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)

Kreditkartendaten sind ein sehr begehrtes Ziel für Kriminelle. Sie lassen sich besonders in kleineren Unternehmen leicht erbeuten und relativ unkompliziert 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.

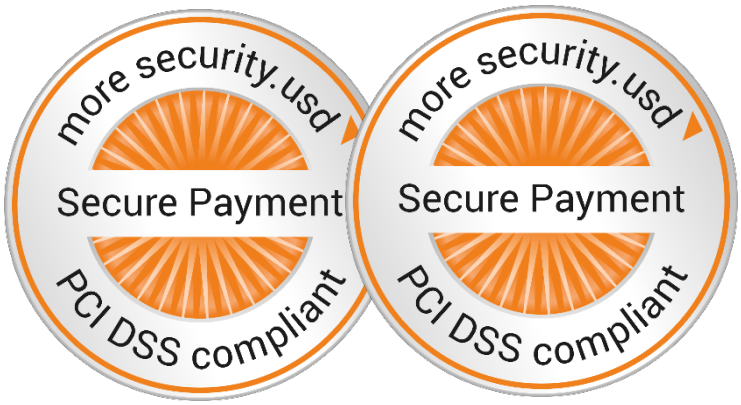
Wird ein Diebstahl von Kreditkarteninformationen aufgedeckt, so zieht dies zunächst einmal kostspielige Untersuchungen nach sich. Dem folgen Schadensersatzansprüche und Strafzahlungen. Zu guter Letzt sorgt die Veröffentlichung des Vorfalls durch die Presse zu einer Rufschädigung, die kaum noch zu beheben ist. Das Vertrauen der Kunden schwindet und die Geschäftstätigkeit trägt einen nachhaltigen Schaden davon.

Die Kreditkartenindustrie hat sich daher im Oktober 2004 weltweit als erste und einzige Branche zusammengeschlossen und das Payment Card Industry Security Standards Council (PCI SSC) gegründet. Durch die im Anschluss stattfindende Vereinheitlichung der Sicherheitsleitlinien der einzelnen Kreditkartenorganisationen entstand schließlich 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 eigenen PCI DSS Konformität kann bei Bekanntwerden von Kreditkartendiebstahl die Haftungsfrage erheblich beeinflussen. Dazu muss allerdings bewiesen werden, dass zum Zeitpunkt des Zwischenfalls alle notwendigen Maßnahmen des PCI DSS umgesetzt und befolgt wurden.

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).


more security. usd
Secure Payment
PCI DSS compliant
more security. usd
Secure Payment
PCI DSS compliant

1.1. Worauf haben es Kriminelle abgesehen?

Im Zentrum des Interesses stehen nicht die physischen Karten selbst, sondern die Kreditkartendaten. Diese befinden sich auf der Karte, zum einen in Form von Beschriftung, zum anderen gespeichert auf Chip und Magnetstreifen.

1) Chip
2) Kartennummer (Primary Account Number, PAN)
3) Gültigkeitsdatum
4) Name des Karteninhabers
5) Magnetstreifen
6) Kartenvalidierungscode, Prüfziffer

Die von Kriminellen begehrten Informationen sind vor allem der Name des Karteninhabers, das Gültigkeitsdatum, die Kreditkartennummer (PAN) sowie die Prüfziffer (CVC2/CVV2/…). Ist man im Besitz dieser Informationen, kann man – z.B. im Internet – auf Kosten des eigentlichen Karteninhabers Zahlungen tätigen. In einigen wenigen Fällen reicht sogar die Kartennummer (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.

