



# Payment Card Industry (PCI) Datensicherheitsstandard

---

## Anforderungen und Sicherheitsbeurteilungsverfahren

**Version 2.0**

Oktober 2010

## Dokumentänderungen

Datum	Version	Beschreibung	Seiten
Oktober 2008	1.2	Zur Einführung von PCI-DSS v1.2 als „PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren“ und zur Abschaffung von Redundanzen zwischen verschiedenen Dokumenten und zur Implementierung sowohl allgemeiner als auch spezifischer Änderungen seit dem PCI-DSS-Sicherheitsprüfverfahren v1.1. Für ausführliche Informationen konsultieren Sie PCI-Datensicherheitsstandard Änderungsübersicht von PCI-DSS Version 1.1 auf 1.2.	
Juli 2009	1.2.1	Fügen Sie den Satz ein, der fälschlicherweise in PCI-DSS v1.1 und v1.2 gelöscht wurde.	5
		Korrigieren Sie in der englischen Version der Prüfverfahren 6.3.7.a und 6.3.7.b „then“ in „than“.	32
		Entfernen Sie im Testverfahren 6.5.b die ausgegraute Markierung in den Spalten „Implementiert“ und „Nicht implementiert“.	33
		Für Arbeitsblätter zu Kompensationskontrollen – Muster, ändern Sie die Formulierung am Seitenanfang in der englischen Version um in „Use this worksheet to define compensating controls for any requirement noted as ‘in place’ via compensating controls.“	64
Oktober 2010	2.0	Aktualisieren und Implementieren der Änderungen seit der Version 1.2.1. Für ausführliche Informationen siehe „PA-DSS-Änderungsübersicht von PA-DSS Version 1.2.1 auf 2.0.“	

# Inhalt

<b>Dokumentänderungen</b> .....	<b>2</b>
<b>Einführung und Überblick über den PCI-Datensicherheitsstandard</b> .....	<b>5</b>
<b>Informationen zur PCI-DSS-Anwendbarkeit</b> .....	<b>7</b>
<b>Beziehung zwischen PCI-DSS und PA-DSS</b> .....	<b>9</b>
<b>Umfang der Beurteilung der Konformität mit PCI-DSS-Anforderungen</b> .....	<b>10</b>
<i>Netzwerksegmentierung</i> .....	10
<i>Drahtlos</i> .....	11
<i>Dritte/Outsourcing</i> .....	11
<i>Stichprobenkontrolle von Unternehmenseinrichtungen und Systemkomponenten</i> .....	12
<i>Kompensationskontrollen</i> .....	13
<b>Anweisungen und Inhalt des Konformitätsberichts</b> .....	<b>14</b>
<i>Berichtsinhalt und -format</i> .....	14
<i>Erneute Validierung offener Punkte</i> .....	17
<i>PCI-DSS-Konformität – Schritte zum Ausfüllen</i> .....	18
<b>Ausführliche PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren</b> .....	<b>19</b>
<b>Erstellung und Wartung eines sicheren Netzwerks</b> .....	<b>20</b>
<i>Anforderung 1: Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten</i> .....	20
<i>Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden</i> .....	25
<b>Schutz von Karteninhaberdaten</b> .....	<b>29</b>
<i>Anforderung 3: Schutz gespeicherter Karteninhaberdaten</i> .....	29
<i>Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze</i> .....	37
<b>Wartung eines Anfälligkeits-Managementprogramms</b> .....	<b>39</b>
<i>Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware</i> .....	39
<i>Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen</i> .....	40
<b>Implementierung starker Zugriffskontrollmaßnahmen</b> .....	<b>47</b>
<i>Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf</i> .....	47
<i>Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff</i> .....	49
<i>Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken</i> .....	55
<b>Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken</b> .....	<b>60</b>

<i>Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten .....</i>	<i>60</i>
<i>Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse.....</i>	<i>65</i>
<b>Befolgung einer Informationssicherheits-Richtlinie .....</b>	<b>70</b>
<i>Anforderung 12: Befolgung einer Informationssicherheits-Richtlinie für das gesamte Personal. ....</i>	<i>70</i>
<b>Anhang A: Zusätzliche PCI-DSS-Anforderungen für von mehreren Benutzern gemeinsam genutzten Hosting-Anbieter</b>	<b>77</b>
<b>Anhang B: Kompensationskontrollen .....</b>	<b>80</b>
<b>Anhang C: Arbeitsblatt zu Kompensationskontrollen.....</b>	<b>82</b>
<b>Arbeitsblatt zu Kompensationskontrollen – Beispiel.....</b>	<b>83</b>
<b>Anhang D: Segmentierung und Stichprobenkontrolle von Unternehmenseinrichtungen/Systemkomponenten .....</b>	<b>85</b>

# 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. Der PCI-DSS liefert grundlegende technische und betriebliche Anforderungen zum Schutz von Karteninhaberdaten. Der PCI-DSS gilt für alle Einrichtungen, die an der Verarbeitung von Zahlungskarten beteiligt sind – einschließlich Vertragsunternehmen, EDV-Dienstleistern, abrechnenden Stellen, Kartemittenten und Dienstleistern sowie anderen Stellen, die Karteninhaberdaten speichern, verarbeiten oder übertragen. Der PCI-DSS setzt sich aus Mindestanforderungen zum Schutz von Karteninhaberdaten zusammen; er kann durch zusätzliche Kontrollen und Verfahren verbessert werden, um mögliche Risiken zu minimieren. Im Folgenden finden Sie eine übergeordnete Übersicht über die 12 PCI-DSS-Anforderungen.

## Überblick über den PCI-Datensicherheitsstandard

<b>Erstellung und Wartung eines sicheren Netzwerks</b>	<ol style="list-style-type: none"> <li>1. Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten</li> <li>2. Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden</li> </ol>
<b>Schutz von Karteninhaberdaten</b>	<ol style="list-style-type: none"> <li>3. Schutz gespeicherter Karteninhaberdaten</li> <li>4. Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze</li> </ol>
<b>Wartung eines Anfälligkeits-Managementprogramms</b>	<ol style="list-style-type: none"> <li>5. Verwendung und regelmäßige Aktualisierung von Antivirensoftware</li> <li>6. Entwicklung und Wartung sicherer Systeme und Anwendungen</li> </ol>
<b>Implementierung starker Zugriffskontrollmaßnahmen</b>	<ol style="list-style-type: none"> <li>7. Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf</li> <li>8. Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff</li> <li>9. Physischen Zugriff auf Karteninhaberdaten beschränken</li> </ol>
<b>Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken</b>	<ol style="list-style-type: none"> <li>10. Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten</li> <li>11. Regelmäßiges Testen der Sicherheitssysteme und -prozesse.</li> </ol>
<b>Befolgung einer Informationssicherheits-Richtlinie</b>	<ol style="list-style-type: none"> <li>12. Befolgung einer Informationssicherheits-Richtlinie für das gesamte Personal.</li> </ol>

Das vorliegende Dokument, der *PCI-Datensicherheitsstandard - Anforderungen und Sicherheitsbeurteilungsverfahren*, kombiniert die 12 PCI-DSS-Anforderungen und die entsprechenden Prüfverfahren in ein Sicherheitsbeurteilungstool. Es wurde zur Verwendung während den PCI-DSS-Konformitätsbeurteilungen als Teil des Validierungsprozesses einer Stelle konzipiert. In den folgenden Abschnitten werden ausführliche Richtlinien und Best Practices dargelegt, um Stellen bei der Durchführung und Berichterstattung der Ergebnisse einer PCI-PSS-Beurteilung zu unterstützen. Die PCI-DSS-Anforderungen und Prüfverfahren beginnen auf **Seite 19**.

Auf der Website des PCI-Security Standards Council (PCI SSC) ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) finden Sie eine Vielzahl zusätzlicher Quellen, einschließlich:

- Compliance-Bescheinigungen
- *PCI-DSS-Navigation: Verständnis der Intention der Anforderungen*
- *Das PCI-DSS-Glossar für Begriffe, Abkürzungen und Akronyme*
- Häufig gestellte Fragen (FAQs)
- Ergänzungen und Richtlinien

**Hinweis:** Die Ergänzungen komplementieren den PCI-DSS und bestimmen zusätzliche Aspekte und Empfehlungen zur Einhaltung der PCI-DSS-Anforderungen – sie ändern, eliminieren oder ersetzen nicht den PCI-DSS oder dessen Anforderungen.

Für weitere Informationen besuchen Sie [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

## Informationen zur PCI-DSS-Anwendbarkeit

Der PCI-DSS ist immer gültig, wenn Kontodaten gespeichert, verarbeitet oder übertragen werden. *Kontodaten* bestehen aus folgenden *Karteninhaberdaten* und *vertraulichen Authentifizierungsdaten*:

<b>Zu den Karteninhaberdaten zählen:</b>	<b>Zu den vertraulichen Authentifizierungsdaten zählen:</b>
<ul style="list-style-type: none"><li>▪ Primary Account Number (PAN)</li><li>▪ Name des Karteninhabers</li><li>▪ Ablaufdatum</li><li>▪ Servicecode</li></ul>	<ul style="list-style-type: none"><li>▪ Vollständige Magnetstreifendaten oder ähnliches auf einem Chip</li><li>▪ CAV2/CVC2/CVV2/CID</li><li>▪ PINs/PIN-Block</li></ul>

**Die primäre Kontonummer stellt einen ausschlaggebenden Faktor in Bezug auf die Anwendbarkeit der PCI-DSS-Anforderungen dar.** Die PCI-DSS-Anforderungen gelten, wenn eine primäre Kontonummer (PAN) gespeichert, verarbeitet oder übertragen wird. Wird die PAN nicht gespeichert, verarbeitet oder übertragen, finden PCI-DSS-Anforderungen keine Anwendung.

Wenn der Name des Inhabers, der Servicecode und/oder das Ablaufdatum zusammen mit der PAN gespeichert, verarbeitet oder übertragen werden, oder anderweitig innerhalb Karteninhaberdaten-Umgebung gegenwärtig sind, müssen diese Daten im Sinne der PCI-DSS-Anforderungen geschützt werden, **mit Ausnahme** der Anforderungen 3.3 und 3.4, die nur bezüglich der PAN Anwendung finden.

Der PCI-DSS stellt eine Mindestkontrollrichtlinie dar, die von lokalen, regionalen oder brancheneigenen Gesetzen und Vorschriften erweitert werden kann. Ferner können die gesetzlichen oder regulatorischen Anforderungen spezifische Schutzmaßnahmen personenbezogener Informationen oder anderer Datenelemente (z. B. der Name des Karteninhabers) fordern oder die Offenlegungspraktiken von Verbraucherdaten einer Einheit definieren. Beispiele hierfür sind Gesetzgebungen bezüglich des Schutzes von Verbraucherdaten, Datenschutz, Identitätsdiebstahl oder Datensicherheit. Der PCI-DSS ersetzt keine lokalen oder regionalen Gesetze, behördliche Regulierungen oder andere gesetzlichen Bestimmungen.

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.

		Datenelement	Speichern zulässig	Machen gespeicherte Kontodaten gemäß der Anforderung 3.4 unleserlich.
Kontodaten	Karteninhaberdaten	Primary Account Number (PAN)	Ja	Ja
		Name des Karteninhabers	Ja	Nein
		Servicecode	Ja	Nein
		Ablaufdatum	Ja	Nein
	Vertrauliche Authentifizierungsdaten <sup>1</sup>	Vollständige Magnetstreifendaten <sup>2</sup>	Nein	Kann gemäß Anforderung 3.2 nicht gespeichert werden
		CAV2/CVC2/CVV2/CID	Nein	Kann gemäß Anforderung 3.2 nicht gespeichert werden
		PIN/PIN-Block	Nein	Kann gemäß Anforderung 3.2 nicht gespeichert werden

Die PCI-DSS-Anforderungen 3.3 und 3.4 finden nur bezüglich der PAN Anwendung. Wenn die PAN zusammen mit anderen Elementen der Karteninhaberdaten gespeichert wird, muss nur die PAN gemäß der PCI-DSS-Anforderung 3.4 unleserlich gemacht werden.

Der PCI-DSS **gilt nur**, wenn PANs gespeichert, verarbeitet und/oder übertragen werden.

<sup>1</sup> Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung nicht gespeichert werden (auch wenn sie verschlüsselt wurden).

<sup>2</sup> Vollständige Verfolgungsdaten vom Magnetstreifen, gleichwertige Daten auf dem Chip oder einem anderen Speicherort.

## Beziehung zwischen PCI-DSS und PA-DSS

Die Nutzung einer PA-DSS-konformen Anwendung allein macht eine Einheit noch nicht PCI-DSS-konform, zumal diese Anwendung in einer PCI-DSS-konformen Umgebung und im Sinne des von dem Zahlungsanwendungsanbieter bereitgestellten PA-DSS-Implementierungshandbuchs implementiert werden muss (gemäß PA-DSS-Anforderung 13.1).

Die Anforderungen für den PA-DSS leiten sich aus den *PCI-DSS-Anforderungen und -Sicherheitsbeurteilungsverfahren* ab (das vorliegende Dokument). Der PA-DSS **Error! Hyperlink reference not valid.** gibt an, welche Elemente von einer Zahlungsanwendung unterstützt werden müssen, um Kunden die Einhaltung des PCI-DSS zu ermöglichen

Sichere Zahlungsanwendungen minimieren bei einer Implementierung in einer PCI-DSS-konformen Umgebung das Potenzial von Sicherheitsverletzungen, die zu einer Kompromittierung von Magnetstreifendaten, von Kartenüberprüfungs-codes und -werten (CAV2, CID, CVC2, CVV2) sowie PINs und PIN-Blöcken führen, und verhindern somit Schädigungen durch Betrug, der auf diese Sicherheitsverletzungen zurückzuführen ist.

