



Payment Card Industry (PCI) Datensicherheitsstandard

Anforderungen und Sicherheitsbeurteilungsverfahren

Version 1.2.1

Juli 2009

Dokumentänderungen

Datum	Version	Beschreibung	Seiten
Oktober 2008	1.2	Einführen von PCI DSS v1.2 mit „PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren“, Eliminieren von Redundanzen in den Dokumenten und Durchführen sowohl allgemeiner als auch spezifischer Änderungen an den PCI DSS-Sicherheitsüberwachungsverfahren von Version 1.1. Die vollständigen Informationen finden Sie unter PCI-Datensicherheitsstandard, Zusammenfassung der Änderungen von PCI DSS-Version 1.1 auf 1.2.	
Juli 2009	1.2.1	Hinzufügen eines Satzes, der beim Wechsel von PCI DSS v1.1 auf v1.2 fälschlicherweise gelöscht wurde.	4
		Entfernen der grauen Markierung in den Spalten „Implementiert“ und „Nicht implementiert“ beim Prüfverfahren 6.5b.	35
		Unter „Arbeitsblatt zu Kompensationskontrollen – Beispiel“: Ändern des Wortlauts oben auf der Seite zu: „Mit diesem Arbeitsblatt können Sie die Kompensationskontrollen für jede Anforderung definieren, bei der über Kompensationskontrollen „JA“ ausgewählt wurde.“	68

Inhalt

Dokumentänderungen	1
Einführung und Überblick über den PCI-Datensicherheitsstandard	4
Informationen zur PCI DSS-Anwendbarkeit	5
Umfang der Beurteilung der Konformität mit PCI DSS-Anforderungen	6
<i>Netzwerksegmentierung</i>	6
<i>Drahtlos</i>	7
<i>Dritte/Outsourcing</i>	7
<i>Stichprobenkontrolle von Unternehmenseinrichtungen und Systemkomponenten</i>	7
<i>Kompensationskontrollen</i>	8
Anweisungen und Inhalt des Konformitätsberichts	9
<i>Berichtsinhalt und -format</i>	9
<i>Erneute Validierung offener Punkte</i>	12
<i>PCI DSS-Konformität – Schritte zum Ausfüllen</i>	12
Ausführliche PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren	13
Erstellung und Wartung eines sicheren Netzwerks.....	14
<i>Anforderung 1: Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten</i>	14
<i>Anforderung 2: Ändern der vom Anbieter festgelegten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter</i>	19
Schutz von Karteninhaberdaten.....	22
<i>Anforderung 3: Schutz gespeicherter Karteninhaberdaten</i>	22
<i>Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze</i>	29
Wartung eines Anfälligkeits-Managementprogramms.....	31
<i>Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware</i>	31
<i>Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen</i>	32
Implementierung starker Zugriffskontrollmaßnahmen.....	39
<i>Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf</i>	39
<i>Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff</i>	41
<i>Anforderung 9: Beschränkung des physischen Zugriffs auf Karteninhaberdaten</i>	46
Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken.....	50
<i>Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten</i>	50
<i>Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse</i>	54
Befolgung einer Informationssicherheits -Richtlinie.....	57
<i>Anforderung 12: Befolgung einer Informationssicherheits-Richtlinie für Mitarbeiter und Subunternehmer</i>	57
Anhang A: Zusätzliche PCI DSS-Anforderungen für Anbieter von gemeinsamem Hosting	64
Anhang B: Kompensationskontrollen	67

Anhang C:	Arbeitsblatt zu Kompensationskontrollen	68
Anhang D:	Konformitätsbescheinigung – Händler	70
Anhang E:	Konformitätsbescheinigung – Dienstleister	74
Anhang F:	PCI DSS-Prüfungen – Umfang und Auswahlen von Stichproben	78

Einführung und Überblick über den PCI-Datensicherheitsstandard

Der PCI-Datensicherheitsstandard (DSS) wurde entwickelt, um die Datensicherheit von Karteninhabern zu verbessern und die umfassende Akzeptanz einheitlicher Datensicherheitsmaßnahmen auf der ganzen Welt zu vereinfachen. Das vorliegende Dokument, *PCI-Datensicherheitsstandard - Anforderungen und Sicherheitsbeurteilungsverfahren*, baut auf den zwölf PCI DSS-Anforderungen auf und kombiniert diese mit entsprechenden Prüfverfahren zu einem Sicherheitsbeurteilungstool. Es richtet sich an Prüfer, die Vor-Ort-Prüfungen für Händler und Dienstanbieter durchführen, die die Konformität mit dem PCI DSS validieren müssen. Im Folgenden finden Sie eine übergeordnete Übersicht über die zwölf PCI DSS-Anforderungen. Die nächsten Seiten enthalten Hintergrundinformationen zum Vorbereiten, Durchführen und Dokumentieren einer PCI DSS-Beurteilung, während die ausführlichen PCI DSS-Anforderungen ab Seite 13 erläutert werden.

Überblick über den PCI-Datensicherheitsstandard

Erstellung und Wartung eines sicheren Netzwerks

- Anforderung 1: Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
Anforderung 2: Ändern der vom Anbieter festgelegten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter

Schutz von Karteninhaberdaten

- Anforderung 3: Schutz gespeicherter Karteninhaberdaten
Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze

Wartung eines Anfälligkeits-Managementprogramms

- Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware
Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

Implementierung starker Zugriffskontrollmaßnahmen

- Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf
Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff
Anforderung 9: Beschränkung des physischen Zugriff auf Karteninhaberdaten

Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken

- Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

Befolgung einer Informationssicherheits-Richtlinie

- Anforderung 12: Befolgung einer Informationssicherheits-Richtlinie

Informationen zur PCI DSS-Anwendbarkeit

In der folgenden Tabelle sind häufig verwendete Elemente an Karteninhaberdaten und vertraulichen Authentifizierungsdaten aufgeführt. Außerdem wird für jedes Datenelement angegeben, ob es zulässig oder verboten ist, das Element zu speichern und ob jedes Datenelement geschützt werden muss. Diese Tabelle erhebt keinen Anspruch auf Vollständigkeit, sondern dient dazu, die verschiedenen Arten von Anforderungen darzustellen, die für jedes Datenelement gelten.

Die PCI DSS-Anforderungen gelten, wenn eine Primary Account Number (PAN) gespeichert, verarbeitet oder übertragen wird. Wenn keine PAN gespeichert, verarbeitet oder übertragen wird, gelten die PCI DSS-Anforderungen nicht.

	Datenelement	Speichern zulässig	Schutz erforderlich	PCI DSS Anf. 3.4
Karteninhaberdaten	Primary Account Number (PAN)	Ja	Ja	Ja
	Name des Karteninhabers ¹	Ja	Ja ¹	Nein
	Servicecode ¹	Ja	Ja ¹	Nein
	Ablaufdatum ¹	Ja	Ja ¹	Nein
Vertrauliche Authentifizierungsdaten ²	Vollständige Magnetstreifen­daten ³	Nein	Nicht zutr.	Nicht zutr.
	CAV2/CVC2/CVV2/CID	Nein	Nicht zutr.	Nicht zutr.
	PIN/PIN-Block	Nein	Nicht zutr.	Nicht zutr.

¹ Diese Datenelemente müssen geschützt werden, wenn sie in Verbindung mit der PAN gespeichert werden. Dieser Schutz sollte gemäß den PCI DSS-Anforderungen für den allgemeinen Schutz der Karteninhaberdaten-Umgebung erfolgen. Darüber hinaus kann eine andere Gesetzgebung (z. B. im Zusammenhang mit dem Schutz persönlicher Verbraucherdaten, Datenschutz, Identitätsdiebstahl oder Datensicherheit) einen besonderen Schutz dieser Daten oder die ordnungsgemäße Weitergabe der Verfahren eines Unternehmens erfordern, wenn im Rahmen der Ausübung der geschäftlichen Tätigkeiten verbraucherbezogene persönliche Daten erfasst werden. PCI DSS gilt jedoch nicht, wenn PANs nicht gespeichert, verarbeitet oder übertragen werden.

² Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung nicht gespeichert werden (auch wenn sie verschlüsselt wurden).

³ Vollständige Verfolgungsdaten vom Magnetstreifen, Magnetstreifenabbild auf dem Chip oder einem anderen Speicherort.

Umfang der Beurteilung der Konformität mit PCI DSS-Anforderungen

Die PCI DSS-Sicherheitsanforderungen gelten für alle Systemkomponenten. „Systemkomponenten“ sind gemäß Definition alle Netzwerkkomponenten, Server oder Anwendungen, die in der Karteninhaberdaten-Umgebung enthalten oder damit verbunden sind. Die Karteninhaberdaten-Umgebung ist der Bestandteil des Netzwerks, der Karteninhaberdaten oder vertrauliche Authentifizierungsdaten beinhaltet. Netzwerkkomponenten umfassen unter anderem Firewalls, Switches, Router, Zugriffspunkte für drahtlose Netzwerke, Netzwerkgeräte und andere Sicherheitsgeräte. Servertypen beinhalten unter anderem: Web, Anwendung, Datenbank, Authentifizierung, Mail, Proxy, Network Time Protocol (NTP) und Domain Name Server (DNS). Anwendungen umfassen alle erworbenen und benutzerdefinierten Anwendungen, darunter auch interne und externe (Internet-)Anwendungen.

Netzwerksegmentierung

Die Netzwerksegmentierung oder Isolierung (Segmentierung) der Karteninhaberdaten-Umgebung vom Rest des Unternehmensnetzwerks ist keine PCI DSS-Anforderung. Sie wird jedoch als Methode empfohlen, die unter Umständen Folgendes verringert:

- Den Umfang der PCI DSS-Beurteilung
- Die Kosten der PCI DSS-Beurteilung
- Die Kosten und Schwierigkeiten der Implementierung und Verwaltung von PCI DSS-Kontrollen
- Das Risiko für ein Unternehmen (wird durch die Konsolidierung von Karteninhaberdaten in weniger, stärker kontrollierte Speicherorte verringert)

Ohne eine adäquate Netzwerksegmentierung (die manchmal als „flaches Netzwerk“ bezeichnet wird), befindet sich das gesamte Netzwerk im Umfang der PCI DSS-Beurteilung. Die Netzwerksegmentierung kann durch interne Netzwerk-Firewalls, Router mit umfassenden Zugriffssteuerungslisten oder anderer Technologie erreicht werden, die den Zugriff auf ein bestimmtes Segment eines Netzwerks einschränkt.

Eine wichtige Voraussetzung, um den Umfang der Karteninhaberdaten-Umgebung zu verringern, ist ein klares Verständnis der Unternehmensanforderungen und -prozesse im Hinblick auf das Speichern, die Verarbeitung oder Übertragung von Karteninhaberdaten. Die Einschränkung von Karteninhaberdaten auf möglichst wenig Speicherorte durch die Beseitigung nicht erforderlicher Daten und die Konsolidierung erforderlicher Daten erfordert unter Umständen die Überarbeitung bewährter Unternehmensverfahren.

Das Dokumentieren von Karteninhaberdaten-Datenflüssen über ein Datenflussdiagramm erleichtert das vollständige Verständnis aller Karteninhaberdaten-Datenflüsse und gewährleistet, dass eine beliebige Netzwerksegmentierung beim Isolieren der Karteninhaberdaten-Umgebung in Kraft tritt.

Wenn die Netzwerksegmentierung implementiert ist und verwendet wird, um den Umfang der PCI DSS-Beurteilung zu verringern, muss der Prüfer überprüfen, dass sich die Segmentierung für diesen Zweck eignet. Auf einer übergeordneten Ebene isoliert eine geeignete Netzwerksegmentierung Systeme, die Karteninhaberdaten speichern, verarbeiten oder übertragen, von Systemen, die dies nicht tun. Die Eignung einer spezifischen Implementierung der Netzwerksegmentierung variiert jedoch in hohem Maße und hängt von verschiedenen Faktoren ab, wie

z. B. der Konfiguration eines bestimmten Netzwerks, den eingesetzten Technologien und anderen Kontrollmechanismen, die unter Umständen implementiert werden.

Anhang F: PCI DSS-Prüfungen – Umfang und Auswählen von Stichproben bietet weitere Informationen zu den Auswirkungen, die das Festlegen des Umfangs während einer PCI DSS-Beurteilung hat.

Drahtlos

Wenn drahtlose Technologie zum Speichern, Verarbeiten oder Übertragen von Karteninhaberdaten (z. B. Point-Of-Sale-Transaktionen, „Line-Busting“) verwendet wird oder wenn ein drahtloses Local Area Network (LAN) mit der Karteninhaberdaten-Umgebung oder einem Teil davon (der beispielsweise nicht eindeutig durch eine Firewall abgegrenzt ist) verbunden ist, gelten die PCI DSS-Anforderungen und Prüfverfahren für drahtlose Umgebungen und müssen ebenfalls ausgeführt werden (z. B. Anforderung 1.2.3, 2.1.1 und 4.1.1). Bevor drahtlose Technologie implementiert wird, sollte ein Unternehmen den Bedarf an der Technologie sorgfältig gegen die Risiken abwägen. Sie sollten den Einsatz drahtloser Technologie nur für die Übertragung nicht vertraulicher Daten in Erwägung ziehen.

Dritte/Outsourcing

Für Dienstanbieter, die sich einer jährlichen Vor-Ort-Beurteilung unterziehen müssen, muss eine Konformitätsvalidierung auf allen Systemkomponenten vorgenommen werden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden.

Ein Dienstanbieter oder Händler beauftragt unter Umständen einen Fremdanbieter damit, Karteninhaberdaten zu speichern, verarbeiten oder übertragen oder Komponenten wie Router, Firewalls, Datenbanken, physische Sicherheit und/oder Server zu verwalten. In diesem Fall kann es zu Auswirkungen auf die Sicherheit der Karteninhaberdaten-Umgebung kommen.

Für die Stellen, die die Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten an Drittdienstanbieter auslagern, muss der Konformitätsbericht (Report on Compliance, ROC) die Rolle jedes Dienstanbieters dokumentieren und eindeutig identifizieren, welche Anforderungen für die geprüfte und welche für den Dienstanbieter gelten. Es gibt zwei Möglichkeiten, mit denen Drittdienstanbieter die Konformität validieren können: 1) Sie können sich selbst einer PCI DSS-Beurteilung unterziehen und ihren Kunden die entsprechenden Konformitätsnachweise vorlegen, oder 2) wenn sie sich keiner eigenen PCI DSS-Beurteilung unterziehen, müssen sie ihre Services im Lauf der PCI DSS-Beurteilungen jedes ihrer Kunden prüfen lassen. Weitere Informationen finden Sie in Teil 3 im Abschnitt „Anweisungen und Inhalt des Konformitätsberichts“ in der Aufzählung, die mit „Für MSP-Prüfungen (Managed Service Provider)“ beginnt.

Darüber hinaus müssen Händler und Dienstanbieter die PCI DSS-Konformität aller zugehörigen Dritten mit Zugriff auf Karteninhaberdaten verwalten und überwachen. *Einzelheiten finden Sie in Anforderung 12.8 in diesem Dokument.*

Stichprobenkontrolle von Unternehmenseinrichtungen und Systemkomponenten

Der Prüfer kann repräsentative Stichproben aus Unternehmenseinrichtungen und Systemkomponenten auswählen, um PCI DSS-Anforderungen zu beurteilen. Diese Stichproben müssen Unternehmenseinrichtungen und Systemkomponenten umfassen, müssen eine repräsentative Auswahl

aller Typen und Standorte von Unternehmenseinrichtungen sowie der Typen von Systemkomponenten darstellen und müssen groß genug sein, um dem Prüfer die Sicherheit zu geben, dass Kontrollmechanismen erwartungsgemäß implementiert werden.

Beispiele für Unternehmenseinrichtungen sind Büroräume, Läden, Franchise-Händler und Unternehmenseinrichtungen an verschiedenen Standorten. Die Stichprobenkontrolle sollte Systemkomponenten für jede Unternehmenseinrichtung umfassen. Nehmen Sie beispielsweise für jede Unternehmenseinrichtung verschiedene Betriebssysteme, Funktionen und Anwendungen auf, die für den zu prüfenden Bereich gelten. In jeder Unternehmenseinrichtung sollte der Prüfer Sun-Server unter Apache WWW, Windows-Server unter Oracle, Mainframe-Systeme unter Legacy-Anwendungen zur Kartenverarbeitung, Datenübertragungsserver unter HP-UX und Linux-Server unter MYSQL wählen. Wenn alle Anwendungen von einem einzigen Betriebssystem (z. B. Windows oder Sun) ausgeführt werden, sollte die Stichprobe zumindest verschiedene Anwendungen (z. B. Datenbankserver, Webserver, Datenübertragungsserver) enthalten. (Siehe Anhang F: PCI DSS-Prüfungen – Umfang und Auswählen von Stichproben.)

Beim Auswählen von Stichproben aus Unternehmenseinrichtungen und Systemkomponenten sollten Prüfer die folgenden Punkte beachten:

- Wenn erforderliche PCI DSS-Standardprozesse implementiert sind, die jede Einrichtung befolgen muss, kann die Stichprobe kleiner ausfallen als es ohne Standardprozesse erforderlich ist, um in angemessener Weise zu gewährleisten, dass jede Einrichtung gemäß dem Standardprozess konfiguriert ist.
- Sind mehrere Typen von Standardprozessen implementiert (z. B. für verschiedene Arten von Systemkomponenten oder Einrichtungen) muss die Stichprobe groß genug sein, um Systemkomponenten oder Einrichtungen einzubeziehen, die mit jeder Art von Prozess gesichert sind.
- Wenn keine PCI DSS-Standardprozesse implementiert sind und jede Einrichtung für ihre Prozesse verantwortlich ist, muss die Stichprobe größer sein, um zu gewährleisten, dass jede Einrichtung die PCI DSS-Anforderungen entsprechend versteht und implementiert.

Siehe auch Anhang F: PCI DSS-Prüfungen – Umfang und Auswählen von Stichproben.

Kompensationskontrollen

Alle Kompensationskontrollen müssen jährlich vom Prüfer dokumentiert, geprüft und validiert werden und gemäß *Anhang B: Kompensationskontrollen* und *Anhang C: Arbeitsblatt zu Kompensationskontrollen* in den ROC aufgenommen werden.

Das Arbeitsblatt zu Kompensationskontrollen (Anhang C) **muss** für jede Kompensationskontrolle ausgefüllt werden. Darüber hinaus sollten Kompensationskontrollergenergebnisse im ROC im Abschnitt zur entsprechenden PCI DSS-Anforderung dokumentiert werden.

Einzelheiten zu „Kompensationskontrollen“ finden Sie in Anhang B und C.

Anweisungen und Inhalt des Konformitätsberichts

Dieses Dokument muss als Vorlage zum Erstellen des *Konformitätsberichts* verwendet werden. Die beurteilte Einheit sollte die entsprechenden Reporting-Anforderungen jeder Zahlungsmarke befolgen, um zu gewährleisten, dass jede Zahlungsmarke den Konformitätsstatus der Einheit anerkennt. Setzen Sie sich mit jeder Zahlungsmarke in Verbindung, um Reporting-Anforderungen und Anweisungen zu ermitteln.