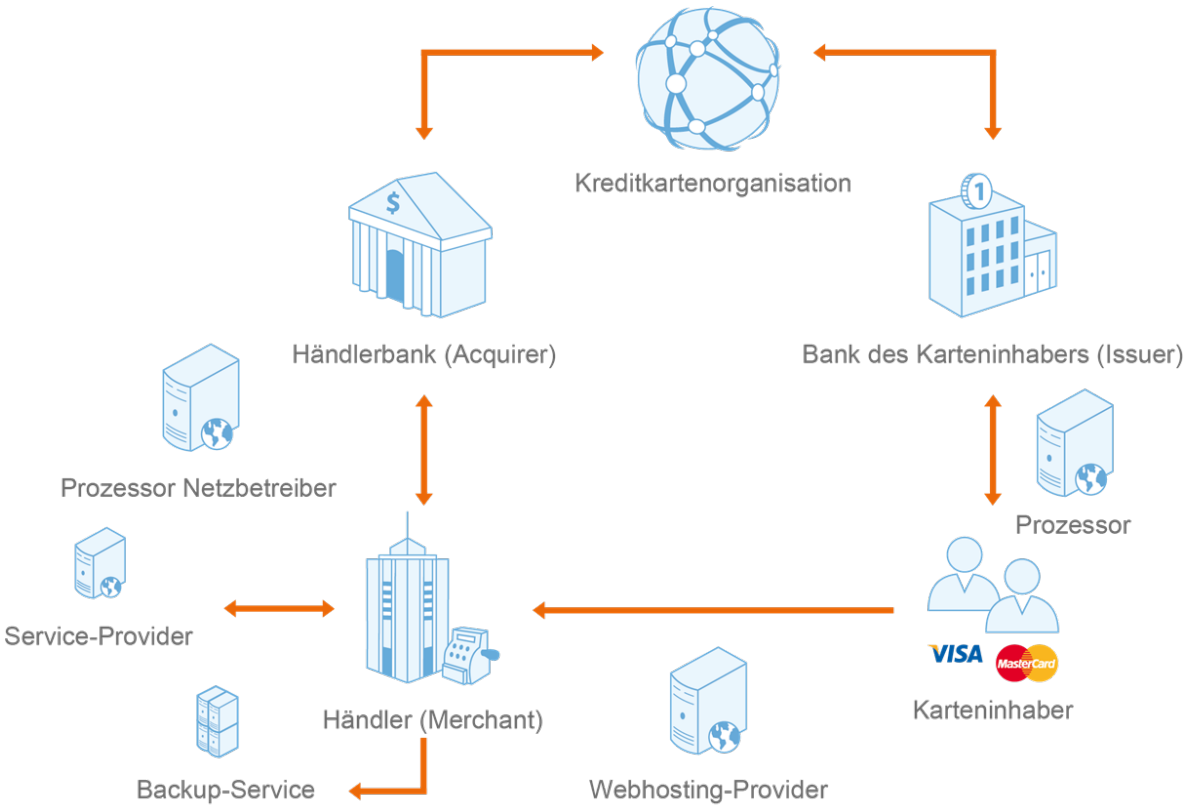
Häufig nutzen Kreditkartendiebe die erbeuteten Daten aber nicht selbst, sondern verkaufen sie weiter. Für gestohlene Kreditkartendaten gibt es einen organisierten Schwarzmarkt im Internet. Das Risiko für die Kriminellen ist dabei vergleichsweise gering. Sie sind meist bestens organisiert und agieren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

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

1.2. Was ist PCI DSS Compliance?

Es gibt keine gesetzliche Verpflichtung zur Einhaltung des PCI DSS. Dennoch ist PCI DSS ein verbindlicher Standard. Das heißt, alle Unternehmen, die Kreditkartendaten speichern, verarbeiten oder übertragen, müssen sich an den Standard halten. Die Vorgabe kommt nicht vom Gesetzgeber, sondern von den Kreditkartenorganisationen selbst. Diese fordern einen Nachweis über die sogenannte PCI DSS Compliance, also die Konformität mit dem Standard. 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. 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. Einige typische Service Provider bei Bezahltransaktionen in der Kreditkartenindustrie sind in der folgenden Abbildung zu sehen. 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.



Kreditkartenbezahlprozess und beteilige Parteien

1.3. Welche Einstufungen und Prüfmethoden sind vorgegeben?

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	Alle Händler mit mehr als 6 Millionen Transaktionen pro Jahr
2	50.000 bis 2,5 Millionen Transaktionen pro Jahr	1 Millionen bis 6 Millionen Transaktionen pro Jahr	Alle Händler mit 1 Millionen bis 6 Millionen Transaktionen pro Jahr
3	< 50.000 Transaktionen pro Jahr	20.000 bis 1 Millionen E-Commerce-Transaktionen pro Jahr	E-Commerce-Händler mit 20.000 bis 1 Millionen Transaktionen pro Jahr
4	-	Alle sonstigen Händler	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 Mio. Transaktionen p.a.	> 300.000 Transaktionen pro Jahr	> 300.000 Transaktionen pro Jahr
2	50.000 bis 2,5 Mio. Transaktionen p.a.	< 300.000 Transaktionen pro Jahr	< 300.000 Transaktionen pro Jahr

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

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

Als akkreditierter Auditor 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.

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 6 Kontrollziele, die sich in 12 Kapitel mit insgesamt 334 Einzelanforderungen aufgliedern. Der Standard umfasst dabei sowohl technische als auch organisatorische und dokumentarische Anforderungen.

