more security. usd

Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS)

Beratungs- und Zertifizierungsleistungen der usd AG

Vertraulich

Inhaltsverzeichnis

1 PCI PA-DSS Zertifizierungsprozess der usd AG

Wir schützen Unternehmen vor Hackern und Kriminellen. Wir verstehen es daher als unsere Aufgabe, Sie auf dem Weg zur erfolgreichen PCI PA-DSS Zertifizierung bestmöglich zu begleiten. Unsere PCI PA-DSS Sicherheitsprüfungen basieren auf den Vorgaben des PCI Security Standards Council (PCI Council) und gliedern sich in die folgenden Phasen:

1.1 Kick-off

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

1.2 Vorbereitung

Zur Vorbereitung auf die PCI PA-DSS Zertifizierung wird die Einhaltung der Anforderungen von usd während einer Gap-Analyse geprüft. Der Auftraggeber hat dadurch die Möglichkeit, vorhandene Abweichungen in der Software, in den wesentlichen Prozessen für Entwicklung sowie den weiteren relevanten Prozessen im PA-DSS Kontext (z.B. Auslieferung von Patches/Updates und Schwachstellenmanagement), Test, Deployment und Support sowie in der dazugehörigen Dokumentation frühzeitig zu erkennen und vor der offiziellen PCI PA-DSS Zertifizierung zu korrigieren. Darüber hinaus bietet usd an, die Software auf technische Schwachstellen und Verwundbarkeiten mittels eines Pentests zu prüfen und die Softwareentwickler und Verantwortlichen im QA-Bereich im Hinblick auf sichere Softwareentwicklung und nicht-funktionale Sicherheitstests zu schulen.

1.3 Zertifizierung

Die PCI PA-DSS Zertifizierung erfolgt in Form eines On-site 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 PA-DSS Anforderungen beim Auftraggeber geprüft wird. Die Ergebnisse des On-site Audits dokumentiert usd inklusive ggf. notwendiger Maßnahmenempfehlungen. Der Auftraggeber korrigiert vorhandene Abweichungen zum PCI PA-DSS. Im Anschluss an die Korrektur der Abweichungen führt usd die Nachprüfung (Re-testing) durch. Parallel erstellt usd den offiziellen Auditbericht. Nach Freigabe durch den Auftraggeber wird der Bericht zum Review von usd an das PCI Council versendet. Nach der Freigabe durch das PCI Council erhält der Auftraggeber von usd ein PCI PA-DSS Zertifikat sowie ein Prüfsiegel für die eigene Webseite.

1.4 Compliance

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

1.5 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.

2 Leistungsbeschreibungen

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

2.1 PCI PA-DSS Workshop

Ein Auditor der usd führt im Rahmen eines Vor-Ort-Termins einen PCI PA-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 PA-DSS im Kontext der Gegebenheiten des Auftraggebers.

Die folgenden Themen werden während des Workshops behandelt:

- Einführung in den PCI PA-DSS
- Vorstellung der konkreten PCI PA-DSS Anforderungen an den Auftraggeber
- Identifikation der zu zertifizierenden Softwaremodule, Geschäfts- und Entwicklungsprozesse und Bereiche
- Verbindliche Definition des PCI PA-DSS Prüfumfangs (Audit Scope)
- Entwicklung einer Zertifizierungsstrategie und Planung des weiteren Vorgehens

Im Verlauf des Workshops stellt der Auftraggeber dafür seine zu prüfenden Applikationen und deren Softwaremodule, dazugehörige Unternehmensprozesse zur Entwicklung, Qualitätssicherung, Deployment und Support vor.

Anhand dieser Informationen zeigt usd die Zertifizierungsrelevanz der Applikationen, Softwaremodule und Prozesse auf, macht auf direkt erkennbare Abweichungen zum PCI PA-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.

2.2 PCI PA-DSS Gap-Analyse

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

Insbesondere bei initialen PCI PA-DSS Zertifizierungen, bei signifikanten Änderungen an bereits zertifizierten Applikationen oder einem Versionswechsel im Sicherheitsstandard empfiehlt sich die Durchführung einer PCI PA-DSS Gap-Analyse.

Die Gap-Analyse erfolgt im Rahmen eines Vor-Ort-Termins. Ein Auditor der usd und die verantwortlichen Ansprechpartner beim Auftraggeber prüfen die relevanten Applikationen und Softwaremodule, Dokumentationen und Prozesse hinsichtlich der Erfüllung des PCI PA-DSS.