Berichtsinhalt und -format

Befolgen Sie die nachstehenden Anweisungen zum Berichtsinhalt und -format, wenn Sie einen Konformitätsbericht erstellen:

1. Executive Summary

Nehmen Sie folgende Punkte auf:

- Beschreibung des Zahlungskartengeschäfts der Einheit, einschließlich:
 - Der Unternehmensrolle mit Zahlungskarten, d. h. wie und warum die Einheit Karteninhaberdaten speichert, verarbeitet und/oder überträgt
Hinweis: Diese Beschreibung sollte nicht einfach von der Website der Einheit übernommen werden, vielmehr sollte es sich um eine maßgeschneiderte Beschreibung handeln, die deutlich macht, dass der Prüfer die Zahlung und die Rolle der Einheit versteht.
 - Der Art und Weise der Zahlungsverarbeitung (direkt, indirekt usw.)
 - Welche Arten von Zahlungskanälen bedient werden, wie beispielsweise „Karte liegt nicht vor“ (z. B. schriftlicher/telefonischer Bestelleingang (MOTO), e-Commerce) oder „Karte liegt vor“
 - Alle Einheiten, die eine Verbindung für die Zahlungsübertragung oder -verarbeitung herstellen, einschließlich Prozessorbeziehungen
- Ein übergeordnetes Netzwerkdiagramm (das aus der Einheit abgerufen oder vom Prüfer erstellt wird) der Networking-Topographie der Einheit, das Folgendes beinhaltet:
 - Verbindungen in das und aus dem Netzwerk
 - Kritische Komponenten in der Karteninhaberdaten-Umgebung, einschließlich POS-Geräte, Systeme, Datenbanken und Webserver
 - Andere erforderliche Zahlungskomponenten

2. Beschreibung des Arbeitsumfangs und des verwendeten Ansatzes

Beschreibung des Umfangs gemäß dem Abschnitt „Umfang der Beurteilung“ im vorliegenden Dokument, einschließlich der folgenden Punkte:

- Umgebung, auf der der Schwerpunkt der Beurteilung lag (z. B. Internet-Zugriffspunkte des Kunden, internes Unternehmenswerk, Verarbeitung von Verbindungen)
- Wenn die Netzwerksegmentierung implementiert ist und eingesetzt wurde, um den Umfang der PCI DSS-Prüfung zu verringern, erläutern Sie diese Segmentierung und wie der Prüfer die Wirksamkeit der Segmentierung validiert hat.
- Dokumentieren und begründen Sie die für beide Einheiten (Speicher, Einrichtungen usw.) und ausgewählten Systemkomponenten verwendete Stichprobenkontrolle, einschließlich:
 - Gesamtpopulation
 - Anzahl der Stichproben
 - Begründung für ausgewählte Stichprobe
 - Angabe, warum die Stichprobengröße ausreicht, damit der Prüfer sich darauf verlassen kann, dass die geprüften Kontrollen Kontrollen darstellen, die in der gesamten Einheit implementiert sind
 - Beschreibung aller Standorte oder Umgebungen, die Karteninhaberdaten speichern, verarbeiten oder übertragen und die aus dem Umfang der Prüfung AUSGESCHLOSSEN wurden und Angabe des Grundes für den Ausschluss dieser Standorte/Umgebungen
- Auflisten aller Einmangesellschaften, die die Konformität mit dem PCI-Datensicherheitsstandard erfordern, und Angabe, ob sie separat oder im Rahmen dieser Beurteilung geprüft werden
- Auflisten aller internationalen Gesellschaften, die die Konformität mit dem PCI-Datensicherheitsstandard erfordern, und Angabe, ob sie separat oder im Rahmen dieser Beurteilung geprüft werden
- Auflisten aller drahtlosen LANs und/oder drahtlosen Zahlungsanwendungen (z. B. POS-Terminals), die mit der Karteninhaberdaten-Umgebung verbunden sind oder sich auf deren Sicherheit auswirken könnten und Beschreiben der für diese drahtlosen Umgebungen implementierten Sicherheit
- Die Version des Dokuments zu den PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren, die zum Durchführen der Beurteilung verwendet wurde
- Zeitrahmen der Beurteilung

3. Details zur geprüften Umgebung

Geben Sie in diesem Abschnitt die folgenden Details an:

- Diagramm jedes Bestandteils der Kommunikationsverbindung, einschließlich LAN, WAN oder Internet
- Beschreibung der Karteninhaberdaten-Umgebung, wie z. B.:
 - Dokumentübertragung und Verarbeitung von Karteninhaberdaten, einschließlich Autorisierung, Erfassung, Verrechnung, Ausgleichsbuchungen und anderer Abläufe

- Auflisten von Dateien und Tabellen, in denen Karteninhaberdaten gespeichert sind, unterstützt von einem erstellten (oder vom Kunden abgerufenen) und vom Prüfer in den Arbeitspapieren verwalteten Bestand. Dieser Bestand sollte für jeden Karteninhaberdaten-Speicher (Datei, Tabelle usw.) Folgendes enthalten:
 - Liste aller Elemente gespeicherter Karteninhaberdaten
 - Angabe, wie Daten gesichert werden
 - Angabe, wie der Zugriff auf Datenspeicher protokolliert wird
- Liste der Hardware und kritischen Software, die in der Karteninhaberdaten-Umgebung eingesetzt wird, sowie einer Beschreibung der Funktion/Nutzung
- Liste der Dienstleister und anderen Einheiten, mit denen das Unternehmen Karteninhaberdaten nutzt (Hinweis: diese Einheiten unterliegen PCI DSS-Anforderung 12.8)
- Liste von verwendeten Drittanbieterzahlungsanwendungen und Versionsnummern, mit der Angabe, ob jede Zahlungsanwendung gemäß PA-DSS validiert wurde. Auch wenn eine Zahlungsanwendung gemäß PA-DSS validiert wurde, muss der Prüfer trotzdem überprüfen, ob die Anwendung auf eine PCI DSS-konforme Art und Weise und in einer PCI DSS-konformen Umgebung und gemäß dem PA-DSS *Implementierungshandbuch des Anwendungsanbieters implementiert wurde. Hinweis: Die Verwendung PA-DSS-validierter Anwendungen ist eine PCI DSS-Anforderung. Bitte erfragen Sie die individuellen PA-DSS-Konformitätsanforderungen bei jeder Zahlungsmarke.*
- Liste der interviewten Personen und deren Titel
- Liste der geprüften Dokumentation
- Für MSP-Prüfungen (Managed Service Provider) muss der Prüfer eindeutig festlegen, welche Anforderungen aus diesem Dokument für den MSP gelten (und in die Prüfung einbezogen werden) und welche Anforderungen nicht in die Prüfung einbezogen werden, da es in diesem Fall den MSP-Kunden obliegt, die Anforderungen in ihren Prüfungen zu berücksichtigen. Aufnehmen von Informationen zu den IP-Adressen des MSP, die im Rahmen der vierteljährlichen Anfälligkeits-Scans des MSP und dazu, welche Adressen von den Kunden des MSP in ihre eigenen vierteljährlichen Scans einbezogen werden müssen.

4. Kontaktinformationen und Berichtsdatum

Nehmen Sie folgende Informationen auf:

- Kontaktinformationen für Händler oder Dienstleister und Prüfer
- Datum des Berichts

5. Ergebnisse des vierteljährlichen Scans

- Fassen Sie die vier letzten Ergebnisse des vierteljährlichen Scans in der Executive Summary sowie in Anmerkungen zu Anforderung 11.2 zusammen.

Hinweis: Es ist für die anfängliche PCI DSS-Konformität nicht erforderlich, dass vier bestandene vierteljährliche Scans abgeschlossen sein müssen, wenn der Prüfer überprüft, dass 1) das letzte Scan-Ergebnis ein positives Ergebnis war, 2) die Einheit

über dokumentierte Richtlinien und Verfahren verfügt, die eine Fortsetzung der vierteljährlichen Scans erfordern, und 3) alle im ersten Scan festgestellten Anfälligkeiten korrigiert wurden, wie in einem erneuten Scan dargestellt. Für die Folgejahre nach der ersten PCI DSS-Prüfung müssen vier bestandene vierteljährliche Scans vorliegen.

- Ein Scan muss alle extern zugänglichen (Internet-Zugang) IP-Adressen, die in der Einheit vorhanden sind, gemäß den PCI DSS-Sicherheitsscanverfahren erfassen.

6. Ergebnisse und Beobachtungen

- Fassen Sie in der Executive Summary alle Ergebnisse zusammen, die möglicherweise nicht in das Standardvorlagenformat des ROC passen.
- Alle Prüfer *müssen* die Vorlage zu den detaillierten PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren verwenden, um detaillierte Berichtsbeschreibungen und Ergebnisse zu jeder Anforderung und Teilanforderung bereitzustellen.
- Der Prüfer *muss* alle Kompensationskontrollen prüfen und dokumentieren, die den Schluss zulassen, dass eine Kontrolle implementiert ist.

Einzelheiten zu „Kompensationskontrollen“ finden Sie im Abschnitt zu Kompensationskontrollen und in Anhang B und C.

Erneute Validierung offener Punkte

Ein Bericht über „implementierte Kontrollen“ ist zur Prüfung der Konformität erforderlich. Der Bericht gilt als nicht implementiert, wenn er „offene Punkte“ enthält oder Punkte, die an einem in der Zukunft liegenden Datum abgeschlossen werden. Der Händler/Dienstleister muss diese Punkte adressieren, bevor die Validierung abgeschlossen wird. Wenn diese Punkte vom Händler/Dienstleister adressiert wurden, führt der Prüfer eine erneute Beurteilung durch um zu validieren, dass alle offenen Punkte geklärt wurden und alle Anforderungen erfüllt werden. Nach der erneuten Validierung stellt der Prüfer einen neuen ROC aus und überprüft, ob die Karteninhaberdaten-Umgebung die Anforderungen vollständig erfüllt und legt den Bericht gemäß den Anweisungen vor (siehe unten).

PCI DSS-Konformität – Schritte zum Ausfüllen

1. Füllen Sie den ROC gemäß vorstehendem Abschnitt „Anweisungen und Inhalt des Konformitätsberichts“ aus.
2. Stellen Sie sicher, dass bestandene Anfälligkeits-Scans von einem PCI SSC Approved Scanning Vendor (ASV) durchgeführt wurden, und holen Sie die Nachweise für die bestandenen Scans beim ASV ein.
3. Füllen Sie die Konformitätsbescheinigung für Dienstleister oder Händler vollständig aus. Konformitätsbescheinigungen finden Sie in Anhang D und E.
4. Reichen Sie den ROC, den Nachweis eines bestandenen Scans und die Konformitätsbescheinigung zusammen mit allen anderen erforderlichen Dokumenten beim Acquirer (Händler) oder bei der Zahlungsmarke oder einer anderen Anforderungsstelle (Dienstleister) ein.

Ausführliche PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren

Die Spaltentitel in der Tabelle für die *PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren* haben folgende Bedeutung:

- **PCI DSS-Anforderungen** – Diese Spalte definiert den Datensicherheitsstandard und listet Anforderungen zum Erreichen der PCI DSS-Konformität auf. Die Konformität wird anhand dieser Anforderungen validiert.
- **Prüfverfahren** – Diese Spalte zeigt Prozesse an, die vom Prüfer zu befolgen sind um zu validieren, dass PCI DSS-Anforderungen „implementiert“ sind.
- **Implementiert** – In dieser Spalte muss der Prüfer eine kurze Beschreibung implementierter Kontrollen eintragen, einschließlich der Kontrollen, die infolge von Kompensationskontrollen implementiert wurden. (Hinweis: dieser Spalte darf *nicht* für Elemente verwendet werden, die noch nicht implementiert sind, oder für offene Punkte, die erst an einem in der Zukunft liegenden Datum abgeschlossen werden.)
- **Nicht implementiert** – In dieser Spalte muss der Prüfer einer kurze Beschreibung von nicht implementierten Kontrollen eintragen. Beachten Sie, dass ein nicht implementierter Bericht nur auf ausdrückliche Anfrage an eine Zahlungsmarke oder einen Acquirer gesendet werden sollte. Weitere Anweisungen zu nicht implementierten Berichten finden Sie in Anhang D und Anhang E: Konformitätsbescheinigungen.
- **Zieldatum/Anmerkungen** – Für die Kontrollen aus der Spalte „Nicht implementiert“ kann der Prüfer ein Zieldatum aufnehmen, bis zu dem der Händler oder Dienstanbieter davon ausgeht, dass die Kontrollen „Implementiert“ sind. Außerdem können hier zusätzliche Hinweise oder Anmerkungen erfasst werden.

Erstellung und Wartung eines sicheren Netzwerks

Anforderung 1: Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten

Firewalls sind Computergeräte, die den zulässigen Datenverkehr zwischen dem Netzwerk eines Unternehmens (intern) und nicht vertrauenswürdigen Netzwerken (extern) sowie den Datenverkehr in und aus vertraulicheren Bereichen innerhalb dem internen vertrauenswürdigen Netzwerk eines Unternehmens kontrollieren. Die Karteninhaberdaten-Umgebung ist ein Beispiel für einen vertraulicheren Bereich innerhalb des vertrauenswürdigen Netzwerks eines Unternehmens.

Eine Firewall untersucht den gesamten Netzwerkverkehr und blockiert die Übertragungen, die die angegebenen Sicherheitskriterien nicht erfüllen. Alle Systeme müssen vor dem unbefugten Zugriff von nicht vertrauenswürdigen Netzwerken geschützt werden, und zwar unabhängig davon, ob Sie über das Internet als E-Commerce, über den Internetzugang der Mitarbeiter über Desktop-Browser, den E-Mail-Zugriff von Mitarbeitern, dedizierte Verbindungen, wie z. B. Business-to-Business-Verbindungen, über drahtlose Netzwerke oder über andere Quellen in das System gelangen. Häufig können scheinbar unbedeutende Wege in und aus nicht vertrauenswürdigen Netzwerken ungeschützte Wege in wichtige Systeme eröffnen. Firewalls sind für jedes Computernetzwerk ein wichtiger Schutzmechanismus.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
1.1 Festlegen von Standards für die Firewall- und Routerkonfiguration, die Folgendes beinhalten:	1.1 Suchen und prüfen Sie die Standards für die Firewall- und Router-Konfiguration und anderer, unten angegebener Dokumentation daraufhin, ob die Standards vollständig sind. Arbeiten Sie folgende Punkte ab:			
1.1.1 Ein offizieller Prozess zur Genehmigung und zum Testen aller Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration	1.1.1 Überprüfen Sie, ob es einen offiziellen Prozess zum Testen und zur Genehmigung aller Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration gibt.			
1.1.2 Ein aktuelles Netzwerkdiagramm mit allen Verbindungen mit Karteninhaberdaten einschließlich aller drahtlosen Netzwerke	1.1.2.a Überprüfen Sie, ob ein aktuelles Netzwerkdiagramm (z. B. ein Diagramm, das Flüsse von Karteninhaberdaten im Netzwerk darstellt) vorhanden ist und alle Verbindungen mit Karteninhaberdaten dokumentiert, einschließlich aller drahtlosen Netzwerke. 1.1.2.b Überprüfen Sie, ob das Diagramm regelmäßig aktualisiert wird.			
1.1.3 Anforderungen für eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone	1.1.3 Überprüfen Sie, ob alle Standards für die Firewall-Konfiguration Anforderungen für eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone enthalten. Überprüfen Sie, ob das aktuelle Netzwerkdiagramm den Standards für die Firewall-Konfiguration entspricht.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
1.1.4 Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die logische Verwaltung der Netzwerkkomponenten	1.1.4 Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration eine Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die logische Verwaltung der Netzwerkkomponenten enthalten.			
1.1.5 Dokumentation und Begründung für den Einsatz aller zulässigen Services, Protokolle und Ports, einschließlich der Dokumentation von Sicherheitsfunktionen für die Protokolle, die als unsicher gelten	1.1.5.a Überprüfen Sie, dass Standards für die Firewall- und Router-Konfiguration eine dokumentierte Liste mit Services, Protokollen und Ports enthalten, die für die Geschäftsausübung erforderlich sind, z. B. Hypertext Transfer Protocol (HTTP) und Secure Sockets Layer (SSL), Secure Shell (SSH) und Virtual Private Network (VPN).			
	1.1.5.b Identifizieren Sie zulässige unsichere Services, Protokolle und Ports, und überprüfen Sie, ob sie erforderlich sind und ob Sicherheitsfunktionen dokumentiert und implementiert wurden, indem für jeden Service die Standards und Einstellungen für die Firewall- und Router-Konfiguration geprüft werden. Ein Beispiel dafür ist FTP, da hier Benutzeranmeldeinformationen als Klartext übertragen werden.			
1.1.6 Anforderung zum Prüfen von Firewall- und Router-Regelsätzen mindestens alle sechs Monate	1.1.6.a Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration mindestens alle sechs Monate eine Prüfung von Firewall- und Router-Regelsätzen erfordern.			
	1.1.6.b Suchen und prüfen Sie Dokumentation, um zu überprüfen, ob die Regelsätze mindestens alle sechs Monate überprüft werden.			
1.2 Aufbauen einer Firewall-Konfiguration, die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der Karteninhaberdaten-Umgebung einschränkt.	1.2 Prüfen Sie Firewall- und Router-Konfigurationen, um wie folgt zu überprüfen, ob Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der Karteninhaberdaten-Umgebung eingeschränkt werden:			
<i>Hinweis: Ein „nicht vertrauenswürdiges Netzwerk“ ist jedes Netzwerk, das außerhalb der Netzwerke liegt, die zu der geprüften Einheit gehören und/oder das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Einheit liegt.</i>				

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
1.2.1 Beschränken des ein- und ausgehenden Netzwerkverkehrs auf den für die Karteninhaberdaten-Umgebung absolut notwendigen Verkehr.	1.2.1.a Überprüfen Sie, ob ein- und ausgehender Netzwerkverkehr auf den für die Karteninhaberdaten-Umgebung notwendigen Verkehr beschränkt wird und ob die Beschränkungen dokumentiert sind.			
	1.2.1.b Überprüfen Sie, ob jeder andere ein- und ausgehende Verkehr eigens abgelehnt wird, z. B. durch die Verwendung einer ausdrücklichen „Alle ablehnen“-Anweisung oder einer impliziten Anweisung zum Ablehnen nach dem Zulassen.			
1.2.2 Sichern und Synchronisieren von Router-Konfigurationsdateien.	1.2.2 Überprüfen Sie, ob Router-Konfigurationsdateien sicher und synchronisiert sind, z. B. sollten ausgeführte Konfigurationsdateien (für die normale Funktion der Router) und Startkonfigurationsdateien (für den Gerätesteuerstart) die gleiche sichere Konfiguration aufweisen.			
1.2.3 Installieren von Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der Karteninhaberdaten-Umgebung und Konfigurieren dieser Firewalls, sodass der gesamte Verkehr aus der drahtlosen Umgebung oder abgelehnt wird oder kontrolliert wird (sofern dieser Verkehr für Geschäftszwecke notwendig ist).	1.2.3 Überprüfen Sie, ob Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und Systemen installiert sind, die Karteninhaberdaten speichern, und ob diese Firewalls den gesamten Verkehr aus der drahtlosen Umgebung in die Karteninhaberdaten-Umgebung ablehnen oder kontrollieren (sofern dieser Verkehr für Geschäftszwecke notwendig ist).			
1.3 Verboten des direkten öffentlichen Zugriffs zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung.	1.3 Überprüfen Sie Firewall- und Router-Konfigurationen gemäß den folgenden Anweisungen, um zu ermitteln, ob es keinen direkten Zugriff zwischen dem Internet und Systemkomponenten gibt, einschließlich des Choke-Routers im Internet, des DMZ-Routers und der Firewall, des DMZ-Karteninhabersegments, des Umkreis-Routers und des internen Karteninhaber-Netzwerksegments.			
1.3.1 Implementieren einer DMZ, um ein- und ausgehenden Verkehr auf Protokolle zu beschränken, die für die Karteninhaberdaten-Umgebung erforderlich sind.	1.3.1 Überprüfen Sie, ob eine DMZ implementiert ist, um ein- und ausgehenden Verkehr auf Protokolle zu beschränken, die für die Karteninhaberdaten-Umgebung erforderlich sind.			
1.3.2 Beschränken des eingehenden Internetverkehrs auf IP-Adressen innerhalb der DMZ.	1.3.2 Überprüfen Sie, ob der eingehende Internetverkehr auf IP-Adressen innerhalb der DMZ beschränkt wird.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
1.3.3 Keine direkten eingehenden oder ausgehenden Routen für Datenverkehr zwischen dem Internet und der Karteninhaberdaten-Umgebung zulassen.	1.3.3 Überprüfen Sie, dass keine direkten eingehenden oder ausgehenden Routen für Datenverkehr zwischen dem Internet und der Karteninhaberdaten-Umgebung vorhanden sind.			
1.3.4 Nicht zulassen, dass interne Adressen aus dem Internet in die DMZ übergeben werden.	1.3.4 Überprüfen Sie, dass interne Adressen nicht aus dem Internet in die DMZ übergeben werden können.			
1.3.5 Beschränken des ausgehenden Datenverkehrs aus der Karteninhaberdaten-Umgebung in das Internet, sodass der ausgehende Verkehr nur auf IP-Adressen innerhalb der DMZ zugreifen kann.	1.3.5 Überprüfen Sie, dass ausgehender Datenverkehr aus der Karteninhaberdaten-Umgebung in das Internet nur auf IP-Adressen innerhalb der DMZ zugreifen kann.			
1.3.6 Implementieren der statusgesteuerten Inspektion, die auch als dynamische Paketfilterung bekannt ist. (Das bedeutet, dass nur „etablierte“ Verbindungen in das Netzwerk zulässig sind.)	1.3.6 Überprüfen Sie, dass die Firewall eine statusgesteuerte Inspektion (dynamische Paketfilterung) durchführt. [Nur etablierte Verbindungen sollten zugelassen werden, und nur, wenn sie mit einer zuvor festgelegten Sitzung verknüpft sind (führen Sie einen Port-Scanner auf allen TCP-Ports mit gesetzten Bits „syn reset“ oder „syn ack“ aus - eine Antwort bedeutet, das Pakete durchgelassen werden, auch wenn sie nicht Bestandteil einer zuvor festgelegten Sitzung sind).]			
1.3.7 Platzieren der Datenbank in einer internen Netzwerkzone, die von der DMZ getrennt ist.	1.3.7 Überprüfen Sie, ob die Datenbank in einer internen Netzwerkzone platziert ist, die von der DMZ getrennt ist.			
1.3.8 Implementieren von IP-Maskierung unter Verwendung des RFC 1918-Adressraums, um zu verhindern, dass interne Adressen übersetzt und im Internet offen gelegt werden können. Verwenden von NAT-Technologien (Network Address Translation), z. B. Port Address Translation (PAT).	1.3.8 Überprüfen Sie für die Stichprobe aus Firewall- und Router-Komponenten, ob NAT oder eine andere Technologie, die den RFC 1918-Adressraum verwendet, eingesetzt wird, um die Übertragung von IP-Adressen aus dem internen Netzwerk in das Internet einzuschränken (IP-Maskierung).			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
1.4 Installieren von persönlicher Firewallsoftware auf allen mobilen und Mitarbeitern gehörenden Computern mit direkter Verbindung mit dem Internet (z. B. Laptops, die von Mitarbeitern verwendet werden), die für den Zugriff auf das Unternehmensnetzwerk eingesetzt werden.	1.4.a Überprüfen Sie, ob auf mobilen und Mitarbeitern gehörenden Computern mit direkter Verbindung mit dem Internet (z. B. Laptops, die von Mitarbeitern verwendet werden), die für den Zugriff auf das Unternehmensnetzwerk eingesetzt werden, persönliche Firewallsoftware installiert und aktiv ist.			
	1.4.b Überprüfen Sie, ob die persönliche Firewallsoftware vom Unternehmen gemäß bestimmter Standards konfiguriert wurde und nicht durch Benutzer mobiler Computer geändert werden kann.			