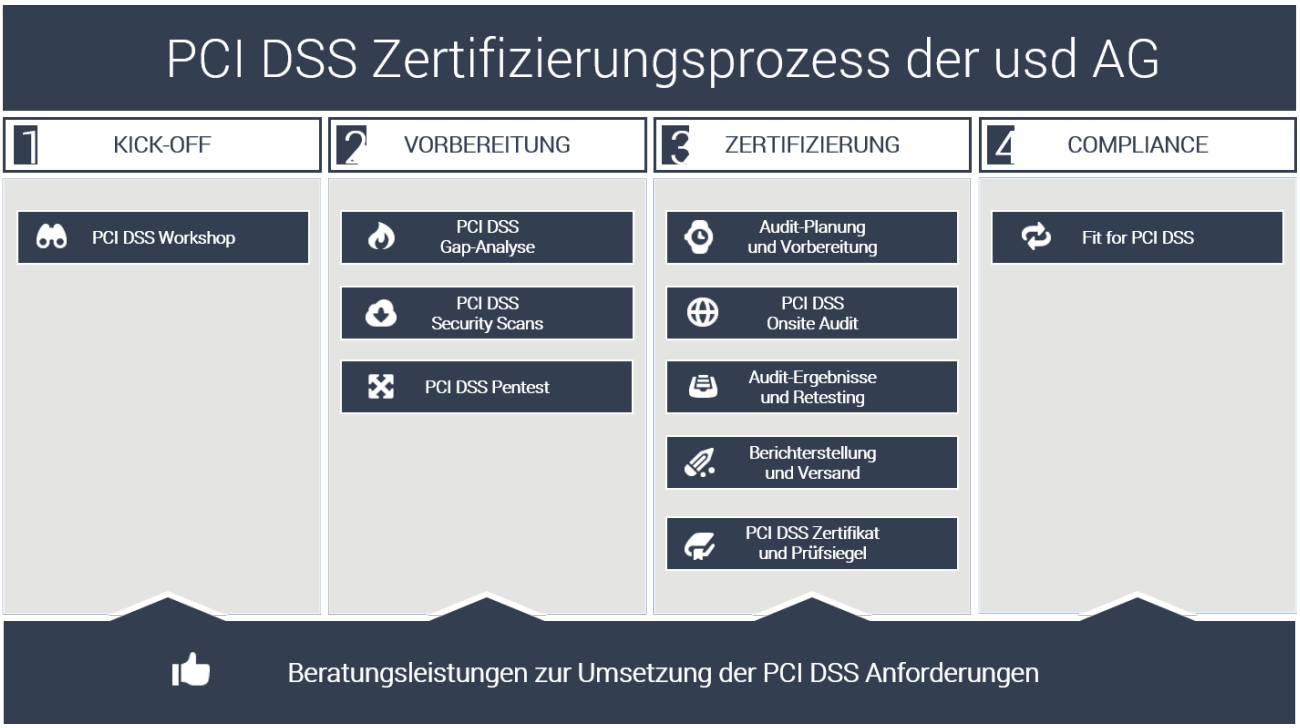
Kontrollziel	Nr.	Kapitel
Aufbau und Betrieb eines sicheren Netzwerkes	**1**	Betrieb einer Firewall-Umgebung
	2	Vermeidung von herstellerspezifischen Standards für Systempasswörter und andere Sicherheitseinstellungen
Schutz der Kreditkartendaten	**3**	Schutz gespeicherter Kreditkartendaten
	4	Verschlüsselte Übermittlung von Kreditkarten- und anderen sensiblen Informationen über öffentliche Netzwerke
Management von Schwachstellen	**5**	Benutzung und regelmäßige Aktualisierung von Antivirus-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

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

2. PCI DSS Zertifizierungsprozess der usd AG

Wir schützen Unternehmen und ihre Kunden vor Hackern und Kriminellen. Wir verstehen es daher als unsere Aufgabe, Sie auf dem Weg zur erfolgreichen PCI DSS Zertifizierung bestmöglich zu begleiten.

Unsere PCI DSS Sicherheitsprüfungen basieren auf den Vorgaben des PCI Security Standards Council und gliedern sich in die folgenden Phasen:



2.1. Kick-off

Im Rahmen eines initialen Workshops wird der Auftraggeber in die Inhalte des PCI DSS eingeführt. Hierbei wird die Anwendbarkeit der einzelnen PCI DSS Anforderungen mit dem Auftraggeber besprochen, der Audit Scope definiert und die nächsten Schritte zur Erreichung der PCI DSS Compliance werden gemeinsam festgelegt.

2.2. Vorbereitung

Zur Vorbereitung auf die PCI DSS Zertifizierung wird die Einhaltung der Anforderungen von usd während einer Gap-Analyse geprüft. Der Auftraggeber hat dadurch die Möglichkeit, vorhandene Abweichungen in Prozessen und Infrastruktur frühzeitig zu erkennen und vor der offiziellen PCI DSS Zertifizierung zu korrigieren. Darüber hinaus bietet usd an, die vierteljährlichen externen und internen PCI DSS Security Scans sowie den jährlichen Pentest durchzuführen.

2.3. Zertifizierung

Die PCI DSS Zertifizierung erfolgt in Form eines Onsite Audits durch einen Auditor der usd. Der konkrete Prüfumfang und Ablauf wird vorab mit dem Auftraggeber festgelegt. Das Audit ist ein formaler Prüfprozess, bei dem die Umsetzung der PCI DSS Anforderungen beim Auftraggeber geprüft wird. Die Ergebnisse des Onsite Audits dokumentiert usd inklusive ggf. notwendiger Maßnahmenempfehlungen. Der Auftraggeber korrigiert vorhandene Abweichungen zum PCI DSS. Im Anschluss führt usd eine selektive Nachprüfung (Retesting) durch. Parallel erstellt usd den offiziellen Auditbericht. Nach Freigabe durch den Auftraggeber wird der Bericht zum Review von usd an die Kreditkartenorganisationen versendet. Nach dem erfolgreichen Nachweis der Compliance erhält der Auftraggeber von usd ein PCI DSS Zertifikat sowie ein Prüfsiegel für die eigene Webseite.

