreiche Untersuchungen haben bewiesen, dass mehr als drei Viertel aller Angriffe durch einfache Mittel und geringen (finanziellen) Aufwand hätten vermieden werden können.

Die Konsequenzen solcher Vorfälle können dagegen erheblichen Schaden verursachen und zu einer nachhaltigen Beeinträchtigung der Geschäftstätigkeit führen. Die Einhaltung der PCI DSS Maßnahmen sollte deshalb unbedingt von jedem Unternehmen angestrebt werden.

1.4 Wie sehen die Anforderungen des PCI DSS aus?

Der PCI DSS umfasst insgesamt 12 Kapitel mit insgesamt 334 Einzelanforderungen. Der Standard umfasst dabei sowohl technische als auch organisatorische und dokumentarische Anforderungen.

Kapitel	Nr.	Anforderungsbereich
Aufbau und Betrieb eines sicheren Netzwerkes	**1**	Betrieb einer Firewall-Umgebung
	2	Vermeidung von herstellerspezifischen Standards für Systempasswörter und andere Sicherheitseinstellungen
Schutz der Kreditkartendaten	**3**	Schutz gespeicherter Kreditkartendaten
	4	Verschlüsselte Übermittlung von Kreditkarten- und anderen sensiblen Informationen über öffentliche Netzwerke
Management von Schwachstellen	**5**	Benutzung und regelmäßige Aktualisierung von Anti-Virus-Software
	6	Entwicklung und Pflege sicherer Systeme und Anwendungen
Starker Zugriffsschutz	**7**	Beschränkung des Zugriffs auf Daten nach dem Need-to-know-Prinzip
	8	Zuordnung einer individuellen User-ID an Personen mit IT-Zugriff
	9	Beschränkung des physischen Zugriffs auf Kreditkarteninformationen
Regelmäßige Prüfung und Test des Netzwerkes	**10**	Überwachung und Nachverfolgung jeglicher Zugriffe auf Netzwerkressourcen und Kreditkartendaten
	11	Regelmäßige Tests der Sicherheitssysteme und -prozesse
Pflege einer Informationssicherheitsrichtlinie	**12**	Pflege einer Richtlinie für die Informationssicherheit

2 Ihr Weg zur PCI DSS Compliance

Wir schützen Unternehmen vor Hackern und Kriminellen. Unsere Aufgabe ist es, Sie auf dem Weg zur erfolgreichen PCI DSS Zertifizierung bestmöglich zu beraten und zu begleiten.

Die nachfolgende Tabelle gibt Aufschluss über unseren PCI DSS Zertifizierungsprozess:

Grundlage	Technische Prüfungen	Zertifizierung	Compliance
Prüfung der eigenen Prozesse pro Kanal der Kreditkartenakzeptanz: PCI DSS Beratung und / oder PCI DSS Scope Workshop PCI DSS GAP-Analyse	PCI DSS Security Scan (externer und interner Scan) Firewall Review Pentest	PCI DSS SAQ PCI DSS Audit	Erhaltung der PCI DSS Compliance

Die einzelnen Schritte des PCI DSS Zertifizierungsprozesses der usd AG werden im Folgenden ausführlich erläutert.

2.1 Grundlage

2.1.1 PCI DSS Beratung

Mit dem Erwerb eines Beraterpaketes bietet Ihnen die usd AG eine Möglichkeit an, mit unseren Sicherheitsexperten konkrete Fragen zur Umsetzung des PCI DSS in Ihrem Unternehmen zu klären. Hierzu gehören beispielsweise eine individuelle Beratung zur schnellen und effizienten Erreichung der PCI DSS Compliance in Ihrem Unternehmenskontext, die Bewertung von technischen und organisatorischen Maßnahmen und die Unterstützung bei der Erstellung von notwendigen Konzepten, Lösungen oder Prozessen. Welche Aufgaben dabei von den Beratern der usd bearbeitet werden, wird flexibel und nach Bedarf gemeinsam mit Ihnen festgelegt.