Hier einige Beispiele dafür, wie Zahlungsanwendungen der Einhaltung des Standards im Wege stehen können:

- Speicherung von Magnetstreifendaten und/oder ähnlichen Daten des Chips im Kundennetzwerk nach der Autorisierung;
- Anwendungen, die Kunden dazu auffordern, andere laut PCI-DSS erforderliche Funktionen, wie Antivirensoftware oder Firewalls, zu deaktivieren, um eine ordnungsgemäße Funktion der Zahlungsanwendung sicherzustellen; und
- die Nutzung unsicherer Methoden durch den Anbieter, um den Kunden einen Online-Support für die Anwendung anzubieten.

Der PA-DSS gilt für Softwareanbieter und andere Entwickler von an Dritte verkauften, vertriebenen oder lizenzierten Zahlungsanwendungen, bei denen Karteninhaberdaten im Zuge der Autorisierung oder Verrechnung gespeichert, verarbeitet oder weitergegeben werden.

Bitte beachten Sie in Bezug auf die Anwendbarkeit des PA-DSS Folgendes:

- Der PA-DSS **gilt** für Zahlungsanwendungen, die üblicherweise „vom Regal“ verkauft und installiert werden, also ohne individuelle Anpassung durch Softwareanbieter.
- Der PA-DSS **gilt nicht** für Zahlungsanwendungen, die von Großhändlern und Dienst Anbietern ausschließlich zur internen Verwendung entwickelt wurden (und nicht an Dritte vertrieben werden), da diese intern entwickelten Zahlungsanwendungen im Rahmen der normalen Prüfung hinsichtlich der PCI-DSS-Einhaltung beim betreffenden Großhändler oder Dienstanbieter ebenfalls geprüft werden.

Für einen ausführlichen Leitfaden zur Bestimmung, ob der PS-PSS für eine bestimmte Zahlungsanwendung gilt, konsultieren Sie bitte die PA-DSS-Anforderungen und Sicherheitsbewertungsverfahren, die Ihnen unter [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) zur Verfügung stehen.

## Umfang der Beurteilung der Konformität mit PCI-DSS-Anforderungen

Die PCI-DSS-Sicherheitsanforderungen gelten für alle Systemkomponenten. Im Rahmen des PCI-DSS sind „Systemkomponenten“ gemäß Definition alle Netzwerkkomponenten, Server oder Anwendungen, die in der Karteninhaberdaten-Umgebung enthalten oder damit verbunden sind. Der Begriff „Systemkomponenten“ umfasst auch sämtliche Virtualisierungskomponenten wie beispielsweise virtuelle Rechner, virtuelle Schalter/Router, virtuelle Appliances, virtuelle Anwendungen/Desktops und Hypervisoren. Die Karteninhaberumgebung besteht aus Personen, Prozessen und Technologien, die Karteninhaberdaten oder vertrauliche Authentifizierungsdaten speichern, verarbeiten oder übertragen. 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 (z. B. Internet-)Anwendungen.

Der erste Schritt in einer PCI-DSS-Bewertung liegt in der eingehenden Bestimmung des Umfangs der Prüfung. Alljährlich sowie vor der jährlichen Bewertung sollte die betreffende Stelle die Richtigkeit ihres PCI-DSS-Umfangs durch die Identifikation aller Speicherorte und Flüsse von Karteninhaberdaten bestätigen und sicherstellen, dass diese in dem PCI-DSS-Umfang enthalten sind. Um die Richtigkeit und Angemessenheit des PCI-DSS-Umfangs zu bestätigen, gehen Sie wie folgt vor:

- Die betreffende Stelle identifiziert und dokumentiert sämtliche vorhandenen Karteninhaberdaten in ihrer Umgebung, um sicherzustellen, dass keine Karteninhaberdaten außerhalb der derzeit definierten Karteninhaberdaten-Umgebung (Englisch: Cardholder data environment, CDE) existieren.
- Sobald alle Speicherorte von Karteninhaberdaten identifiziert und dokumentiert sind, setzt die betreffende Stelle die entsprechenden Ergebnisse ein, um zu überprüfen, ob der PCI-DSS-Umfang angemessen ist (die Ergebnisse können z. B. in Form eines Diagramms oder eines Bestands der Speicherorte von Karteninhaberdaten dargestellt werden).
- Die Stelle prüft die Aufnahme aller lokalisierten Karteninhaberdaten in dem Umfang der PCI-DSS-Bewertung und Teile der CDE, sofern diese Daten nicht gelöscht oder in die/der derzeit definierten CDE übertragen/konsolidiert wurden.
- Die Stelle bewahrt entsprechende Unterlagen auf, um nachzuweisen, wie der PCI-DSS-Umfang bestätigt wurde, sowie die Ergebnisse für eventuelle Kontrollen durch den Prüfer und/oder als Referenz für den Bestätigungsvorgang des PCI-DSS-Umfangs im Folgejahr.

### **Netzwerksegmentierung**

Die Netzwerksegmentierung oder Isolierung (Segmentierung) der Karteninhaberdaten-Umgebung vom Rest des Netzwerks der betreffenden Stelle ist keine PCI-DSS-Anforderung. Sie wird jedoch unbedingt als Methode empfohlen, um unter Umständen Folgendes zu verringern:

- 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 mithilfe einer Vielzahl von physischen oder logischen Mitteln erreicht werden, beispielsweise durch angemessen konfigurierte interne Netzwerk-Firewalls, Router mit umfassenden Zugriffssteuerungslisten oder andere Technologien, die den Zugriff auf ein bestimmtes Segment eines Netzwerks einschränken.

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 D: Die Segmentierung und Stichprobenkontrolle von Unternehmenseinrichtungen/Systemkomponenten liefern weitere Informationen über die Auswirkungen der Netzwerksegmentierung- und stichprobenkontrolle auf den Umfang einer PCI-DSS-Bewertung.*

## **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 ausgeführt werden (z. B. Anforderung 1.2.3, 2.1.1 und 4.1.1). Bevor drahtlose Technologie implementiert wird, sollte eine Stelle den Technologiebedarf sorgfältig gegen die Risiken abwägen. Sie sollten den Einsatz drahtloser Technologie nur für die Übertragung nicht vertraulicher Daten in Erwägung ziehen.

## **Dritte/Outsourcing**

Für Dienstleister, die sich einer jährlichen Vor-Ort-Beurteilung unterziehen müssen, muss eine Konformitätsvalidierung auf allen Systemkomponenten in der Karteninhaberdaten-Umgebung vorgenommen werden.

Ein Dienstleister 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 Drittdienstleister auslagern, muss der Konformitätsbericht (Report on Compliance, ROC) die Rolle jedes Dienstleisters dokumentieren und eindeutig identifizieren, welche Anforderungen für die bewertete Stelle und welche für den Dienstleister gelten. Es gibt zwei Möglichkeiten, mit denen Drittdienstleister die Konformität validieren können:

- 1) Sie können sich selbst einer PCI-DSS-Bewertung unterziehen und ihren Kunden die entsprechenden Konformitätsnachweise vorlegen; oder
- 2) Wenn sie sich keiner eigenen PCI-DSS-Beurteilung unterziehen, müssen sie ihre Services im Laufe der PCI-DSS-Beurteilungen aller ihrer Kunden prüfen lassen.

Weitere Informationen finden Sie in Teil 3 in „Einzelheiten über die überprüfte Umgebung“ im Abschnitt „Anweisungen und Inhalt des Konformitätsberichts“ in der Aufzählung, die mit „Für MSP-Prüfungen (Managed Service Provider)“ beginnt.

Darüber hinaus müssen Händler und Dienstleister 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**

Die Stichprobenkontrolle ist keine PCI-DSS-Anforderung. Nichtsdestotrotz kann der Prüfer nach Betrachtung des Gesamtumfangs und der Komplexität der zu bewertenden Umgebung unabhängig repräsentative Stichproben aus Unternehmenseinrichtungen und Systemkomponenten auswählen, um PCI-DSS-Anforderungen zu beurteilen. Diese Stichproben müssen zunächst für Unternehmenseinrichtungen und anschließend für Systemkomponenten innerhalb der einzelnen ausgewählten Unternehmenseinrichtungen festgelegt werden. Diese Stichproben müssen eine repräsentative Auswahl aller Typen und Standorte von Unternehmenseinrichtungen sowie der Typen von Systemkomponenten innerhalb der ausgewählten Unternehmenseinrichtungen sein. Die Stichproben müssen groß genug sein, um dem Prüfer die Sicherheit zu geben, dass Kontrollmechanismen erwartungsgemäß implementiert werden.

Die Stichprobenkontrolle von Unternehmenseinrichtungen/Systemkomponenten für eine Bewertung reduziert nicht den Umfang der Karteninhaberdaten-Umgebung oder der Anwendbarkeit der PCI-DSS-Anforderungen. Ganz gleich, ob von einer Stichprobenkontrolle Gebrauch gemacht wird oder nicht, die PCI-DSS-Anforderungen gelten für die gesamte Karteninhaberdaten-Umgebung. Wenn eine Stichprobenkontrolle durchgeführt wird, gilt es sicherzustellen, dass sämtliche Stichproben die anwendbaren PCI-DSS-Anforderungen einhalten. Eine Stichprobenkontrolle der PCI-DSS-Anforderungen an sich ist nicht gestattet.

Unternehmenseinrichtungen sind unter anderem: Büroräume, Läden, Franchise-Händler, Verarbeitungseinrichtungen, Datenzentren oder andere Einrichtungen an verschiedenen Standorten. Die Stichprobenkontrolle sollte Systemkomponenten aller Unternehmenseinrichtungen umfassen. Nehmen Sie beispielsweise für jede Unternehmenseinrichtung verschiedene Betriebssysteme, Funktionen und Anwendungen auf, die für den zu prüfenden Bereich gelten.

Zur Verdeutlichung kann der Prüfer ein Beispiel in jeder Unternehmenseinrichtung zur Aufnahme von Sun-Servern 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 einer einzelnen Version eines einzigen Betriebssystems (z. B. Windows 7 oder Solaris 10) ausgeführt werden, sollte die Stichprobe zumindest verschiedene Anwendungen (z. B. Datenbankserver, Webserver, Datenübertragungsserver) enthalten.

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

- Wenn standardisierte, zentralisierte PCI-DSS-Sicherheits- und Betriebsprozesse und -kontrollen zur Konsistenzsicherung implementiert sind, welche von den einzelnen Unternehmenseinrichtungen und Systemkomponenten eingehalten werden müssen, können die Stichproben begrenzter ausfallen, als wenn keine standardisierten Prozesse/Kontrollen vorhanden sind. Die Stichprobe muss groß genug sein, um dem Prüfer die Sicherheit zu geben, dass alle Unternehmenseinrichtungen und Systemkomponenten gemäß den Standardprozessen aufgebaut sind.
- Sollte mehr als eine Art von standardisierten Sicherheits- und/oder Betriebsprozessen implementiert sein (z. B. für verschiedene Arten von Sicherheitseinrichtungen/Systemkomponenten), muss die Stichprobe groß genug sein, um Unternehmenseinrichtungen/Systemkomponenten aller einzelnen Prozesstypen aufzunehmen.
- Wenn keine standardisierten PCI-DSS-Prozesse/Kontrollen implementiert sind und alle Unternehmenseinrichtungen/Systemkomponenten über einen nicht standardisierten Prozess verwaltet werden, muss die Stichprobe größer sein, damit der Prüfer die Gewissheit hat, dass alle Unternehmenseinrichtungen/Systemkomponenten die PCI-DSS-Anforderungen korrekt umgesetzt haben.

Wenn Stichprobenkontrollen eingesetzt werden, muss der Prüfer immer:

- Dokumentieren Sie, warum die jeweilige Stichprobentechnik und -größe ausgewählt wurde,
- Dokumentieren und validieren Sie die zur Ermittlung der Stichprobengröße usw. verwendeten standardisierten PCI-PSS-Prozesse und Kontrollen und
- Erläutern Sie, inwieweit die Stichprobe angemessen und repräsentativ für den gesamten Bestand ist.

**Siehe:** Anhang D:  
Segmentierung und  
Stichprobenkontrolle von  
Unternehmenseinrichtungen  
und Systemkomponenten.

Die Prüfer müssen den Grund aller Stichprobenkontrollen für jede Bewertung erneut validieren. Wenn eine Stichprobenkontrolle durchgeführt wird, müssen für jede Bewertung verschiedene Stichproben von Unternehmenseinheiten und Systemkomponenten gewählt werden.