Die Validierung erfolgt hauptsächlich in Form von Interviews der verantwortlichen Mitarbeiter zu den 14 Kapiteln des PCI PA-DSS und in Form von Dokumentenanalysen. Auf Wunsch prüfen wir außerdem die relevanten Applikationen auf ihre PCI PA-DSS Compliance. Der konkrete Ablauf der Gap-Analyse wird in Abstimmung mit dem Auftraggeber festgelegt.

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

2.3 PCI PA-DSS Pentest

Im Rahmen der PCI PA-DSS Zertifizierung müssen die relevanten Applikationen im Rahmen eines Pentests auf Schwachstellen und Sicherheitslücken überprüft werden. In diesem Kontext bietet usd zur Vorbereitung auf das On-site Audit an, einen Penetrationstest entsprechend den Anforderungen des PCI PA-DSS (nachfolgend auch „Pentest“) auf Applikationsebene durchzuführen.

Anhand des Pentests sollen Schwachstellen und Sicherheitslücken gezielt identifiziert, daraus resultierende Risiken benannt und Wege aufgezeigt werden, die Sicherheit der geprüften 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 PA-DSS Pentest erfolgt auf Basis eines Grey-Box-Tests. Dies bedeutet, dass usd spezifische Informationen über die Geschäftsanwendungen des Auftraggebers zur Verfügung gestellt bekommt (Beschreibung der bereitgestellten Funktionen, Softwarearchitektur, 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 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** zurückführen. 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 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 besprochen. Auf offene Fragen des Auftraggebers wird im Rahmen des Abschlussmeetings jederzeit eingegangen.

2.4 Secure Coding Advanced Seminar

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- und Testprozessen sowie die Schulung der verantwortlichen Softwareentwickler im Hinblick auf Secure Coding Aspekte eine entscheidende Rolle.

Gemäß PCI PA-DSS Requirement 5.1.7 vermittelt ein Referent der usd im Rahmen eines Vor-Ort-Seminars den Teilnehmern das Wissen, das sie benötigen, um Bedrohungen und Risiken frühzeitig zu erkennen und einzuschätzen sowie Applikationen nachhaltig sicher zu entwickeln und zu betreiben. Alternativ bieten wir Ihnen die Möglichkeit, Ihre Entwickler über unsere Security Awareness Plattform durch das Trainingsmodul „Secure Coding Online“ zu sensibilisieren.

2.5 Audit Planung 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 On-site 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.

2.6 PCI PA-DSS On-site Audit

Ein akkreditierter Auditor der usd führt das PCI PA-DSS On-site Audit auf Basis des Standards in der aktuellen Version 3.2 (veröffentlich im Mai 2016) durch. Die Audit-Prozeduren sind durch das PCI Council vorgegeben und können auf den offiziellen Webseiten unter http://www.pcisecuritystandards.org eingesehen werden.

Das On-site Audit ist ein formaler Prüfprozess. Der verantwortliche Auditor prüft hierbei alle für den PCI PA-DSS relevanten Sachverhalte. Das On-site Audit erfolgt in Form von Dokumentenanalysen, Interviews mit den verantwortlichen Mitarbeitern sowie durch Prüfung der relevanten Prozesse und Softwaremodule auf allen erforderlichen Betriebsplattformen.

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

1) Keine Speicherung von sensitiven Daten (Magnetstreifen, CVV2 oder PIN/PIN-Block)
2) Schutz gespeicherter Kreditkartendaten
3) Bereitstellung sicherer Authentisierungsmechanismen
4) Protokollierung von Vorgängen innerhalb der Anwendungen
5) Entwicklung sicherer Anwendungen
6) Schutz von drahtloser Kommunikation
7) Test der Anwendung auf Schwachstellen und Bereitstellung von Patches
8) Ermöglichen einer sicheren Netzwerk-Konfiguration
9) Keine Speicherung von Kreditkartendaten auf vom Internet erreichbaren Systemen
10) Ermöglichen eines sicheren Remote-Zugriffs auf die Anwendung
11) Verschlüsselung sensitiver Daten bei Netzwerkübertragungen
12) Verschlüsselung aller Remote-Administrationszugriffe
13) Pflege des PCI PA-DSS Implementation Guide
14) Verantwortlichkeiten für PCI PA-DSS Compliance und Betriebsdokumentation sowie Trainingsprogramme für Mitarbeiter, Kunden, Reseller und Integratoren

Die Mitwirkung der Entwickler und des Supports ist während des On-site Audits, insbesondere für die Prüfung der Software, notwendig.