Nachfolgend beschrieben sind Beispiele für konkrete Beratungsleistungen der usd im Umfeld des PCI DSS.

PCI DSS Policy Templates

Unternehmen sind im Rahmen der PCI DSS Compliance dazu verpflichtet, vorhandene Sicherheitsprozesse und Konfigurationsstandards usw. in Form von Richtlinien (Policies) und Dokumentation formal festzuschreiben und einmal jährlich zu aktualisieren.

Genau dafür hat die usd ein Paket an Vorlagen (Templates) für jeden PCI DSS Selbstbeurteilungsfragebogen (SAQ) entwickelt. Mit Hilfe dieser Dokumentenvorlagen unterstützt die usd Sie bei der initialen Erstellung aller PCI DSS relevanten Richtlinien. Die bereitgestellten Dokumente entsprechen grundsätzlich den Anforderungen des PCI DSS.

Zu den PCI DSS Policy Templates gehören je nach Notwendigkeit des gewählten SAQ beispielsweise Vorlagen zum Umgang mit Dienstleistern, zur technischen Systemsicherheit, zur Passwortrichtlinie und zum Vorfallreaktionsplan.

Security Awareness Training

Nur regelmäßig geschulte Mitarbeiter erkennen Gefahren und Sicherheitsvorfälle und wissen sich dann richtig zu verhalten. Auch deshalb ist „Security Awareness“, also das Bewusstsein für Sicherheit, Bestandteil aller Sicherheitsstandards. Egal ob PCI DSS, ISO 2700x, oder Datenschutz - regelmäßige, dokumentierte Awareness-Schulungen aller Mitarbeiter sind Pflicht.

2.1.2 PCI DSS Scope Workshop

Im Rahmen eines initialen PCI DSS Scope Workshops werden Sie in die Inhalte des PCI DSS eingeführt. Ziel des Scope Workshops ist die Auseinandersetzung mit den konkreten Prüfungsanforderungen des PCI DSS. Ferner bespricht ein Auditor der usd AG mit Ihnen, ob bei Ihnen Maßnahmen zur Reduzierung des PCI DSS Prüfumfangs möglich sind.

Ein Auditor der usd führt den Scope Workshop im Rahmen eines Vor-Ort-Termins mit Ihren technischen und organisatorischen Ansprechpartnern durch.

Die folgenden Themen werden während des Workshops behandelt.

- Einführung in den PCI DSS
- Vorstellung der konkreten PCI DSS Anforderungen
- Identifikation der zu zertifizierenden Geschäftsbereiche und Prozesse
- Datenflussanalyse der Kreditkartendaten
- Ermittlung der zu zertifizierenden IT-Systeme und Anwendungen
- Überprüfung der Notwendigkeit eines PCI DSS Pentests sowie ggf. der Definition der Pentest-Umgebung (Pentest Scope)
- Identifikation von Maßnahmen zur Minimierung des Prüfumfangs sowie der Zertifizierungsmaßnahmen (beispielsweise Netzwerksegmentierung, Ende-zu-Ende-Verschlüsselung)
- Verbindliche Definition des PCI DSS Prüfumfangs (Audit Scope)
- Entwicklung einer Zertifizierungsstrategie und Planung des weiteren Vorgehens

Im Verlauf des Scope Workshops stellen Sie dafür Ihre Unternehmensstruktur, Service- und Geschäftsprozesse, Kreditkartendatenflüsse und die zu betrachtenden IT-Systeme und Applikationen vor.

Anhand dieser Informationen zeigt ein Auditor der usd die Zertifizierungsrelevanz der einzelnen Geschäftsbereiche, Prozesse und IT-Systeme auf, macht auf direkt erkennbare Abweichungen zum PCI DSS aufmerksam und erarbeitet gemeinsam mit Ihnen die nächsten Schritte.

Auf Wunsch werden spezielle Themengebiete und Fragen aufgegriffen und von einem Auditor der usd erläutert bzw. gemeinsam mit Ihnen diskutiert.