### **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 Einhaltung 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. Zusammenfassung für die Geschäftsleitung**

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:

- Dokumentieren der Art und Weise, in der der Prüfer die Richtigkeit des PCI-DSS-Umfangs für die Bewertung validiert hat, einschließlich:
  - Der zur Identifizierung und Dokumentierung aller vorhandenen Karteninhaberdaten verwendeten Methoden und Prozesse;
  - Der Art und Weise, wie die Ergebnisse ausgewertet und dokumentiert wurden;
  - Wie die Effektivität und Genauigkeit der verwendeten Methoden überprüft wurde;
  - Die Bestätigung des Prüfers, dass der Umfang der Bewertung korrekt und angemessen ist.
- 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.
- Wenn während der Bewertung eine Stichprobenkontrolle eingesetzt wird, dokumentieren Sie für jeden ausgewählten Kontrollprobensatz (von Unternehmenseinrichtungen/Systemkomponenten) Folgendes:
  - Gesamtbestand;
  - Anzahl der Stichproben;
  - Begründung für die ausgewählte Stichprobe;
  - Eine Beschreibung der standardisierten PCI-DSS-Sicherheits- und Betriebsprozesse und -kontrollen, die verwendet wurden, um die Stichprobengröße zu bestimmen, sowie eine Beschreibung, wie die Prozesse/Kontrollen validiert wurden;
  - Eine Erläuterung, inwieweit die Stichprobe angemessen und repräsentativ für den gesamten Bestand ist;
  - Eine Beschreibung aller Standorte oder Umgebungen, die Karteninhaberdaten speichern, verarbeiten oder übertragen und die aus dem Umfang der Prüfung AUSGESCHLOSSEN wurden sowie die Angabe des Grundes für den Ausschluss dieser Standorte/Umgebungen;
- Eine Auflistung aller Einmanngesellschaften, die die Konformität mit dem PCI-Datensicherheitsstandard erfordern, und Angabe, ob sie separat oder im Rahmen dieser Beurteilung geprüft werden;
- Eine Auflistung aller internationalen Gesellschaften, die die Konformität mit dem PCI-Datensicherheitsstandard erfordern, und Angabe, ob sie separat oder im Rahmen dieser Beurteilung geprüft werden;
- Eine Auflistung 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, das zum Durchführen der Beurteilung verwendet wurde.

### 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.:
  - Dokumentation über die Übertragung und Verarbeitung von Karteninhaberdaten, einschließlich Autorisierung, Erfassung, Verrechnung, Ausgleichsbuchungen und anderer Abläufe;
  - Eine Auflistung der 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:
    - Eine Liste aller Elemente gespeicherter Karteninhaberdaten;
    - Eine Erläuterung, wie Daten gesichert werden;
    - Eine Erläuterung, wie der Zugriff auf Datenspeicher protokolliert wird;
- Eine Liste der Hardware und kritischen Software, die in der Karteninhaberdaten-Umgebung eingesetzt wird, sowie einer Beschreibung der Funktion/Nutzung;
- Eine Liste der Dienstleister und Dritten, mit denen die betreffende Stelle gemeinsam Karteninhaberdaten nutzt.

**Hinweis:** Diese Einheiten unterliegen der 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 keine PCI-DSS-Anforderung. Bitte erfragen Sie die individuellen PA-DSS-Konformitätsanforderungen für jede Zahlungsmarke.)

- Eine Liste der befragten Personen, deren Unternehmen, Titel und besprochene Themen.
- Eine 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 geprüft werden 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 Dienstanbieter und Prüfer
- Zeitrahmen der Beurteilung – Geben Sie die Dauer und den Zeitraum an, in dem die Bewertung stattgefunden hat.
- Datum des Berichts

#### 5. Ergebnisse des vierteljährlichen Scans

- Fassen Sie die vier letzten Ergebnisse des vierteljährlichen ASV-Scans in der Zusammenfassung für die Geschäftsleitung sowie in den Anmerkungen zu Anforderung 11.2.2 zusammen.

**Hinweis:** *Es ist nicht notwendig, dass vier bestandene vierteljährliche Scans für die anfängliche PCI-DSS-Konformität vorliegen, wenn der Prüfer folgende Punkte überprüft:*

- 1) *Das letzte Scan-Ergebnis war ein bestandener Scan,*
- 2) *Die betreffende Stelle hat die Richtlinien und Prozesse, die eine Fortsetzung der vierteljährlichen Scans erfordern, dokumentiert, und*
- 3) *Alle in dem anfänglichen Scan entdeckten Schwächen wurden, wie im erneuten Scan gezeigt, korrigiert.*

*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 dem *PCI-Programmführer für zugelassene Scanninganbieter (ASV) erfassen.*

#### 6. Ergebnisse und Beobachtungen

Fassen Sie in der Zusammenfassung für die Geschäftsleitung alle Ergebnisse zusammen, die möglicherweise nicht in das Standardvorlagenformat des ROC passen.

Alle Prüfer *sind verpflichtet:*

- Die Vorlage zu den detaillierten PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren zu verwenden, um detaillierte Berichtsbeschreibungen und Ergebnisse zu jeder Anforderung und Teilanforderung bereitzustellen.
- Stellen Sie sicher, dass alle Antworten mit „Nicht zutreffend“ klar erläutert werden.
- Alle Kompensationskontrollen zu prüfen und zu dokumentieren, die den Schluss zulassen, dass eine Kontrolle implementiert ist.

*Einzelheiten zu „Kompensationskontrollen“ finden Sie im Abschnitt zu Kompensationskontrollen oben 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/Dienstanbieter muss diese Punkte adressieren, bevor die Validierung abgeschlossen wird. Sobald diese Punkte vom Händler/Dienstanbieter 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 durch den PCI-SSC zugelassenen Scanninganbieter (ASV) durchgeführt wurden, und holen Sie die Nachweise für die bestandenen Scans beim ASV ein.
3. Füllen Sie die Konformitätsbescheinigung je nachdem für Dienstanbieter oder Händler vollständig aus. Konformitätsbescheinigungen sind verfügbar auf der PCI-SSC-Website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)).
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 (Dienstanbieter) 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 für jede Anforderung eine kurze Beschreibung implementierter Kontrollen eintragen, einschließlich Beschreibungen der Kontrollen, die infolge von Kompensationskontrollen oder einer „nicht zutreffenden“ Anforderung implementiert wurden.
- **Nicht implementiert** – Diese Spalte muss von Prüfer verwendet werden, um eine kurze Beschreibung von nicht implementierten Kontrollen einzutragen. Beachten Sie, dass ein nicht implementierter Bericht nur auf ausdrückliche Anfrage an eine Zahlungsmarke oder einen Acquirer gesendet werden sollte. Für weitere Anweisungen zu nicht implementierten Berichten konsultieren Sie die auf der Website des PCI-SSC verfügbaren Konformitätsbescheinigungen ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)).
- **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.

**Hinweis:** Diese Spalte darf nicht für Kontrollen verwendet werden, die noch nicht implementiert sind, oder für offene Punkte, die erst an einem in der Zukunft liegenden Datum abgeschlossen werden.

## Erstellung und Wartung eines sicheren Netzwerks

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

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

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.

Es können auch andere Systeme mit Firewall-Funktionalitäten eingesetzt werden, vorausgesetzt, sie erfüllen die Mindestanforderungen für Firewalls gemäß Anforderung 1. Wenn andere Systemkomponenten mit Firewall-Funktionalitäten innerhalb der Karteninhaberumgebung eingesetzt werden, müssen diese Komponenten in den Umfang und die Bewertung nach Anforderung 1 aufgenommen werden.

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>1.1</b> Festlegen von Standards für die Firewall- und Routerkonfiguration, die Folgendes beinhalten:	<b>1.1</b> Erhalten 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:			
<b>1.1.1</b> Ein offizieller Prozess zur Genehmigung und zum Testen aller Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration	<b>1.1.1</b> Überprüfen Sie, ob es einen offiziellen Prozess zum Testen und zur Genehmigung aller Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration gibt.			
<b>1.1.2</b> Ein aktuelles Netzwerkdiagramm mit allen Verbindungen mit Karteninhaberdaten einschließlich aller drahtlosen Netzwerke	<b>1.1.2.a</b> 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.			
	<b>1.1.2.b</b> Überprüfen Sie, ob das Diagramm regelmäßig aktualisiert wird.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>1.1.3</b> Anforderungen für eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone	<b>1.1.3.a</b> 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.			
	<b>1.1.3.b</b> Überprüfen Sie, ob das aktuelle Netzwerkdiagramm den Standards für die Firewall-Konfiguration entspricht.			
<b>1.1.4</b> Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die logische Verwaltung der Netzwerkkomponenten	<b>1.1.4</b> Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration eine Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die logische Verwaltung der Netzwerkkomponenten enthalten.			
<b>1.1.5</b> Dokumentation und Begründung für den Einsatz aller zulässigen Services, Protokolle und Ports, einschließlich der Dokumentation von Sicherheitsfunktionen für die Protokolle, die als unsicher gelten.  Zu unsicheren Diensten, Protokollen oder Ports gehören unter anderem FTP, Telnet, POP3, IMAP und SNMP.	<b>1.1.5.a</b> Überprüfen Sie, ob 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).			
	<b>1.1.5.b</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.			
<b>1.1.6</b> Anforderung zum Prüfen von Firewall- und Router-Regelsätzen mindestens alle sechs Monate	<b>1.1.6.a</b> Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration mindestens alle sechs Monate eine Prüfung von Firewall- und Router-Regelsätzen erfordern.			
	<b>1.1.6.b</b> Erhalten und prüfen Sie Dokumentationen, um zu überprüfen, ob die Regelsätze mindestens alle sechs Monate überprüft werden.			
<b>1.2</b> Aufbauen von Firewall- und Router-Konfigurationen, die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der Karteninhaberdaten-Umgebung einschränken.  <b>Hinweis:</b> Ein „nicht vertrauenswürdige Netzwerk“ ist jedes Netzwerk, das außerhalb der Netzwerke liegt, die zu der	<b>1.2</b> 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:			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<i>geprüften Einheit gehören und/oder das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Einheit liegt.</i>				
<b>1.2.1</b> Beschränken des ein- und ausgehenden Netzwerkverkehrs auf den für die Karteninhaberdaten-Umgebung absolut notwendigen Verkehr.	<b>1.2.1.a</b> Überprüfen Sie, ob ein- und ausgehender Netzwerkverkehr auf den für die Karteninhaberdaten-Umgebung notwendigen Verkehr beschränkt wird und ob die Beschränkungen dokumentiert sind.  <b>1.2.1.b</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.			
<b>1.2.2</b> Sichern und Synchronisieren von Router-Konfigurationsdateien.	<b>1.2.2</b> Überprüfen Sie, ob Router-Konfigurationsdateien sicher und synchronisiert sind, z. B. sollten ausgeführte Konfigurationsdateien (für die normale Funktion der Router) und Startkonfigurationsdateien (für den Geräteneustart) die gleiche sichere Konfiguration aufweisen.			
<b>1.2.3</b> Installieren von Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der Karteninhaberdaten-Umgebung und Konfigurieren dieser Firewalls, sodass der gesamte Verkehr aus der drahtlosen Umgebung entweder abgelehnt oder kontrolliert wird (sofern dieser Verkehr für Geschäftszwecke notwendig ist).	<b>1.2.3</b> 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).			
<b>1.3</b> Verboten des direkten öffentlichen Zugriffs zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung.	<b>1.3</b> Überprüfen der Firewall- und Routerkonfigurationen– einschließlich, jedoch nicht beschränkt auf den Choke Router im Internet, den DMZ-Router und die Firewall, das DMZ-Karteninhabersegment, den Perimeter-Router und das interne Karteninhabernetzwerksegment–um zu bestimmen, dass, wie unten erläutert, kein direkter Zugriff zwischen dem Internet und den Systemkomponenten im internen Karteninhabernetzwerksegment besteht.			
<b>1.3.1</b> Implementieren einer DMZ, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene, öffentlich erhältliche	<b>1.3.1</b> Überprüfen, ob eine DMZ implementiert ist, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene, öffentlich erhältliche Dienste, Protokolle und Ports anbieten.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
Dienste, Protokolle und Ports anbieten.				
<b>1.3.2</b> Beschränken des eingehenden Internetverkehrs auf IP-Adressen innerhalb der DMZ.	<b>1.3.2</b> Überprüfen, ob der eingehende Internetverkehr auf IP-Adressen innerhalb der DMZ beschränkt wird.			
<b>1.3.3</b> Keine direkten eingehenden oder ausgehenden Verbindungen für Datenverkehr zwischen dem Internet und der Karteninhaberdaten-Umgebung zulassen.	<b>1.3.3</b> Überprüfen, dass keine direkten eingehenden oder ausgehenden Verbindungen für Datenverkehr zwischen dem Internet und der Karteninhaberdaten-Umgebung zugelassen wird.			
<b>1.3.4</b> Nicht zulassen, dass interne Adressen aus dem Internet in die DMZ übergeben werden.	<b>1.3.4</b> Überprüfen, dass interne Adressen nicht aus dem Internet in die DMZ übergeben werden können.			
<b>1.3.5</b> Keinen nicht autorisierten ausgehenden Datenverkehr von der Karteninhaberdaten-Umgebung zum Internet zulassen.	<b>1.3.5</b> Überprüfen, dass ausgehender Datenverkehr von der Karteninhaberdaten-Umgebung zum Internet ausdrücklich zulassen ist.			
<b>1.3.6</b> Implementieren der statusgesteuerten Inspektion, die auch als dynamische Paketfilterung bekannt ist. (Das bedeutet, dass nur „etablierte“ Verbindungen in das Netzwerk zulässig sind.)	<b>1.3.6</b> Überprüfen, dass die Firewall eine statusgesteuerte Inspektion (dynamische Paketfilterung) durchführt. (Es sollten nur etablierte Verbindungen zugelassen werden und auch nur dann, wenn sie Bestandteil einer zuvor festgelegten Sitzung sind.)			
<b>1.3.7</b> Speichern von Systemkomponenten, die Karteninhaberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauenswürdigen Netzwerken getrennt ist.	<b>1.3.7</b> Überprüfen, dass sich die Systemkomponenten, die Karteninhaberdaten beinhalten, in einer internen Netzwerkzone befinden, die sowohl von der DMZ als auch von anderen nicht vertrauenswürdigen Netzwerken getrennt ist.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>1.3.8</b> Keine Weitergabe von privaten IP-Adressen und Routing-Informationen an unbefugte Dritte.</p> <p><b>Hinweis:</b> Zu den Methoden zum Verbergen von IP-Adressen zählen unter anderen:</p> <ul style="list-style-type: none"> <li>▪ Network Address Translation (NAT)</li> <li>▪ Das Platzieren von Servern mit Karteninhaberdaten hinter Proxy-Servern/Firewalls oder Inhalts-Caches,</li> <li>▪ Löschen oder Filtern von Route-Advertisements für private Netzwerke, die registrierte Adressen verwenden,</li> <li>▪ Interne Nutzung eines RFC1918-Adressraums anstatt registrierter Adressen.</li> </ul>	<p><b>1.3.8.a</b> Überprüfen, ob Methoden implementiert wurden, um die Offenlegung privater IP-Adressen und Routing-Informationen von internen Netzwerken an das Internet zu verhindern.</p> <hr/> <p><b>1.3.8.b</b> Überprüfen, ob die Offenlegung privater IP-Adressen und Routing-Informationen an externe Stellen zugelassen ist.</p>			
<p><b>1.4</b> Installieren von persönlicher Firewallsoftware auf allen mobilen und Mitarbeitern gehörenden Computern mit direkter Verbindung zum Internet (z. B. Laptops, die von Mitarbeitern verwendet werden), die für den Zugriff auf das Unternehmensnetzwerk eingesetzt werden.</p>	<p><b>1.4.a</b> Überprüfen, ob auf mobilen und Mitarbeitern gehörenden Computern mit direkter Verbindung zum Internet (z. B. Laptops, die von Mitarbeitern verwendet werden), die für den Zugriff auf das Unternehmensnetzwerk eingesetzt werden, persönliche Firewallsoftware installiert und aktiv ist.</p> <hr/> <p><b>1.4.b</b> Überprüfen, ob die persönliche Firewallsoftware vom Unternehmen gemäß bestimmter Standards konfiguriert wurde und nicht durch Benutzer mobiler Computer und/oder Computer von Mitarbeitern geändert werden kann.</p>			

## Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden

Böswillige Personen (innerhalb oder außerhalb einer Stelle) 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
2.1 Ändern der vom Anbieter angegebenen Standardeinstellungen vor jeder Installation eines Systems im Netzwerk, einschließlich, jedoch nicht beschränkt auf die Einführung von Kennwörtern, SNMP-Community-Zeichenfolgen und Löschung nicht benötigter Konten.	2.1 Wählen Sie eine Stichprobe aus Systemkomponenten und versuchen Sie, sich unter Verwendung der vom Anbieter angegebenen Standardkonten und -kennwörter (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.)			
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.	2.1.1 Überprüfen Sie die folgenden Punkte im Hinblick auf Anbieterstandardeinstellungen für drahtlose Umgebungen:			
	2.1.1.a Prüfen Sie, ob die Standardwerte der Verschlüsselungsschlüssel zum Zeitpunkt der Installation geändert wurden und jedes Mal geändert werden, wenn ein Mitarbeiter, der die Schlüssel kennt, das Unternehmen verlässt oder die Position wechselt.			
	2.1.1.b Prüfen Sie, ob die Standard-SNMP-Community-Zeichenfolgen auf drahtlosen Geräten geändert wurden.			
	2.1.1.c Prüfen Sie, ob die Standardkennwörter/-sätze auf Zugriffspunkte geändert wurden.			
	2.1.1.d Prüfen Sie, ob Firmware auf drahtlosen Geräten aktualisiert wird, um starke Verschlüsselung für die Authentifizierung und Übertragung über drahtlose Netzwerke zu unterstützen.			
	2.1.1.e Prüfen Sie, ob andere sicherheitsbezogene drahtlose Anbieterstandardeinstellungen geändert wurden, sofern zutreffend.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>2.2</b> Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit akzeptierter Standards zur Systemstabilisierung zählen unter anderem:</p> <ul style="list-style-type: none"> <li>▪ Center for Internet Security (CIS)</li> <li>▪ International Organization for Standardization (ISO)</li> <li>▪ SysAdmin Audit Network Security (SANS) Institut</li> <li>▪ National Institute of Standards and Technology (NIST)</li> </ul>	<p><b>2.2.a</b>Überprüfen Sie die Systemkonfigurationsstandards des Unternehmens für alle Arten von Systemkomponenten, und prüfen Sie, ob die Systemkonfigurationsstandards branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen.</p>			
	<p><b>2.2.b</b> Überprüfen Sie, ob die Systemkonfigurationsstandards gemäß Anforderung 6.2 aktualisiert werden, sobald neue Schwachstellen identifiziert werden.</p>			
	<p><b>2.2.c</b> Überprüfen Sie, ob Systemkonfigurationsstandards angewendet werden, wenn neue Systeme konfiguriert werden.</p>			
	<p><b>2.2.d</b> Überprüfen Sie, ob Systemkonfigurationsstandards jedes der unten aufgeführten Elemente enthalten (2.2.1 - 2.2.4).</p>			
<p><b>2.2.1</b> Implementieren Sie nur eine primäre Funktion pro Server, um zu vermeiden, dass auf einem Server gleichzeitig mehrere Funktionen mit verschiedenen Sicherheitsniveauanforderungen existieren. (Webserver, Datenbankserver und DNS sollten beispielsweise auf separaten Servern implementiert sein.)</p> <p><b>Hinweis:</b> Wenn Virtualisierungstechnologien eingesetzt werden, implementieren Sie pro virtuelle Systemkomponente nur eine primäre Funktion.</p>	<p><b>2.2.1.a</b>Überprüfen Sie für eine Stichprobe von Systemkomponenten, dass nur eine primäre Funktion pro Server implementiert ist.</p>			
	<p><b>2.2.1.b</b>Wenn Virtualisierungstechnologien eingesetzt werden, überprüfen Sie, dass pro virtuelle Systemkomponente oder Gerät nur eine primäre Funktion implementiert ist.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>2.2.2</b> Aktivieren Sie entsprechend des Bedarfs der Systemfunktion ausschließlich erforderliche und sichere Dienste, Protokolle, Daemons usw.</p> <p>Implementieren Sie Sicherheitsfunktionen für alle erforderlichen Dienste, Protokolle oder Daemons, die als unsicher eingestuft sind – Verwenden Sie z. B. gesicherte Technologien wie etwa SSH, S-FTP, SSL oder IPSec VPN, um unsichere Dienste wie beispielsweise NetBIOS, File-Sharing, Telnet, FTP etc. zu schützen.</p>	<p><b>2.2.2.a</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten aktivierte Systemservices, Daemons und Protokolle. Überprüfen Sie, ob ausschließlich erforderliche Dienste und Protokolle aktiviert sind.</p>			
	<p><b>2.2.2.b</b> Identifizieren Sie sämtliche aktivierten Dienste, Daemons oder Protokolle. Überprüfen Sie, ob diese notwendig sind und ob entsprechende Sicherheitsfunktionen dokumentiert und implementiert sind.</p>			
<p><b>2.2.3</b> Konfigurieren von Systemsicherheitsparametern, um Missbrauch zu verhindern.</p>	<p><b>2.2.3.a</b> Führen Sie Gespräche mit Systemadministratoren und/oder Sicherheitsbeauftragten, um zu überprüfen, ob diese die gängigen Sicherheitsparametereinstellungen für Systemkomponenten kennen.</p>			
	<p><b>2.2.3.b</b> Überprüfen Sie, ob gängige Sicherheitsparametereinstellungen in den Systemkonfigurationsstandards enthalten sind.</p>			
	<p><b>2.2.3.c</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob gängige Sicherheitsparameter entsprechend festgelegt sind.</p>			
<p><b>2.2.4</b> Entfernen aller unnötigen Funktionen wie z. B. Skripte, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver.</p>	<p><b>2.2.4.a</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob alle unnötigen Funktionen (z. B. Skripte, Treiber, Features, Untersysteme, Dateisysteme usw.) entfernt wurden</p>			
	<p><b>2.2.4.b.</b> Überprüfen Sie, ob aktivierte Funktionen dokumentiert sind und sichere Konfiguration unterstützen.</p>			
	<p><b>2.2.4.c.</b> Überprüfen Sie, ob auf den Systemkomponenten der Stichprobe ausschließlich dokumentierte Funktionen vorhanden sind.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>2.3</b> Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs mithilfe einer starken Kryptographie. Verwenden von Technologien wie SSH, VPN oder SSL/TLS für die webbasierte Verwaltung und sonstigen Nichtkonsolen-Verwaltungszugriff.</p>	<p><b>2.3</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, dass der Nichtkonsolen-Verwaltungszugriff durch folgende Maßnahmen verschlüsselt ist:</p>			
	<p><b>2.3.a</b> Befolgen Sie ein Administratorprotokoll auf jedem System, um zu überprüfen, ob eine starke Verschlüsselungsmethode aufgerufen wird, bevor das Administrator Kennwort angefordert wird.</p>			
	<p><b>2.3.b</b> Überprüfen Sie Dienste und Parameterdateien auf Dateien, um festzustellen, ob Telnet und andere Remote-Anmeldebefehle nicht für die interne Nutzung verfügbar sind.</p>			
	<p><b>2.3.c</b> Überprüfen Sie, ob der Administratorzugriff auf die webbasierten Managementschnittstellen mit einer starken Kryptographie verschlüsselt ist.</p>			
<p><b>2.4</b> Gemeinsam verwendete Hosting-Anbieter müssen die gehostete Umgebung und Karteninhaberdaten aller Stellen schützen. Diese Anbieter müssen bestimmte Anforderungen erfüllen, wie in <i>Anhang A: Zusätzliche PCI-DSS-Anforderungen für gemeinsam verwendete Hosting-Provider dargestellt</i>.</p>	<p><b>2.4</b> Durchführen der Testverfahren <b>A.1.1</b> bis <b>A.1.4</b>, die erläutert werden 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, ob gemeinsam verwendete Hosting-Anbieter die gehostete Umgebung und die Daten ihrer Stellen (Händler und Dienstleister) schützen.</p>			

## Schutz von Karteninhaberdaten

### Anforderung 3: Schutz gespeicherter Karteninhaberdaten

Schutzmethoden wie Verschlüsselung, Abkürzen von Zahlen (Trunkierung), Maskierung und Hashing sind kritische Bestandteile des Schutzes von Karteninhaberdaten. Wenn ein Eindringling andere Sicherheitskontrollen 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 betrachtet 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 unverschlüsselte PAN nicht mittels Messaging-Technologien für Endanwender wie etwa E-Mails oder Instant Messaging zu senden.