2.4. Compliance

Nach der PCI DSS Zertifizierung wird der Auftraggeber von usd bei dem fortlaufenden Erhalt der Compliance durch vierteljährliche Workshops unterstützt. Für den PCI DSS relevante Änderungen beim Auftraggeber, gleichermaßen wie Änderungen am Sicherheitsstandard selbst, werden gemeinsam besprochen und sich daraus ergebende Maßnahmen zur Erhaltung der PCI DSS Compliance diskutiert.

2.5. Übergreifende Beratungsleistungen

Phasenübergreifend bietet usd individuelle Beratungsleistungen zur Umsetzung der PCI DSS Anforderungen an. Zu unseren Leistungen gehören beispielsweise die Beratung zur schnellen und effizienten Erreichung der Compliance, zur Reduktion des Audit Scopes, zur Bewertung von technischen und organisatorischen Maßnahmen, zur Unterstützung bei der Erstellung von notwendigen Konzepten, Lösungen oder Prozessen sowie ein Security Awareness Training für Mitarbeiter.

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:

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

3. Leistungsbeschreibungen

Die Leistungen der usd werden in den nachfolgenden Kapiteln im Detail beschrieben und erläutert.

3.1. PCI DSS Workshop

Ein Auditor der usd führt im Rahmen eines Vor-Ort-Termins einen PCI DSS Workshop mit technischen und organisatorischen Ansprechpartnern des Auftraggebers durch.

Ziel des Workshops ist die Einführung in die Inhalte sowie die Vermittlung und Definition der konkreten Prüfungsanforderungen des PCI DSS im Kontext der Gegebenheiten des Auftraggebers.

Die folgenden Themen werden während des Workshops behandelt:

- Einführung in den PCI DSS
- Vorstellung der konkreten PCI DSS Anforderungen an den Auftraggeber
- 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 des Pentest Scopes
- Identifikation von Maßnahmen zur Minimierung des Prüfumfangs sowie der Zertifizierungsmaßnahmen (z.B. Netzwerk-Segmentierung, End-to-End-Encryption)
- Verbindliche Definition des PCI DSS Prüfumfangs (Audit Scope)
- Entwicklung einer Zertifizierungsstrategie und Planung des weiteren Vorgehens

Im Verlauf des Workshops stellt der Auftraggeber dafür seine Unternehmensstruktur, Service- und Geschäftsprozesse, Kreditkartendatenflüsse und die zu betrachtenden IT-Systeme und Applikationen vor.

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

Auf Wunsch werden spezielle Themengebiete und Fragen aufgegriffen und von usd erläutert bzw. gemeinsam mit dem Auftraggeber diskutiert.

3.2. PCI DSS Gap-Analyse

Die Gap-Analyse dient zur Vorbereitung des Auftraggebers auf die PCI DSS Zertifizierung. Ziel der Prüfung ist es, Abweichungen zum PCI DSS frühzeitig, im Idealfall lange vor der eigentlichen Zertifizierung, zu erkennen und Lösungen zur Korrektur zu diskutieren.

Insbesondere bei initialen PCI DSS Zertifizierungen, bei signifikanten Änderungen an bereits zertifizierten Kundenumgebungen oder einem Versionswechsel im Sicherheitsstandard empfiehlt sich die Durchführung einer PCI DSS Gap-Analyse. Die PCI DSS Gap-Analyse erfolgt im Rahmen eines Vor-Ort-Termins. Ein Auditor der usd und die verantwortlichen Ansprechpartner beim Auftraggeber prüfen die IT-Systeme, Applikationen, Dokumentation, Prozesse und Örtlichkeiten hinsichtlich der Erfüllung des PCI DSS.

Die Validierung erfolgt hauptsächlich in Form von Interviews der verantwortlichen Mitarbeiter zu den 12 Kapiteln des PCI DSS und in Form von Dokumentenanalysen. Auf Wunsch prüfen wir außerdem die relevanten IT-Systeme und Applikationen auf ihre PCI DSS Compliance und führen eine Vor-Ort-Begehung entsprechender Örtlichkeiten durch. Der konkrete Ablauf der Gap-Analyse wird in Abstimmung mit dem Auftraggeber festgelegt.

Abweichungen zum Standard werden von usd im Rahmen eines detaillierten Maßnahmenkatalogs zur Korrektur der identifizierten Schwachstellen dokumentiert. Eventuelle Fragen des Auftraggebers werden von usd beantwortet.

3.3. PCI DSS Security Scans

Der PCI DSS fordert im Requirement 11.2 die Durchführung von externen und internen Netzwerk-, Betriebssystem- und Applikations-Vulnerability Scans aller relevanten IT-Systeme (Netzwerke, Server, Clients usw.) mindestens einmal im Quartal und nach signifikanten Änderungen.