2.1.3 PCI DSS GAP-Analyse

Bei einer initialen PCI DSS Zertifizierung mit bereits bekanntem PCI DSS Scope, bei wesentlichen Änderungen an einem bereits zertifizierten PCI DSS Anwendungsbereich oder bei einem Versionswechsel im PCI DSS Standard empfehlen wir zur Vorbereitung auf die offizielle PCI DSS Zertifizierung die Durchführung einer PCI DSS Gap-Analyse. Die Einhaltung der PCI DSS Anforderungen werden von der usd AG bei Ihnen geprüft. Dadurch haben Sie die Möglichkeit, vorhandene Abweichungen vom PCI DSS Standard frühzeitig zu erkennen und vor der offiziellen PCI DSS Zertifizierung (PCI DSS Audit) zu korrigieren. Dadurch reduziert sich der Zertifizierungsaufwand wesentlich.

2.2 Technische Prüfungen

Der PCI DSS fordert regelmäßige technische Prüfungen Ihrer Anwendungen und IT-Systeme durch Security Scans und Penetrationstests. Security Scans werden durchgeführt, um IT-Systeme auf bekannte Sicherheitslücken (Schwachstellen) zu prüfen. Die Durchführung der Scans und Bewertung der Ergebnisse sind automatisiert. Penetrationstests (kurz Pentests) werden manuell durchgeführt. IT-Systeme werden mit Pentests u.a. auf die korrekte Implementierung von Systemen geprüft, beispielsweise darauf, ob die Netzwerksegmentierung von Bezahlterminals / virtuelle Terminals korrekt durchgeführt wurde.

2.2.1 Externer PCI DSS Security Scan

Zum Nachweis der PCI DSS Compliance müssen Unternehmen, die Kreditkartendaten verarbeiten, speichern oder weiterleiten, ihre IT-Systeme mit einem externen Security Scan auf Schwachstellen überprüfen. Die Security Scans sind von einem zertifizierten Anbieter (Approved Scanning Vendor / ASV) vierteljährlich und nach wesentlichen Änderungen der IT-Systeme durchzuführen. Zusätzlich sind auch die IT-Systeme zu prüfen, die einen maßgeblichen Einfluss auf die Sicherheit der Kreditkartendaten haben.

Unterstützung durch die usd AG

Wir empfehlen die Nutzung der PCI DSS Plattform der usd AG (https://pci.usd.de/). Nach Ihrer Registrierung auf der Plattform und der Bestellung eines PCI DSS Security Scans planen Sie eigenständig auf der Plattform, an welchem Datum und zu welcher Uhrzeit der PCI DSS Security Scan durchgeführt werden soll. Mit den Security Scans der usd erfüllen Sie die PCI DSS Anforderung 11.2.2. Auf unserer PCI DSS Plattform erhalten Sie nach der erfolgreichen Durchführung einen detaillierten technischen Bericht inklusive Management Summary.

Sollte der durchgeführte PCI DSS Security Scan nicht den notwendigen Compliance-Status ergeben, können Sie innerhalb von 28 Tagen mit Re-Scans und ohne zusätzliche Kosten prüfen, ob die ggf. identifizierten Schwachstellen erfolgreich beseitigt wurden.

2.2.2 Interner PCI DSS Security Scan

Mit den internen Security Scans überprüfen Sie Ihre IT-Systeme (Server, Netzwerke, Webserver, Webshops, etc.) auf viele tausend bekannte und ständig aktualisierte Schwachstellen. Mit der Anforderung 11.2.1 fordert der PCI DSS die Durchführung vierteljährlicher interner Schwachstellen-Scans.

Unterstützung durch die usd AG

Die internen Security Scans werden von der usd AG je IP-Adresse durchgeführt. Erkannte Schwachstellen werden dabei nicht ausgenutzt, sodass eine Gefährdung des ordnungsgemäßen Betriebs Ihrer IT-Systeme nahezu ausgeschlossen ist. Sie erhalten das Scanergebnis in Form einer Zusammenfassung und eines umfassenden technischen Berichts. Dieser enthält alle gefundenen Schwachstellen sowie detaillierte Vorschläge zu deren Behebung.