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

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>3.1</b> Beschränken Sie das Speichern von Karteninhaberdaten auf ein Minimum, indem Sie wie folgt Richtlinien und Verfahren zur Datenaufbewahrung und zum Löschen von Daten implementieren.	<b>3.1</b> Erhalten und prüfen Sie die Richtlinien und Verfahren zur Datenaufbewahrung und zum Löschen von Daten, und führen Sie die folgenden Schritte aus:			
<b>3.1.1</b> Implementieren einer Richtlinie zur Datenaufbewahrung und zum Löschen von Daten, die folgende Punkte berücksichtigt: <ul style="list-style-type: none"> <li>▪ Begrenzen der Speichermenge und der Aufbewahrungszeit auf die für rechtliche, gesetzliche oder geschäftliche Zwecke festgelegten Vorgaben.</li> <li>▪ Prozesse zum Löschen von Daten, sobald diese nicht mehr benötigt werden.</li> <li>▪ Spezifische</li> </ul>	<b>3.1.1.a</b> 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).			
	<b>3.1.1.b</b> Überprüfen Sie, ob Richtlinien und Verfahren Bestimmungen zum sicheren Löschen von Daten enthalten, wenn diese nicht mehr aus rechtlichen, gesetzlichen oder geschäftlichen Gründen benötigt werden, einschließlich des Löschens von Karteninhaberdaten.			
	<b>3.1.1.c</b> Überprüfen Sie, ob Richtlinien und Verfahren alle Aspekte zum Speichern von Karteninhaberdaten abdecken.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p>Aufbewehrungsanforderungen für Karteninhaberdaten</p> <ul style="list-style-type: none"> <li>Ein vierteljährlicher automatischer oder manueller Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten, die den festgelegten Aufbewahrungszeitraum überschritten haben.</li> </ul>	<p><b>3.1.1.d</b> Überprüfen Sie, ob Richtlinien und Verfahren mindestens einen der folgenden Aspekte beinhalten:</p> <p>Einen programmatischen (automatischen oder manuellen) Prozess zum mindestens vierteljährlichen Löschen gespeicherter Karteninhaberdaten, die den in der Datenaufbewahrungsrichtlinie festgelegten Zeitraum überschritten haben.</p> <p>Anforderungen für eine mindestens vierteljährliche Überprüfung dazu, ob die gespeicherten Karteninhaberdaten nicht den in der Datenaufbewahrungsrichtlinie festgelegten Zeitraum überschreiten.</p>			
<p><b>3.2</b> Speichern Sie keine vertraulichen Authentifizierungsdaten nach der Autorisierung (auch wenn diese verschlüsselt sind).</p> <p>Vertrauliche Authentifizierungsdaten umfassen die Daten, die in den folgenden Anforderungen 3.2.1 bis 3.2.3 aufgeführt sind:</p> <p><b>Hinweis:</b> <i>Kartnemittenten und Unternehmen, die Ausstellungsdienste unterstützen, dürfen vertrauliche Authentifizierungsdaten speichern, wenn dafür eine Begründung vorliegt und die Daten sicher gespeichert werden.</i></p>	<p><b>3.1.1.e</b> Überprüfen Sie stichprobenartig bei Systemkomponenten, die Karteninhaberdaten speichern, ob die gespeicherten Daten nicht den in der Datenaufbewahrungsrichtlinie festgelegten Zeitraum überschreiten.</p> <p><b>3.2.a</b> Bei Kartnemittenten und/oder Unternehmen, die Ausstellungsdienste unterstützen und vertrauliche Authentifizierungsdaten speichern, überprüfen Sie, ob für die Speicherung dieser vertraulichen Authentifizierungsdaten eine Begründung vorliegt und die Daten sicher gespeichert werden.</p> <p><b>3.2.b</b> Bei allen anderen Stellen, erhalten und überprüfen Sie, wenn vertrauliche Authentifizierungsdaten empfangen und gelöscht werden, die Prozesse zum Löschen der Daten, um sicherzustellen, dass die Daten nicht wiederhergestellt werden können.</p> <p><b>3.2.c</b> Führen Sie für jedes Element der unten aufgeführten vertraulichen Authentifizierungsdaten die folgenden Schritte aus:</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>3.2.1</b> 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.</p> <p><b>Hinweis:</b> Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:</p> <ul style="list-style-type: none"> <li>▪ Der Name des Karteninhabers</li> <li>▪ Primäre Kontonummer (Englisch: Primary Account Number, PAN)</li> <li>▪ Ablaufdatum</li> <li>▪ Servicecode</li> </ul> <p>Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.</p>	<p><b>3.2.1</b> Überprüfen Sie für einen Stichprobe von Systemkomponenten die Datenquellen, einschließlich, aber nicht beschränkt auf die im nachstehenden aufgeführten Datenquellen, und prüfen Sie, ob die vollständigen Inhalte eines beliebigen Tracks vom Magnetstreifen auf der Kartenrückseite oder ähnliche Daten auf einem Chip unter keinen Umständen gespeichert werden:</p> <ul style="list-style-type: none"> <li>▪ Eingehende Transaktionsdaten</li> <li>▪ Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler)</li> <li>▪ Verlaufsdateien</li> <li>▪ Trace-Dateien</li> <li>▪ Mehrere Datenbankschemata</li> <li>▪ Datenbankinhalt</li> </ul>			
<p><b>3.2.2</b> 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><b>3.2.2</b> Für eine Stichprobe von Systemkomponenten, überprüfen Sie die Datenquellen, einschließlich, aber nicht beschränkt auf die Tatsache, ob der drei- oder vierstelligen 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"> <li>▪ Eingehende Transaktionsdaten</li> <li>▪ Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler)</li> <li>▪ Verlaufsdateien</li> <li>▪ Trace-Dateien</li> <li>▪ Mehrere Datenbankschemata</li> <li>▪ Datenbankinhalt</li> </ul>			
<p><b>3.2.3</b> Speichern Sie keine persönlichen Identifizierungsnummern (PIN) oder verschlüsselte PIN-Blöcke.</p>	<p><b>3.2.3</b> Für eine Stichprobe von Systemkomponenten prüfen Sie die Datenquellen, einschließlich, aber nicht beschränkt auf folgende Punkte, und überprüfen Sie, dass PINs und verschlüsselte PIN-Blöcke unter keinen Umständen gespeichert werden:</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
	<ul style="list-style-type: none"> <li>▪ Eingehende Transaktionsdaten</li> <li>▪ Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler)</li> <li>▪ Verlaufsdateien</li> <li>▪ Trace-Dateien</li> <li>▪ Mehrere Datenbankschemata</li> <li>▪ Datenbankinhalt</li> </ul>			
<p><b>3.3</b> Verbergen Sie die PAN bei der Anzeige (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden).</p> <p><b>Hinweise:</b></p> <ul style="list-style-type: none"> <li>▪ <i>Diese Anforderung gilt nicht für Mitarbeiter und andere Parteien, die die vollständige PAN aus rechtmäßigen geschäftlichen Gründen einsehen müssen.</i></li> <li>▪ <i>Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten - z. B. für POS-Belege.</i></li> </ul>	<p><b>3.3</b> Erhalten 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 verborgen werden. Davon ausgenommen sind Personen, die die vollständige PAN aus rechtmäßigen geschäftlichen Gründen einsehen müssen.</p>			
<p><b>3.4</b> Machen Sie die PAN überall dort unleserlich, wo sie gespeichert wird (auch auf tragbaren digitalen Medien, Sicherungsmedien und in Protokollen). Setzen Sie dazu eines der folgenden Verfahren ein:</p> <ul style="list-style-type: none"> <li>▪ Unidirektionale Hashes, die auf einer starken Kryptographie basieren (es muss von der vollständigen PAN ein Hash erstellt werden)</li> <li>▪ Abkürzung (die Hash-Funktion kann nicht verwendet werden, um das</li> </ul>	<p><b>3.4.a</b> Erhalten und prüfen Sie Dokumentationen über das System, das zum Schutz 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"> <li>▪ Unidirektionale Hashes, die auf einer starken Kryptographie basieren</li> <li>▪ Abkürzung</li> <li>▪ Index-Token und -Pads (Pads müssen sicher aufbewahrt werden)</li> <li>▪ Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren</li> </ul>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p>abgekürzte Segment der PAN zu ersetzen)</p> <ul style="list-style-type: none"> <li>▪ Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden)</li> <li>▪ Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren.</li> </ul> <p><b>Hinweis:</b> Für eine Person mit böswilligen Absichten ist es eine relativ einfache Übung, die originalen PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die abgekürzte als auch auf die Hash-Version einer PAN hat. Wenn die gehashte und die abgekürzte Version derselben PAN in der Umgebung derselben Stelle nebeneinander bestehen, müssen zusätzliche Kontrollen eingesetzt werden, um sicherzustellen, dass gehashte und abgekürzte Versionen nicht verglichen werden können, um die originale PAN zu rekonstruieren.</p>	<p><b>3.4.b</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><b>3.4.c</b> Überprüfen Sie eine Stichprobe austauschbarer Datenträger (z. B. Sicherungsbänder), um zu bestätigen, dass die PAN unleserlich gemacht wurde.</p>			
	<p><b>3.4.d</b> Überprüfen Sie eine Stichprobe von Audit-Protokollen, um zu bestätigen, dass die PAN unleserlich gemacht oder aus den Protokollen entfernt wurde.</p>			
<p><b>3.4.1</b> Wenn Datenträgerverschlüsselung verwendet wird (anstelle der Datenbankverschlüsselung auf Datei- oder Spaltenebene), muss der logische Zugriff unabhängig von nativen Zugriffskontrollmechanismen des Betriebssystems verwaltet werden (z. B. indem lokale Benutzerkontodatenbanken nicht verwendet werden). Entschlüsselungsschlüssel dürfen nicht mit Benutzerkonten verknüpft sein.</p>	<p><b>3.4.1.a</b> 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><b>3.4.1.b</b> Überprüfen Sie, ob kryptographische Schlüssel sicher gespeichert sind (z. B. auf austauschbaren Datenträgern, die durch starke Zugriffskontrollen entsprechend geschützt sind).</p>			
	<p><b>3.4.1.c</b> Überprüfen Sie, ob Karteninhaberdaten auf austauschbaren Datenträgern unabhängig vom Speicherort verschlüsselt sind.</p> <p><b>Hinweis:</b> Wenn keine Datenträgerverschlüsselung zur Verschlüsselung austauschbarer Datenträger eingesetzt wird, müssen die auf diesen Datenträgern gespeicherten Daten mithilfe einer anderen Methode verschlüsselt werden.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>3.5</b> Schützen Sie Schlüssel, die für den Schutz der Karteninhaberdaten eingesetzt werden, vor Weitergabe und Missbrauch:</p> <p><i>Hinweis: Diese Anforderung gilt auch für Schlüssel zum Verschlüsseln von Schlüsseln, die zum Schutz von Schlüsseln zum Verschlüsseln von Daten verwendet werden—diese Schlüssel zum Verschlüsseln von Schlüsseln müssen mindestens so sicher wie der Schlüssel zum Verschlüsseln von Daten sein.</i></p>	<p><b>3.5</b> 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:</p>			
<p><b>3.5.1</b> Schränken Sie den Zugriff auf kryptographische Schlüssel auf die unbedingt notwendige Anzahl von Wächtern ein.</p>	<p><b>3.5.1</b> Prüfen Sie Benutzerzugriffslisten darauf, ob der Zugriff auf Schlüssel auf möglichst wenige Wächter beschränkt ist.</p>			
<p><b>3.5.2</b> Speichern Sie kryptographische Schlüssel sicher an möglichst wenigen Speicherorten und in möglichst wenigen Formen.</p>	<p><b>3.5.2.a</b> 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.</p>			
	<p><b>3.5.2.b</b> Identifizieren Sie die Speicherorte von Schlüsseln, um zu überprüfen, ob die Schlüssel an so wenigen Orten und in so wenigen Formen wie möglich aufbewahrt werden.</p>			
<p><b>3.6</b> Dokumentieren und implementieren Sie alle Schlüsselverwaltungsprozesse und -verfahren für kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, einschließlich der Folgenden:</p> <p><i>Hinweis: Zahlreiche Branchenstandards für die Schlüsselverwaltung sind über verschiedene Ressourcen verfügbar, unter anderem über NIST (unter <a href="http://csrc.nist.gov">http://csrc.nist.gov</a>).</i></p>	<p><b>3.6.a</b> Überprüfen Sie, ob Schlüsselverwaltungsprozesse für Schlüssel, die zur Verschlüsselung von Karteninhaberdaten eingesetzt werden, implementiert wurden.</p>			
	<p><b>3.6.b</b> Nur für Dienstleister: Wenn der Dienstleister Schlüssel gemeinsam mit seinen Kunden für die Übertragung oder Speicherung von Karteninhaberdaten verwendet, überprüfen Sie, ob der Dienstleister den Kunden gemäß Anforderungen 3.6.1 bis 3.6.8 unten Dokumentationen bereitstellt, die Anweisungen zur sicheren Übertragung, Speicherung und Aktualisierung von Kundenschlüsseln enthalten.</p>			
	<p><b>3.6.c</b> Überprüfen Sie die Verfahren zur Schlüsselverwaltung, und führen Sie die folgenden Schritte aus:</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>3.6.1</b> Erstellung starker kryptographischer Schlüssel	<b>3.6.1</b> Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die die Erstellung starker Schlüssel erfordern.			
<b>3.6.2</b> Sichere Verteilung kryptographischer Schlüssel	<b>3.6.2</b> Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die die sichere Verteilung von Schlüsseln erfordern.			
<b>3.6.3</b> Sicheres Speichern kryptographischer Schlüssel	<b>3.6.3</b> Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die das sichere Speichern von Schlüsseln erfordern.			
<b>3.6.4</b> Änderungen kryptographischer Schlüssel für Schlüssel, die das Ende ihrer Schlüssellebensdauer erreicht haben (z. B. nach Ablauf einer festgelegten Zeitspanne und/oder nachdem von einem bestimmten Schlüssel eine gegebene Menge an Geheimtext generiert wurde), so wie von dem entsprechenden Anwendungsanbieter oder Schlüsselinhaber definiert und entsprechend bewährter Branchenverfahren und -richtlinien (z. B. NIST Special Publication 800-57).	<b>3.6.4</b> Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die Schlüsseländerungen nach Ablauf der angegebenen Schlüssellebensdauer erfordern.			
<b>3.6.5</b> Entfernung oder Austausch (z. B. mittels Archivierung, Vernichtung und/oder Rückruf) von Schlüsseln je nach Notwendigkeit, wenn die Integrität des Schlüssels gefährdet ist (z. B. Ausscheiden eines Mitarbeiters, der einen Klartext-Schlüssel kennt, usw.) oder Grund zur Annahme besteht, dass bestimmte Schlüssel beschädigt sind.	<b>3.6.5.a</b> Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die die Löschung von Schlüsseln erfordern, wenn deren Integrität gefährdet ist.			
	<b>3.6.5.b</b> Überprüfen Sie, ob die Verfahren zur Schlüsselverwaltung implementiert sind, die den Austausch von Schlüsseln mit bekannten oder vermeintlichen Schäden erfordern.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>Hinweis:</b> Wenn entfernte oder ausgetauschte kryptographische Schlüssel aufbewahrt werden müssen, sind diese Schlüssel auf eine sichere Art und Weise zu archivieren (z. B. mittels Schlüssel zum Verschlüsseln von Schlüsseln). Archivierte kryptographische Schlüssel dürfen nur zu Entschlüsselungs-/Überprüfungszwecken verwendet werden.</p>	<p><b>3.6.5.c</b> Wenn entfernte oder ausgetauschte kryptographische Schlüssel aufbewahrt werden, stellen Sie sicher, dass diese Schlüssel nicht für Verschlüsselungsvorgänge verwendet werden.</p>			
<p><b>3.6.6</b> Wenn manuelle Verwaltungsvorgänge kryptographischer Klartext-Schlüssel verwendet werden, müssen diese Vorgänge mittels einer geteilten Kenntnis und doppelten Kontrollen verwaltet werden (z. B. zwei oder drei Personen, die jeweils nur ihren eigenen Bestandteil des Schlüssels kennen, um den gesamten Schlüssel neu zu erstellen).</p> <p><b>Hinweis:</b> Zu den manuellen Verfahren zur Schlüsselverwaltung zählen unter anderen: Schlüsselgenerierung, Übertragung, Ladung, Speicherung und Vernichtung.</p>	<p><b>3.6.6</b> Überprüfen Sie, ob die manuellen Verfahren zur Schlüsselverwaltung für Klartext-Schlüssel eine geteilte Kenntnis und doppelte Kontrollen der Schlüssel erfordern.</p>			
<p><b>3.6.7</b> Verhindern der unbefugten Ersetzung kryptographischer Schlüssel.</p>	<p><b>3.6.7</b> Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die die Verhinderung der unbefugten Ersetzung von Schlüsseln fordern.</p>			
<p><b>3.6.8</b> Wächter kryptographischer Schlüssel müssen formal bestätigen, dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen.</p>	<p><b>3.6.8</b> Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die eine Bestätigung der Schlüsselwächter dazu voraussetzen (entweder in schriftlicher oder elektronischer Form), dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen.</p>			

#### 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 bei Authentifizierungsprotokollen sind auch weiterhin Ziele böswilliger Personen, die diese Sicherheitslücken ausnutzen, um sich privilegierten Zugriff auf Karteninhaberdaten-Umgebungen zu verschaffen.