Die PCI DSS Security Scans der usd umfassen folgende Leistungen:

- Mit einem normierten, international anerkannten Verfahren werden die relevanten IT-Systeme des Auftraggebers auf viele tausend bekannte und ständig aktualisierte Schwachstellen automatisiert überprüft.
- Die PCI DSS Security Scans werden je IP-Adresse durchgeführt, erkannte Schwachstellen werden nicht ausgenutzt. Eine Gefährdung des ordnungsgemäßen Betriebs der geprüften IT-Systeme ist nahezu ausgeschlossen.
- Das Scanergebnis wird in Form einer Management Summary sowie eines umfassenden technischen Berichts von usd in englischer Sprache dokumentiert. Dieser enthält alle gefundenen Schwachstellen sowie detaillierte Vorschläge zu deren Behebung.
- Bei externen PCI DSS Security Scans kann der Auftraggeber innerhalb von vier Wochen durch kostenlose Re-Scans prüfen, ob die ggf. identifizierten Schwachstellen erfolgreich beseitigt wurden.
- Werden keine nach PCI DSS kritischen Schwachstellen (mehr) gefunden, ist die IT-Infrastruktur PCI DSS compliant.

Die externen PCI DSS Security Scans bieten wir in unserer Rolle als Approved Scanning Vendor (ASV) über die usd PCI Plattform unter http://pci.usd.de an. Zur Inanspruchnahme der Leistungen gelten die dort aufgeführten allgemeinen Geschäftsbedingungen.

Die internen PCI DSS Security Scans erfolgen wahlweise über eine gesicherte VPN-Verbindung über das Internet oder durch einen IT-Sicherheitsexperten der usd vor Ort beim Auftraggeber.

Aufgrund der außerordentlich dynamischen Bedrohungslage sollten PCI DSS Security Scans regelmäßig durchgeführt werden. Gemäß PCI DSS müssen die externen und internen Scans mindestens alle drei Monate erfolgen.

Vulnerability Management – wann sinnvoll?

Insbesondere bei IT-Infrastrukturen, die mehr als 100 Server und/oder Workstations umfassen, stellen wir häufig fest, dass ein einzelner Schwachstellenscan bereits sehr viele Ergebnisse liefert. Berichte werden dadurch schnell unübersichtlich und die Bearbeitung von Schwachstellen schwerfällig. Hier empfiehlt sich die Implementierung einer Vulnerability Management Lösung. Wir unterstützen Sie gerne dabei.

3.4. PCI DSS Pentest

Im Rahmen der PCI DSS Zertifizierung müssen gemäß Requirement 11.3 die Anforderungen an den Betrieb sicherer IT-Systeme beim Auftraggeber geprüft werden. In diesem Kontext bietet usd an, einen Penetrationstest entsprechend den Anforderungen des PCI DSS (nachfolgend auch „Pentest“) auf Netzwerk-, Betriebssystem- und Applikationsebene durchzuführen.

Anhand des Pentests sollen Schwachstellen und Sicherheitslücken gezielt identifiziert, daraus resultierende Risiken benannt und Wege aufgezeigt werden, 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) sowie
- NIST SP800-115 (Technical Guide to Information Security Testing and Assessment).

Der PCI DSS Pentest erfolgt auf Basis eines Grey-Box-Tests. Dies bedeutet, dass usd spezifische Informationen über die Zielsysteme und Geschäftsanwendungen des Auftraggebers zur Verfügung gestellt bekommt (IP-Adressen, Beschreibung der bereitgestellten Funktionen, Systemarchitektur, Benutzer- und Konfigurationshandbücher usw.).

Gefundene Schwachstellen und Sicherheitslücken werden ausschließlich belegt, mit dem Auftraggeber besprochen und erst auf ausdrücklichen Wunsch ausgenutzt, um direkten Zugriff auf IT-Systeme und Daten zu erlangen. Der Auftraggeber wird täglich über erfolgreiche Angriffe und damit verbundene Schwachstellen informiert.

Kick-off-Meeting:

Die Vorbereitung des Pentests erfolgt im Rahmen eines Kick-off-Meetings mit den technischen und organisatorischen Verantwortlichen des Auftraggebers. Hierbei werden die zu prüfenden IT-Systeme und Applikationen spezifiziert, notwendige Benutzerkonten und Zugriffswege abgestimmt, Ansprechpartner und Eskalationswege definiert und der Testablauf im Detail besprochen.

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 dabei gerne mit einem Security Scan oder einem Pentest.

Pentest auf Netzwerk- und Betriebssystemebene:

Informationen über die Zielsysteme werden im ersten Schritt aktiv ermittelt, indem eine direkte Kommunikation zu den Systemen aufgebaut wird. Das Sicherheitsteam der usd versucht dabei an Credentials, detaillierte Netzwerk-Informationen, aktive Serverdienste sowie deren Version zu gelangen.