2.2.3 Firewall Reviews

Eine Firewall dient der Absicherung des gesamten Netzverkehrs und blockiert die ungewollte Datenübertragung. Eine korrekte Konfiguration der Firewall ist unabdingbar, um beispielsweise mögliche Angriffe aus dem Internet erfolgreich zu verhindern. Die Firewall-Regelsätze sollten daher regelmäßig auf unnötige, veraltete oder fehlerhafte Regeln überprüft werden.

Unterstützung durch die usd AG

Ein Auditor der usd führt die in der PCI DSS Anforderung 1.1.7 geforderten Firewall Reviews halbjährlich durch. Zu Beginn des ersten Firewall Reviews steht der initiale Kick-off-Termin. Dieser wird in Form von 1-2-tägigen Workshops bei Ihnen vor Ort durchgeführt. Die Firewall Reviews werden anschließend halbjährlich wiederholt.

Sofern Ihre IT-Umgebung unverändert bleibt, ist ein initialer Kick-off Workshop bei den darauffolgenden Firewall Reviews nicht notwendig.

Im Rahmen des Reviews werden von der usd die Firewall-Konfigurationen sowie die Firewall-Regeln untersucht.

Die Überprüfung der Konfiguration und Regeln erfolgt durch Analyse der von Ihnen zur Verfügung gestellten Firewall-Konfigurationsauszüge. Eventuell werden zusätzlich Interviews mit den Administratoren des Firewall-Teams geführt.

Abweichungen zum PCI DSS werden von der usd in einem technischen Bericht dokumentiert und Ihnen in Form eines detaillierten Maßnahmenkatalogs zur Korrektur der identifizierten Schwachstellen zur Verfügung gestellt. Sie korrigierten im Anschluss die identifizierten Abweichungen anhand der Maßnahmenempfehlungen der usd und dokumentieren die Schwachstellenbehebung bis zum nächsten Firewall Review. Die Einhaltung der PCI DSS Anforderung 1.1.7 wird durch den technischen Bericht der usd sowie durch Ihre Dokumentation der Schwachstellenbehebung bestätigt.

Die Durchführung der halbjährlichen Firewall-Reviews erfolgt in Form von Telefon- und Webkonferenzen (falls nötig) und wird ansonsten anhand der Konfigurationsdateien offline bei der usd durchgeführt.

2.2.4 Pentest

Der Pentest ist ein umfassender Sicherheitstest von Netzwerken, Betriebssystemen oder Applikationen. Die Prüfung der Sicherheit aller Systembestandteile und Anwendungen wird mit Mitteln und Methoden durchgeführt, die ein Angreifer nutzt, um in fremde Systeme einzudringen. Aufgrund seiner hohen Aussagekraft über mögliche Verwundbarkeiten Ihrer Systeme und Anwendungen muss gemäß den Anforderungen des PCI DSS einmal jährlich und nach wesentlichen Änderungen der Systeme und/oder Anwendungen ein Pentest durchgeführt werden (Anforderung 11.3.1/11.3.4 A). Diesbezüglich werden Sie von uns beraten und unterstützt.

<u>Unterstützung durch die usd AG</u>
Die usd AG hat ein spezielles Pentest-Verfahren entwickelt, das die PCI DSS Anforderungen effizient erfüllt und die Sicherheit Ihrer Systeme nachhaltig erhöht. Wir bieten Ihnen die Möglichkeit, Ihre IT-Infrastruktur individuell von einem unserer Experten überprüfen zu lassen. Zur Informationsbeschaffung nutzt er professionelle Werkzeuge und versucht gezielt, individuell und erfinderisch, in die Systeme des Unternehmens einzudringen. Diese Simulation eines realen Hackerangriffs liefert qualitativ hochwertige Ergebnisse.