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>4.1</b> Verwenden Sie starke Kryptographie- und Sicherheitsprotokolle (z. B. SSL/TLS, IPSEC, SSH usw.), damit sensible Karteninhaberdaten während der Übertragung über offene und öffentliche Netzwerke geschützt sind.</p> <p><i>Beispiele für offene, öffentliche Netzwerke, die in den Umfang des PCI-DSS fallen, sind unter anderen:</i></p> <ul style="list-style-type: none"> <li>▪ Das Internet</li> <li>▪ Drahtlose Technologien</li> <li>▪ GSM-Kommunikationen (Global System for Mobile)</li> <li>▪ General Packet Radio Service (GPRS).</li> </ul>	<p><b>4.1</b> Überprüfen Sie die Verwendung von Sicherheitsprotokollen, wo immer Karteninhaberdaten über offene, öffentliche Netzwerke übertragen oder empfangen werden.</p> <p>Überprüfen Sie, ob während der Datenübertragung wie folgt eine starke Kryptographie eingesetzt wird:</p>			
	<p><b>4.1.a</b> 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.</p>			
	<p><b>4.1.b</b> Überprüfen Sie, ob nur vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert werden.</p>			
	<p><b>4.1.c</b> Überprüfen Sie, ob das Protokoll implementiert ist, um ausschließlich sichere Konfigurationen zu verwenden und dass keine unsicheren Versionen oder Konfigurationen unterstützt werden.</p>			
	<p><b>4.1.d</b> Überprüfen Sie, ob für die verwendete Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet wird. (Prüfen Sie Anbieterempfehlungen/bewährte Verfahren.)</p>			
	<p><b>4.1.e</b> Für SSL/TLS-Implementierungen:</p> <ul style="list-style-type: none"> <li>▪ Überprüfen Sie, ob HTTPS als Bestandteil der Browser-URL (Universal Record Locator) angezeigt wird.</li> <li>▪ Überprüfen Sie, dass keine Karteninhaberdaten erforderlich sind, wenn HTTPS nicht in der URL angezeigt wird.</li> </ul>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>4.1.1</b> Stellen Sie sicher, 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> <p><i>Hinweis: Die Nutzung von WEB als Sicherheitskontrolle ist seit dem 30. Juni 2010 untersagt.</i></p>	<p><b>4.1.1</b> 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><b>4.2</b> Versenden Sie niemals ungeschützte PANs über Messaging-Technologien für Endbenutzer (z. B. E-Mail, Instant Messaging, Chat usw.).</p>	<p><b>4.2.a</b> Überprüfen Sie, ob die PAN unleserlich gemacht oder mittels einer starken Kryptographie gesichert wurde, wann immer sie über Messaging-Technologien für Endbenutzer übermittelt wird.</p> <p><b>4.2.b</b> Überprüfen Sie das Vorhandensein einer Richtlinie, die festlegt, dass ungeschützte PANs nicht über Messaging-Technologien für Endbenutzer gesendet werden dürfen.</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 Laufe zahlreicher vom Unternehmen genehmigter Aktivitäten in das Netzwerk eindringen, dazu gehört auch die Nutzung von E-Mail und Internet durch Mitarbeiter, 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
<b>5.1</b> Implementieren von Virenschutzsoftware auf allen Systemen, die häufig von böswilliger Software befallen werden (insbesondere Personal Computer und Server).	<b>5.1</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, einschließlich aller Betriebssystemarten, die häufig von böswilliger Software befallen werden, ob eine Virenschutzsoftware implementiert ist, wenn eine anwendbare Virenschutztechnologie vorhanden ist.			
<b>5.1.1</b> Stellen Sie sicher, dass alle Virenschutzprogramme in der Lage sind, alle bekannten Malware-Typen zu erkennen, zu entfernen und davor zu schützen.	<b>5.1.1</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob alle Virenschutzprogramme alle bekannten Malware-Typen (z. B. Viren, Trojaner, Würmer, Spyware, Adware und Rootkits) erkennen, entfernen und davor schützen.			
<b>5.2</b> Stellen Sie sicher, dass alle Antivirenmechanismen auf dem Laufenden sind, aktiv ausgeführt werden und in der Lage sind, Audit-Protokolle zu generieren.	<b>5.2</b> Überprüfen Sie, ob 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:			
	<b>5.2.a</b> Rufen Sie die Richtlinie ab, und überprüfen Sie, ob sie die Aktualisierung von Virenschutzsoftware und -definitionen erfordert.			
	<b>5.2.b</b> Überprüfen Sie, ob auf der Master-Installation der Software automatische Updates und periodische Scans aktiviert sind.			
	<b>5.2.c</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, einschließlich aller Betriebssystemtypen, die häufig von Malware befallen werden, ob automatische Updates und regelmäßige Scans aktiviert sind.			
	<b>5.2.d</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob 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 einen 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 sicheren Codierungsverfahren verhindert werden.

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>6.1</b> Stellen Sie sicher, dass alle Systemkomponenten und Softwareanwendungen vor bekannten Sicherheitslücken mithilfe der neuesten Sicherheitspatches des jeweiligen Herstellers geschützt sind. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden.</p> <p><b>Hinweis:</b> 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.</p>	<p><b>6.1.a</b> 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><b>6.1.b</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>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>6.2</b> Erstellen Sie einen Prozess zur Identifizierung und Bestimmung einer Risikobewertung für neu festgestellte Sicherheitslücken.</p> <p><b>Hinweise:</b></p> <ul style="list-style-type: none"> <li>▪ Die Risikobewertungen müssen auf den Best Practices der Branche aufbauen. Ein Kriterium, um eine Schwäche mit einem „hohen“ Risiko einzustufen, könnte beispielsweise eine CVSS-Grundbewertung von 4.0 oder höher sein und/oder ein Patch von einem Anbieter, das als „kritisch“ bewertet wird, und/oder eine Schwäche, die eine wichtige Systemkomponente betrifft.</li> <li>▪ Die in 6.2.a beschriebene Bewertung von Sicherheitslücken wird bis 30. Juni 2012 als Best Practices angesehen, danach wird sie zu einer Anforderung.</li> </ul>	<p><b>6.2.a</b> Führen Sie Gespräche mit zuständigen Mitarbeitern, um zu überprüfen, ob Prozesse zum Identifizieren neuer Sicherheitslücken implementiert sind und ob für diese Sicherheitslücken eine Risikobewertung durchgeführt wurde. (Zumindest die wichtigsten, schwerwiegendsten Schwächen sollten mit „schwerwiegend“ gekennzeichnet werden.</p> <p><b>6.2.b</b> Überprüfen Sie, ob Prozesse zum Identifizieren neuer Sicherheitslücken die Verwendung von externen Quellen für Informationen zu Sicherheitslücken umfassen.</p>			
<p><b>6.3</b> Entwickeln Sie Softwareanwendungen (interne und externe, inklusive Web-Administrationszugriff auf das Produkt) gemäß PCI-DSS (z. B. sichere Authentifizierung und Protokollierung) und auf Grundlage von Best Practices der Branche. Integrieren Sie die Informationssicherheit durchweg über den gesamten Softwareentwicklungszyklus. Diese Prozesse müssen Folgendes umfassen:</p>	<p><b>6.3.a</b> Erhalten und untersuchen Sie schriftliche Softwareentwicklungsprozesse, um zu überprüfen, ob die Prozesse auf Branchenstandards und/oder bewährten Praktiken basieren.</p> <p><b>6.3.b</b> Überprüfen Sie schriftliche Softwareentwicklungsprozesse, um festzustellen, ob die Informationssicherheit während des gesamten Lebenszyklus enthalten ist.</p> <p><b>6.3.c</b> Überprüfen Sie schriftliche Softwareentwicklungsprozesse, um festzustellen, ob die Softwareanwendungen gemäß den PCI-DSS-Anforderungen entwickelt werden.</p> <p><b>6.3.d</b> Überprüfen Sie anhand einer Untersuchung schriftlicher Softwareentwicklungsprozesse, anhand von Gesprächen mit Softwareentwicklern folgende Punkte:</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>6.3.1</b> Löschung benutzerdefinierter Anwendungskonten, Benutzernamen und Kennwörter, bevor Anwendungen aktiv oder an Kunden freigegeben werden	<b>6.3.1</b> Benutzerdefinierte Anwendungskonten, Benutzernamen und/oder Kennwörter werden entfernt, bevor das System in Produktion geht oder an Kunden freigegeben wird.			
<b>6.3.2</b> Überprüfung benutzerdefinierter Programmcodes vor der Freigabe für die Produktion oder an Kunden, um alle potenziellen Programmanfälligkeiten zu identifizieren.  <i><b>Hinweis:</b> Diese Anforderung für Code-Prüfungen gilt für den gesamten benutzerdefinierten (internen und öffentlichen) Code als Teil des Systementwicklungszyklus. Code-Prüfungen können durch qualifiziertes internes Personal oder durch Dritte ausgeführt werden. Webanwendungen unterliegen auch zusätzlichen Kontrollen, wenn sie öffentlich sind, um laufende Bedrohungen und Sicherheitslücken nach der Implementierung gemäß der Definition in der PCI-DSS-Anforderung 6.6 zu adressieren.</i>	<b>6.3.2.a</b> Erhalten und prüfen Sie Richtlinien, um zu bestätigen, dass alle benutzerdefinierten Anwendungscodeänderungen wie folgt geprüft werden müssen (mit manuellen oder automatisierten Prozessen): <ul style="list-style-type: none"> <li>▪ 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.</li> <li>▪ Codeprüfungen gewährleisten, dass der Code gemäß sicheren Codierungsrichtlinien erstellt wird (siehe PCI-DSS-Anforderung 6.5).</li> <li>▪ Vor der Freigabe werden entsprechende Korrekturen implementiert.</li> <li>▪ Ergebnisse der Codeprüfung werden vor der Freigabe vom Management geprüft und genehmigt.</li> </ul>			
	<b>6.3.2.b</b> Wählen Sie eine Stichprobe aus kürzlich vorgenommenen benutzerspezifischen Anwendungsänderungen aus, und überprüfen Sie, ob der benutzerdefinierte Anwendungscode gemäß Punkt 6.3.2.a oben geprüft wird.			
<b>6.4</b> Befolgen von Änderungskontrollprozessen und -verfahren für alle Änderungen an Systemkomponenten. Die Prozesse müssen Folgendes umfassen:	<b>6.4</b> Überprüfen Sie anhand einer Untersuchung der Verfahren zur Änderungskontrolle, anhand von Gesprächen mit Softwareentwicklern und Netzwerkadministratoren und der Untersuchung relevanter Daten (Netzwerkkonfigurationsdokumentation, Produktions- und Testdaten usw.) folgende Punkte:			
<b>6.4.1</b> Separate Entwicklungs-, Test- und Produktionsumgebungen	<b>6.4.1</b> 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
6.4.2 Trennung der Aufgaben zwischen Entwicklungs-, Test- und Produktionsumgebungen	6.4.2 Es besteht eine Trennung der Aufgaben zwischen Mitarbeitern, die den Entwicklungs-/Testumgebungen zugewiesen sind, und Mitarbeitern, die der Produktionsumgebung zugeteilt sind.			
6.4.3 Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet	6.4.3 Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet.			
6.4.4 Löschung von Testdaten und -konten, bevor Produktionssysteme aktiv werden	6.4.4 Testdaten und -konten werden gelöscht, bevor ein Produktionssystem aktiv wird.			
6.4.5 Änderung von Kontrollverfahren für die Implementierung von Sicherheitspatches und Softwareänderungen. Die Verfahren müssen Folgendes umfassen:	6.4.5.a Überprüfen Sie, ob die Änderungskontrollverfahren im Hinblick auf die Implementierung von Sicherheitspatches und Softwareänderungen dokumentiert sind und ob diese Verfahren die folgenden Punkte 6.4.5.1 – 6.4.5.4 erfordern.			
	6.4.5.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:			
6.4.5.1 Dokumentation der Auswirkungen.	6.4.5.1 Überprüfen Sie, ob Dokumentationen zu den Auswirkungen in der Änderungskontrolldokumentation für jede geprüfte Änderung enthalten sind.			
6.4.5.2 Dokumentierte Genehmigung von Änderungen durch autorisierte Parteien.	6.4.5.2 Überprüfen Sie, ob für jede geprüfte Änderung, eine dokumentierte Genehmigung der Änderungen durch autorisierte Parteien vorhanden ist.			
6.4.5.3 Testen der Funktionalität, um sicherzustellen, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt.	6.4.5.3.a Stellen Sie sicher, dass für jede geprüfte Änderung Funktionalitätstests durchgeführt werden, um sicherzustellen, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt.			
	6.4.5.3.b Überprüfen Sie bei benutzerspezifischen Codeänderungen, dass alle Updates auf ihre Konformität mit der PCI-DSS-Anforderung 6.5 getestet wurden, bevor sie implementiert werden.			
6.4.5.4 Back-Out-Verfahren.	6.4.5.4 Überprüfen Sie, ob für jede geprüfte Änderung Back-Out-Verfahren erstellt werden.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>6.5</b> Entwickeln Sie Anwendungen auf Grundlage sicherer Programmierungsrichtlinien. Vorbeugung häufiger Programmierungsanfälligkeiten in Softwareentwicklungsprozessen, einschließlich der folgenden Punkte:</p> <p><i><b>Hinweis:</b> Die unter 6.5.1 bis 6.5.9 aufgeführten Schwachstellen entsprechen zum Zeitpunkt der Veröffentlichung dieser Version des PA-DSS den Best Practices der Branche. Da jedoch die Best Practices der Branche im Anfälligkeits-Management aktualisiert werden (z. B. der OWASP Leitfaden, SANS CWE Top 25, CERT Secure Coding, usw.), müssen für diese Anforderungen die aktuellen Best Practices verwendet werden.</i></p>	<p><b>6.5.a</b> Suchen und prüfen Sie Softwareentwicklungsprozesse. Stellen Sie sicher, dass Prozesse Schulungen im Hinblick auf sichere Codierungsverfahren für Entwickler erfordern und auf den Best Practices der Branche sowie Leitfäden basieren.</p> <p><b>6.5.b</b> Führen Sie Gespräche mit stichprobenartig ausgewählten Entwicklern, und stellen Sie Nachweise dafür zusammen, dass diese mit sicheren Codierungsverfahren vertraut sind.</p> <p><b>6.5.c.</b> Überprüfen Sie, ob Prozesse implementiert sind, um zu gewährleisten, dass Anwendungen mindestens nicht für Folgendes anfällig sind:</p>			
<p><b>6.5.1</b> Injektionsfehler, insbesondere bei der SQL-Injektion. Injektion von Betriebssystembefehlen, LDAP- und Xpath-Injektionsfehler sowie andere Injektionsfehler sind ebenfalls zu berücksichtigen.</p>	<p><b>6.5.1</b> Injektionsfehler, insbesondere bei der SQL-Injektion. (Validieren Sie die Eingabe, um zu überprüfen, ob Benutzerdaten nicht die Bedeutung von Befehlen und Abfragen ändern und parametrisierte Abfragen verwenden können, usw.)</p>			
<p><b>6.5.2</b> Pufferüberlauf</p>	<p><b>6.5.2</b> Pufferüberlauf (Validieren von Puffergrenzen und Kürzen von Eingabestrings.)</p>			
<p><b>6.5.3</b> Unsicherer kryptographischer Speicher</p>	<p><b>6.5.3</b> Unsicherer kryptographischer Speicher (Verhindern Sie kryptographische Fehler)</p>			
<p><b>6.5.4</b> Unsichere Mitteilungen</p>	<p><b>6.5.4</b> Unsichere Mitteilungen (Verschlüsseln Sie alle authentifizierten und vertraulichen Mitteilungen ordnungsgemäß)</p>			
<p><b>6.5.5</b> Unsachgemäße Fehlerhandhabung</p>	<p><b>6.5.5</b> Unsachgemäße Fehlerbehandlung (Geben Sie keine Informationen über Fehlermeldungen preis)</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>6.5.6</b> Alle „schwerwiegenden“ Schwächen werden entsprechend des Identifikationsprozesses von Schwächen dargelegt (wie in der PCI-DSS-Anforderung 6.2 definiert).</p> <p><i><b>Hinweis:</b> Diese Anforderung wird bis zum 30. Juni 2012 als Best Practice angesehen, danach wird sie zu einer Anforderung.</i></p>	<p><b>6.5.6</b> Alle „schwerwiegenden“ Schwächen gemäß der PCI-DSS-Anforderung 6.2.</p>			
<p><i><b>Hinweis:</b> Die nachstehenden Anforderungen 6.5.7 bis 6.5.9 gelten für webbasierte Anwendungen und Anwendungsschnittstellen (intern oder extern):</i></p>				
<p><b>6.5.7</b> Siteübergreifendes Scripting (XSS)</p>	<p><b>6.5.7</b> Siteübergreifendes Scripting (XSS) (Validierung aller Parameter vor der Aufnahme, Verwendung einer kontextspezifischen Außerkraftsetzungsfunktion usw.)</p>			
<p><b>6.5.8</b> Kontrolle unangemessener Zugriffe wie unsichere direkte Objektverweise, unterlassene Einschränkung des URL-Zugriffs und Directory Traversal)</p>	<p><b>6.5.8</b> Kontrolle unangemessener Zugriffe wie unsichere direkte Objektverweise, unterlassene Einschränkung des URL-Zugriffs und Directory Traversal (Angemessene Authentifizierung von Benutzern und Eingabebereinigung. Machen Sie interne Objektverweise nicht Benutzern zugänglich.)</p>			
<p><b>6.5.9</b> Cross-Site Request Forgery (CSRF)</p>	<p><b>6.5.9</b> Cross-Site Request Forgery (CSRF). (Antworten Sie nicht auf Autorisierungsinformationen und Token, die automatisch von Browsern gesendet werden.)</p>			