Die gesammelten Informationen werden im Folgenden auf ihre Bedeutsamkeit untersucht. Um bewerten zu können, welche der vorliegenden Informationen verlässlich sind, werden die Daten verglichen und bezüglich ihrer Konsistenz geprüft.

Anhand der gewonnen Informationen werden potentielle Schwachstellen auf Netzwerk- und Betriebssystemebene identifiziert. Daraufhin wird versucht, die identifizierten Schwachstellen auszunutzen, um aktiv Zugriff auf die Zielsysteme und gespeicherte Daten zu erlangen. Dafür werden die Zielsysteme einem manuellen Pentest unterzogen. Abhängig von dem jeweiligen Dienst kombiniert unser Sicherheitsteam dabei manuelle Prüfverfahren mit Standard-Tools für Pentests.

Pentest auf Applikationsebene:

Im Rahmen des Pentests werden die relevanten Applikationen des Auftraggebers auf Schwachstellen und Verwundbarkeiten überprüft. Das Sicherheitsteam der usd versucht hierbei, unautorisierten Zugriff auf vertrauliche Informationen und auch darunterliegende IT-Systeme zu erlangen.

Der Pentest erfolgt üblicherweise in zwei Phasen:

- Innerhalb der ersten Phase wird die Perspektive eines unautorisierten Nutzers nachgebildet. Der Pentest erfolgt von „außen“ (ohne ein gültiges Benutzerkonto) und stellt das typische Angriffsszenario eines Hackers dar.
- In der zweiten Phase stellt der Auftraggeber gültige Benutzerkonten zur Verfügung, um den Pentest autorisiert durchzuführen.

Klassische Problemstellungen in Webapplikationen und Webservices wie Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), SQL-Injections, Directory Traversal oder Code Injections werden vom Sicherheitsteam der usd identifiziert.

Darüber hinaus werden, soweit möglich, die Sicherheitsfunktionen der zu prüfenden Applikationen umgangen und Fehler in der Business-/Applikationslogik ausgenutzt. Dazu zählen beispielsweise die Prüfung der Benutzer-Authentifizierung sowie des Session Managements, die Eskalation von Benutzerrechten, Passwortangriffe auf potentielle Benutzerkonten, das Ausnutzen ungesicherter Administrationsschnittstellen oder die Provokation von Buffer Overflows und die Eskalation von Systemrechten.

Berichterstellung und Abschlussmeeting:

Nach Abschluss der Untersuchung wird das Sicherheitsteam der usd über das Ergebnis der erbrachten Leistungen schriftlich berichten. 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 dem Auftraggeber diskutiert und besprochen. Auf offene Fragen des Auftraggebers wird im Rahmen des Abschlussmeetings jederzeit eingegangen.

3.5. PCI DSS Auditplanung und Vorbereitung

Zunächst stimmen ein Auditor der usd und die verantwortlichen Ansprechpartner des Auftraggebers den zu prüfenden Audit Scope gemeinsam ab. Im Anschluss wird auf dieser Basis der konkrete Ablauf des Onsite Audits im Detail festgelegt. Die Ergebnisse werden in Form eines Prüfplans inklusive einer Auflistung aller Audit Sessions und Prüfthemen von usd dokumentiert und dem Auftraggeber zur Verfügung gestellt.

3.6. PCI DSS Onsite Audit

Ein Auditor der usd führt das PCI DSS Onsite 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).

Das Onsite Audit ist ein formaler Prüfprozess. Der verantwortliche Auditor prüft hierbei alle für PCI DSS relevanten Sachverhalte. Das Onsite Audit erfolgt in Form von Interviews mit den verantwortlichen Mitarbeitern, Begehungen von relevanten Örtlichkeiten, Dokumentenreviews und technischer Prüfungen aller relevanten IT-Systeme und Applikationen.

Nachfolgend aufgeführt sind die zu prüfenden Kapitel des PCI DSS, die sich jeweils in Einzelrichtlinien konkretisieren:

1) Betrieb einer Firewall-Umgebung
2) Vermeidung von herstellerspezifischen Standards für Systempasswörter und andere Sicherheitseinstellungen
3) Schutz gespeicherter Kreditkartendaten
4) Verschlüsselung bei der Übermittelung von Kreditkartendaten über öffentliche Netze
5) Benutzung und regelmäßige Aktualisierung von Antivirus-Software
6) Entwicklung und Pflege sicherer Systeme und Anwendungen
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
10) Überwachung und Nachverfolgung jeglicher Zugriffe auf Netzwerkressourcen und Kreditkartendaten
11) Regelmäßige Tests der Sicherheitssysteme und -prozesse
12) Pflege einer Richtlinie, die Informationssicherheit adressiert

Die Mitwirkung des zuständigen Betriebspersonals ist während des Onsite Audits notwendig.