Anhand des Pentests werden Schwachstellen und Sicherheitslücken gezielt identifiziert, daraus resultierende Risiken benannt und Wege aufgezeigt, die Sicherheit der geprüften IT-Systeme und Applikationen zu verbessern.

Die Vorgehensweise der usd im Rahmen des Pentests richtet sich nach allgemein zugänglichen IT-Sicherheitsstandards wie:

- OSSTMM (Open Source Security Testing Methodology Manual),
- BSI-Modell für Pentests (Durchführungskonzept für Pentests),
- OWASP (Open Web Application Security Project)
- NIST SP800-115 (Technical Guide to Information Security Testing and Assessment).

Gefundene Schwachstellen und Sicherheitslücken werden verifiziert, mit Ihnen besprochen und erst auf ausdrücklichen Wunsch ausgenutzt, um direkten Zugriff auf IT-Systeme und Daten zu erlangen. Sie werden täglich über erfolgreiche Angriffe und damit verbundene Schwachstellen informiert.

Nach Abschluss der Untersuchung dokumentiert das Sicherheitsteam der usd für Sie die Ergebnisse des Pentests in einem formalen Ergebnisbericht. Neben den identifizierten Risiken werden dabei auch entsprechende Maßnahmenempfehlungen zur Behebung der Schwachstellen durch die IT-Sicherheitsexperten der usd gegeben.

Im Rahmen einer Telefonkonferenz werden die identifizierten Schwachstellen sowie Maßnahmenempfehlungen mit Ihnen besprochen. Auf Ihre offenen Fragen wird im Rahmen des Abschlussmeetings jederzeit eingegangen.

2.3 Zertifizierung

2.3.1 PCI DSS Selbstbeurteilungsfragebogen

Mit dem PCI DSS Selbstbeurteilungsfragebogen (SAQ / Self-Assessment Questionnaire) beurteilen Händler ihre PCI DSS Compliance selbst. Händler, welche im Level 3 und 4 eingestuft wurden, sind einmal jährlich aufgefordert, den für ihr Unternehmen passenden SAQ pro Akzeptanzkanal zu beantworten (siehe Kapitel 1.3).

Das PCI SSC hat acht unterschiedliche SAQs entwickelt und veröffentlicht. Je nach Kanal der Kreditkartenakzeptanz und den eingesetzten Zahlungsprozessen, wird der passende SAQ (www.pcisecuritystandards.org/document_library?category=saqs#results) gewählt und beantwortet.

Die nachfolgende Tabelle gibt einen Überblick über die einzelnen SAQs:

SAQ Typ	Beschreibung	Akzeptanzkanal
A	Sämtliche Zahlungsprozesse werden an PCI DSS zertifizierte Dienstleister ausgelagert. Die eigenen Systeme verarbeiten keine Kreditkartendaten und es erfolgt keine elektronische Speicherung von Kreditkartendaten	E-Commerce oder MOTO / Mail Order Telephone Order (Kreditkarte liegt nicht vor)
A-EP	Die Bezahlseite wird vom Händler zur Verfügung gestellt und vom Kunden an den Zahlungsdienstleister gesendet oder in die Bezahlseite werden Elemente vom eigenen Server eingebunden. Die Kartendaten werden nicht von den Systemen des Händlers gespeichert.	E-Commerce (Kreditkarte liegt nicht vor)
B	Kreditkartendaten werden ausschließlich über das Bezahlterminal übertragen, welches mit dem Telefon oder dem Mobilfunknetz verbunden ist. Es erfolgt keine elektronische Speicherung von Kreditkartendaten.	POS / Point of Sale / Bezahlterminal (Kreditkarte liegt vor)
B-IP	Kreditkartendatendaten werden über ein Bezahlterminal übertragen, welches via Internet verbunden ist. Das Bezahlterminal ist im Netzwerk isoliert von anderen IP-angebundenen Geräten und es erfolgt keine elektronische Speicherung von Kreditkartendaten.	POS / Point of Sale / Bezahlterminal (Kreditkarte liegt vor)
C	Kreditkartendaten werden über eine Zahlungsanwendung oder ein elektronisches Kassensystem direkt abgewickelt. Die Zahlungsanwendung ist im Netzwerk isoliert und es erfolgt keine elektronische Speicherung von Kreditkartendaten.	POS / Point of Sale / Bezahlterminal (Kreditkarte liegt vor) oder MOTO / Mail Order Telephone Order (Kreditkarte liegt nicht vor)
C-VT	Kreditkartendaten werden über eine Webanwendung (virtuelles Terminal) abgewickelt. Das virtuelle Terminal ist im Netzwerk isoliert und es erfolgt keine elektronische Speicherung von Kreditkartendaten.	MOTO / Mail Order Telephone Order (Kreditkarte liegt nicht vor)

