TOPCERTIFIER
www.topcertifier.com

SERVICE-METHODE PCI DSS

Datensicherheitsstandard der Zahlungskartenindustrie.

TOPCERTIFIER
www.topcertifier.com

EINFÜHRUNG PCI DSS

TOPCertifier präsentiert eine vereinfachte PCI-DSS-Lückenanalyse-Checkliste, die Ihnen bei der Identifizierung hilft Bereiche, in denen Ihr Unternehmen möglicherweise Verbesserungen benötigt, um PCI DSS (Payment) einzuhalten Anforderungen des Card Industry Data Security Standard). Diese Checkliste bietet eine grundlegende Rahmen zur Bewertung Ihrer Ausrichtung auf PCI DSS und dient als erster Schritt Beurteilung Ihrer Compliance.

ABSCHNITT 1: DATENSICHERHEIT

- Werden die Zahlungskartendaten bei der Übertragung und Speicherung ordnungsgemäß verschlüsselt
- Sensible Authentifizierungsdaten, wie z. B. CVV-Nummern, werden nach der Autorisierung nicht gespeichert
- Gibt es eine Richtlinie zum Schutz von Karteninhaberdaten und sensiblen Authentifizierungsdaten

ABSCHNITT 2: NETZWERK- UND FIREWALL-SICHERHEIT

- Werden Netzwerkkonfigurationen und Firewall-Regeln regelmäßig überprüft und aktualisiert
- Gibt es ein Netzwerkdiagramm, das den Fluss der Karteninhaberdaten veranschaulicht
- Sind Sicherheitsrichtlinien und -verfahren zur Sicherung der Netzwerkinfrastruktur vorhanden

ABSCHNITT 3: ZUGRIFFSKONTROLLE

- Sind die Zugriffsrechte der Benutzer auf der Grundlage geschäftlicher Notwendigkeiten eingeschränkt
- ist eine Multi-Faktor-Authentifizierung für den Fernzugriff auf das Netzwerk implementiert
- Werden Benutzerkonten bei Beendigung oder Rollenwechsel umgehend deaktiviert

ABSCHNITT 4: VULNERABILITÄTSMANAGEMENT

- Werden Sicherheitspatches umgehend angewendet, um Schwachstellen zu beheben
- Gibt es einen Prozess für Schwachstellenscans und Penetrationstests
- Werden kritische Sicherheitspatches überprüft und nach Risiko priorisiert

ABSCHNITT 5: SICHERHEITSRICHTLINIEN UND -VERFAHREN

- Werden umfassende Sicherheitsrichtlinien und -verfahren dokumentiert und verbreitet
- Gibt es ein Sicherheitsbewusstseinsschulungsprogramm für Mitarbeiter
- Werden Sicherheitsrichtlinien überprüft und bei Bedarf aktualisiert

ABSCHNITT 6: ÜBERWACHUNG UND PROTOKOLLIERUNG

- Werden Sicherheitsereignisse und Protokolle regelmäßig überprüft und überwacht
- Gibt es einen Prozess zur Durchführung von Echtzeitwarnungen bei verdächtigen Aktivitäten
- Sind Vorfallreaktions- und Meldeverfahren eingerichtet

ABSCHNITT 7: REAKTION AUF VORFÄLLE

- Gibt es einen Plan zur Reaktion auf Vorfälle, in dem die Schritte zur Bewältigung von Sicherheitsvorfällen dargelegt sind
- Sind die Mitarbeiter darin geschult, Sicherheitsvorfälle zu erkennen und zu melden
- Gibt es einen dokumentierten Prozess für die Analyse und Verbesserung nach einem Vorfall

ABSCHNITT 8: PHYSIKALISCHE SICHERHEIT

- Sind physische Zugangskontrollen vorhanden, um unbefugten Zugriff auf Karteninhaberdaten zu verhindern
- ist der Zugang zu sicheren Bereichen eingeschränkt und überwacht
- Werden für sensible Bereiche Videoüberwachung und Besucherprotokolle geführt

ABSCHNITT 9: DRITTANBIETER

- Werden Drittanbieter auf PCI-DSS-Konformität geprüft
- Gibt es schriftliche Vereinbarungen mit Dienstleistern, um den Schutz der Karteninhaberdaten zu gewährleisten
- Gibt es einen Prozess zur Überwachung und Bewertung der Sicherheitspraktiken Dritter

Bitte beachten Sie, dass diese Checkliste einen allgemeinen Überblick bietet und es wichtig ist, eine durchzuführen gründliche Analyse speziell für die Prozesse und den Kontext Ihrer Organisation. Darüber hinaus ist es Es wird empfohlen, mit PCI-DSS-Experten oder -Beratern zusammenzuarbeiten, um eine umfassende Untersuchung durchzuführen Gap-Analyse für Ihr Unternehmen.