3.7. PCI DSS Auditergebnisse und Retesting

Mitarbeiter sind aufgrund der Prüfungssituation nervös und vergessen relevante Informationen im Interview. IT-Systeme wurden kurz vor dem Audit installiert und entsprechen noch nicht den PCI DSS Vorgaben. Anwendungen loggen unbeabsichtigt sensitive Kreditkartendaten ohne das Wissen des Auftraggebers.

Unsere Erfahrungen aus einer Vielzahl erfolgreicher PCI DSS Zertifizierungen haben gezeigt, dass trotz umfangreicher Vorbereitungen dennoch während des Onsite Audits weitere Abweichungen zum PCI DSS festgestellt werden.

Identifizierte Abweichungen stellen dabei keinesfalls einen Grund zum Nichtbestehen der PCI DSS Zertifizierung dar. Der Auftraggeber hat bereits während des Onsite Audits und bis zu vier Wochen danach die Möglichkeit, korrigierende Maßnahmen zu implementieren.

Hierzu dokumentiert usd die Ergebnisse des Audits tagesaktuell inklusive ggf. notwendiger, konkreter Maßnahmenempfehlungen zur Korrektur der identifizierten Abweichungen. Anhand dieser Dokumentation korrigiert der Auftraggeber die Abweichungen. Danach führt usd eine selektive Nachprüfung durch.

3.8. PCI DSS Berichterstellung und Versand

Zum Nachweis der Compliance bei der Kreditkartenorganisation bzw. dem verantwortlichen Acquirer erstellt usd gemäß den formalen Vorgaben des PCI Councils sowie unter Berücksichtigung der PCI DSS Einstufung des Auftraggebers einen formalen Auditbericht.[1]

Mit diesem Auditbericht wird die Umsetzung der einzelnen PCI DSS Anforderungen beim Auftraggeber beschrieben und die Vorgehensweise des Auditors zur Überprüfung der jeweiligen Anforderung für die Kreditkartenorganisationen dokumentiert.

Der finale Auditbericht wird von einem zweiten Auditor der usd qualitätsgesichert. Dieser Schritt gewährleistet dem Auftraggeber, dass die Compliance-Bestätigung ohne Rückfragen der Kreditkartenorganisationen und damit verbundener Verzögerungen direkt nach dem Einreichen des Auditberichts erfolgt.

Nach der Qualitätssicherung reicht usd den Auditbericht gemeinsam mit der Attestation of Compliance (AoC) bei den Kreditkartenorganisationen ein.

3.9. PCI DSS Zertifikat und Prüfsiegel

Mit erfolgreicher Zertifizierung stellt usd dem Auftraggeber ein PCI DSS Zertifikat im PDF-Format aus. Zusätzlich erhält der Auftraggeber über die usd PCI DSS Plattform unter http://pci.usd.de ein Prüfsiegel zur Verwendung auf der eigenen Internetpräsenz. Das Aussehen und die Sprache des Prüfsiegels können über die usd PCI DSS Plattform angepasst werden.

Das PCI DSS Prüfsiegel der usd ist bereits bei tausenden namhaften Unternehmen im Einsatz und wird monatlich rund 5 Millionen Mal über das Internet abgerufen.

[1] Level 1-Händler sowie Level 1-Dienstleister erhalten einen Report on Compliance (RoC), während Level 2-Dienstleister sowie Level 2-4 Händler üblicherweise einen Self Assessment-Questionnaire (SAQ) erhalten. Auf Wunsch erstellen wir einen RoC auch für diese Levels.

3.10. Fit for PCI DSS

Mit „Fit for PCI DSS“ bietet die usd ein Beratungspaket zum unterjährigen Erhalt der PCI DSS Compliance an. Auch nach dem erfolgreichen Abschluss der Zertifizierung gilt es, die Sicherheitsanforderungen des PCI DSS im Betrieb einzuhalten. Darüber hinaus müssen Änderungen an Infrastruktur, Prozessen und Organisationsstrukturen des Auftraggebers konform zu den PCI DSS Anforderungen umgesetzt werden.

Hierfür können die verantwortlichen Ansprechpartner des Auftraggebers 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 besprechen und überprüfen lassen.

3.11. PCI DSS Beratungsleistungen der usd

Gerne unterstützen wir den Auftraggeber in allen Phasen bei der Erreichung der PCI DSS Compliance durch individuelle Beratungsleistungen. Welche Aufgaben dabei von den Beratern der usd bearbeitet werden, wird flexibel und nach Bedarf gemeinsam festgelegt.

Zu unseren Leistungen gehören beispielsweise die Beratung zur schnellen und effizienten Erreichung der Compliance, zur Reduktion des Audit Scopes, zur Bewertung von technischen und organisatorischen Maßnahmen, zur Unterstützung bei der Erstellung von notwendigen Konzepten, Lösungen oder Prozessen.
Nachfolgend beschrieben sind drei weitere Beispiele für konkrete Beratungsleistungen der usd im Umfeld des PCI DSS.