P2PE	Kreditkartendaten werden über ein speziell für P2PE zertifiziertes Bezahlterminal direkt zum Zahlungsdienstleister übertragen. Es erfolgt keine elektronische Speicherung von Kreditkartendaten.	POS / Point of Sale / Bezahlterminal (Kreditkarte liegt vor)
D (für Händler)	Kreditkartendaten werden vom Händler elektronisch entgegengenommen, verarbeitet und/oder gespeichert. Alternativ greift dieser Fragebogen, wenn keiner der vorab genannten SAQ auf die Umgebung des Händlers zutrifft.	E-Commerce oder MOTO / Mail Order Telephone Order (Kreditkarte liegt nicht vor) oder POS / Point of Sale / Bezahlterminal (Kreditkarte liegt vor)

Unterstützung durch die usd AG

Wir empfehlen die Nutzung der PCI DSS Plattform der usd AG (https://pci.usd.de/). Die Registrierung auf der Plattform ist kostenfrei. Auf der Plattform wird der zutreffende SAQ pro Akzeptanzkanal durch einen Auswahl-Assistenten ermittelt. Anschließend wird der ermittelte SAQ online beantwortet.

Sollten Sie bei der PCI DSS Einstufung Ihres Unternehmens, bei der Beantwortung des SAQ und/oder bei sonstigen Fragen Unterstützung benötigen, helfen Ihnen unsere Sicherheitsexperten gerne, beispielsweise durch eines unserer Beraterpakete (Kapitel 2.1.1). Unser kleines und mittleres Beratungspaket wird in der Regel per Telefon durchgeführt. Das große Beraterpaket kann auf Wunsch bei Ihnen vor Ort durchgeführt werden.

Wussten Sie schon…?

…nach aktuellen Untersuchungen lassen sich **54% der erfolgreichen Hackerangriffe auf Verwundbarkeiten in Netzwerkkomponenten und Servern** zurückzuführen. Webapplikationen geraten jedoch immer häufiger in den Fokus und sollten deshalb unbedingt auf typische Schwachstellen überprüft werden. Wir unterstützen Sie gerne dabei mit einem Security Scan oder einem Pentest.

2.3.2 PCI DSS Audit

Das Audit ist ein formaler Prüfprozess. Ein Auditor führt das PCI DSS Audit auf Basis des Standards in der aktuellen Version durch. Die formalen Audit-Prozeduren sind durch das PCI SSC vorgegeben und können auf den offiziellen Webseiten eingesehen werden (http://www.pcisecuritystandards.org).

Der verantwortliche Auditor prüft hierbei alle für PCI DSS relevanten Sachverhalte. Das Audit erfolgt in Form von Interviews mit den verantwortlichen Mitarbeitern, Begehungen von relevanten Örtlichkeiten, Dokumentenreviews und der technischen Prüfung aller relevanten IT-Systeme und Applikationen. Händler, welche im Level 1 und 2 eingestuft sind, sind einmal jährlich aufgefordert, ein Audit durchzuführen (siehe Kapitel 1.3).