Anforderung 2: Ändern der vom Anbieter festgelegten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter

Böswillige Personen (in einem Unternehmen und außerhalb) verwenden häufig Standardkennwörter von Anbietern und andere Standardeinstellungen, um Systeme zu beeinträchtigen. Diese Kennwörter und Einstellungen sind in Hacker-Gemeinschaften bekannt und können durch öffentliche Informationen mühelos ausfindig gemacht werden.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>2.1 Ändern der vom Anbieter angegebenen Standardeinstellungen vor jeder Installation eines Systems im Netzwerk - z. B. durch die Einführung von Kennwörtern, SNMP-Community-Zeichenfolgen und Beseitigung nicht benötigter Konten.</p>	<p>2.1 Wählen Sie eine Stichprobe aus Systemkomponenten, kritischen Servern und drahtlosen Zugangspunkten, und versuchen Sie, sich unter Verwendung von vom Anbieter angegebenen Standardkonten und -kennwörtern (mit der Hilfe des Systemadministrators) anzumelden, um zu überprüfen, ob Standardkonten und -kennwörter geändert wurden. (Vom Anbieter vorgegebene Konten/Kennwörter finden Sie in Anbieterhandbüchern und Quellen im Internet.)</p>			
<p>2.1.1 Für drahtlose Umgebungen, die mit der Karteninhaberdaten-Umgebung verbunden sind oder Karteninhaberdaten übertragen, Ändern der drahtlosen Anbieterstandardeinstellungen, einschließlich, aber nicht beschränkt auf drahtlose Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen. Gewährleisten, dass drahtlose Gerätesicherheitseinstellungen für eine starke Verschlüsselungstechnologie für Authentifizierung und Übertragung aktiviert sind.</p>	<p>2.1.1 Überprüfen Sie die folgenden Punkte im Hinblick auf Anbieterstandardeinstellungen für drahtlose Umgebungen, und stellen Sie sicher, dass alle drahtlosen Netzwerke starke Verschlüsselungsmechanismen (z. B. AES) implementieren:</p> <ul style="list-style-type: none"> ▪ Die Standardwerte der Verschlüsselungsschlüssel wurden zum Zeitpunkt der Installation geändert und werden jedes Mal geändert, wenn ein Mitarbeiter, der die Schlüssel kennt, das Unternehmen verlässt oder die Position wechselt. ▪ Standard-SNMP-Community-Zeichenfolgen auf drahtlosen Geräten wurden geändert ▪ Standardkennwörter/-sätze auf Zugriffspunkten wurden geändert ▪ Firmware auf drahtlosen Geräten wird aktualisiert, um starke Verschlüsselung für die Authentifizierung und Übertragung über drahtlose Netzwerke zu unterstützen ▪ Andere sicherheitsbezogene drahtlose Anbieterstandardeinstellungen, sofern zutreffend 			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
2.2 Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen.	2.2.a Überprüfen Sie die Systemkonfigurationsstandards des Unternehmens für alle Arten von Systemkomponenten, und prüfen Sie, ob die Systemkonfigurationsstandards branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen, wie z. B. SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST) und Center for Internet Security (CIS).			
	2.2.b Überprüfen Sie, dass Systemkonfigurationsstandards jedes der unten (unter 2.2.1 - 2.2.4) aufgeführten Elemente enthalten.			
	2.2.c Überprüfen Sie, ob Systemkonfigurationsstandards angewendet werden, wenn neue Systeme konfiguriert werden.			
2.2.1 Implementieren nur einer primären Funktion pro Server.	2.2.1 Überprüfen Sie für eine Stichprobe von Systemkomponenten, dass nur eine primäre Funktion pro Server implementiert ist. Webserver, Datenbankserver und DNS sollten beispielsweise auf separaten Servern implementiert sein.			
2.2.2 Deaktivieren aller unnötigen und unsicheren Dienste und Protokolle (nicht direkt für die Ausführung der spezifischen Gerätefunktion erforderliche Funktionen).	2.2.2 Überprüfen Sie für eine Stichprobe von Systemkomponenten aktivierte Systemservices, Daemons und Protokolle. Überprüfen Sie, dass nicht benötigte oder unsichere Services oder Protokolle nicht aktiviert sind oder dass der entsprechende Einsatz des Service begründet und dokumentiert ist. FTP wird z. B. nicht verwendet oder wird über SSH oder andere Technologie verschlüsselt.			
2.2.3 Konfigurieren von Systemsicherheitsparametern, um Missbrauch zu verhindern.	2.2.3.a Führen Sie Gespräche mit Systemadministratoren und/oder Sicherheitsbeauftragten, um zu überprüfen, ob diese die gängigen Sicherheitsparametereinstellungen für Systemkomponenten kennen.			
	2.2.3.b Überprüfen Sie, ob gängige Sicherheitsparametereinstellungen in den Systemkonfigurationsstandards enthalten sind.			
	2.2.3.c Überprüfen Sie für eine Stichprobe von Systemkomponenten, dass gängige Sicherheitsparameter entsprechend festgelegt sind.			
2.2.4 Entfernen aller unnötigen Funktionen wie z. B. Skripte, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver.	2.2.4 Überprüfen Sie für eine Stichprobe von Systemkomponenten, dass alle unnötigen Funktionen (z. B. Skripte, Treiber, Features, Untersysteme, Dateisysteme usw.) entfernt werden. Überprüfen Sie, ob aktivierte Funktionen dokumentiert werden und die sichere Konfiguration unterstützen und ob in den Geräten, die der Stichprobenkontrolle unterzogen werden, nur dokumentierte Funktionen vorhanden sind.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>2.3 Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs. Verwenden von Technologien wie SSH, VPN oder SSL/TLS für die webbasierte Verwaltung und sonstigen Nichtkonsolen-Verwaltungszugriff.</p>	<p>2.3 Überprüfen Sie für eine Stichprobe von Systemkomponenten, dass der Nichtkonsolen-Verwaltungszugriff durch folgende Maßnahmen verschlüsselt ist:</p> <ul style="list-style-type: none"> ▪ Beobachten Sie eine Administratoranmeldung auf jedem System, um zu überprüfen, dass eine starke Verschlüsselungsmethode aufgerufen wird, bevor das Administratorkennwort angefordert wird: ▪ Prüfen von Services und Parameterdateien auf Dateien, um festzulegen, dass Telnet und andere Remote-Anmeldebefehle nicht für die interne Nutzung verfügbar sind; und ▪ Überprüfen, dass der Administratorzugriff auf die webbasierten Managementschnittstellen mit starker Kryptographie verschlüsselt ist. 			
<p>2.4 Gemeinsam verwendete Hosting-Anbieter müssen die gehostete Umgebung und Karteninhaberdaten jeder Einheit schützen. Diese Anbieter müssen bestimmte Anforderungen erfüllen, wie in <i>Anhang A: Zusätzliche PCI DSS-Anforderungen für gemeinsam verwendete Hosting-Provider</i> dargestellt.</p>	<p>2.4 Durchführen der Testverfahren A.1.1 bis A.1.4, die in <i>Anhang A: Zusätzliche PCI DSS-Anforderungen für gemeinsam verwendete Hosting-Anbieter</i> für PCI DSS-Beurteilungen gemeinsam verwendeter Hosting-Anbieter, um zu überprüfen, dass gemeinsam verwendete Hosting-Anbieter die gehostete Umgebung und die Daten ihrer Einheiten (Händler und Dienstleister) schützen.</p>			

Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

Schutzmethoden wie Verschlüsselung, Abkürzung, Maskierung und Hashing sind kritische Bestandteile des Schutzes von Karteninhaberdaten. Wenn ein Eindringling andere Netzwerksicherheitskontrollen umgeht und Zugriff auf verschlüsselte Daten ohne die entsprechenden kryptographischen Schlüssel erlangt, sind die Daten nicht leserlich und für diese Person unbrauchbar. Andere effektive Methoden zum Schutz gespeicherter Daten sollten als Möglichkeit zur Risikoabschwächung angesehen werden. Zu den Methoden zur Risikominimierung gehört es beispielsweise, Karteninhaberdaten nur zu speichern, wenn dies unbedingt erforderlich ist, Karteninhaberdaten abzukürzen, wenn die vollständige PAN nicht benötigt wird, und die PAN nicht in unverschlüsselten E-Mails zu senden.

Die Definition für „starke Kryptographie“ und andere PCI DSS-Begriffe finden Sie im *Glossar, Abkürzungen und Akronyme zum PCI DSS*.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>3.1 Beschränken des Speicherns von Karteninhaberdaten auf ein Minimum. Entwickeln einer Richtlinie zur Datenaufbewahrung und zum Löschen von Daten. Begrenzen der Speichermenge und der Aufbewahrungszeit auf die für geschäftliche, rechtliche und/oder gesetzliche Zwecke, wie in der Richtlinie zur Datenaufbewahrung dokumentiert.</p>	<p>3.1 Suchen und prüfen Sie die Unternehmensrichtlinien und -verfahren zur Datenaufbewahrung und zum Löschen von Daten, und führen Sie die folgenden Schritte aus:</p> <ul style="list-style-type: none"> ▪ Überprüfen Sie, ob Richtlinien und Verfahren rechtliche, gesetzliche und geschäftliche Anforderungen für die Datenaufbewahrung beinhalten, einschließlich besonderer Anforderungen für die Aufbewahrung von Karteninhaberdaten (z. B. müssen Karteninhaberdaten aus den geschäftlichen Gründen Y für den Zeitraum X aufbewahrt werden) ▪ Überprüfen Sie, ob Richtlinien und Verfahren Bestimmungen zum Löschen von Daten enthalten, wenn diese nicht mehr aus rechtlichen, gesetzlichen oder geschäftlichen Gründen benötigt werden, einschließlich des Löschens von Karteninhaberdaten ▪ Überprüfen Sie, ob Richtlinien und Verfahren alle Aspekte zum Speichern von Karteninhaberdaten abdecken ▪ Überprüfen Sie, ob Richtlinien und Verfahren einen programmatischen (automatischen) Prozess enthalten, um gespeicherte Karteninhaberdaten, die über Aufbewahrungsanforderungen hinausgehen, mindestens vierteljährlich zu entfernen, oder alternativ Anforderungen für eine Prüfung, die mindestens vierteljährlich durchgeführt wird, um zu überprüfen, dass gespeicherte Karteninhaberdaten nicht über Aufbewahrungsanforderungen hinausgehen 			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>3.2 Kein Speichern vertraulicher Authentifizierungsdaten nach der Autorisierung (auch wenn diese verschlüsselt sind). Vertrauliche Authentifizierungsdaten umfassen die Daten, die in den folgenden Anforderungen 3.2.1 bis 3.2.3 aufgeführt sind:</p>	<p>3.2 Wenn vertrauliche Authentifizierungsdaten empfangen und gelöscht werden, suchen und prüfen Sie die Prozesse zum Löschen der Daten, um zu überprüfen, ob die Daten nicht wiederhergestellt werden können. Führen Sie für jedes Element der unten aufgeführten vertraulichen Authentifizierungsdaten die folgenden Schritte aus:</p>			
<p>3.2.1 Speichern Sie nicht den gesamten Inhalt einer Spur auf dem Magnetstreifen (auf der Kartenrückseite, in einem Chip oder an anderer Stelle). Diese Daten werden auch als Full Track, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet. <i>Hinweis: Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:</i></p> <ul style="list-style-type: none"> ▪ Der Name des Karteninhabers, ▪ Primary Account Number (PAN), ▪ Ablaufdatum und ▪ Servicecode <p><i>Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.</i></p> <p><i>Hinweis: Weitere Informationen finden Sie im Glossar, Abkürzungen und Akronyme zum PCI DSS.</i></p>	<p>3.2.1 Überprüfen Sie für eine Stichprobe von Systemkomponenten die folgenden Punkte, und prüfen Sie, ob die vollständigen Inhalte eines beliebigen Tracks vom Magnetstreifen auf der Kartenrückseite unter keinen Umständen gespeichert werden:</p> <ul style="list-style-type: none"> ▪ Eingehende Transaktionsdaten ▪ Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler) ▪ Verlaufsdateien ▪ Trace-Dateien ▪ Mehrere Datenbankschemata ▪ Datenbankinhalt 			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>3.2.2 Speichern Sie nicht den Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte), der zur Verifizierung bei Transaktionen verwendet wird, bei denen die Karte nicht physisch vorliegt.</p> <p><i>Hinweis: Weitere Informationen finden Sie im Glossar, Abkürzungen und Akronyme zum PCI DSS.</i></p>	<p>3.2.2 Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob der drei- oder vierstellige Kartenprüfcode oder -wert auf der Vorderseite der Karte oder dem Unterschriftenfeld (CVV2, CVC2, CID, CAV2) unter keinen Umständen gespeichert wird:</p> <ul style="list-style-type: none"> ▪ Eingehende Transaktionsdaten ▪ Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler) ▪ Verlaufsdateien ▪ Trace-Dateien ▪ Mehrere Datenbankschemata ▪ Datenbankinhalt 			
<p>3.2.3 Speichern Sie keine persönliche Identifizierungsnummern (PIN) oder verschlüsselten PIN-Blocks.</p>	<p>3.2.3 Prüfen Sie für eine Stichprobe von Systemkomponenten folgende Punkte, und überprüfen Sie, ob PINs und verschlüsselte PIN-Blöcke unter keinen Umständen gespeichert werden:</p> <ul style="list-style-type: none"> ▪ Eingehende Transaktionsdaten ▪ Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler) ▪ Verlaufsdateien ▪ Trace-Dateien ▪ Mehrere Datenbankschemata ▪ Datenbankinhalt 			
<p>3.3 Maskieren Sie die PAN bei der Anzeige (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden).</p> <p><i>Hinweise:</i></p> <ul style="list-style-type: none"> ▪ <i>Diese Anforderung gilt nicht für Mitarbeiter und andere Parteien, die die vollständige PAN aus rechtmäßigen geschäftlichen Gründen einsehen müssen.</i> ▪ <i>Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten - z. B. für POS-Belege.</i> 	<p>3.3 Suchen und prüfen Sie schriftliche Richtlinien, und prüfen Sie die PAN-Anzeige (z. B. auf dem Bildschirm, auf Papierbelegen), um zu überprüfen, ob PANs (Primary Account Numbers) beim Anzeigen von Karteninhaberdaten maskiert werden. Davon ausgenommen sind Personen, die die vollständige PAN aus rechtmäßigen geschäftlichen Gründen einsehen müssen.</p>			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>3.4 Machen Sie die PAN mindestens überall dort unleserlich, wo sie gespeichert wird (auch auf tragbaren digitalen Medien, Sicherungsmedien, in Protokollen). Setzen Sie dazu eines der folgenden Verfahren ein:</p> <ul style="list-style-type: none"> ▪ Unidirektionale Hashes, die auf einer starken Kryptographie basieren ▪ Abkürzung ▪ Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden) ▪ Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren. <p>Unter den Kontoinformationen MUSS MINDESTENS die PAN unleserlich gemacht werden.</p> <p><i>Hinweise:</i></p> <ul style="list-style-type: none"> ▪ <i>Wenn ein Unternehmen die PAN aus irgendeinem Grund nicht unleserlich machen kann, finden Sie weitere Informationen hin Anhang B: Kompensationskontrollen.</i> ▪ <i>„Starke Kryptographie“ ist im Glossar, Abkürzungen und Akronyme zum PCI DSS definiert.</i> 	<p>3.4.a Suchen und prüfen Sie Dokumentation über das System, das zum Schützen der PAN eingesetzt wird, einschließlich des Anbieters, des System-/Prozesstyps und der Verschlüsselungsalgorithmen (sofern zutreffend). Überprüfen Sie, ob die PAN mit einer der folgenden Methoden unleserlich gemacht wurde:</p> <ul style="list-style-type: none"> ▪ Unidirektionale Hashes, die auf einer starken Kryptographie basieren ▪ Abkürzung ▪ Index-Token und -Pads (Pads müssen sicher aufbewahrt werden) ▪ Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren <p>3.4.b Überprüfen Sie mehrere Tabellen oder Dateien aus einer Stichprobe aus Daten-Repositorys daraufhin, ob die PAN unleserlich gemacht wurde (d. h. nicht als normaler Text gespeichert wurde).</p> <p>3.4.c Überprüfen Sie eine Stichprobe austauschbarer Datenträger (z. B. Sicherungsbänder), um zu bestätigen, dass die PAN unleserlich gemacht wird.</p> <p>3.4.d Überprüfen Sie eine Stichprobe von Audit-Protokollen, um zu bestätigen, dass die PAN aus den Protokollen entfernt wird.</p>			
<p>3.4.1 Wenn Datenträgerverschlüsselung verwendet wird (anstelle der Datenbankverschlüsselung auf Datei- oder Spaltenebene), muss der logische Zugriff unabhängig von nativen Zugriffskontrollmechanismen des Betriebssystems (z. B. indem lokale Benutzerkontodatenbanken nicht verwendet werden) verwaltet werden.</p>	<p>3.4.1.a Wenn Datenträgerverschlüsselung verwendet wird, überprüfen Sie, ob der logische Zugriff auf verschlüsselte Dateisysteme über einen Mechanismus implementiert wird, der vom nativen Betriebssystemmechanismus (z. B. keine Verwendung lokaler Benutzerkontodatenbanken) getrennt ist.</p> <p>3.4.1.b Überprüfen Sie, ob kryptographische Schlüssel sicher gespeichert sind (z. B. auf austauschbaren Datenträgern, die durch starke Zugriffskontrollen entsprechend geschützt sind).</p>			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
Entschlüsselungsschlüssel dürfen nicht mit Benutzerkonten verknüpft sein.	3.4.1.c Überprüfen Sie, ob Karteninhaberdaten auf austauschbaren Datenträgern unabhängig vom Speicherort verschlüsselt sind. <i>Hinweis: Datenträgerverschlüsselung kann häufig austauschbare Datenträger nicht verschlüsseln. Daher müssen Daten, die auf diesen Datenträgern gespeichert sind, separat verschlüsselt werden.</i>			
3.5 Schützen Sie kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, vor der Weitergabe und vor Missbrauch:	3.5 Überprüfen Sie die Prozesse zum Schützen von Schlüsseln, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, vor Weitergabe und Missbrauch, indem Sie folgende Schritte ausführen:			
3.5.1 Schränken Sie den Zugriff auf kryptographische Schlüssel auf die unbedingt notwendige Anzahl von Wächtern ein.	3.5.1 Prüfen Sie Benutzerzugriffslisten darauf, ob der Zugriff auf Schlüssel auf sehr weniger Wächter beschränkt ist.			
3.5.2 Speichern Sie kryptographische Schlüssel sicher an möglichst wenigen Speicherorten und in möglichst wenig Formen.	3.5.2 Überprüfen Sie Systemkonfigurationsdateien daraufhin, ob Schlüssel im verschlüsselten Format gespeichert sind und ob Schlüssel zum Verschlüsseln von Schlüsseln getrennt von Schlüsseln zum Verschlüsseln von Daten aufbewahrt werden.			
3.6 Dokumentieren und implementieren Sie alle Schlüsselverwaltungsprozesse und -verfahren für kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, wie z. B.:	3.6.a Überprüfen Sie, ob für Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, Verfahren für die Schlüsselverwaltung vorhanden sind. <i>Hinweis: Zahlreiche Branchenstandards für die Schlüsselverwaltung sind über verschiedene Ressourcen verfügbar, unter anderem über NIST (unter http://csrc.nist.gov).</i>			
	3.6.b Nur für Dienstanbieter: Wenn der Dienstanbieter Schlüssel gemeinsam mit seinen Kunden für die Übertragung von Karteninhaberdaten verwendet, überprüfen Sie, ob der Dienstanbieter den Kunden Dokumentation bereitstellt, die Anweisungen zum sicheren Speichern und Ändern von Kundenschlüsseln enthält (die zum Übertragen von Daten zwischen Kunde und Dienstanbieter verwendet werden).			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
	3.6.c Überprüfen Sie die Verfahren zur Schlüsselverwaltung, und führen Sie die folgenden Schritte aus:			
3.6.1 Erstellung starker kryptographischer Schlüssel	3.6.1 Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die die Erstellung starker Schlüssel erfordern.			
3.6.2 Sichere Verteilung kryptographischer Schlüssel	3.6.2 Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die die sichere Verteilung von Schlüsseln erfordern.			
3.6.3 Sicheres Speichern kryptographischer Schlüssel	3.6.3 Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die das sichere Speichern von Schlüsseln erfordern.			
3.6.4 Regelmäßige Änderungen kryptographischer Schlüssel <ul style="list-style-type: none"> ▪ Wie von der jeweiligen Anwendung als notwendig erachtet und empfohlen (z. B. erneute Schlüsselvergabe), vorzugsweise automatisch ▪ Mindestens jährlich 	3.6.4 Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die mindestens jährlich regelmäßige Schlüsseländerungen erfordern.			
3.6.5 Entfernung oder Austausch von alten oder vermeintlich beschädigten kryptographischen Schlüsseln	3.6.5.a Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die das Entfernen alter Schlüssel erfordern (z. B.: durch Archivieren, Vernichten und Rückruf).			
	3.6.5.b Überprüfen Sie, ob die Verfahren zur Schlüsselverwaltung implementiert sind, die den Austausch von Schlüsseln mit bekannten oder vermeintlichen Schäden erfordern.			
3.6.6 Teilen Sie die Kenntnis und Festlegung der doppelten Kontrolle über kryptographische Schlüssel auf	3.6.6 Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die geteilte Kenntnis und die doppelte Kontrolle von Schlüsseln erfordern (z. B. zwei oder drei Personen, die jeweils nur ihren eigenen Bestandteil des Schlüssels kennen, um den gesamten Schlüssel neu zu erstellen).			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
3.6.7 Verhindern der unbefugten Ersetzung kryptographischer Schlüssel	3.6.7 Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die die Verhinderung der unbefugten Ersetzung von Schlüsseln erfordern.			
3.6.8 Wächter kryptographischer Schlüssel müssen ein Formular unterzeichnen, das besagt, dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen.	3.6.8 Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die es von Schlüsselwächtern erfordern, ein Formular zu unterzeichnen, das besagt, dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen.			

Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze

Vertrauliche Informationen müssen während der Übertragung über Netzwerke, auf die böswillige Personen mühelos zugreifen können, verschlüsselt werden. Falsch konfigurierte drahtlose Netzwerke und Sicherheitslücken bei der Legacy-Verschlüsselung und Authentifizierungsprotokollen können zu dauerhaften Zielen böswilliger Personen werden, die diese Sicherheitslücken ausnutzen, um sich privilegierten Zugriff auf Karteninhaberdaten-Umgebungen zu verschaffen.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>4.1 Verwenden von starker Kryptographie und Sicherheitsprotokollen wie SSL/TLS oder IPSEC, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen.</p> <p><i>Beispiele für offene, öffentliche Netzwerke, die in den Umfang des PCI DSS fallen, sind:</i></p> <ul style="list-style-type: none"> ▪ Das Internet ▪ Drahtlose Technologien ▪ GSM-Kommunikationen (Global System for Mobile) und ▪ General Packet Radio Service (GPRS). 	<p>4.1.a Überprüfen Sie die Verwendung von Verschlüsselung (z. B. SSL/TLS oder IPSEC), wenn Karteninhaberdaten über offene, öffentliche Netzwerke übertragen oder empfangen werden.</p> <ul style="list-style-type: none"> ▪ Überprüfen Sie, ob während der Datenübertragung starke Verschlüsselung eingesetzt wird. ▪ Für SSL-Implementierungen: <ul style="list-style-type: none"> – Überprüfen Sie, ob der Server die neuesten Patch-Versionen unterstützt. – Überprüfen Sie, ob HTTPS als Bestandteil der Browser-URL (Universal Record Locator) angezeigt wird. – Überprüfen Sie, dass keine Karteninhaberdaten erforderlich sind, wenn HTTPS nicht in der URL angezeigt wird. ▪ Wählen Sie eine Stichprobe aus Transaktionen bei deren Eingang aus, und beobachten Sie Transaktionen während der Ausführung, um zu überprüfen, ob Karteninhaberdaten während der Übertragung verschlüsselt werden. ▪ Überprüfen Sie, dass nur vertrauenswürdige SSL/TLS-Schlüssel-/Zertifikate akzeptiert werden. ▪ Überprüfen Sie, dass für die verwendete Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet wird. (Prüfen Sie Anbieterempfehlungen/bewährte Verfahren.) 			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>4.1.1 Gewährleisten, dass drahtlose Netzwerke, die Karteninhaberdaten übertragen oder mit der Karteninhaberdaten-Umgebung verbunden sind, bewährte Branchenverfahren (z. B. IEEE 802.11i) einsetzen, um die starke Verschlüsselung für die Authentifizierung und Übertragung zu implementieren.</p> <ul style="list-style-type: none"> ▪ <i>Für neue drahtlose Implementierungen ist es nicht zulässig, WEP nach dem 31. März 2009 zu implementieren.</i> ▪ <i>Für bestehende drahtlose Implementierungen ist es nicht zulässig, WEP nach dem 30. Juni 2010 zu implementieren.</i> 	<p>4.1.1 Überprüfen Sie für drahtlose Netzwerke, die Karteninhaberdaten übertragen oder mit der Karteninhaberdaten-Umgebung verbunden sind, dass bewährte Branchenverfahren (z. B. IEEE 802.11i) eingesetzt werden, um die starke Verschlüsselung für die Authentifizierung und Übertragung zu implementieren.</p>			
<p>4.2 Kein Senden unverschlüsselter PANs über Messaging-Technologien für Endbenutzer (z. B. E-Mail, Instant Messaging, Chat).</p>	<p>4.2.a Überprüfen Sie, dass starke Kryptographie verwendet wird, wenn Karteninhaberdaten über Messaging-Technologien für Endanwender gesendet werden.</p>			
	<p>4.2.b Überprüfen Sie das Vorhandensein einer Richtlinie, die festlegt, dass unverschlüsselte PANs nicht über Messaging-Technologien für Endanwender gesendet werden.</p>			

Wartung eines Anfälligkeits-Managementprogramms

Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware

Böswillige Software, die häufig als „Malware“ bezeichnet wird und Viren, Würmer und Trojaner umfasst, kann im Lauf zahlreicher vom Unternehmen genehmigter Aktivitäten in das Netzwerk eindringen, darunter auch der Nutzung von E-Mail und Internet durch Mitarbeiter, durch mobile Computer und Speichergeräte. Dies führt zur Ausnutzung von Sicherheitslücken. Virenschutzsoftware muss auf allen Systemen eingesetzt werden, die häufig von Malware befallen werden, um Systeme von aktuellen und zukünftigen Bedrohungen durch böswillige Software zu schützen.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
5.1 Implementieren von Virenschutzsoftware auf allen Systemen, die häufig von böswilliger Software befallen werden (insbesondere Personal Computer und Server).	5.1 Überprüfen Sie für eine Stichprobe von Systemkomponenten, einschließlich aller Betriebssystemtypen, die häufig von böswilliger Software befallen werden, dass Virenschutzsoftware implementiert ist, wenn eine anwendbare Virenschutztechnologie vorhanden ist.			
5.1.1 Gewährleisten, dass alle Virenschutzprogramme in der Lage sind, alle bekannten Malware-Typen zu erkennen, zu entfernen und davor zu schützen.	5.1.1 Überprüfen Sie für eine Stichprobe von Systemkomponenten, dass alle Virenschutzprogramme alle bekannten Malware-Typen (z. B. Viren, Trojaner, Würmer, Spyware, Adware und Rootkits) erkennen, entfernen und davor schützen.			
5.2 Gewährleisten, dass alle Antivirenmechanismen auf dem Laufenden sind, aktiv ausgeführt werden und in der Lage sind, Audit-Protokolle zu generieren.	5.2 Überprüfen Sie, dass sämtliche Virenschutzsoftware auf dem neuesten Stand ist, aktiv ausgeführt wird und in der Lage ist, Protokolle zu generieren. Führen Sie dazu die folgenden Schritte aus:			
	5.2.a Rufen Sie die Richtlinie ab, und überprüfen Sie, ob sie die Aktualisierung von Virenschutzsoftware und -definitionen erfordert.			
	5.2.b Überprüfen Sie, ob die Master-Installation der Software für automatische Updates und regelmäßige Scans aktiviert ist.			
	5.2.c Überprüfen Sie für eine Stichprobe von Systemkomponenten, einschließlich aller Betriebssystemtypen, die häufig von Malware befallen werden, ob automatische Updates und regelmäßige Scans aktiviert sind.			
	5.2.d Überprüfen Sie für eine Stichprobe von Systemkomponenten, dass die Protokollerstellung der Virenschutzsoftware aktiviert ist und dass die Protokolle gemäß PCI DSS-Anforderung 10.7 aufbewahrt werden.			

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

Skrupellose Personen nutzen Sicherheitslücken aus, um sich privilegierten Zugriff auf Systeme zu verschaffen. Zahlreiche dieser Sicherheitslücken werden durch Sicherheitspatches geschlossen, die vom Anbieter bereitgestellt werden und von den Einheiten installiert werden müssen, die die Systeme verwalten. Alle kritischen Systeme müssen mit den neuesten Versionen der entsprechenden Software-Patches für den Schutz vor Ausnutzung und Beeinträchtigung von Karteninhaberdaten durch böswillige Personen und Software versehen sein.

Hinweis: Geeignete Software-Patches sind Patches, die hinreichend bewertet und getestet wurden, um zu ermitteln, dass die Patches nicht in Konflikt mit vorhandenen Sicherheitskonfigurationen stehen. Für intern entwickelte Anwendungen können zahlreiche Sicherheitslücken durch den Einsatz von Standardprozessen zur Systementwicklung und sichere Codierungsverfahren verhindert werden.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>6.1 Gewährleisten, dass für alle Systemkomponenten und Softwareanwendungen die neuesten Sicherheitspatches des jeweiligen Herstellers installiert wurden. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden.</p> <p><i>Hinweis: Ein Unternehmen kann den Einsatz eines risikobasierten Ansatzes in Erwägung ziehen, um seine Patch-Installationen zu priorisieren. Beispielsweise kann kritischer Infrastruktur (z. B. öffentliche Geräte und Systeme, Datenbanken) eine höhere Priorität eingeräumt werden als weniger kritischen internen Geräten, um zu gewährleisten, dass Systeme und Geräte mit hoher Priorität innerhalb eines Monats und weniger kritische Geräte und Systeme innerhalb von drei Monaten adressiert werden.</i></p>	<p>6.1.a Vergleichen Sie für eine Stichprobe von Systemkomponenten und zugehörige Software die Liste der auf jedem System installierten Sicherheitspatches mit der neuesten Sicherheitspatch-Liste des Anbieters, um zu überprüfen, ob aktuelle Anbieterpatches installiert sind.</p>			
	<p>6.1.b Überprüfen Sie Richtlinien im Zusammenhang mit der Installation von Sicherheitspatches, um zu prüfen, ob sie die Installation aller kritischen neuen Sicherheitspatches innerhalb eines Monats erfordern.</p>			
<p>6.2 Festlegen eines Prozesses zur Identifizierung neu festgestellter Sicherheitsanfälligkeiten (z. B. Abonnieren von im Internet frei verfügbaren Alarmdiensten). Aktualisieren von Konfigurationsstandards gemäß PCI DSS-Anforderung 2.2, um neue Sicherheitslückenprobleme zu adressieren.</p>	<p>6.2.a Führen Sie Gespräche mit zuständigen Mitarbeitern, um zu überprüfen, dass Prozesse zum Identifizieren neuer Sicherheitslücken implementiert sind.</p>			
	<p>6.2.b Überprüfen Sie, ob Prozesse zum Identifizieren neuer Sicherheitslücken die Verwendung von externen Quellen für Informationen zu Sicherheitslücken und die Aktualisierung der in Anforderung 2.2 geprüften Systemkonfigurationsstandards umfassen, wenn neue Sicherheitsprobleme auftreten.</p>			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
6.3 Entwickeln von Softwareanwendungen gemäß PCI DSS (z. B. sichere Authentifizierung und Protokollierung) und anhand von Best Practices der Branche und Integrieren von Informationssicherheit während des gesamten Softwareentwicklungszyklus. Diese Prozesse müssen Folgendes umfassen:	6.3.a Suchen und untersuchen Sie schriftliche Softwareentwicklungsprozesse, um zu überprüfen, dass die Prozesse auf Branchenstandards basieren, dass Sicherheit während des gesamten Lebenszyklus integriert ist und dass Softwareanwendungen gemäß PCI DSS entwickelt werden.			
	6.3.b Überprüfen Sie anhand einer Untersuchung schriftlicher Softwareentwicklungsprozesse, anhand von Gesprächen mit Softwareentwicklern und der Untersuchung relevanter Daten (Netzwerkkonfigurationsdokumentation, Produktions- und Testdaten usw.) folgende Punkte:			
6.3.1 Testen aller Sicherheitspatches und System- und Softwarekonfigurationsänderungen vor der Implementierung, einschließlich, aber nicht beschränkt auf Folgendes:	6.3.1 Alle Änderungen (einschließlich Patches) werden vor der Implementierung getestet.			
6.3.1.1 Validierung der gesamten Eingabe (zum Verhindern von siteübergreifender Skripterstellung, Injektionsfehlern, böswilliger Dateiausführung usw.)	6.3.1.1 Validierung der gesamten Eingabe (zum Verhindern von siteübergreifender Skripterstellung, Injektionsfehlern, böswilliger Dateiausführung usw.)			
6.3.1.2 Validierung der ordnungsgemäßen Fehlerbehandlung	6.3.1.2 Validierung der ordnungsgemäßen Fehlerbehandlung			
6.3.1.3 Validierung des sicheren kryptographischen Speichers	6.3.1.3 Validierung des sicheren kryptographischen Speichers			
6.3.1.4 Validierung sicherer Mitteilungen	6.3.1.4 Validierung sicherer Mitteilungen			
6.3.1.5 Validierung der ordnungsgemäßen rollenbasierten Zugriffssteuerung (RBAC)	6.3.1.5 Validierung der ordnungsgemäßen rollenbasierten Zugriffssteuerung (RBAC)			
6.3.2 Separate Entwicklungs-, Test- und Produktionsumgebungen	6.3.2 Die Entwicklungs-/Testumgebungen sind von der Produktionsumgebung getrennt, und zum Durchsetzen dieser Trennung ist eine Zugriffssteuerung implementiert.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
6.3.3 Trennung der Aufgaben zwischen Entwicklungs-, Test- und Produktionsumgebungen	6.3.3 Es besteht eine Trennung der Aufgaben zwischen Mitarbeitern, die den Entwicklungs-/Testumgebungen zugewiesen sind, und Mitarbeitern, die der Produktionsumgebung zugeteilt sind.			
6.3.4 Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet	6.3.4 Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet oder werden vor der Verwendung bereinigt.			
6.3.5 Entfernen von Testdaten und -konten, bevor Produktionssysteme aktiv werden	6.3.5 Testdaten und -konten werden entfernt, bevor ein Produktionssystem aktiv wird.			
6.3.6 Entfernen benutzerdefinierter Anwendungskonten, Benutzernamen und Kennwörter, bevor Anwendungen aktiv oder an Kunden freigegeben werden	6.3.6 Benutzerdefinierte Anwendungskonten, Benutzernamen und/oder Kennwörter werden entfernt, bevor das System in Produktion geht oder an Kunden freigegeben wird.			
6.3.7 Überprüfung benutzerdefinierter Programmcodes vor der Freigabe an die Produktion oder an Kunden, um alle potenziellen Programmanfälligkeiten zu identifizieren <i>Hinweis: Diese Anforderung für Code-Prüfungen gilt für den gesamten benutzerdefinierten (internen und öffentlichen) Code als Teil des Systementwicklungszyklus gemäß PCI DSS-Anforderung 6.3. Code-Prüfungen können durch qualifiziertes internes Personal oder durch Dritte ausgeführt werden. Webanwendungen unterliegen auch zusätzlichen Kontrollen, wenn sie</i>	6.3.7.a Suchen und prüfen Sie Richtlinien, um zu bestätigen, dass alle benutzerdefinierten Anwendungscodeänderungen für <i>interne Anwendungen</i> wie folgt geprüft werden müssen (mit manuellen oder automatisierten Prozessen): <ul style="list-style-type: none"> ▪ Codeänderungen werden von anderen Personen geprüft als dem ursprünglichen Ersteller des Codes sowie von Personen, die mit Verfahren zur Codeprüfung und sicheren Codierungsverfahren vertraut sind. ▪ Vor der Freigabe werden entsprechende Korrekturen implementiert. ▪ Ergebnisse der Codeprüfung werden vor der Freigabe vom Management geprüft und genehmigt. 			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>öffentlich sind, um laufende Bedrohungen und Sicherheitslücken nach der Implementierung gemäß der Definition in PCI DSS-Anforderung 6.6 zu adressieren.</p>	<p>6.3.7.b Suchen und prüfen Sie Richtlinien, um zu bestätigen, dass alle benutzerdefinierten Anwendungscodeänderungen für <i>Webanwendungen</i> wie folgt geprüft werden müssen (mit manuellen oder automatisierten Prozessen):</p> <ul style="list-style-type: none"> ▪ Codeänderungen werden von anderen Personen geprüft als dem ursprünglichen Ersteller des Codes sowie von Personen, die mit Verfahren zur Codeprüfung und sicheren Codierungsverfahren vertraut sind. ▪ Codeprüfungen gewährleisten, dass Code gemäß sicheren Codierungsrichtlinien erstellt wird, wie z. B. dem <i>Open Web Security Project Guide</i> (siehe PCI DSS-Anforderung 6.5). ▪ Vor der Freigabe werden entsprechende Korrekturen implementiert. ▪ Ergebnisse der Codeprüfung werden vor der Freigabe vom Management geprüft und genehmigt. 			
	<p>6.3.7.c Wählen Sie eine Stichprobe aus kürzlich vorgenommenen Anwendungsänderungen aus, und überprüfen Sie, ob der benutzerdefinierte Anwendungscode gemäß Punkt 6.3.7a und 6.3.7b geprüft wird.</p>			
<p>6.4 Befolgen von Änderungskontrollverfahren für alle Änderungen an Systemkomponenten. Die Verfahren müssen Folgendes umfassen:</p>	<p>6.4.a Suchen und untersuchen Sie unternehmensweite Änderungskontrollverfahren im Hinblick auf die Implementierung von Sicherheitspatches und Softwareänderungen, und überprüfen Sie, dass diese Verfahren die folgenden Punkte 6.4.1 – 6.4.4 erfordern.</p>			
	<p>6.4.b Verfolgen Sie für eine Stichprobe von Systemkomponenten und neueren Änderungen/Sicherheitspatches diese Änderungen zurück zur diesbezüglichen Änderungskontrolldokumentation. Führen Sie für jede untersuchte Änderung die folgenden Schritte aus:</p>			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
6.4.1 Dokumentation der Auswirkungen	6.4.1 Überprüfen Sie, dass die Dokumentation der Kundenauswirkungen in der Änderungskontrolldokumentation für jede geprüfte Änderung enthalten ist.			
6.4.2 Verwaltung der Abzeichnung durch die jeweiligen Parteien	6.4.2 Überprüfen Sie, dass jede geprüfte Änderung durch entsprechende Parteien abgezeichnet wurde.			
6.4.3 Testen der betrieblichen Funktionalität	6.4.3 Überprüfen Sie, dass die betriebliche Funktionalität für jede geprüfte Änderung getestet wird.			
6.4.4 Back-Out-Verfahren	6.4.4 Überprüfen Sie, dass für jede geprüfte Änderung Back-Out-Verfahren erstellt werden			
6.5 Entwickeln aller Webanwendungen (intern und extern und einschließlich des Webverwaltungszugriffs auf die Anwendung) anhand sicherer Codierungsrichtlinien, wie z. B. dem <i>Open Web Application Security Project Guide</i> . Berücksichtigen der Vorbeugung häufiger Programmierungsanfälligkeiten in Softwareentwicklungsprozessen, einschließlich der folgenden Punkte: <i>Hinweis: Die unter 6.5.1 bis 6.5.10 aufgeführten Schwachstellen waren im OWASP-Handbuch zum Zeitpunkt der Veröffentlichung von PCI DSS v1.2.1 aktuell. Wenn das OWASP-Handbuch aktualisiert wird, muss jedoch die aktuelle Version für diese Anforderungen verwendet werden.</i>	6.5.a Suchen und prüfen Sie Softwareentwicklungsprozesse für alle webbasierten Anwendungen. Überprüfen Sie, dass Prozesse Schulungen im Hinblick auf sichere Codierungsverfahren für Entwickler erfordern und auf Leitfäden basieren, wie z. B. dem OWASP -Handbuch (http://www.owasp.org).			
	6.5.b Führen Sie Gespräche mit stichprobenartig ausgewählten Entwicklern, und stellen Sie Nachweise dafür zusammen, dass diese mit sicheren Codierungsverfahren vertraut sind.			
	6.5.c Überprüfen Sie, dass Prozesse implementiert sind, um zu gewährleisten, dass Webanwendungen nicht für Folgendes anfällig sind:			
6.5.1 Siteübergreifendes Scripting (XSS)	6.5.1 Siteübergreifendes Scripting (XSS) (Validieren Sie alle Parameter vor der Aufnahme.)			
6.5.2 Injektionsfehler, insbesondere bei der SQL-Injektion. LDAP- und Xpath-Injektionsfehler sowie andere Injektionsfehler sind ebenfalls zu berücksichtigen.	6.5.2 Injektionsfehler, insbesondere bei der SQL-Injektion (Validieren Sie die Eingabe, um zu überprüfen, dass Benutzerdaten nicht die Bedeutung von Befehlen und Abfragen ändern können.)			
6.5.3 Böswillige Dateiausführung	6.5.3 Böswillige Dateiausführung (Validieren Sie die Eingabe, um zu überprüfen, dass die Anwendung keine Dateinamen oder Dateien von Benutzern akzeptiert.)			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
6.5.4 Unsichere direkte Objektverweise	6.5.4 Unsichere direkte Objektverweise (Machen Sie interne Objektverweise nicht Benutzern zugänglich.)			
6.5.5 Cross-Site Request Forgery (CSRF)	6.5.5 Cross-Site Request Forgery (CSRF) (Antworten Sie nicht auf Autorisierungsinformationen und Token, die automatisch von Browsern gesendet werden.)			
6.5.6 Informationslecks und unsachgemäße Fehlerbehandlung	6.5.6 Informationslecks und unsachgemäße Fehlerbehandlung (Geben Sie keine Informationen über Fehlermeldungen oder andere Mittel preis.)			
6.5.7 Geknackte Authentifizierungs- und Sitzungsverwaltung	6.5.7 Geknackte Authentifizierungs- und Sitzungsverwaltung (Authentifizieren Sie Benutzer ordnungsgemäß, und schützen Sie Kontoanmeldeinformationen und Sitzungstoken.)			
6.5.8 Unsicherer kryptographischer Speicher	6.5.8 Unsicherer kryptographischer Speicher (Verhindern Sie kryptographische Fehler.)			
6.5.9 Unsichere Mitteilungen	6.5.9 Unsichere Mitteilungen (Verschlüsseln Sie alle authentifizierten und vertraulichen Mitteilungen ordnungsgemäß.)			
6.5.10 Unterlassene Einschränkung des URL-Zugriffs	6.5.10 Unterlassene Einschränkung des URL-Zugriffs (setzen Sie die Zugriffssteuerung konsistent in der Präsentationsebene und der Geschäftslogik für alle URLs durch.)			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>6.6 Für öffentliche Webanwendungen laufende Adressierung neuer Bedrohungen und Schwachstellen und Gewährleisten, dass diese Anwendungen durch <i>eine</i> der folgenden Methoden geschützt werden:</p> <ul style="list-style-type: none"> ▪ Prüfen öffentlicher Webanwendungen durch manuelle oder automatisierte Tools oder Methoden zum Bewerten der Anwendungssicherheit mindestens jährlich sowie nach Änderungen ▪ Installieren einer Webanwendungs-Firewall vor öffentlichen Webanwendungen 	<p>6.6 Stellen Sie für <i>öffentliche</i> Webanwendungen sicher, dass <i>eine</i> der folgenden Methoden implementiert ist:</p> <ul style="list-style-type: none"> ▪ Überprüfen Sie, dass öffentliche Webanwendungen wie folgt geprüft werden (mit manuellen oder automatisierten Tools oder Methoden zur Beurteilung der Anwendungssicherheit): <ul style="list-style-type: none"> - Mindestens jährlich - Nach jeder Änderung - Durch ein Unternehmen, das auf Anwendungssicherheit spezialisiert ist - Dass alle Sicherheitslücken geschlossen werden - Dass die Anwendung nach den Korrekturen erneut bewertet wird ▪ Überprüfen Sie, dass vor öffentlichen Webanwendungen eine Webanwendungs-Firewall implementiert wird, um webbasierte Angriffe zu erkennen und zu verhindern. <p><i>Hinweis: „Ein Unternehmen, das auf Anwendungssicherheit spezialisiert ist“, kann ein Drittunternehmen oder eine interne Organisation sein, sofern sich die Prüfer auf Anwendungssicherheit spezialisieren und die Unabhängigkeit vom Entwicklungsteam nachweisen können.</i></p>			

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf

Um zu gewährleisten, dass nur autorisierte Mitarbeiter auf kritische Daten zugreifen können, müssen Systeme und Prozesse implementiert sein, die den Zugriff anhand des Informationsbedarfs und gemäß Zuständigkeiten beschränken.