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

## Implementierung starker Zugriffskontrollmaßnahmen

### Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

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 Erhalten und untersuchen Sie eine schriftliche Richtlinie für die Datensteuerung, und überprüfen Sie, ob 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 tätigkeitsbezogene 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 für Personen anhand der Tätigkeitsklassifizierung und -funktion zugewiesen werden (wird auch als „rollenbasierte Zugriffssteuerung“ oder RBAC bezeichnet).			
7.1.3 Voraussetzung einer dokumentierten Genehmigung durch autorisierte Parteien, in der die erforderlichen Berechtigungen angegeben sind.	7.1.3 Bestätigen Sie, dass für alle Zugriffe eine dokumentierte Genehmigung autorisierter Parteien erforderlich ist (schriftlich oder elektronisch) und dass darin die erforderlichen Berechtigungen angegeben werden müssen.			
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><b>7.2</b> 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><b>7.2</b> Prüfen Sie anhand von Systemeinstellungen und der Anbieterdokumentation wie folgt, ob ein Zugriffskontrollsystem implementiert ist:</p>			
<p><b>7.2.1</b> Abdeckung aller Systemkomponenten</p>	<p><b>7.2.1</b> Bestätigen Sie, dass in allen Systemkomponenten Zugriffskontrollsysteme implementiert sind.</p>			
<p><b>7.2.2</b> Zuweisung von Berechtigungen zu einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion</p>	<p><b>7.2.2</b> Bestätigen Sie, dass Zugriffskontrollsysteme konfiguriert sind, um Berechtigungen durchzusetzen, die einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion zugewiesen sind.</p>			
<p><b>7.2.3</b> Standardeinstellung „Alle ablehnen“</p> <p><i><b>Hinweis:</b> 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>	<p><b>7.2.3</b> Bestätigen Sie, dass die Zugriffskontrollsysteme die Standardeinstellung „Alle ablehnen“ aufweisen.</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.

**Hinweis:** Diese Anforderungen gelten für alle Konten, einschließlich Point-of-Sale-Konten mit administrativen Fähigkeiten und alle Konten, die verwendet werden, um Karteninhaberdaten anzuzeigen oder auf Systeme mit Karteninhaberdaten zuzugreifen. Allerdings gelten die Anforderungen 8.1, 8.2 und 8.5.8 bis 8.5.15 nicht für Benutzerkonten mit einer Point-of-Sale-Zahlungsanwendung, die immer nur auf eine Kartennummer für eine einzige Transaktion Zugriff haben (z. B. Kassierer-Konten).