<u>Bereitstellung eines PCI DSS Policy Sets:</u>
Unternehmen sind im Rahmen der PCI DSS Compliance dazu verpflichtet, die IT-Infrastruktur, Kreditkartendatenflüsse, vorhandene Sicherheitsprozesse, Konfigurationsstandards usw. in Form von Richtlinien und Dokumentation formal festzuschreiben und einmal jährlich zu aktualisieren.

Genau dafür hat die usd ein PCI DSS Policy Set entwickelt. Mithilfe dieser Dokumentenvorlagen unterstützt die usd den Auftraggeber bei der initialen Erstellung aller für den PCI DSS relevanten Richtlinien.

Zum PCI DSS Policy Set gehören beispielsweise ein Konfigurationsstandard für Firewalls und Router (Req. 1.1), eine Passwortrichtlinie (Req. 8.5), Besucherregelungen (Req. 9.2.a, 9.4) und eine Informationssicherheitsrichtlinie (Req. 12.1, 12.3, 12.4, 12.5).

Die bereitgestellten Dokumente entsprechen grundsätzlich den Anforderungen des PCI DSS, müssen allerdings im Nachgang vom Auftraggeber an die eigenen Rahmenbedingungen angepasst werden.

Interne PCI DSS Reviews:

Ein Auditor der usd führt die im PCI DSS Requirement 12.11 geforderten internen Reviews vierteljährlich durch. Im Rahmen dessen wird die Einhaltung der nachfolgenden Prozesse von usd überprüft:

- Durchführung von täglichen Log-Reviews
- Durchführung von Firewall Rule-Set Reviews
- Anwendung von Konfigurationsstandards auf neue Systeme
- Reaktion auf Security Alerts
- Einhaltung von Change Management Prozessen

Die Validierung der Prozesse erfolgt durch Interviews mit den verantwortlichen Mitarbeitern des Auftraggebers, Dokumentenanalysen und der Prüfung von relevanten IT-Systemen.

Abweichungen vom PCI DSS werden von usd dokumentiert und dem Auftraggeber in Form eines detaillierten Maßnahmenkatalogs zur Korrektur der identifizierten Schwachstellen zur Verfügung gestellt. Eventuelle Rückfragen des Auftraggebers werden durch usd beantwortet.

Der Auftraggeber korrigiert im Anschluss die identifizierten Abweichungen anhand der Maßnahmenempfehlungen der usd. Daraufhin führt usd eine selektive Nachprüfung durch. Dies dient insbesondere der Vermeidung von aufkommenden Rückfragen durch den zuständigen Auditor bei dem jährlich stattfindenden Onsite Audit. Abschließend erstellt usd für jedes Review einen Ergebnisbericht, der die Einhaltung der Anforderungen des Requirement 12.11 bestätigt.

Die Durchführung der internen PCI DSS Reviews erfolgt in Form von Vor-Ort-Workshops oder mittels Telefon- und Webkonferenzen.

Online Security Awareness Training für Mitarbeiter:

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, FAIT oder MaRisk – regelmäßige, dokumentierte Awareness Schulungen aller Mitarbeiter sind Pflicht.

Mit der Online Security Awareness Plattform erhält der Auftraggeber ein flexibel nutzbares Instrument zur regelmäßigen Durchführung von Online Sicherheitstrainings inklusive zugehöriger Erfolgskontrolle für seine Mitarbeiter. Nachweispflichten zur Durchführung von Security Awareness Trainings, wie zum Beispiel Requirement 12.6 des Payment Card Industry Data Security Standards (PCI DSS), werden mit den Reporting-Funktionen der Plattform erfüllt.

Secure Coding Advanced Seminar für Entwickler und Administratoren:

Anwendungen geraten immer häufiger in den Fokus von Kriminellen und stellen die Ursache zahlreicher aktueller Sicherheitsvorfälle dar. Die Sicherheit auf der Anwendungsebene gewinnt damit zunehmend an Bedeutung.

Neben den typischen Sicherheitsaspekten wie der Authentisierung und der Verschlüsselung gehört beispielsweise die Validierung von Eingabe- und Ausgabewerten zu den elementaren Sicherheitsvorkehrungen in heutigen Anwendungen.

Im Kampf gegen diese neuen Bedrohungen spielt die Implementierung von Sicherheitsmaßnahmen in den Entwicklungs-, Test- und Betriebsprozess sowie die Schulung der verantwortlichen Softwareentwickler und Administratoren im Hinblick auf Secure Coding Aspekte sowie die Härtung von IT-Systemen eine entscheidende Rolle.
Im Rahmen eines Vor-Ort-Seminars vermittelt ein Referent der usd den Teilnehmern das Wissen, Bedrohungen und Risiken frühzeitig zu erkennen und einzuschätzen sowie Applikationen nachhaltig sicher zu entwickeln und zu betreiben.

Wie erreichen Sie uns?

Sie haben Fragen zu unseren Pentests. Sprechen Sie uns persönlich an. Unser Vertrieb steht Ihnen per Telefon unter +49 6102 86310 oder per E-Mail an vertrieb@usd.de zur Verfügung.

Wir freuen uns auf die Zusammenarbeit mit Ihnen.