„Informationsbedarf“ besteht, wenn Zugriffsrechte nur auf die minimale Menge an Daten und Berechtigungen erteilt werden, die zum Ausüben einer Tätigkeit erforderlich sind.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
7.1 Beschränken des Zugriffs auf Systemkomponenten und Karteninhaberdaten auf die Personen, deren Tätigkeit diesen Zugriff erfordert. Zugriffsbeschränkungen müssen Folgendes umfassen:	7.1 Suchen und untersuchen Sie eine schriftliche Richtlinie für die Datensteuerung, und überprüfen Sie, dass die Richtlinie Folgendes enthält:			
7.1.1 Beschränkung von Zugriffsrechten für Benutzernamen auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogene Verpflichtungen erforderlich sind	7.1.1 Bestätigen Sie, dass Zugriffsrechte für Benutzernamen auf Mindestberechtigungen beschränkt sind, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind.			
7.1.2 Die Zuweisung von Berechtigungen basiert auf der Tätigkeitsklassifizierung und -funktion einzelner Mitarbeiter	7.1.2 Bestätigen Sie, dass Berechtigungen Personen anhand der Tätigkeitsklassifizierung und -funktion zugewiesen werden (wird auch als „rollenbasierte Zugriffssteuerung“ oder RBAC bezeichnet).			
7.1.3 Anforderung für ein vom Management unterzeichnetes Autorisierungsformular, das erforderliche Berechtigungen angibt	7.1.3 Bestätigen Sie, dass ein Autorisierungsformular für den gesamten Zugriff erforderlich ist, dass es erforderliche Berechtigungen angeben muss und dass es vom Management unterzeichnet sein muss.			
7.1.4 Implementierung eines automatisierten Zugriffskontrollsystems	7.1.4 Bestätigen Sie, dass Zugriffskontrollen über ein automatisiertes Zugriffskontrollsystem implementiert werden.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>7.2 Festlegen eines Zugriffskontrollsystems für Systemkomponenten mit mehreren Benutzern, das den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem muss Folgendes umfassen:</p>	<p>7.2 Prüfen Sie anhand von Systemeinstellungen und der Anbieterdokumentation wie folgt, ob ein Zugriffskontrollsystem implementiert ist:</p>			
<p>7.2.1 Abdeckung aller Systemkomponenten</p>	<p>7.2.1 Bestätigen Sie, dass in allen Systemkomponenten Zugriffskontrollsysteme implementiert sind.</p>			
<p>7.2.2 Zuweisung von Berechtigungen zu einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion</p>	<p>7.2.2 Bestätigen Sie, dass Zugriffskontrollsysteme konfiguriert sind, um Berechtigungen durchzusetzen, die einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion zugewiesen sind.</p>			
<p>7.2.3 Standardeinstellung „Alle ablehnen“</p>	<p>7.2.3 Bestätigen Sie, dass die Zugriffskontrollsysteme die Standardeinstellung „Alle ablehnen“ aufweisen</p> <p><i>Hinweis: Einige Zugriffskontrollsysteme sind standardmäßig auf „Alle zulassen“ gesetzt und lassen dadurch den Zugriff zu, bis eine Regel erstellt wird, die den Zugriff ausdrücklich ablehnt.</i></p>			

Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff

Durch die Zuweisung einer eindeutigen Kennung (ID) zu jeder Person mit Zugriff ist jede(r) Einzelne uneingeschränkt für die eigenen Handlungen verantwortlich. Wenn ein solches System der Verantwortlichkeit implementiert ist, können Maßnahmen an wichtigen Daten und Systemen nur von bekannten und autorisierten Benutzern vorgenommen werden, und sämtliche Maßnahmen lassen sich auf den jeweiligen Initiator zurückführen.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
8.1 Zuweisen einer eindeutigen Benutzer-ID für alle Benutzer, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird.	8.1 Stellen Sie sicher, dass alle Benutzer eine eindeutige ID für den Zugriff auf Systemkomponenten oder Karteninhaberdaten erhalten.			
8.2 Zuweisung einer eindeutigen ID und Einsatz von mindestens einer der folgenden Methoden zur Authentifizierung sämtlicher Benutzer: <ul style="list-style-type: none"> ▪ Kennwort oder Kennsatz ▪ Authentifizierung mittels zweier Faktoren (z. B. Token-Geräte, Smartcards, biometrische Systeme oder öffentliche Schlüssels) 	8.2 Gehen Sie wie folgt vor, um zu überprüfen, ob sich die Benutzer mittels einer eindeutigen ID und eines zusätzlichen Authentifizierungsmerkmals (z. B. Kennwort) für den Zugriff auf die Karteninhaberdaten authentifiziert haben: <ul style="list-style-type: none"> ▪ Untersuchen Sie Dokumente, aus denen hervorgeht, welche Authentifizierungsmethoden verwendet wurden. ▪ Schauen Sie sich bei jeder Authentifizierungsmethode und jeder Systemkomponente eine Authentifizierung genauer daraufhin an, ob diese in Übereinstimmung mit den dokumentierten Authentifizierungsmethoden erfolgt. 			
8.3 Authentifizierung anhand zweier Faktoren beim Remote-Zugriff (Netzwerkzugriff von außerhalb des Netzwerks) von Mitarbeitern, Administratoren und Dritten. Zur Verfügung stehen Technologien wie Remote-Authentifizierung und Einwahldienst (RADIUS) oder Terminal Access Controller Access Control System (TACACS) mit Tokens bzw. VPN (auf SSL/TLS- oder IPSEC-Basis) mit individuellen Zertifikaten.	8.3 Gehen Sie wie folgt vor, um die Implementierung der Zwei-Faktoren-Authentifizierung für den Remote-Netzwerkzugriff zu überprüfen: Beobachten Sie, wie ein Mitarbeiter (z. B. ein Administrator) eine Remote-Verbindung zum Netzwerk herstellt, und überprüfen Sie, ob hierfür ein Kennwort und ein zusätzliches Authentifizierungselement erforderlich ist (z. B. eine Smartcard, ein Token oder eine PIN).			
8.4 Geschützte Übertragung und Speicherung von Kennwörtern auf sämtlichen Systemkomponenten unter Verwendung einer sicheren Verschlüsselung (siehe <i>Glossar, Abkürzungen und Akronyme zum PCI DSS</i>).	8.4.a Testen Sie stichprobenartig die Kennwortdateien von Systemkomponenten auf die Verschlüsselung von Kennwörtern bei Übertragung und Speicherung.			
	8.4.b Bei Diensteanbietern müssen darüber hinaus die Kennwortdateien daraufhin geprüft werden, ob Kundenkennwörter verschlüsselt werden.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
8.5 Verwendung der entsprechenden Benutzerauthentifizierungs- und Kennwortverwaltungskontrollen für Nichtverbraucherbenutzer und Administratoren auf allen Systemkomponenten nach folgender Maßgabe:	8.5 Überprüfen Sie die Verfahren und befragen Sie Mitarbeiter hinsichtlich der Umsetzung der Benutzerauthentifizierung und der Kennwortverwaltung. Gehen Sie dabei wie folgt vor:			
8.5.1 Kontrollieren der Vorgänge zum Hinzufügen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsobjekten.	8.5.1.a Wählen Sie stichprobenartig Benutzer-IDs von Administratoren und allgemeinen Benutzern aus. Überprüfen Sie, ob die einzelnen Benutzer entsprechend den Richtlinien des Unternehmens zur Systemnutzung berechtigt sind. Gehen Sie dafür wie folgt vor: <ul style="list-style-type: none"> ▪ Untersuchen Sie für jede ID ein Autorisierungsformular. ▪ Überprüfen Sie, ob die in die Stichprobe aufgenommenen Benutzer-IDs in Übereinstimmung mit dem Autorisierungsformular (inklusive der angegebenen Rechte und sämtlicher eingeholter Signaturen) implementiert wurden, indem Sie Informationen aus dem Autorisierungsformular zum System nachverfolgen. 			
8.5.2 Überprüfen der Benutzeridentität, bevor Kennwörter zurückgesetzt werden.	8.5.2 Untersuchen Sie die Kennwortverfahren, und beobachten Sie das Sicherheitspersonal. Achten Sie darauf, ob bei Benutzeranforderungen zum Zurücksetzen des Kennworts, die telefonisch, per E-Mail oder über das Internet bzw. auf anderem nicht-persönlichen Weg beim Personal eingehen, die Identität des Benutzers vor dem Zurücksetzen des Kennworts überprüft wird.			
8.5.3 Festlegen eindeutiger Werte für die anfänglichen Kennwörter der einzelnen Benutzer und sofortige Änderung nach der ersten Verwendung.	8.5.3 Untersuchen Sie die Kennwortverfahren, und beobachten Sie das Sicherheitspersonal. Achten Sie darauf, dass neue Benutzer eindeutige anfängliche Kennwörter erhalten und dass diese Kennwörter nach der ersten Nutzung geändert werden.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
8.5.4 Sofortige Deaktivierung des Zugriffs ehemaliger Benutzer.	8.5.4 Prüfen Sie stichprobenartig, ob die IDs von Mitarbeitern, die in den letzten sechs Monaten aus dem Unternehmen ausgeschieden sind, deaktiviert bzw. aus den Zugriffslisten der aktuellen Benutzer gelöscht wurden.			
8.5.5 Entfernen bzw. Deaktivieren inaktiver Benutzerkonten mindestens alle 90 Tage.	8.5.5 Überprüfen Sie, ob seit mehr als 90 Tagen inaktive Konten entfernt oder deaktiviert werden.			
8.5.6 Aktivieren der von Anbietern/Lieferanten für die Remote-Wartung verwendeten Konten ausschließlich während der erforderlichen Zeit.	8.5.6 Überprüfen Sie, ob die zur Unterstützung und Wartung verwendeten Konten im Regelfall deaktiviert sind – d. h., sie sollten nur dann aktiviert werden, wenn der Anbieter sie benötigt, und die Verwendung sollte überwacht werden.			
8.5.7 Vermitteln der geltenden Kennwortverfahren und -richtlinien an alle Benutzer mit Zugriff auf Karteninhaberdaten.	8.5.7 Befragen Sie stichprobenartig einige Benutzer nach ihren Kenntnissen der Kennwortverfahren und -richtlinien.			
8.5.8 Keine Vergabe von Konten und Kennwörtern für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung.	8.5.8.a Zur Ermittlung einer Stichprobe von Systemkomponenten stehen die Benutzer-ID-Listen zur Verfügung. Prüfen Sie Folgendes: <ul style="list-style-type: none"> ▪ Allgemeine Benutzer-IDs und -konten werden deaktiviert und entfernt. ▪ Es gibt keine gemeinsamen Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen. ▪ Es werden keine gemeinsamen und allgemeinen Benutzer-IDs zur Administration von Systemkomponenten verwendet. 			
	8.5.8.b Untersuchen Sie Kennwortrichtlinien und -verfahren, und sorgen Sie dafür, dass Gruppenkennwörter und gemeinsame Kennwörter explizit untersagt sind.			
	8.5.8.c Stellen Sie durch Interviews mit Systemadministratoren sicher, dass selbst auf Anfrage keine Gruppen- bzw. gemeinsamen Kennwörter vergeben werden.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>8.5.9 Ändern der Benutzerkennwörter mindestens alle 90 Tage.</p>	<p>8.5.9 Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Benutzer mindestens alle 90 Tage ihr Kennwort ändern müssen.</p> <p>Bei Dienst Anbietern sind darüber hinaus interne Prozesse und Kunden- bzw. Benutzerdokumente daraufhin zu überprüfen, ob Kundenkennwörter regelmäßig geändert werden müssen und ob die Kunden Hinweise dazu erhalten, wann und unter welchen Umständen die Kennwörter geändert werden müssen.</p>			
<p>8.5.10 Festlegen einer Mindestlänge für Kennwörter von 7 Zeichen.</p>	<p>8.5.10 Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Kennwörter mindestens sieben Zeichen lang sein müssen.</p> <p>Bei Dienst Anbietern müssen zusätzlich interne Prozesse und Kunden-/Benutzerdokumente daraufhin überprüft werden, ob es Mindestlängen für Kennwörter gibt.</p>			
<p>8.5.11 Verwenden von Kennwörtern, die sowohl numerische als auch alphabetische Zeichen enthalten.</p>	<p>8.5.11 Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Kennwörter numerische und alphabetische Zeichen enthalten müssen.</p> <p>Bei Dienst Anbietern müssen zusätzlich interne Prozesse und Kunden-/Benutzerdokumente daraufhin überprüft werden, ob darin gefordert wird, dass Kennwörter numerische und alphabetische Zeichen enthalten.</p>			
<p>8.5.12 Festlegen, dass sich ein neues Kennwort von den letzten vier Kennwörtern unterscheiden muss.</p>	<p>8.5.12 Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob gefordert wird, dass sich ein neues Kennwort von den letzten vier Kennwörtern unterscheidet.</p> <p>Bei Dienst Anbietern müssen zusätzlich interne Prozesse und Kunden-/Benutzerdokumente daraufhin überprüft werden, ob darin gefordert wird, dass sich ein neues Kennwort von den letzten vier Kennwörtern unterscheidet.</p>			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
8.5.13 Begrenzen der wiederholten Zugriffsversuche durch Sperren der Benutzer-ID nach spätestens sechs Versuchen.	8.5.13 Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob gefordert wird, dass ein Benutzerkonto nach spätestens sechs ungültigen Anmeldeversuchen gesperrt wird. Bei Dienst Anbietern müssen zusätzlich interne Prozesse und Kunden-/Benutzerdokumente daraufhin überprüft werden, ob ein Benutzerkonto nach spätestens sechs ungültigen Anmeldeversuchen gesperrt wird.			
8.5.14 Festlegen einer Aussperrdauer von mindestens 30 Minuten, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann.	8.5.14 Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob eine mindestens 30-minütige Aussperrdauer gilt, innerhalb derer das Konto nur durch den Administrator zurückgesetzt werden kann.			
8.5.15 Festlegen, dass die Benutzer nach mehr als 15-minütiger Inaktivität das Kennwort erneut eingeben und das Terminal reaktivieren müssen.	8.5.15 Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Benutzer nach mehr als 15-minütiger Inaktivität das Kennwort erneut eingeben und das Terminal reaktivieren müssen.			
8.5.16 Festlegen, dass für den gesamten Zugriff auf Datenbanken mit Karteninhaberdaten eine Authentifizierung erforderlich ist. (Dies umfasst Zugriff durch Anwendungen, Administratoren und alle anderen Benutzer.)	8.5.16.a Überprüfen Sie die Konfigurationseinstellungen für Datenbank und Anwendungen, und achten Sie bei der Benutzerauthentifizierung und beim Datenbankzugriff auf Folgendes: <ul style="list-style-type: none"> ▪ Alle Benutzer müssen sich vor dem Zugriff authentifizieren. ▪ Sämtliche Zugriffe, Anfragen und Aktionen der Benutzer im Bezug auf die Datenbank (z. B. Verschieben, Kopieren und Löschen) erfolgen ausschließlich programmgesteuert (z. B. über gespeicherte Verfahren). ▪ Der Direktzugriff sowie Datenbankabfragen bleiben Datenbankadministratoren vorbehalten. 			
	8.5.16.b Überprüfen Sie die Datenbankanwendungen daraufhin, dass die zugehörigen Anwendungs-IDs nur von den Anwendungen und nicht von Einzelbenutzern oder anderen Prozessen verwendet werden können.			

Anforderung 9: Beschränkung des physischen Zugriffs auf Karteninhaberdaten

Der physische Zugriff auf Daten oder Systeme mit Karteninhaberdaten bietet Einzelpersonen die Gelegenheit, auf Geräte oder Daten zuzugreifen und Systeme oder Ausdrücke zu entfernen. Daher sollte der physische Zugriff entsprechend beschränkt sein.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>9.1 Verwenden angemessener Zugangskontrollen, um den physischen Zugriff auf Systeme für Karteninhaberdaten zu überwachen und zu beschränken.</p>	<p>9.1 Überprüfen Sie, ob für die einzelnen Computerräume, Rechenzentren und sonstigen Bereiche, in denen sich Systeme mit Karteninhaberdaten befinden, Zugangskontrollen existieren.</p> <ul style="list-style-type: none"> ▪ Überprüfen Sie, ob der Zugang über eine elektronische Ausweiskontrolle oder per Schlüssel erfolgt. ▪ Schauen Sie sich an, wie der Anmeldeversuch eines Systemadministrators an den Konsolen willkürlich ausgewählter Systeme mit Karteninhaberdaten abläuft, und überprüfen Sie, ob die Sperre zur Verhinderung der unbefugten Nutzung vorhanden funktioniert. 			
<p>9.1.1 Überwachen des Zugang zu zugangsbeschränkten Bereichen mit Hilfe von Videokameras und anderen Kontrollsystemen. Überprüfen der gesammelten Daten und Korrelation mit anderen Daten. Speichern der Daten mindestens drei Monate lang, wenn dies gesetzlich zulässig ist.</p> <p><i>Hinweis: „Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Nicht hierzu zählen die Bereiche, in denen lediglich Point-of-Sale-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).</i></p>	<p>9.1.1 Überprüfen Sie, ob der Zugang zu zugangsbeschränkten Bereichen mit Hilfe von Videokameras und anderen Kontrollsystemen überwacht wird. Videokameras und sonstige Kontrollsysteme müssen vor Manipulation oder Deaktivierung geschützt werden. Überprüfen Sie, ob Videokameras bzw. sonstige Kontrollsysteme überwacht werden und dass die von diesen Geräten aufgezeichneten Daten mindestens drei Monate lang gespeichert werden.</p>			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
9.1.2 Beschränken des physischen Zugriffs auf öffentlich zugängliche Netzwerkbuchsen.	9.1.2 Ermitteln Sie durch Gespräche mit Netzwerkadministratoren und durch eigene Beobachtungen, ob Netzwerkbuchsen nur dann von befugten Mitarbeitern aktiviert werden, wenn sie benötigt werden. In Konferenzräumen, die von Besuchern genutzt werden, sollten beispielsweise keine Netzwerk-Ports mit DHCP-Unterstützung aktiviert sein. Achten Sie ansonsten darauf, dass Besucher nicht alleine bzw. unbeobachtet in Bereichen mit aktiven Netzwerkbuchsen arbeiten können.			
9.1.3 Beschränken des physischen Zugriffs auf WLAN-Zugriffspunkte, Gateways und Handgeräte.	9.1.3 Überprüfen Sie, ob der physische Zugriff auf WLAN-Zugriffspunkte, Gateways und Handgeräte angemessen beschränkt wird.			
9.2 Entwickeln von Verfahren, die es dem Personal erleichtern, zwischen Mitarbeitern und Besuchern zu unterscheiden, insbesondere in Bereichen, in denen auf Karteninhaberdaten zugegriffen werden kann. <i>„Mitarbeiter“ bezieht sich hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter und externe Mitarbeiter sowie Berater, die am Standort der jeweiligen Stelle „beheimatet“ sind. Ein „Besucher“ wird als Lieferant, Gast eines Mitarbeiters, Servicepersonal oder jede Person definiert, die die Einrichtung für kurze Zeit betreten muss, meist nicht länger als einen Tag.</i>	9.2.a Überprüfen Sie die Verfahren, nach denen den Mitarbeitern (und Besuchern) Ausweise ausgestellt werden, und achten Sie darauf, dass mit den Verfahren folgende Punkte abgedeckt sind: <ul style="list-style-type: none"> ▪ Ausstellen euer Ausweise, Ändern der Zugangs- bzw. Zugriffsanforderungen, Deaktivieren der Zugangsberechtigung für ausgeschiedene Mitarbeiter und bei auslaufendem Besucherstatus ▪ Beschränkter Zugriff auf Ausweissystem 			
	9.2.b Beobachten Sie Personen innerhalb der Einrichtung im Hinblick auf die Frage, ob sich Mitarbeiter leicht von Besuchern unterscheiden lassen.			
9.3 Sicherstellen, dass alle Besucher wie folgt behandelt werden:	9.3 Überprüfen Sie, ob die Kontrolle von Mitarbeitern/Besuchern wie folgt umgesetzt wird:			
9.3.1 Autorisierung zum Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder verwaltet werden.	9.3.1 Beobachten Sie, ob Besucher über entsprechende Ausweise verfügen und diese benutzen. Versuchen Sie, ins Rechenzentrum zu gelangen, und testen Sie dabei, ob ein Besucherausweis tatsächlich dazu führt, dass kein unbeaufsichtigter Zugang zu Bereichen mit Karteninhaberdaten gewährt wird.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
9.3.2 Begrenzt gültige Zugangserlaubnis (z. B. Ausweis oder Zugangsgesamt) für Besucher, aus der hervorgeht, dass es sich nicht um Mitarbeiter handelt.	9.3.2 Untersuchen Sie die Ausweise für Mitarbeiter und Besucher daraufhin, ob sich mit ihrer Hilfe leicht zwischen Mitarbeitern und Besuchern bzw. externen Personen unterscheiden lässt und ob die Besucherausweise nur begrenzt gültig sind.			
9.3.3 Bitte um Rückgabe der Zugangserlaubnis, wenn die Besucher die Einrichtung verlassen oder die Erlaubnis ausläuft.	9.3.3 Beobachten Sie, ob Besucher die Zugangserlaubnis beim Verlassen der Einrichtung bzw. beim Auslaufen der Erlaubnis zurückgeben.			
9.4 Überprüfen der Besucheraktivität anhand eines Besucherprotokolls. Protokollieren des Namen des Besuchers, des Firmennamens und des Namens des Mitarbeiters, der dem Besucher Zugang gewährt. Aufbewahren des Besucherprotokolls für die Dauer von mindestens drei Monaten, wenn dies gesetzlich zulässig ist.	9.4.a Überprüfen Sie, ob es ein Besucherprotokoll gibt, in dem der Zugang zur Einrichtung sowie zu den Computerräumen und Rechenzentren, in denen Karteninhaberdaten gespeichert oder übertragen werden, protokolliert wird.			
	9.4.b Überprüfen Sie, ob das Protokoll zumindest den Namen des Besuchers, den Firmennamen und den Namen des Mitarbeiters, der den Zugang gewährt, enthält, und ob das Protokoll mindestens drei Monate lang aufbewahrt wird.			
9.5 Aufbewahren von Sicherungskopien an einem sicheren Ort, vorzugsweise in räumlicher Entfernung, wie z. B. an einem Alternativ- oder Backup-Standort oder bei einem kommerziellen Anbieter von Speicherkapazitäten. Überprüfen der Sicherheit dieses Standorts mindestens einmal pro Jahr.	9.5 Kontrollieren Sie, ob der für die Speicherung gewählte Standort mindestens einmal im Jahr auf die Sicherheit der dort aufbewahrten Sicherungskopien überprüft wird.			
9.6 Sicherstellen der physischen Sicherheit aller Papierdokumente und elektronischen Medien mit Karteninhaberdaten.	9.6 Überprüfen Sie, ob die Verfahren zum Schutz von Karteninhaberdaten Kontrollen zur physischen Sicherheit von Papierdokumenten und elektronischen Medien (Computern, elektronischen Wechselmedien, Netzwerk- und DFÜ-Hardware, Quittungen, Berichten und Faxseiten) umfassen.			
9.7 Strikte Kontrolle der internen bzw. externen Verteilung dieser Art von Medien mit Karteninhaberdaten.	9.7 Überprüfen Sie, ob eine Richtlinie zur Kontrolle der Verteilung von Medien mit Karteninhaberdaten vorhanden ist und ob diese Richtlinie sämtliche Medien abdeckt (d. h. auch die, die an Einzelpersonen verteilt wurden).			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
9.7.1 Klassifizieren der Medien, damit sie als vertraulich identifiziert werden können.	9.7.1 Überprüfen Sie, ob sämtliche Medien so klassifiziert werden, dass sie als vertraulich identifiziert werden können.			
9.7.2 Senden der Medien per sicherem Kurier oder mit einer anderen Liefermethode, die präzise verfolgt werden kann?	9.7.2 Überprüfen Sie, ob ein Protokoll über alle Medien, die diese Einrichtung verlassen, geführt wird, ob dieser Versand vom Management genehmigt wird und ob der Versand per sicherem Kurier oder mit einer anderen Liefermethode, die präzise verfolgt werden kann, erfolgt.			
9.8 Sicherstellen, dass das Management den Transfer sämtlicher Medien mit Karteninhaberdaten aus einem geschützten Bereich genehmigen muss (insbesondere, wenn die Medien an Einzelne weitergegeben werden).	9.8 Überprüfen Sie bei aktuellen und an mehreren Tagen genommenen Stichproben aus den Protokollen zur Standortverfolgung von Medien mit Karteninhaberdaten, ob alle wichtigen Details protokolliert wurden und die Genehmigung durch das Management vorlag.			
9.9 Strikte Kontrolle der Aufbewahrung und des Zugriffs auf Medien mit Karteninhaberdaten.	9.9 Untersuchen Sie die Richtlinie zur Kontrolle der Aufbewahrung und Verwaltung von Ausdrucken und elektronischen Medien, und prüfen Sie, ob darin eine regelmäßige Inventur der vorhandenen Medien vorgesehen ist.			
9.9.1 Ordnungsgemäße Verwaltung von Medieninventurlisten und Durchführung mindestens einer jährlichen Medieninventur.	9.9.1 Untersuchen Sie das Medien-Inventurprotokoll, und achten Sie darauf, dass eine Inventur der vorhandenen Medien mindestens einmal pro Jahr stattfindet.			
9.10 Löschen/Vernichten von Medien mit Karteninhaberdaten, sobald die Daten nicht mehr zu geschäftlichen oder juristischen Zwecken benötigt werden.	9.10 Untersuchen Sie die Richtlinie zur regelmäßigen Löschung/Vernichtung von Medien, und überprüfen Sie, ob diese Richtlinie für sämtliche Medien, auf denen Karteninhaberdaten enthalten sind, gilt. Gehen Sie dabei wie folgt vor:			
9.10.1 Einsatz von Aktenvernichtern für Ausdrücke usw.	9.10.1.a Überprüfen Sie, ob Ausdrücke der Aktenvernichtung zugeführt werden und nach allgemeinem Ermessen ausgeschlossen werden kann, dass diese Dokumente wiederhergestellt werden.			
	9.10.1.b Überprüfen Sie, ob Container zur Aufbewahrung von zu löschenden Daten geschützt sind. Achten Sie beispielsweise darauf, dass ein Container mit zu vernichtenden Akten mit einem Schloss gesichert ist.			
9.10.2 Löschen von Karteninhaberdaten auf elektronischen Medien in einer Art und Weise, die eine Wiederherstellung der Daten unmöglich macht.	9.10.2 Überprüfen Sie, ob die Karteninhaberdaten auf elektronischen Medien nach Branchenstandards unbrauchbar und nicht wiederherstellbar gemacht werden bzw. dass die Medien ansonsten physisch unbrauchbar gemacht werden (z. B. durch Entmagnetisierung).			

Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken

Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten

Protokollierungssysteme und die Möglichkeit, Benutzeraktivitäten nachzuverfolgen, sind wichtige Elemente bei dem Versuch, eine Zugriffsschutzverletzung zu verhindern oder aufzuspüren bzw. deren Auswirkungen so gering wie möglich zu halten. Durch Protokolle in den verschiedenen Umgebungen kann die Ursache von Problemen schnell gefunden werden. Außerdem können Warnmeldungen ausgegeben und Analysen erstellt werden. Die Ursache für eine Sicherheitsverletzung lässt sich ohne Protokolle der Systemaktivität nur sehr schwer ermitteln.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
10.1 Einrichten eines Prozesses zur Verknüpfung des gesamten Zugriffs auf Systemkomponenten (insbesondere des Zugriffs mit Administratorprivilegien wie root) mit den einzelnen Benutzern.	10.1 Prüfen Sie durch Befragung des Systemadministrators und durch eigene Beobachtung, ob Audit-Trails für die Systemkomponenten vorhanden und aktiv sind.			
10.2 Implementierung automatisierter Audit-Trails für alle Systemkomponenten zur Rekonstruktion der folgenden Ereignisse:	10.2 Führen Sie durch Gespräche, die Untersuchung von Audit-Protokollen und die Prüfung der Protokolleinstellungen Folgendes durch:			
10.2.1 Alle individuellen Zugriffe auf Karteninhaberdaten	10.2.1 Prüfen Sie, ob alle individuellen Zugriffe auf Karteninhaberdaten protokolliert werden.			
10.2.2 Alle von einer Einzelperson mit root- oder Administratorrechten vorgenommene Aktionen	10.2.2 Prüfen Sie, ob alle von einer Einzelperson mit root- oder Administratorrechten vorgenommenen Aktionen protokolliert werden.			
10.2.3 Zugriff auf alle Audit-Trails	10.2.3 Prüfen Sie, ob der Zugriff auf alle Audit-Trails protokolliert wird.			
10.2.4 Ungültige logische Zugriffsversuche	10.2.4 Prüfen Sie, ob ungültige logische Zugriffsversuche protokolliert werden.			
10.2.5 Verwendung von Identifizierungs- und Authentifizierungssystemen	10.2.5 Prüfen Sie, ob die Verwendung von Identifizierungs- und Authentifizierungssystemen protokolliert wird.			
10.2.6 Initialisierung der Audit-Protokolle	10.2.6 Prüfen Sie, ob die Initialisierung der Audit-Protokolle protokolliert wird.			
10.2.7 Erstellen und Löschen von Objekten auf Systemebene	10.2.7 Prüfen Sie, ob das Erstellen und Löschen von Objekten auf Systemebene protokolliert wird.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
10.3 Aufzeichnen von mindestens den folgenden Audit-Trail-Einträgen für alle Systemkomponenten zu jedem Ereignis:	10.3 Führen Sie durch Gespräche und eigene Beobachtung zu jedem zu protokollierenden Ereignis (aus 10.2) Folgendes durch:			
10.3.1 Benutzer-ID	10.3.1 Prüfen Sie, ob die Benutzer-ID in den Protokolleinträgen enthalten ist.			
10.3.2 Art des Ereignisses	10.3.2 Prüfen Sie, ob die Art des Ereignisses in den Protokolleinträgen enthalten ist.			
10.3.3 Datum und Uhrzeit	10.3.3 Prüfen Sie, ob die Datums- und Zeitangabe in den Protokolleinträgen enthalten ist.			
10.3.4 Erfolg oder Fehler	10.3.4 Prüfen Sie, ob der Hinweis auf die erfolgreiche oder fehlgeschlagene Ausführung in den Protokolleinträgen enthalten ist.			
10.3.5 Ursprung des Ereignisses	10.3.5 Prüfen Sie, ob der Ursprung des Ereignisses in den Protokolleinträgen enthalten ist.			
10.3.6 Identität oder Name der betroffenen Daten, Systemkomponenten oder Ressourcen	10.3.6 Überprüfen Sie, ob die Identität oder der Name der betroffenen Daten, Systemkomponenten oder Ressourcen in den Protokolleinträgen enthalten ist.			
10.4 Synchronisation aller kritischen Systemuhren und -zeiten.	10.4 Prüfen Sie den Prozess zum Ermitteln und zur Weitergabe der richtigen Zeit innerhalb der Organisation sowie stichprobenartig die zeitbedingten Systemparametereinstellungen bei Systemkomponenten. Überprüfen Sie, ob folgende Elemente im Prozess enthalten und implementiert sind:			
	10.4.a Überprüfen Sie, ob eine bekannte und stabile Version des Network Time Protocol (NTP) oder einer ähnlichen Technologie entsprechend den PCI DSS-Anforderungen 6.1 und 6.2 für die Zeitsynchronisierung verwendet wird.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
	<p>10.4.b Achten Sie darauf, dass interne Server keine Zeitsignale von externen Quellen empfangen. [Innerhalb der Organisation empfangen zwei oder drei zentrale Zeitserver externe Zeitsignale [entweder über ein spezielles Funksignal, per GPS-Satellit oder aus einer externen Quelle auf der Grundlage der Internationalen Atomzeit bzw. der Koordinierten Weltzeit (UTC; früher GMT)] und sorgen im Austausch untereinander für eine höchstmögliche Genauigkeit. Darüber hinaus leiten sie die Zeitinformationen an andere interne Server weiter.]</p>			
	<p>10.4.c Überprüfen Sie, ob spezielle externe Hosts vorhanden sind, von denen die Zeitserver NTP-Zeitaktualisierungen empfangen (und verhindern, dass die Uhr von einer Einzelperson manipuliert werden kann). Diese Zeitaktualisierungen können mit einem symmetrischen Schlüssel verschlüsselt werden. Außerdem können Zugriffssteuerungslisten erstellt werden, aus denen die IP-Adressen der Clients hervorgehen, die den NTP-Dienst nutzen. Hierdurch wird die Nutzung nicht autorisierter interner Zeitserver verhindert. Weitere Informationen finden Sie unter www.ntp.org.</p>			
10.5 Schutz der Audit-Trails vor Veränderungen.	10.5 Ermitteln Sie in Gesprächen mit Systemadministratoren und durch die Untersuchung von Berechtigungen, ob Audit-Trails so geschützt sind, dass sie nicht geändert werden können. Gehen Sie wie folgt vor:			
10.5.1 Beschränken der Anzeige der Audit-Trails auf Personen mit arbeitsbedingtem Bedarf.	10.5.1 Überprüfen Sie, ob Einzelpersonen nur mit arbeitsbedingtem Bedarf auf Audit-Trail-Dateien zugreifen können.			
10.5.2 Schutz von Audit-Trail-Dateien vor nicht autorisierten Änderungen.	10.5.2 Überprüfen Sie, ob die Dateien des aktuellen Audit-Trails mit Zugriffssteuerungssystemen, räumlicher Trennung und/oder Netzwerktrennung vor unbefugten Änderungen geschützt werden.			
10.5.3 Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.	10.5.3 Überprüfen Sie, ob Dateien des aktuellen Audit-Trails sofort auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen, gesichert werden.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
10.5.4 Erstellen von Protokollen für nach außen gerichtete Technologien auf einem Protokollserver im internen LAN.	10.5.4 Überprüfen Sie, ob Protokolle für nach außen gerichtete Technologien (z. B. Wireless-Systeme, Firewalls, DNS, E-Mail) auf sicheren, zentralen und internen Protokollservern oder Medien abgelegt bzw. dorthin kopiert werden.			
10.5.5 Verwenden von Software zur Dateiintegritätsüberwachung und Änderungserfassung für Protokolle, damit bei der Änderung von bestehenden Protokoll Daten ein Alarm ausgelöst wird (nicht jedoch bei der Eingabe neuer Daten).	10.5.5 Überprüfen Sie die Verwendung der Software zur Dateiintegritätsüberwachung und Änderungserfassung für Protokolle, indem Sie die Systemeinstellungen und die überwachten Dateien sowie die Ergebnisse der Überwachung untersuchen.			
10.6 Mindestens einmal tägliche Untersuchung der Protokolle für alle Systemkomponenten. Protokollüberprüfungen müssen die Server mit Sicherheitsfunktionen wie Intrusion Detection System (IDS) und Authentication, Authorization and Accounting (AAA)-Protokollserver (z. B. RADIUS) umfassen. <i>Hinweis: Zur Konformität mit Anforderung 10.6 können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.</i>	10.6.a Untersuchen Sie Sicherheitsrichtlinien und -verfahren daraufhin, ob sie Verfahren zur mindestens einmal täglich stattfindenden Prüfung von Sicherheitsprotokollen enthalten und dass Ausnahmen zwingend überprüft werden müssen.			
	10.6.b Prüfen Sie durch Gespräche und eigene Beobachtungen, ob regelmäßig die Protokolle sämtlicher Systemkomponenten geprüft werden.			
10.7 Aufbewahren der Audit-Trail-Verlaufdaten für den Zeitraum mindestens eines Jahres, wobei ein mindestens dreimonatiger Zeitraum sofort für die Analyse bereitstehen muss (beispielsweise online, archiviert oder aus einer Sicherung wiederherstellbar).	10.7.a Untersuchen Sie die Sicherheitsrichtlinien und -verfahren daraufhin, ob sie Aufbewahrungsrichtlinien für das Audit-Protokoll mit einer mindestens einjährigen Aufbewahrungsfrist enthalten.			
	10.7.b Überprüfen Sie, ob Audit-Protokolle mindestens ein Jahr lang verfügbar sind und dass Prozesse zur sofortigen Wiederherstellung des Protokolls aus den mindestens drei letzten Monaten zur Verfügung stehen.			

Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

Schwachstellen in der Sicherheit bleiben meist nicht lange unentdeckt. Auch neue Software führt häufig zu zusätzlichen Gefahren. Systemkomponenten, Prozesse und individuelle Software müssen regelmäßig getestet werden, da sich nur so eine effektive Sicherheit in einer sich ändernden Umgebung erzielt werden kann.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
11.1 Regelmäßige, mindestens einmal im Quartal erfolgende Tests auf WLAN-Zugriffspunkte mit einem Analysegerät oder Einsatz eines Wireless IDS/IPS-Systems zur Ermittlung aller im Betrieb befindlichen Wireless-Geräte.	11.1.a Überprüfen Sie, ob mindestens einmal pro Quartal ein Wireless-Analysegerät eingesetzt wird oder ein Wireless IDS/IPS-System zur Ermittlung sämtlicher Wireless-Geräte implementiert und konfiguriert wurde.			
	11.1.b Überprüfen Sie beim Einsatz eines Wireless IDS/IPS-Systems, ob das Personal bei einem Alarm benachrichtigt wird.			
	11.1 c Überprüfen Sie, ob im Vorfalreaktionsplan (Anforderung 12.9) eine Reaktion für den Fall definiert ist, dass nicht autorisierte Wireless-Geräte entdeckt werden.			
11.2 Ausführen interner und externer Netzwerkanfälligkeitsscans mindestens vierteljährlich und nach jeder signifikanten Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Änderung der Firewall-Regeln, Produkt-Upgrades). <i>Hinweis: Vierteljährliche externe Netzwerkanfälligkeitsscans müssen von einem Approved Scanning Vendor (ASV) durchgeführt werden, der vom Payment Card Industry Security Standards</i>	11.2.a Untersuchen Sie die Ergebnisse der Anfälligkeitsscans aus den letzten vier Quartalen für die Komponenten internes Netzwerk, Host und Anwendung, und prüfen Sie, ob die Geräte in der Umgebung, in der Karteninhaberdaten gespeichert werden, regelmäßig Sicherheitstests unterzogen werden. Überprüfen Sie, ob der Scan-Vorgang so lange durchgeführt wird, bis das gefundene Fehler behoben wurden. <i>Hinweis: Nach Netzwerkänderungen durchgeführte externe Scans sowie interne Scans können vom entsprechend qualifizierten internen Personal des Unternehmens oder von einem Drittanbieter ausgeführt werden.</i>			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p><i>Council (PCI SSC) zugelassen wurde. Nach Netzwerkänderungen durchgeführte Scans können vom internen Personal des Unternehmens ausgeführt werden.</i></p>	<p>11.2.b Überprüfen Sie, ob der externe Scan vierteljährlich in Übereinstimmung mit den PCI-Sicherheitsscanverfahren durchgeführt wird. Prüfen Sie dabei die Ergebnisse der vier letzten Quartale beim externen Netzanfälligkeitsscan, und beachten Sie folgende Punkte:</p> <ul style="list-style-type: none"> ▪ In den letzten 12 Monaten müssen mindestens 4 Quartals-Scans stattgefunden haben. ▪ Die Ergebnisse der einzelnen Scans entsprechen den PCI-Sicherheitsscanverfahren (beispielsweise keine dringenden Probleme bzw. keine kritischen oder hohen Anfälligkeiten). ▪ Die Scans wurden von einem durch PCI SSC zugelassenen Approved Scanning Vendor durchgeführt. <p><i>Hinweis: Es ist für die anfängliche PCI DSS-Konformität nicht erforderlich, dass vier bestandene vierteljährliche Scans abgeschlossen sein müssen, wenn der Prüfer überprüft, dass 1) das letzte Scan-Ergebnis ein positives Ergebnis war, 2) die Einheit über dokumentierte Richtlinien und Verfahren verfügt, die eine Fortsetzung der vierteljährlichen Scans erfordern, und 3) alle im ersten Scan festgestellten Anfälligkeiten korrigiert wurden, wie ein erneuter Scan beweist. Für die Folgejahre nach der ersten PCI DSS-Prüfung müssen vier bestandene vierteljährliche Scans vorliegen.</i></p>			
	<p>11.2.c Überprüfen Sie, ob nach signifikanten Änderungen am Netzwerk interne und/oder externe Scans durchgeführt wurden. Untersuchen Sie hierfür die Scan-Ergebnisse des letzten Jahres. Überprüfen Sie, ob der Scan-Vorgang so lange durchgeführt wird, bis das gefundene Fehler behoben wurden.</p>			
<p>11.3 Durchführen externer und interner Penetrationstests mindestens einmal im Jahr und nach jeder signifikanten Infrastruktur- oder Anwendungsaktualisierung oder -änderung (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver). Diese Penetrationstests müssen Folgendes enthalten:</p>	<p>11.3.a Untersuchen Sie die Ergebnisse des aktuellsten Penetrationstests, und prüfen Sie, ob der Penetrationstest mindestens einmal im Jahr und nach jeder signifikanten Änderung der Umgebung durchgeführt wird. Überprüfen Sie, ob angemerkte Anfälligkeiten korrigiert wurden und ob anschließend ein erneuter Test durchgeführt wurde.</p>			
	<p>11.3.b Überprüfen Sie, ob der Test von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt wurde und gegebenenfalls, ob der Tester für eine unabhängige Organisation tätig ist (muss kein QSA oder ASV sein).</p>			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
11.3.1 Penetrationstests auf Netzwerkebene	11.3.1 Überprüfen Sie, ob der Penetrationstest auch Tests auf Netzwerkebene umfasst. Die Tests müssen Komponenten enthalten, die Netzwerkfunktionen und Betriebssysteme unterstützen.			
11.3.2 Penetrationstests auf Anwendungsebene	11.3.2 Überprüfen Sie, ob der Penetrationstest auch Tests auf Anwendungsebene umfasst. Bei Webanwendungen müssen die Tests mindestens die in Anforderung 6.5 aufgeführten Anfälligkeiten umfassen.			
11.4 Nutzung von Systemen zur Erkennung und/oder Verhinderung von Eindringversuchen zur Überwachung des kompletten Datenverkehrs in der Umgebung, in der sich Karteninhaberdaten befinden, und Alarmierung des Personals bei mutmaßlichen Sicherheitsverletzungen. Ständige Aktualisierung der Intrusionserfassungs- und -vorbeugungssysteme.	11.4a Überprüfen Sie die Nutzung von Systemen zur Erkennung und/oder Verhinderung von Eindringversuchen, und stellen Sie sicher, dass der komplette Datenverkehr in der Umgebung, in der sich Karteninhaberdaten befinden, überwacht wird.			
	11.4.b Überprüfen Sie, ob IDS und/oder IPS so konfiguriert sind, dass das Personal bei mutmaßlichen Sicherheitsverletzungen alarmiert wird.			
	11.4.c Untersuchen Sie die IDS/IPS-Konfigurationen, und prüfen Sie, ob IDS/IPS-Geräte im Sinne eines optimalen Schutzes entsprechend den Anbieteranweisungen konfiguriert, gewartet und aktualisiert werden.			
11.5 Bereitstellen von Software zur Überwachung der Dateiintegrität, die einen Alarm ausgibt, wenn es zu nicht autorisierten Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien kommt, und Konfiguration der Software für einen mindestens einmal pro Woche durchzuführenden Vergleich wichtiger Dateien. <i>Hinweis: Für die Dateiintegritätsüberwachung sind wichtige Dateien in der Regel Dateien, die sich nicht regelmäßig ändern, deren Änderung aber auf eine Sicherheitsverletzung im System oder das Risiko einer Verletzung hinweisen könnte. Produkte zur Dateiintegritätsüberwachung sind in der Regel mit wichtigen Dateien für das jeweilige Betriebssystem vorkonfiguriert. Andere wichtige Dateien wie solche für benutzerdefinierte Anwendungen müssen von der jeweiligen Stelle (Händler oder Dienstanbieter) beurteilt und definiert werden.</i>	11.5 Überprüfen Sie die Nutzung von Produkten zur Überwachung der Dateiintegrität innerhalb der Umgebung mit Karteninhaberdaten, indem Sie die Systemeinstellungen und die überwachten Dateien sowie Ergebnisse aus der Aktivitätsüberwachung untersuchen. Beispiele für Dateien, die überwacht werden sollten: <ul style="list-style-type: none"> ▪ Ausführbare Systemdateien ▪ Ausführbare Anwendungsdateien ▪ Konfigurations- und Parameterdateien ▪ Zentral gespeicherte Protokoll- und Audit-Dateien (alt oder archiviert) 			

Befolgung einer Informationssicherheits-Richtlinie

Anforderung 12: Befolgung einer Informationssicherheits-Richtlinie für Mitarbeiter und Subunternehmer

Eine strenge Sicherheitsrichtlinie gibt den Takt für das gesamte Unternehmen vor und dient den Mitarbeitern als Richtschnur dafür, was von ihnen verlangt wird. Sämtliche Mitarbeiter sollten sich darüber im Klaren sein, dass Daten Gefahren ausgesetzt sind und dass sie für deren Schutz verantwortlich sind. „Mitarbeiter“ bezieht sich hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter und externe Mitarbeiter sowie Berater, die am Standort der jeweiligen Stelle „beheimatet“ sind.