2.7 Auditergebnisse und Retesting

Eine mögliche Ursache für Findings können beispielsweise fehlende bzw. unvollständige Dokumente sein. Die Analyse und ein Pentest der zu prüfenden Anwendung kann die unbeabsichtigte Speicherung von sensitiven Daten oder Schwachstellen aufzeigen.

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

Identifizierte Abweichungen stellen dabei keinesfalls einen Grund zum Nichtbestehen der PCI PA-DSS Zertifizierung dar. Der Auftraggeber hat bereits während des On-site Audits und auch 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 Nachprüfung der korrigierten Abweichungen durch.

2.8 Berichterstellung und Versand

Zum Nachweis der Compliance bei dem PCI Security Standards Council erstellt der Auditor der usd gemäß den Vorgaben des PCI PA-DSS den Report on Validation (RoV).

Mit diesem Auditbericht wird die Umsetzung der einzelnen PCI PA-DSS Anforderungen beim Auftraggeber beschrieben und die Vorgehensweise des Auditors zur Überprüfung der jeweiligen Anforderung für das PCI Security Standards Council dokumentiert.

Der finale Auditbericht wird von einem zweiten Auditor der usd qualitätsgesichert, bevor dieser an das PCI Security Standards Council übermittelt wird. Das Council prüft innerhalb von 30 Kalendertagen nach Zahlungseingang den finalen Auditbericht.

2.9 PCI PA-DSS Zertifikat und Prüfsiegel

Nach Freigabe des Auditberichts durch das PCI Council wird die Anwendung als validierte Bezahlanwendung auf der Seite des PCI Councils veröffentlicht. Ergänzend dazu stellt usd dem Auftraggeber ein PCI PA-DSS Zertifikat im PDF-Format aus. Zusätzlich stellt usd ein PCI PA-DSS Prüfsiegel zur Verwendung auf der Internetpräsenz des Auftraggebers zur Verfügung.

Das usd PCI PA-DSS Prüfsiegel kann zum Nachweis der Compliance gegenüber Kunden eingesetzt werden und das Vertrauen in die Qualität der Anwendung und die Sicherheit der verarbeiteten Daten verbessern.

2.10 Fit for PCI PA-DSS

Mit „Fit for PCI PA-DSS“ bietet die usd ein Beratungspaket zum Erhalt der PCI PA-DSS Compliance an. Auch nach dem erfolgreichen Abschluss der Zertifizierung gilt es, die Sicherheitsanforderungen des PCI PA-DSS im Entwicklungsprozess und bei der Kundenbetreuung einzuhalten. Darüber hinaus müssen Änderungen an der Software und an dazugehörigen Prozessen zur Qualitätssicherung und Deployment des Auftraggebers konform zu den PCI PA-DSS Anforderungen umgesetzt werden.

Hierfür können die verantwortlichen Ansprechpartner des Auftraggebers auf Berater der usd zurückgreifen und die Einhaltung der PCI PA-DSS Anforderungen im Betrieb und bei sonstigen Änderungen in Form von vierteljährlichen Vor-Ort-Workshops besprechen und überprüfen lassen.

2.11 Re-Zertifizierung von Softwareänderungen

Änderungen an zertifizierten Anwendungen können durch eine Re-Zertifizierung geprüft und veröffentlicht werden. Ein Auditor der usd führt hierzu eine gemeinsame Bewertung der Änderung sowie eine angepasste Re-Zertifizierung durch und übernimmt anschließend auch die Übermittlung der Ergebnisse an das PCI Council. Wir unterstützen Sie bei sämtlichen Arten von Änderungen gemäß PCI PA-DSS Program Guide (High Impact, Low Impact, No Impact, Administrative).

2.12 PCI PA-DSS Beratungsleistungen der usd

Gerne unterstützen wir den Auftraggeber in allen Phasen bei der Erreichung der PCI PA-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 und zur Unterstützung bei der Erstellung von notwendigen Konzepten, Lösungen oder Prozessen.

Wie erreichen Sie uns?

Sie haben Fragen zu unseren Leistungen und Produkten?
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.