Unterstützung durch die usd AG

Zum Beginn der PCI DSS Zertifizierung stimmt ein Auditor der usd mit verantwortlichen Ansprechpartnern Ihres Unternehmens die zu prüfende Audit-Umgebung (Audit Scope) ab. Der konkrete Prüfumfang und Ablauf wird im Abschluss mit Ihnen im Detail festgelegt. Die Ergebnisse werden in Form eines Prüfplans inklusive einer Auflistung aller Audit-Sitzungen und Prüfthemen von der usd dokumentiert und Ihnen zur Verfügung gestellt. Während des Audits ist die Mitwirkung des zuständigen Betriebspersonals notwendig.

Bereits während des Audits und bis zu vier Wochen danach haben Sie die Möglichkeit, vorhandene Abweichungen zum PCI DSS zu korrigieren. Hierzu dokumentiert die usd AG die Ergebnisse des Audits tagesaktuell inklusive ggf. notwendiger, konkreter Maßnahmenempfehlungen zur Korrektur der identifizierten Abweichungen. Anschließend führt die usd eine selektive Nachprüfung durch.
Zum Nachweis der Compliance bei den Kreditkartenorganisationen bzw. der verantwortlichen Händlerbank (Acquirer), erstellt die usd AG gemäß den formalen Vorgaben des PCI Councils sowie unter Berücksichtigung Ihrer PCI DSS Einstufung einen Report on Compliance und die Attestation of Compliance.

Der finale Auditbericht wird von einem zweiten Auditor der usd qualitätsgesichert. Nach der Qualitätssicherung reicht die usd AG den Auditbericht gemeinsam mit der Attestation of Compliance (AoC) bei der zuständigen Händlerbank ein.

Mit erfolgreicher Zertifizierung stellt Ihnen die usd AG ein PCI DSS Zertifikat im PDF-Format aus. Zusätzlich können Sie über die usd PCI DSS Plattform (http://pci.usd.de) ein Prüfsiegel zur Verwendung in Ihrem Onlineshop herunterladen.

Das sagen unsere Kunden.

zalando

Herr Benjamin Pannier, Managing Director Zalando Payments GmbH:

„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“.

2.4 Erhaltung der PCI DSS Compliance

Auch nach dem erfolgreichen Abschluss der Zertifizierung gilt es, die Sicherheitsanforderungen des PCI DSS im Betrieb einzuhalten. Darüber hinaus müssen Versionsänderungen im PCI DSS Standard sowie Änderungen an Infrastruktur, Prozessen und Organisationsstrukturen konform zu den PCI DSS Anforderungen umgesetzt werden.

Unterstützung durch die usd AG

Nach der PCI DSS Zertifizierung bietet die usd AG eine Beratungsleistung zur Erhaltung Ihrer PCI DSS Compliance an. Dadurch können Sie auf Berater der usd zurückgreifen und die Einhaltung der PCI DSS Anforderungen im Betrieb und bei sonstigen Änderungen in Form von vierteljährlichen Vor-Ort-Workshops überprüfen lassen. Die sich daraus ergebenden Maßnahmen zur Erhaltung Ihrer PCI DSS Compliance werden gemeinsam mit Ihnen besprochen.

Welche Vorteile haben Sie von der Zertifizierung?

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:

- Identifizierung von Risiken bei der Verarbeitung von Kreditkarten- und sonstigen Kundendaten
- Sie demonstrieren Ihren Kunden, dass Sie die Sicherheit der Kundendaten ernst nehmen
- Zusätzlich verbessern Sie Ihren Schutz vor finanziellen Haftungs-risiken, Rechtskosten und Kosten zur Beweissicherung
- Sie vermeiden negative Schlagzeilen in der Presse

3 Kontakt

Wie erreichen Sie uns?

Sie haben Fragen zu unseren PCI DSS Leistungen. Sprechen Sie uns persönlich an. Unser Vertrieb steht Ihnen per Telefon unter +49 6102 8631 190 oder per E-Mail an vertrieb@usd.de zur Verfügung.

Wir freuen uns auf die Zusammenarbeit mit Ihnen.