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
12.1 Festlegen, Veröffentlichen, Verwalten und Verbreiten einer Sicherheitsrichtlinie mit den folgenden Zielen:	12.1 Untersuchen Sie die Sicherheitsrichtlinie, und prüfen Sie, ob die Richtlinie veröffentlicht und an alle relevanten Systembenutzer (Anbieter, Subunternehmer und Geschäftspartner) weitergeleitet wurde.			
12.1.1 Sie umfasst sämtliche PCI DSS-Anforderungen.	12.1.1 Überprüfen Sie, ob die Richtlinie sämtliche PCI DSS-Anforderungen umfasst.			
12.1.2 Sie umfasst einen jährlichen Prozess zur Ermittlung von Bedrohungen und Anfälligkeiten, der zu einer offiziellen Risikobeurteilung führt.	12.1.2 Überprüfen Sie, ob die Richtlinie zur Informationssicherheit einen jährlichen Prozess zur Ermittlung von Bedrohungen und Anfälligkeiten umfasst, der zu einer offiziellen Risikobeurteilung führt.			
12.1.3 Sie umfasst eine Überprüfung mindestens einmal im Jahr sowie Aktualisierungen bei Umgebungsänderungen.	12.1.3 Überprüfen Sie, ob die Richtlinie zur Informationssicherheit mindestens einmal im Jahr überarbeitet und an die geänderten Geschäftsziele bzw. Risiken angepasst wird.			
12.2 Entwickeln von Routineverfahren für die Betriebssicherheit, die den Anforderungen in dieser Spezifikation entsprechen (z. B. Benutzerkonto-Wartungsverfahren und Protokollüberprüfungsverfahren).	12.2.a Überprüfen Sie die Routineverfahren für die Betriebssicherheit. Überprüfen Sie, ob sie im Einklang mit dieser Spezifikation stehen und administrative und technische Verfahren für die einzelnen Anforderungen enthalten.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
12.3 Entwickeln von Verwendungsrichtlinien für wichtige Technologien, mit denen die Mitarbeiter arbeiten (Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Notebooks, PDAs, E-Mail-Programme und Browser), und Definition der korrekten Verwendung dieser Technologien für Mitarbeiter und Subunternehmer. Die Verwendungsrichtlinien umfassen folgende Punkte:	12.3 Untersuchen Sie die Richtlinie auf wichtige Technologien für Mitarbeiter, und führen Sie Folgendes durch:			
12.3.1 Ausdrückliche Genehmigung durch das Management	12.3.1 Überprüfen Sie, ob in der Verwendungsrichtlinie eine ausdrückliche Genehmigung des Managements für die Verwendung dieser Technologien festgelegt ist.			
12.3.2 Authentifizierung zur Verwendung der Technologie	12.3.2 Überprüfen Sie, ob die Technologie laut Verwendungsrichtlinie nur nach Authentifizierung durch eine Benutzer-ID und ein Kennwort oder ein anderes Element (z. B. ein Token) genutzt werden kann.			
12.3.3 Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff	12.3.3 Überprüfen Sie, ob laut Verwendungsrichtlinie eine Liste sämtlicher Geräte und der zur Verwendung der Geräte befugten Personen angelegt werden muss.			
12.3.4 Etikettierung von Geräten mit Hinweis zu Eigner und Zweck sowie Kontaktinformationen	12.3.4 Überprüfen Sie, ob die Verwendungsrichtlinie eine Etikettierung von Geräten mit Hinweis zu Eigner und Zweck sowie Kontaktinformationen vorschreibt.			
12.3.5 Akzeptable Verwendung der Technologie	12.3.5 Überprüfen Sie, ob in der Verwendungsrichtlinie festgelegt ist, welche Verwendung der Technologie akzeptabel ist.			
12.3.6 Akzeptable Netzwerkorte für die Technologien	12.3.6 Überprüfen Sie, ob in der Verwendungsrichtlinie festgelegt ist, welche Netzwerkorte für die Technologie akzeptabel sind.			
12.3.7 Liste der vom Unternehmen zugelassenen Produkte	12.3.7 Überprüfen Sie, ob in der Verwendungsrichtlinie eine Liste mit vom Unternehmen zugelassenen Produkten vorgeschrieben ist.			
12.3.8 Automatisches Trennen von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität	12.3.8 Überprüfen Sie, ob in der Verwendungsrichtlinie eine automatische Trennung von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität festgelegt ist.			
12.3.9 Aktivierung von Remotezugriff-Technologien für Lieferanten nur im Bedarfsfall und mit sofortiger Deaktivierung nach der Verwendung	12.3.9 Überprüfen Sie, ob die Verwendungsrichtlinie eine Aktivierung von Remotezugriff-Technologien für Lieferanten nur im Bedarfsfall und mit sofortiger Deaktivierung nach der Verwendung vorsieht.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
12.3.10 Karteninhaberdaten können bei einem Remotezugriff nicht auf lokale Festplatten und elektronische Wechselmedien kopiert oder verschoben werden	12.3.10 Überprüfen Sie, ob in der Verwendungsrichtlinie festgelegt ist, dass Karteninhaberdaten bei einem Remotezugriff nicht auf lokale Festplatten und elektronische Wechselmedien kopiert oder verschoben werden dürfen.			
12.4 Klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter und Subunternehmer in den Sicherheitsrichtlinien und Verfahren.	12.4 Überprüfen Sie, ob die Sicherheitsrichtlinien eine klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter und Subunternehmer enthalten.			
12.5 Zuweisen der folgenden Managementverantwortungsbereiche in puncto Informationssicherheits zu einer Einzelperson oder einem Team.	12.5 Überprüfen Sie, welchem Sicherheitsbeauftragten oder welchem für die Sicherheit zuständigen Mitglied des Managements die formale Verantwortung für die Informationssicherheit übertragen wurde. Untersuchen Sie die Richtlinien und Verfahren zur Informationssicherheit, und prüfen Sie, ob folgende Verantwortlichkeiten konkret und formal geregelt wurden:			
12.5.1 Festlegen, Dokumentieren und Verteilen von Sicherheitsrichtlinien und -verfahren	12.5.1 Überprüfen Sie, ob die Verantwortlichkeit für die Erstellung und Verteilung von Sicherheitsrichtlinien und -verfahren formal geregelt wurde.			
12.5.2 Überwachung und Analyse von Sicherheitsalarmen und -informationen und Verteilung an das jeweilige Personal.	12.5.2 Überprüfen Sie, ob die Verantwortlichkeit für die Überwachung und Analyse von Sicherheitsalarmen sowie für die Weitergabe von Informationen an das zuständige Personal formal zugewiesen wurde.			
12.5.3 Festlegen, Dokumentieren und Weitergeben von Reaktions- und Eskalationsverfahren für Sicherheitsvorfälle, die eine rechtzeitige und effektive Vorgehensweise in allen Situationen gewährleisten.	12.5.3 Überprüfen Sie, ob die Verantwortlichkeit für die Festlegung, Dokumentation und Weitergabe von Reaktions- und Eskalationsverfahren für Sicherheitsvorfälle formal geregelt wurde.			
12.5.4 Verwalten von Benutzerkonten einschließlich Hinzufügen, Löschen und Ändern	12.5.4 Überprüfen Sie, ob die Verantwortlichkeit für die Verwaltung von Benutzerkonten und für das Authentifizierungsmanagement formal geregelt wurde.			
12.5.5 Überwachung und Kontrolle des gesamten Datenzugriffs	12.5.5 Überprüfen Sie, ob die Verantwortlichkeit für die Überwachung und Kontrolle des gesamten Datenzugriffs formal geregelt wurde.			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
12.6 Implementierung eines offiziellen Sicherheitsbewusstseinsprogramms, mit dem allen Mitarbeitern die Bedeutung der Sicherheit der Karteninhaberdaten vermittelt wird	12.6.a Überprüfen Sie, ob ein offizielles Sicherheitsbewusstseinsprogramm für alle Mitarbeiter verfügbar ist.			
	12.6.b Untersuchen Sie die Verfahren und die Dokumentation des Sicherheitsbewusstseinsprogramms, und führen Sie Folgendes durch:			
12.6.1 Schulung der Mitarbeiter bei Einstellung und danach mindestens einmal im Jahr.	12.6.1.a Überprüfen Sie, ob im Sicherheitsbewusstseinsprogramm mehrere Methoden zur Vermittlung des Bewusstseins für Sicherheitsprobleme angesprochen werden (beispielsweise Poster, Briefe, Memos, webbasierte Schulungen und Schwerpunktprogramme).			
	12.6.1.b Überprüfen Sie, ob die Mitarbeiter zur Einstellung und danach mindestens einmal im Jahr an entsprechenden Schulungen teilnehmen.			
12.6.2 Mindestens einmal pro Jahr gegebene schriftliche Bestätigung der Mitarbeiter, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens kennen	12.6.2 Überprüfen Sie, ob im Sicherheitsbewusstseinsprogramm festgelegt ist, dass die Mitarbeiter mindestens einmal im Jahr (schriftlich, elektronisch oder auf anderem Wege) bestätigen, dass sie die Richtlinie des Unternehmens zur Informationssicherheit kennen.			
12.7 Prüfen potenzieller Mitarbeiter (siehe Definition unter Punkt 9.2) vor der Einstellung, um das Risiko interner Angriffe so gering wie möglich zu halten. <i>Für Mitarbeiter wie z. B. Kassierer und Kassiererinnen, die bei Transaktionen nie Zugriff auf mehrere Kartennummern gleichzeitig haben, ist diese Anforderung lediglich eine Empfehlung.</i>	12.7 Überprüfen Sie in einem Gespräch mit der Leitung der Personalabteilung, ob Hintergrundinformationen zu Bewerbern geprüft werden (innerhalb der jeweiligen gesetzlichen Grenzen), wenn diese Personen Zugriff auf Karteninhaberdaten erhalten oder in der Umgebung mit Karteninhaberdaten arbeiten. (Beispiele für Hintergrundinformationen sind frühere Tätigkeiten, eventuelle Vorstrafen, die finanzielle Situation und Referenzen bisheriger Arbeitgeber.)			
12.8 Umsetzung und Einhaltung von Richtlinien und Verfahren zur Verwaltung von Diensteanbietern, falls diese ebenfalls Zugriff auf Karteninhaberdaten erhalten. Hierunter fallen die folgenden Punkte:	12.8 Wenn die betreffende Stelle Karteninhaberdaten an Diensteanbieter (z. B. Einrichtungen für die Aufbewahrung von Sicherungsbändern, Anbieter verwalteter Dienste wie Webhosting-Unternehmen und Sicherheitsdiensteanbieter oder Unternehmen, die Daten zur Aufklärung eventueller Betrugsversuche benötigen) weitergibt, prüfen Sie folgende Punkte, indem Sie Beobachtungen durchführen, Richtlinien und Verfahren prüfen und die zugehörige Dokumentation untersuchen:			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
12.8.1 Führen einer Liste mit Dienstanbietern.	12.8.1 Überprüfen Sie, ob eine Liste mit Dienstanbietern geführt wird.			
12.8.2 Schriftliche Vereinbarung, die eine Bestätigung umfasst, dass der Dienstanbieter für die Sicherheit der Karteninhaberdaten in seinem Besitz haftet.	12.8.2 Überprüfen Sie, ob eine schriftliche Vereinbarung existiert, die eine Bestätigung umfasst, dass die Dienstanbieter für die Sicherheit der Karteninhaberdaten haften.			
12.8.3 Festlegung eines eindeutigen Verfahrens für die Inanspruchnahme von Dienstanbietern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht.	12.8.3 Überprüfen Sie, ob Richtlinien und Verfahren für die Auswahl von Dienstanbietern vorliegen und ob bei der Wahl des Anbieters die erforderliche Sorgfalt beachtet wurde.			
12.8.4 Nutzung eines Programms zur Überwachung der Dienstanbieter-Konformität mit dem PCI-Datensicherheitsstandard.	12.8.4 Überprüfen Sie, ob an der betreffenden Stelle ein Programm zur Überwachung der Dienstanbieter-Konformität mit dem PCI-Datensicherheitsstandard eingesetzt wird.			
12.9 Implementieren eines Vorfalreaktionsplans, der eine sofortige Reaktion auf Sicherheitsverletzungen im System ermöglicht.	12.9 Untersuchen Sie den Vorfalreaktionsplan sowie zugehörige Verfahren, und führen Sie Folgendes durch:			

(Fortsetzung auf der nächsten Seite)

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>12.9.1 Erstellen des Vorfallreaktionsplans, der im Fall einer Sicherheitsverletzung im System umgesetzt wird. Der Plan umfasst mindestens die folgenden Punkte:</p> <ul style="list-style-type: none"> ▪ Rollen, Verantwortungsbereiche und Kommunikations- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken ▪ Konkrete Verfahren für die Reaktion auf Vorfälle ▪ Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs ▪ Verfahren zur Datensicherung ▪ Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen ▪ Abdeckung sämtlicher wichtigen Systemkomponenten ▪ Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle 	<p>12.9.1 Überprüfen Sie, ob der Vorfallreaktionsplan Folgendes umfasst:</p> <ul style="list-style-type: none"> ▪ Rollen, Verantwortungsbereiche und Kommunikationsstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken ▪ Konkrete Verfahren für die Reaktion auf Vorfälle ▪ Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs ▪ Verfahren zur Datensicherung ▪ Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen (z. B. das California Bill 1386, in dem vorgeschrieben wird, dass Unternehmen bei einer tatsächlichen oder mutmaßlichen Sicherheitsverletzung die Betroffenen benachrichtigen müssen, falls sich in der Datenbank Bürger des Staates Kalifornien befinden). ▪ Abdeckung sämtlicher wichtigen Systemkomponenten ▪ Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle 			
<p>12.9.2 Testen des Plans mindestens einmal im Jahr.</p>	<p>12.9.2 Überprüfen Sie, ob der Plan mindestens einmal im Jahr getestet wird.</p>			
<p>12.9.3 Rund-um-die-Uhr-Bereitstellung von bestimmtem Personal, das auf Alarme reagiert.</p>	<p>12.9.3 Überprüfen Sie durch Beobachtung und Untersuchung der Richtlinien, ob rund um die Uhr sofort auf Vorfälle reagiert sowie sämtlichen Verdachtsmomente hinsichtlich nicht autorisierter Aktivität nachgegangen wird. Prüfen Sie darüber hinaus, ob unbefugte WLAN-Zugriffspunkte erkannt, wichtige IDS-Alarme verfolgt und/oder Berichte zu nicht autorisierten Änderungen an wichtigen Systemen oder Inhaltsdateien angezeigt werden.</p>			
<p>12.9.4 Schulung von Mitarbeitern mit Verantwortung im Bereich der Reaktion auf Sicherheitsverletzungen.</p>	<p>12.9.4 Überprüfen Sie durch Beobachtungen und Untersuchung der Richtlinien, ob Mitarbeiter, die Verantwortung bei Sicherheitsverletzungen tragen, regelmäßig geschult werden.</p>			

PCI DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>12.9.5 Beachtung von Alarmen aus Systemen zur Erkennung und/oder Verhinderung von Eindringversuchen und zur Überwachung der Dateintegrität.</p>	<p>12.9.5 Überprüfen Sie durch Beobachtung und Untersuchung der Prozesse, ob die Überwachung und die Reaktion auf Alarme von Sicherheitssystemen (wie die Erkennung unbefugter WLAN-Zugriffspunkte) im Vorfallsreaktionsplan enthalten sind.</p>			
<p>12.9.6 Entwickeln eines Prozesses zur Änderung und Weiterentwicklung des Vorfallsreaktionsplan je nach eigenen Erfahrungen und Branchenentwicklungen.</p>	<p>12.9.6 Überprüfen Sie durch Beobachtung und Untersuchung von Richtlinien, ob ein Prozess zur Änderung und Weiterentwicklung des Vorfallsreaktionsplan nach den eigenen Erfahrungen und Branchenentwicklungen vorhanden ist.</p>			

Anhang A: Zusätzliche PCI DSS-Anforderungen für Anbieter von gemeinsamem Hosting

Anforderung A.1: Von mehreren Benutzern genutzte Hosting-Anbieter müssen die Umgebung mit Karteninhaberdaten schützen

Wie in Anforderung 12.8 erläutert, müssen sämtliche Dienstleister, die auf Karteninhaberdaten zugreifen können (auch gemeinsam genutzte Hosting-Anbieter), den PCI-Datensicherheitsstandard erfüllen. Außerdem geht aus Anforderung 2.4 hervor, dass gemeinsam genutzte Hosting-Anbieter die gehostete Umgebung und die Daten jeder Stelle schützen müssen. Aus diesem Grund müssen die Hosting-Anbieter auch die Anforderungen in diesem Anhang erfüllen.

Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>A.1 Schutz der gehosteten Umgebung und der Daten jeder Stelle (d. h. Händler, Dienstleister oder andere Stelle) wie in A.1.1 bis A.1.4: Ein Hosting-Anbieter muss diese Anforderungen sowie die anderen relevanten Abschnitte des PCI-Datensicherheitsstandards erfüllen.</p> <p><i>Hinweis: Auch wenn ein Hosting-Anbieter diese Anforderungen erfüllt, ist nicht garantiert, dass die Stelle, die den Hosting-Anbieter nutzt, die Konformitätskriterien erfüllt. Jede Stelle muss PCI DSS-konform arbeiten und die Konformität von Fall zu Fall beurteilen.</i></p>	<p>A.1 Wählen Sie insbesondere bei einer PCI DSS-Beurteilung eines gemeinsam genutzten Hosting-Anbieters zur Prüfung, ob die gehosteten Umgebungen und Daten der einzelnen Stellen (Händler und Dienstleister) geschützt werden, stichprobenartig verschiedene Server (Microsoft Windows und Unix/Linux) aus einem repräsentativen Querschnitt aus Hosting-Händlern und -Dienstleistern aus, und führen Sie die unter A.1.1 bis A.1.4 beschriebenen Tests durch.</p>			
<p>A.1.1 Sicherstellen, dass an den einzelnen Stellen nur Prozesse ausgeführt werden, die Zugriff auf die Karteninhaberdaten-Umgebung dieser Stelle haben.</p>	<p>A.1.1 Wenn ein gemeinsam genutzter Hosting-Anbieter Stellen (beispielsweise Händlern oder Dienstleistern) die Möglichkeit gibt, eigene Anwendungen auszuführen, überprüfen Sie, ob diese Anwendungsprozesse mit der eindeutigen ID der Stelle ausgeführt werden. Beispiel:</p> <ul style="list-style-type: none"> ▪ Keine Stelle im System kann die Benutzer-ID eines gemeinsamen Webservers verwenden. ▪ Sämtliche von einer Stelle verwendeten CGI-Skripte müssen als eindeutige Benutzer-ID der Stelle erstellt und ausgeführt werden. 			

Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
<p>A.1.2 Beschränken des Zugriffs und der Rechte der einzelnen Stellen auf die eigene Umgebung mit Karteninhaberdaten.</p>	<p>A.1.2.a Sorgen Sie dafür, dass die Benutzer-ID eines Anwendungsprozesses nicht über besondere Rechte (root/admin) verfügt.</p>			
	<p>A.1.2.b Überprüfen Sie, ob die einzelnen Stellen (Händler, Dienstanbieter) Lese-, Schreib- und Ausführungsberechtigungen nur für eigene Dateien und Verzeichnisse oder für notwendige Systemdateien (eingeschränkt durch Dateisystemberechtigungen, Zugriffssteuerungslisten, chroot, jailshell usw.) aufweisen. WICHTIG: Die Dateien einer Stelle können nicht von einer Gruppe gemeinsam genutzt werden.</p>			
	<p>A.1.2.c Stellen Sie sicher, dass die Benutzer einer Stelle keinen Schreibzugriff auf gemeinsam genutzte Systemdateien erhalten.</p>			
	<p>A.1.2.d Überprüfen Sie, ob die Anzeige von Protokolleinträgen auf die protokollbesitzende Stelle beschränkt ist.</p>			
	<p>A.1.2.e Überprüfen Sie, ob für die folgenden Systemressourcen Beschränkungen gelten (damit die einzelnen Stellen die Serverressourcen nicht komplett für sich in Anspruch nehmen und Anfälligkeiten wie Fehler-, Konkurrenz- und Neustartbedingungen, die beispielsweise zu Pufferüberläufen führen können, ausnutzen kann):</p> <ul style="list-style-type: none"> ▪ Festplattenkapazität ▪ Bandbreite ▪ Arbeitsspeicher ▪ Prozessor 			
<p>A.1.3 Aktivierung eindeutiger mit mit PCI DSS-Anforderung 10 konformer Protokollierungs- und Audit-Trails für die Karteninhaberdaten-Umgebung jeder Stelle.</p>	<p>A.1.3.a Überprüfen Sie, ob der gemeinsame Hosting-Anbieter die Protokollierung für jede einzelne Händler- und Dienstanbieterumgebung wie folgt aktiviert hat:</p> <ul style="list-style-type: none"> ▪ Protokolle werden für gängige Anwendungen von Drittanbietern aktiviert. ▪ Protokolle sind standardmäßig aktiviert. 			

Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/ Anmerkungen
	<ul style="list-style-type: none"> ▪ Protokolle können von der Stelle, die sie besitzt, eingesehen werden. ▪ Die Besitzer der Protokolle erhalten eine Mitteilung zum genauen Speicherort der Protokolle. 			
A.1.4 Aktivieren von Prozessen für eine rechtzeitige gerichtliche Untersuchung im Falle einer Sicherheitsverletzung bei einem gehosteten Händler oder Dienstanbieter.	A.1.4 Überprüfen Sie, ob der gemeinsam genutzte Hosting-Anbieter über schriftlich festgehaltene Richtlinien verfügt, die eine rechtzeitige gerichtliche Untersuchung von betroffenen Servern im Falle einer Sicherheitsverletzung ermöglichen.			

Anhang B: Kompensationskontrollen

Kompensationskontrollen können in den meisten Fällen, in denen eine Stelle eine explizite PCI DSS-Anforderung aufgrund von legitimen technischen oder dokumentierten geschäftlichen Einschränkungen nicht exakt erfüllen kann, in Erwägung gezogen werden. Voraussetzung hierfür ist jedoch, dass der mit der Nichterfüllung verbundene Risikozuwachs durch die Implementierung von Kontrollen an anderer Stelle kompensiert wird.

Kompensationskontrollen müssen die folgenden Kriterien erfüllen:

1. Sie müssen in Absicht und Anspruch den ursprünglichen PCI DSS-Anforderungen entsprechen.
2. Sie müssen ein vergleichbares Schutzniveau wie die ursprüngliche PCI DSS-Anforderung bieten. Dies bedeutet, dass die Kompensationskontrolle die Risiken, gegen die die ursprüngliche PCI DSS-Anforderung gerichtet war, in ausreichendem Maße verhindert. (Die Absicht hinter den einzelnen PCI DSS-Anforderungen ist unter *PCI DSS-Navigation* erläutert.)
3. Sie müssen mindestens so weitreichend wie andere PCI DSS-Anforderungen sein. (Die reine Konformität mit anderen PCI DSS-Anforderungen reicht als Kompensation nicht aus.)

Beachten Sie folgende Anhaltspunkte für die Definition von „mindestens so weitreichend“:

Hinweis: Die Punkte a) bis c) sind nur als Beispiel gedacht. Sämtliche Kompensationskontrollen müssen vom Prüfer, der auch die PCI DSS-Prüfung vornimmt, daraufhin geprüft werden, ob sie eine ausreichende Kompensation darstellen. Die Effektivität einer Kompensationskontrolle hängt von der jeweiligen Umgebung ab, in der die Kontrolle implementiert wird, von den umgebenden Sicherheitskontrollen und der Konfiguration der Kontrolle. Unternehmen muss bewusst sein, dass eine bestimmte Kompensationskontrolle nicht in allen Umgebungen effektiv ist.

- a) Vorhandene PCI DSS-Anforderungen können NICHT als Kompensationskontrollen betrachtet werden, wenn sie für das in Frage kommende Element ohnehin erforderlich sind. Beispiel: Kennwörter für den nicht über die Konsole vorgenommenen Administratorzugriff müssen verschlüsselt versendet werden, damit Administrator Kennwörter nicht von Unbefugten abgefangen werden können. Als Kompensation für eine fehlende Kennwortverschlüsselung können nicht andere PCI DSS-Kennwortanforderungen wie das Aussperren von Eindringlingen, die Einrichtung komplexer Kennwörter usw. ins Feld geführt werden, das sich mit diesen Anforderungen das Risiko eines Abfangens unverschlüsselter Kennwörter nicht reduzieren lässt. Außerdem sind die anderen Kennwortkontrollen bereits Bestandteil der PCI DSS-Anforderungen für das betreffende Element (Kennwort).
 - b) Vorhandene PCI DSS-Anforderungen können EVENTUELL als Kompensationskontrollen betrachtet werden, wenn sie zwar für einen anderen Bereich, nicht aber für das in Frage kommende Element erforderlich sind. Beispiel: Beim Remotezugriff ist nach PCI DSS eine Authentifizierung anhand zweier Faktoren erforderlich. Die Authentifizierung anhand zweier Faktoren *innerhalb des internen Netzwerks* kann für den nicht über die Konsole stattfindenden Administratorzugriff als Kompensationskontrolle betrachtet werden, wenn eine Übertragung verschlüsselter Kennwörter nicht möglich ist. Die Zwei-Faktoren-Authentifizierung ist eine akzeptable Kompensationskontrolle, wenn (1) die Absicht der ursprünglichen Anforderung erfüllt wird (das Risiko des Abfangens unverschlüsselter Kennwörter wird verhindert) und (2) die Authentifizierung in einer sicheren Umgebung ordnungsgemäß konfiguriert wurde.
 - c) Die vorhandenen PCI DSS-Anforderungen können mit neuen Kontrollen zusammen als Kompensationskontrolle fungieren. Beispiel: Ein Unternehmen kann Karteninhaberdaten nicht nach Anforderung 3.4 unlesbar machen (z. B. durch Verschlüsselung). In diesem Fall könnte eine Kompensation darin bestehen, dass mit einem Gerät bzw. einer Kombination aus Geräten, Anwendungen und Kontrollen folgende Punkte sichergestellt sind: (1) interne Netzwerksegmentierung; (2) Filtern von IP- oder MAC-Adressen und (3) Zwei-Faktor-Authentifizierung innerhalb des internen Netzwerks.
4. Sie müssen dem zusätzlichen Risiko, das durch die Nichteinhaltung der PCI DSS-Anforderung entsteht, angemessen sein.

Der Prüfer führt im Rahmen der jährlichen PCI DSS-Beurteilung eine eingehende Überprüfung der Kompensationskontrollen durch und stellt dabei unter Beachtung der vier oben genannten Kriterien fest, ob die jeweiligen Kompensationskontrollen einen angemessenen Schutz vor den Risiken bieten, wie er mit der ursprünglichen PCI DSS-Anforderung erzielt werden sollte. Zur Wahrung der Konformität müssen Prozesse und Kontrollen implementiert sein, mit denen die Wirksamkeit der Kompensationskontrollen auch nach Abschluss der Beurteilung gewährleistet bleibt.

Anhang C: Arbeitsblatt zu Kompensationskontrollen

Mit diesem Arbeitsblatt können Sie Kompensationskontrollen für sämtliche Anforderungen definieren, bei denen die ursprüngliche PCI DSS-Anforderung nicht erfüllt werden kann. Kompensationskontrollen müssen außerdem im ROC im Abschnitt zur entsprechenden PCI DSS-Anforderung dokumentiert werden.

Hinweis: Nur Unternehmen, die eine Risikoanalyse vorgenommen und legitime technologische oder dokumentierte geschäftliche Hindernisse nachweisen können, können den Einsatz von Kompensationskontrollen zu Konformitätszwecken in Erwägung ziehen.

Anforderungsnummer und -definition:

	Erforderliche Informationen	Erklärung
1. Einschränkungen	Führen Sie Einschränkungen auf, die die Konformität mit der Originalanforderung ausschließen.	
2. Ziel	Definieren Sie das Ziel der ursprüngliche Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	
3. Ermitteltes Risiko	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	
4. Definition der Kompensationskontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	
5. Validierung der Kompensationskontrollen	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	
6. Verwaltung	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	

Arbeitsblatt zu Kompensationskontrollen – Beispiel

Mit diesem Arbeitsblatt können Sie die Kompensationskontrollen für jede Anforderung definieren, bei der über Kompensationskontrollen „JA“ ausgewählt wurde.

Anforderungsnummer: 8.1– *Werden alle Benutzer mit einem eindeutigen Benutzernamen identifiziert, bevor ihnen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird?*

	Erforderliche Informationen	Erklärung
1. Einschränkungen	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	<i>Unternehmen XYZ verwendet eigenständige Unix-Server ohne LDAP. Daher ist die Anmeldung als „root“ erforderlich. Es ist für Unternehmen XYZ nicht möglich, die Anmeldung „root“ zu verwalten und alle „root“-Aktivitäten für jeden einzelnen Benutzer zu protokollieren.</i>
2. Ziel	Definieren Sie das Ziel der ursprüngliche Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	<i>Die Anforderung eindeutiger Anmeldungsinformationen verfolgt zwei Ziele. Zum einen ist es aus Sicherheitsgründen nicht akzeptabel, wenn Anmeldeinformationen gemeinsam verwendet werden. Zum anderen kann bei gemeinsamer Verwendung von Anmeldeinformationen nicht definitiv geklärt werden, ob eine bestimmte Person für eine bestimmte Aktion verantwortlich ist.</i>
3. Ermitteltes Risiko	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	<i>Für das Zugriffskontrollsystem entsteht ein zusätzliches Risiko, da nicht gewährleistet ist, dass alle Benutzer eine eindeutige ID haben und verfolgt werden können.</i>
4. Definition der Kompensationskontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	<i>Unternehmen XYZ erfordert von allen Benutzern die Anmeldung an den Servern über ihre Desktopcomputer unter Verwendung des Befehls SU. SU ermöglicht einem Benutzer den Zugriff auf das Konto „root“ und die Durchführung von Aktionen unter dem Konto „root“, wobei der Vorgang im Verzeichnis „SU-log“ protokolliert werden kann. Auf diese Weise können die Aktionen der einzelnen Benutzer über das SU-Konto verfolgt werden.</i>
5. Validierung der Kompensationskontrollen	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	<i>Unternehmen XYZ demonstriert dem Prüfer die Ausführung des Befehls SU und die Tatsache, dass die Einzelpersonen, die den Befehl ausführen, mit „root“-Rechten angemeldet sind.</i>
6. Verwaltung	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	<i>Unternehmen XYZ demonstriert Prozesse und Verfahren, mit denen sichergestellt wird, dass SU-Konfigurationen nicht durch Änderung, Bearbeitung oder Löschen so bearbeitet werden können, dass eine Ausführung von „root“-Befehlen ohne individuelle Benutzerverfolgung bzw. Protokollierung möglich würde.</i>



Anhang D: Konformitätsbescheinigung – Händler

Payment Card Industry (PCI)- Datensicherheitsstandard

Konformitätsbescheinigung für Vor-Ort-Beurteilungen – Händler

Version 1.2.1

Juli 2009

Anleitung zum Einreichen

Dieses Dokument muss von einem qualifizierten Sicherheitsprüfer (QSA) oder Händler (falls die Validierung von der internen Audit-Abteilung übernommen wird) als Erklärung der Konformität des Händlers mit dem Payment Card Industry-Datensicherheitsstandard (PCI DSS) ausgefüllt werden. Füllen Sie sämtliche zutreffenden Abschnitte aus, und senden Sie das Dokument an den Acquirer oder die Marke, die die Zahlung angefordert hat.

Teil 1. Informationen zum qualifizierten Sicherheitsprüfer

Name des Unternehmens:					
QSA-Leiter:		Titel:			
Telefonnr.:		E-Mail:			
Geschäftsadresse:		Ort:			
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

Teil 2. Informationen zum Händlerunternehmen

Name des Unternehmens:		DBA(s):			
Name des Ansprechpartners:		Titel:			
Telefonnr.:		E-Mail:			
Geschäftsadresse:		Ort:			
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

Teil 2a. Typ des Händlerunternehmens (alle zutreffenden Optionen auswählen)

- Einzelhändler
 Telekommunikation
 Lebensmittel und Supermärkte
 Erdöl/Erdgas
 E-Commerce
 Post-/Telefonbestellung
 Reise und Unterhaltung
 Sonstiges Unternehmen (bitte angeben):

Liste der Einrichtungen und Standorte, die in der PCI DSS-Prüfung berücksichtigt wurden:

Teil 2b. Beziehungen

Steht Ihr Unternehmen in Beziehung zu einem oder mehreren Drittdienstleistern (z. B. Gateways, Webhosting-Unternehmen, Buchungspersonal von Fluggesellschaften, Vertreter von Kundentreueprogrammen usw.)? Ja Nein

Hat Ihr Unternehmen eine Beziehung zu mehr als einem Acquirer? Ja Nein

Teil 2c. Transaktionsverarbeitung

Verwendete Zahlungsanwendung: _____ Version der Zahlungsanwendung: _____

Teil 3. PCI DSS-Validierung

Auf der Grundlage der Ergebnisse des Konformitätsberichts (ROC) vom (*date of ROC*) stellt (QSA *Name/Merchant Name*) den folgenden Konformitätsstatus für die in Teil 2 dieses Dokuments vom (*date*) ermittelte Stelle fest (Zutreffendes ankreuzen):

Konform: Sämtliche Anforderungen aus dem ROC sind „implementiert“⁴, und vom durch PCI SSC zugelassenen Approved Scanning Vendor (*ASV Name*) wurde ein Scan mit positivem Ergebnis durchgeführt. (*Merchant Company Name*) bietet vollständige Konformität mit PCI DSS (*insert version number*).

Nicht konform: Einige Anforderungen des ROC sind „nicht implementiert“, was insgesamt zur Beurteilung **NICHT KONFORM** geführt hat, **oder** es wurde noch kein Scan mit positivem Ergebnis von einem durch PCI SSC zugelassenen Approved Scanning Vendor durchgeführt, weswegen (*Merchant Company Name*) nicht vollständig mit PCI DSS konform ist.

Zieldatum für Konformität:

Eine Stelle, die dieses Formular mit dem Status „Nicht konform“ einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

Teil 3a. Bestätigung des Status „Konform“

Händler bestätigt:

- Der ROC wurde nach den Vorgaben von *PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren* (Version (*insert version number*)) durchgeführt.
- Alle Informationen im oben genannten ROC und in dieser Bescheinigung stellen die Ergebnisse der Beurteilung in allen zentralen Aspekten korrekt dar.
- Der Händler hat gegenüber dem Anbieter der Zahlungsanwendung bestätigt, dass im Zahlungssystem nach der Autorisierung keine vertraulichen Authentifizierungsdaten gespeichert werden.
- Der Händler kennt die PCI-Datensicherheitsstandards und erkennt an, dass er jederzeit vollständige PCI DSS-Konformität aufweisen muss.
- Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung Magnetstreifen Daten (aus einer Spur)⁵, CAV2-, CVC2-, CID-, CVV2⁶- oder PIN-Daten⁷ gespeichert wurden.

Teil 3b. Bestätigungen durch QSA und Händler

Unterschrift des leitenden QSA ↑	Datum:
---	---------------

Name des leitenden QSA:	Titel:
--------------------------------	---------------

Unterschrift des Beauftragten des Händlers ↑	Datum:
---	---------------

Name des Beauftragten des Händlers:	Titel:
--	---------------

⁴ Als „Implementiert“ sind auch vom QSA bzw. vom internen Audit des Händlers geprüfte Kompensationskontrollen aufzufassen. Wenn die Kompensationskontrollen die mit der Anforderung im Zusammenhang stehenden Risiken angemessen vermindern, muss der QSA die Anforderung als „Implementiert“ betrachten.

⁵ Im Magnetstreifen verschlüsselte Daten, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Stellen dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifen Daten speichern. Die einzigen Elemente der Spurdaten, die beibehalten werden dürfen, sind Kontonummer, Ablaufdatum und Name.

⁶ Der drei- oder vierstellige Wert, der im oder rechts neben dem Unterschriftenfeld bzw. vorne auf einer Zahlungskarte aufgedruckt ist und zur Verifizierung von Transaktionen bei nicht vorliegender Karte verwendet wird.

⁷ Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht.

Teil 4. Aktionsplan für Status „Nicht konform“

Bitte wählen Sie den jeweiligen Konformitätsstatus für jede Anforderung aus. Wenn Sie einen der Punkte mit „Nein“ beantworten, müssen Sie das Datum angeben, an dem das Unternehmen die Anforderung erfüllt. Geben Sie außerdem eine kurze Beschreibung der Aktionen an, die unternommen werden, damit die Anforderung erfüllt werden. *Sprechen Sie sich mit Ihrem Acquirer oder Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

PCI-Anforderung	Beschreibung	Konformitätsstatus (eine Option auswählen)	Abhilfedatum und Aktionen (bei Konformitätsstatus „Nein“)
1	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
2	Ändern der vom Anbieter festgelegten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
3	Schutz gespeicherter Karteninhaberdaten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
5	Verwendung und regelmäßige Aktualisierung von Antivirensoftware	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
8	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
9	Beschränkung des physischen Zugriffs auf Karteninhaberdaten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
12	Befolgung einer Informationssicherheits-Richtlinie	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	





Anhang E: Konformitätsbescheinigung – Dienstleister

**Payment Card Industry (PCI)-
Datensicherheitsstandard**

**Konformitätsbescheinigung für
Vor-Ort-Beurteilungen – Dienstleister**

Version 1.2.1

Juli 2009

Anleitung zum Einreichen

Der qualifizierte Sicherheitsprüfer (QSA) und der Dienstleister müssen dieses Dokument als Erklärung der Konformität des Dienstleisters mit dem Payment Card Industry-Datensicherheitsstandard (PCI DSS) ausfüllen. Füllen Sie sämtliche zutreffenden Abschnitte aus, und senden Sie das Dokument an die Zahlungsmarke.

Teil 1. Informationen zum qualifizierten Sicherheitsprüfer

Name des Unternehmens:					
QSA-Leiter:			Titel:		
Telefonnr.:			E-Mail:		
Geschäftsadresse:			Ort:		
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

Teil 2. Informationen zum Dienstleisterunternehmen

Name des Unternehmens:			DBA(s):		
Name des Ansprechpartners:			Titel:		
Telefonnr.:			E-Mail:		
Geschäftsadresse:			Ort:		
Bundesstaat/Provinz:		Land:		PLZ:	
URL:					

Teil 2a. Angebotene Dienste (alle zutreffenden auswählen)

- | | | |
|---|--|---|
| <input type="checkbox"/> Autorisierung | <input type="checkbox"/> Treueprogramme | <input type="checkbox"/> 3-D Secure-Zugriffskontrollserver |
| <input type="checkbox"/> Umtausch | <input type="checkbox"/> IPSP (E-Commerce) | <input type="checkbox"/> Verarbeitung von Magnetstreifentransaktionen |
| <input type="checkbox"/> Zahlungs-Gateway | <input type="checkbox"/> Abwicklung und Abrechnung | <input type="checkbox"/> Verarbeitung von MO/TO-Transaktionen |
| <input type="checkbox"/> Hosting | <input type="checkbox"/> Problembearbeitung | <input type="checkbox"/> Sonstiges (bitte genau angeben): |

Liste der Einrichtungen und Standorte, die in der PCI DSS-Prüfung berücksichtigt wurden:

Teil 2b. Beziehungen

Hat Ihr Unternehmen eine Beziehung mit einem oder mehreren Drittdienstleistern (z. B. Gateways, Webhosting-Unternehmen, Buchungspersonal von Fluggesellschaften, Vertreter von Kundentreueprogrammen usw.)? Ja Nein

Teil 2c. Transaktionsverarbeitung

Wie und in welcher Kapazität speichert, verarbeitet bzw. überträgt Ihr Unternehmen Karteninhaberdaten?

Verwendete Zahlungsanwendung:

Version der Zahlungsanwendung:

Teil 3. PCI DSS-Validierung

Auf der Grundlage der Ergebnisse des Konformitätsberichts (ROC) vom (*date of ROC*) stellt (*QSA Name*) den folgenden Konformitätsstatus für die in Teil 2 dieses Dokuments vom (*date*) ermittelte Stelle fest (Zutreffendes ankreuzen):

- Konform:** Sämtliche Anforderungen aus dem ROC sind „erfüllt“⁸, und vom durch PCI SSC zugelassenen Approved Scanning Vendor (*ASV Name*) wurde ein Scan mit positivem Ergebnis durchgeführt. (*Service Provider Name*) bietet vollständige Konformität mit PCI DSS (*insert version number*).
- Nicht konform:** Einige Anforderungen des ROC sind „nicht erfüllt“, was insgesamt zur Beurteilung **NICHT KONFORM** geführt hat, **oder** es wurde noch kein Scan mit positivem Ergebnis von einem durch PCI SSC zugelassenen Approved Scanning Vendor durchgeführt, weswegen (*Service Provider Name*) nicht vollständig mit PCI DSS konform ist.

Zieldatum für Konformität:

Eine Stelle, die dieses Formular mit dem Status „Nicht konform“ einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. *Sprechen Sie sich mit Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

Teil 3a. Bestätigung des Status „Konform“

QSA und Dienstleister bestätigen:

- Der ROC wurde nach den Vorgaben von *PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren* (Version (*insert version number*)) durchgeführt.
- Alle Informationen im oben genannten ROC und in dieser Bescheinigung stellen die Ergebnisse der Beurteilung in allen zentralen Aspekten korrekt dar.
- Der Dienstleister kennt die PCI-Datensicherheitsstandards und erkennt an, dass er jederzeit vollständige PCI DSS-Konformität aufweisen muss.
- Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung Magnetstreifen­daten (aus einer Spur)⁹, CAV2-, CVC2-, CID-, CVV2¹⁰- oder PIN-Daten¹¹ gespeichert wurden.

Teil 3b. Bestätigungen von QSA und Dienstleister

Unterschrift des leitenden QSA ↑		Datum:
Name des leitenden QSA:		Titel:

Unterschrift des Beauftragten des Dienstleisters ↑		Datum:
Name des Beauftragten des Dienstleisters:		Titel:

⁸ Als „Implementiert“ sind auch vom QSA geprüfte Kompensationskontrollen aufzufassen. Wenn die Kompensationskontrollen die mit der Anforderung im Zusammenhang stehenden Risiken angemessen vermindern, muss der QSA die Anforderung als „Implementiert“ betrachten.

⁹ Im Magnetstreifen verschlüsselte Daten, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Stellen dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifen­daten speichern. Die einzigen Elemente der Spurdaten, die beibehalten werden dürfen, sind Kontonummer, Ablaufdatum und Name.

¹⁰ Der drei- oder vierstellige Wert, der im oder rechts neben dem Unterschriftenfeld bzw. vorne auf einer Zahlungskarte aufgedruckt ist und zur Verifizierung von Transaktionen bei nicht vorliegender Karte verwendet wird.

¹¹ Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht.

Teil 4. Aktionsplan für Status „Nicht konform“

Bitte wählen Sie den jeweiligen Konformitätsstatus für jede Anforderung aus. Wenn Sie einen der Punkte mit „Nein“ beantworten, müssen Sie das Datum angeben, an dem das Unternehmen die Anforderung erfüllt. Geben Sie außerdem eine kurze Beschreibung der Aktionen an, die unternommen werden, damit die Anforderung erfüllt werden. *Sprechen Sie sich mit Ihrer/Ihren Zahlungsmarke(n) ab, bevor Sie Teil 4 ausfüllen, da nicht alle Zahlungsmarken diesen Abschnitt erfordern.*

PCI-Anforderung	Beschreibung	Konformitätsstatus (eine Option auswählen)	Abhilfedatum und Aktionen (bei Konformitätsstatus „Nein“)
1	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
2	Ändern der vom Anbieter festgelegten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
3	Schutz gespeicherter Karteninhaberdaten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
5	Verwendung und regelmäßige Aktualisierung von Antivirensoftware	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
8	Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
9	Beschränkung des physischen Zugriffs auf Karteninhaberdaten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
12	Befolgung einer Informationssicherheits-Richtlinie	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	



Anhang F: PCI DSS-Prüfungen – Umfang und Auswahlen von Stichproben