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>8.1</b> Zuweisen einer eindeutigen Benutzer-ID für alle Benutzer, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird.</p>	<p><b>8.1</b> Stellen Sie sicher, dass alle Benutzer eine eindeutige ID für den Zugriff auf Systemkomponenten oder Karteninhaberdaten erhalten.</p>			
<p><b>8.2</b> Zuweisung einer eindeutigen ID und Einsatz von mindestens einer der folgenden Methoden zur Authentifizierung sämtlicher Benutzer:</p> <ul style="list-style-type: none"> <li>▪ Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz</li> <li>▪ Etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard</li> <li>▪ Etwas, das Sie sind, wie zum Beispiel biometrische Daten</li> </ul>	<p><b>8.2</b> 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:</p> <ul style="list-style-type: none"> <li>▪ Untersuchen Sie Dokumente, aus denen hervorgeht, welche Authentifizierungsmethoden verwendet wurden.</li> <li>▪ Schauen Sie sich bei jeder Authentifizierungsmethode und jeder Systemkomponente eine Authentifizierung genauer daraufhin an, ob diese in Übereinstimmung mit den dokumentierten Authentifizierungsmethoden erfolgt.</li> </ul>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>8.3</b> Authentifizierung anhand zweier Faktoren beim Remote-Zugriff (Netzwerkzugriff von außerhalb des Netzwerks) von Mitarbeitern, Administratoren und Dritten. (z. B. Remote-Authentifizierung und Einwahldienst (RADIUS) mit Tokens; Terminal Access Controller Access Control System (TACACS) mit Tokens oder andere Technologien, die eine Zwei-Faktor-Authentifizierung unterstützen.)</p> <p><i><b>Hinweis:</b> Bei der Zwei-Faktor-Authentifizierung müssen zwei der drei Authentifizierungsmethoden (siehe Anforderung 8.2 für eine Beschreibung der Authentifizierungsmethoden) bei der Authentifizierung eingesetzt werden. Wenn ein Faktor zweimalig verwendet wird (z. B. wenn zwei separate Kennwörter eingesetzt werden) handelt es sich nicht um eine Zwei-Faktor-Authentifizierung.</i></p>	<p><b>8.3</b> 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 zwei der drei Authentifizierungsmethoden erforderlich sind.</p>			
<p><b>8.4</b> Geschützte Übertragung und Speicherung von Kennwörtern auf sämtlichen Systemkomponenten unter Verwendung einer sicheren Verschlüsselung.</p>	<p><b>8.4.a</b> Testen Sie stichprobenartig die Kennwortdateien von Systemkomponenten auf die Verschlüsselung von Kennwörtern bei Übertragung und Speicherung.</p> <p><b>8.4.b</b> Bei Diensteanbietern müssen darüber hinaus die Kennwortdateien daraufhin geprüft werden, ob Kundenkennwörter verschlüsselt werden.</p>			
<p><b>8.5</b> Verwendung der geeigneten Benutzeridentifizierungs- und Authentifizierungsverwaltung für Nichtverbraucherbenutzer und Administratoren auf allen Systemkomponenten nach folgender Maßgabe:</p>	<p><b>8.5</b> Überprüfen Sie die Verfahren und befragen Sie Mitarbeiter hinsichtlich der Umsetzung der Benutzeridentifizierungs- und Authentifizierungsverwaltung. Gehen Sie dabei wie folgt vor:</p>			
<p><b>8.5.1</b> Kontrollieren der Vorgänge zum Hinzufügen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen</p>	<p><b>8.5.1</b> Wählen Sie stichprobenartig Benutzer-IDs von Administratoren und allgemeinen Benutzern aus. Überprüfen Sie, ob die einzelnen Benutzer entsprechend der Richtlinie zur</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
und anderen Identifizierungsobjekten.	Systemnutzung berechtigt sind. Gehen Sie dafür wie folgt vor: <ul style="list-style-type: none"> <li>▪ Untersuchen Sie für jede ID ein Autorisierungsformular.</li> <li>▪ 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.</li> </ul>			
<b>8.5.2</b> Überprüfen der Benutzeridentität, bevor Kennwörter zurückgesetzt werden.	<b>8.5.2</b> Untersuchen Sie die Kennwort-/Authentifizierungsverfahren, und beobachten Sie das Sicherheitspersonal, um sicherzustellen, dass 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.			
<b>8.5.3</b> Festlegen von Kennwörtern für die erste Verwendung und Zurücksetzen dieser Kennwörter auf einen eindeutigen Wert für jeden Benutzer und sofortige Änderung nach der ersten Verwendung.	<b>8.5.3</b> Untersuchen Sie die Kennwortverfahren, und beobachten Sie das Sicherheitspersonal, um zu überprüfen, ob Kennwörter neuer Benutzer für die erste Verwendung und zurückgesetzte Kennwörter für vorhandene Benutzer nach der ersten Nutzung auf einen eindeutigen Wert gesetzt werden.			
<b>8.5.4</b> Sofortige Deaktivierung des Zugriffs ehemaliger Benutzer.	<b>8.5.4</b> Prüfen Sie stichprobenartig, ob die IDs von Benutzern, die in den letzten sechs Monaten aus dem Unternehmen ausgeschieden sind, deaktiviert bzw. aus den Zugriffslisten der aktuellen Benutzer gelöscht wurden.			
<b>8.5.5</b> Entfernen bzw. Deaktivieren inaktiver Benutzerkonten mindestens alle 90 Tage.	<b>8.5.5</b> Überprüfen Sie, ob seit mehr als 90 Tagen inaktive Konten entfernt oder deaktiviert werden.			
<b>8.5.6</b> Aktivieren der von Anbietern für den Remote-Zugriff verwendeten Konten ausschließlich während der erforderlichen Zeit. Überwachung des aktiven Remote-Zugriffs auf Konten durch den Anbieter.	<b>8.5.6.a</b> Überprüfen Sie, ob die zum Zugriff, zur Unterstützung und Wartung verwendeten Konten im Regelfall deaktiviert sind und nur dann aktiviert werden, wenn der Anbieter sie benötigt.			
	<b>8.5.6.b</b> Überprüfen Sie, ob der aktive Remote-Zugriff auf Konten durch den Anbieter überwacht wird.			
<b>8.5.7</b> Teilen Sie allen Benutzern, die Zugriff auf Karteninhaberdaten haben, die Authentifizierungsmethoden und -	<b>8.5.7</b> Befragen Sie stichprobenartig einige Benutzer nach ihren Kenntnissen der Authentifizierungsmethoden und -richtlinien.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
richtlinien mit.				
<b>8.5.8</b> Verwenden Sie keine Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder andere Authentifizierungsmethoden.	<b>8.5.8.a</b> Zur Ermittlung einer Stichprobe von Systemkomponenten prüfen Sie die Benutzer-ID-Listen, um Folgendes zu bestätigen: <ul style="list-style-type: none"> <li>▪ Allgemeine Benutzer-IDs und -konten werden deaktiviert und entfernt;</li> <li>▪ Es gibt keine gemeinsamen Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen;</li> <li>▪ Es werden keine gemeinsamen und allgemeinen Benutzer-IDs zur Administration von Systemkomponenten verwendet.</li> </ul> <b>8.5.8.b</b> Untersuchen Sie Authentifizierungsrichtlinien und -verfahren, um zu überprüfen, ob Gruppenkennwörter oder andere Authentifizierungsverfahren ausdrücklich untersagt sind. <b>8.5.8.c</b> Stellen Sie durch Interviews mit Systemadministratoren sicher, dass selbst auf Anfrage keine Gruppen- bzw. gemeinsamen Kennwörter vergeben oder andere Authentifizierungsmethoden genutzt werden.			
<b>8.5.9</b> Ändern der Benutzerkennwörter mindestens alle 90 Tage.	<b>8.5.9.a</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass die Benutzer mindestens alle 90 Tage ihr Kennwort ändern müssen. <b>8.5.9.b</b> Bei Dienst Anbietern sind darüber hinaus interne Prozesse und Kunden- bzw. Benutzerdokumente daraufhin zu überprüfen, ob Kennwörter von Nichtverbraucherbenutzern regelmäßig geändert werden müssen und ob die Nichtverbraucherbenutzer Hinweise dazu erhalten, wann und unter welchen Umständen die Kennwörter geändert werden müssen.			
<b>8.5.10</b> Festlegen einer Mindestlänge für Kennwörter von mindestens sieben Zeichen.	<b>8.5.10.a</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass Kennwörter mindestens sieben Zeichen lang sein müssen. <b>8.5.10.b</b> Bei Dienst Anbietern müssen zusätzlich interne Prozesse und Kunden-/Benutzerdokumente daraufhin überprüft werden, ob es Mindestlängen für Kennwörter von Nichtverbraucherbenutzern gibt.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>8.5.11</b> Verwenden von Kennwörtern, die sowohl numerische als auch alphabetische Zeichen enthalten.	<b>8.5.11.a</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Systemkonfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass die Kennwörter numerische und alphabetische Zeichen enthalten müssen.			
	<b>8.5.11.b</b> Bei Dienst Anbietern müssen zusätzlich interne Prozesse und Kunden-/Benutzerdokumente daraufhin überprüft werden, ob Kennwörter von Nichtverbraucherbenutzern numerische und alphabetische Zeichen enthalten müssen.			
<b>8.5.12</b> Festlegen, dass sich ein neues Kennwort von den letzten vier Kennwörtern unterscheiden muss.	<b>8.5.12.a</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass sich ein neues Kennwort von den letzten vier Kennwörtern unterscheiden muss.			
	<b>8.5.12.b</b> Bei Dienst Anbietern müssen zusätzlich interne Prozesse und Kunden-/Benutzerdokumente daraufhin überprüft werden, ob darin gefordert wird, dass sich neue Kennwörter von Nichtverbraucherbenutzern von den letzten vier Kennwörtern unterscheiden.			
<b>8.5.13</b> Begrenzen der wiederholten Zugriffsversuche durch Sperren der Benutzer-ID nach spätestens sechs Versuchen.	<b>8.5.13.a</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Authentifizierungsparameter so eingestellt sind, dass ein Benutzerkonto nach spätestens sechs ungültigen Anmeldeversuchen gesperrt wird.			
	<b>8.5.13.b</b> Bei Dienst Anbietern müssen zusätzlich interne Prozesse und Kunden-/Benutzerdokumente daraufhin überprüft werden, ob Konten von Nichtverbraucherbenutzern nach spätestens sechs ungültigen Anmeldeversuchen gesperrt werden.			
<b>8.5.14</b> Festlegen einer Aussperrdauer von mindestens 30 Minuten, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann.	<b>8.5.14</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Systemkonfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass eine mindestens 30-minütige Aussperrdauer gilt, innerhalb derer das Konto nur durch den Administrator zurückgesetzt werden kann.			
<b>8.5.15</b> Festlegen, dass sich die Benutzer nach mehr als 15-minütiger Inaktivität erneut anmelden und das Terminal oder die Sitzung reaktivieren	<b>8.5.15</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Systemkonfigurationseinstellungen daraufhin, ob die Sperre des Systems bzw. der Sitzung nach einer mindestens 15-minütigen Inaktivitätszeit eintritt.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
müssen.				
<p><b>8.5.16</b> Festlegen, dass für den gesamten Zugriff auf Datenbanken mit Karteninhaberdaten eine Authentifizierung erforderlich ist. (Dies umfasst Zugriff durch Anwendungen, Administratoren und alle anderen Benutzer.)</p> <p>Schränken Sie den Direktzugriff oder Datenbankabfragen auf Datenbankadministratoren ein.</p>	<p><b>8.5.16.a</b> Überprüfen Sie die Konfigurationseinstellungen für Datenbank und Anwendungen daraufhin, ob sich alle Benutzer vor dem Zugriff authentifizieren müssen.</p>			
	<p><b>8.5.16.b</b> Überprüfen Sie, ob die Konfigurationseinstellungen für Datenbank und Anwendungen sämtliche Zugriffe, Anfragen und Aktionen der Benutzer im Bezug auf die Datenbank (z. B. Verschieben, Kopieren und Löschen) ausschließlich programmgesteuert (z. B. über gespeicherte Verfahren) erfolgen.</p>			
	<p><b>8.5.16.c</b> Überprüfen Sie, ob die Konfigurationseinstellungen für Datenbank und Anwendungen den direkten Zugriff auf die oder Anfragen bezüglich der Datenbank ausschließlich Datenbankadministratoren vorbehalten.</p>			
	<p><b>8.5.16.d</b> Überprüfen Sie die Datenbankanwendungen und die zugehörigen Anwendungs-IDs daraufhin, dass diese Anwendungs-IDs nur von den Anwendungen (und nicht von Einzelbenutzern oder anderen Prozessen) verwendet werden können.</p>			

## Anforderung 9: *Physischen Zugriff auf Karteninhaberdaten beschränken*

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. Zum Zwecke der Anforderung 9 bezieht sich der Begriff „Mitarbeiter vor Ort“ hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter und Subunternehmen sowie Berater, die am Standort der jeweiligen Stelle arbeiten. Ein „Besucher“ wird als Lieferant, Gast eines Mitarbeiters vor Ort, Servicemitarbeiter oder jede Person definiert, die die Einrichtung für kurze Zeit betreten muss, meist nicht länger als einen Tag. Der Begriff „Medien“ bezieht sich auf alle Papierdokumente und elektronischen Medien mit Karteninhaberdaten.

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>9.1</b> Verwenden angemessener Zugangskontrollen, um den physischen Zugriff auf Systeme für Karteninhaberdaten zu überwachen und zu beschränken.</p>	<p><b>9.1</b> 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"> <li>▪ Überprüfen Sie, ob der Zugang über eine elektronische Ausweiskontrolle oder per Schlüssel erfolgt.</li> <li>▪ 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 funktioniert.</li> </ul>			
<p><b>9.1.1</b> Überwachen des Zugangs zu zugangsbeschränkten Bereichen mithilfe von Videokameras und/oder 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><b>Hinweis:</b> „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><b>9.1.1.a</b> Überprüfen Sie, ob der Zugang zu zugangsbeschränkten Bereichen mithilfe von Videokameras und/oder Kontrollsystemen überwacht wird.</p>			
	<p><b>9.1.1.b</b> Überprüfen Sie, ob Videokameras und/oder Kontrollsysteme vor Manipulation oder Deaktivierung geschützt sind.</p>			
	<p><b>9.1.1.c</b> Überprüfen Sie, ob Videokameras und/oder Kontrollsysteme überwacht werden und ob die von diesen Kameras oder anderen Systemen aufgezeichneten Daten mindestens drei Monate lang gespeichert werden.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>9.1.2</b> Beschränken des physischen Zugriffs auf öffentlich zugängliche Netzwerkbuchsen.</p> <p>Beispielsweise sollten für Besucher zugängliche Bereiche keine aktiven Netzwerkbuchsen haben, sofern der Netzwerkzugriff nicht ausdrücklich zugelassen ist.</p>	<p><b>9.1.2</b> Ermitteln Sie durch Gespräche mit Netzwerkadministratoren und durch eigene Beobachtungen, ob Netzwerkbuchsen nur dann von befugten Mitarbeitern vor Ort aktiviert werden, wenn sie benötigt werden. Achten Sie ansonsten darauf, dass Besucher nicht alleine bzw. unbeobachtet in Bereichen mit aktiven Netzwerkbuchsen arbeiten können.</p>			
<p><b>9.1.3</b> Beschränken Sie den physischen Zugriff auf WLAN-Zugriffspunkte, Gateways, Handgeräte, Netzwerk- und Kommunikationshardware und Telekommunikationsleitungen.</p>	<p><b>9.1.3</b> Überprüfen Sie, ob der physische Zugriff auf WLAN-Zugriffspunkte, Gateways, Handgeräte, Netzwerk- und Kommunikationshardware und Telekommunikationsleitungen entsprechend eingeschränkt ist.</p>			
<p><b>9.2</b> Entwickeln Sie Verfahren, die die Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern erleichtern, insbesondere in Bereichen, in denen auf Karteninhaberdaten zugegriffen werden kann.</p>	<p><b>9.2.a</b> Überprüfen Sie die Prozesse und die Verfahren, nach denen den Mitarbeitern vor Ort und Besuchern Ausweise ausgestellt werden, und achten Sie darauf, dass mit den Verfahren folgende Punkte abgedeckt sind:</p> <ul style="list-style-type: none"> <li>▪ Ausstellen neuer Ausweise,</li> <li>▪ Zugangs- bzw. Zugriffsanforderungen und</li> <li>▪ Deaktivieren der Zugangsberechtigung für ausgeschiedene Mitarbeiter vor Ort und bei auslaufendem Besucherstatus</li> </ul>			
	<p><b>9.2.b</b> Überprüfen Sie, ob der Zugriff auf das Ausweissystem ausschließlich befugtem Personal vorbehalten ist.</p>			
	<p><b>9.2.c</b> Überprüfen Sie die derzeit verwendeten Ausweise, um sicherzustellen, dass sie die Besucher klar identifizieren und leicht zwischen Mitarbeitern vor Ort und Besuchern unterschieden werden kann.</p>			
<p><b>9.3</b> Stellen Sie sicher, dass alle Besucher wie folgt behandelt werden:</p>	<p><b>9.3</b> Überprüfen Sie, ob die Besucherkontrollen wie folgt umgesetzt werden:</p>			
<p><b>9.3.1</b> Autorisierung zum Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder verwaltet werden.</p>	<p><b>9.3.1</b> Beobachten Sie die Nutzung von Besucher-ID-Ausweisen, um sicherzustellen, dass ein Besucher-ID-Ausweis keinen unbeaufsichtigten Zugang zu Bereichen mit Karteninhaberdaten gewährt.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>9.3.2</b> Es wird ein physisches Token (z. B. ein Ausweis oder Zugangsgert) mit begrenzter Gultigkeit und das Besucher als solche identifiziert, ausgeteilt.	<b>9.3.2.a</b> Beobachten Sie Personen innerhalb der Einrichtung, um die Nutzung der Besucher-ID-Batches zu bestatigen und sicherzustellen, dass die Besucher leicht von dem Personal vor Ort unterschieden werden konnen.			
	<b>9.3.2.b</b> Ueberprufen Sie, ob die Besucherausweise eine begrenzte Gultigkeit haben.			
<b>9.3.3</b> Bitte um Ruckgabe der physischen Token, wenn die Besucher die Einrichtung verlassen oder die Erlaubnis auslauft.	<b>9.3.3</b> Beobachten Sie, ob Besucher den ID-Ausweis beim Verlassen der Einrichtung bzw. beim Auslaufen der Erlaubnis zuruckgeben.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>9.4</b> Überprüfen Sie die Besucheraktivität anhand eines Besucherprotokolls. Dokumentieren Sie den Namen des Besuchers, den Firmennamen und den Namen des Mitarbeiters vor Ort, der dem Besucher Zugang gewährt. Aufbewahren des Besucherprotokolls für die Dauer von mindestens drei Monaten, wenn dies gesetzlich zulässig ist.</p>	<p><b>9.4.a</b> 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.</p>			
<p><b>9.5</b> Aufbewahren von Sicherungskopien an einem sicheren Ort, vorzugsweise in einer anderen Einrichtung, wie z. B. an einer Alternativ- oder Backup-Stelle oder bei einem kommerziellen Anbieter von Speicherkapazitäten. Überprüfen der Sicherheit dieses Standorts mindestens einmal pro Jahr.</p>	<p><b>9.5.a</b> Überprüfen Sie die physischen Sicherheitsvorkehrungen der Speicherstelle, um sich davon zu überzeugen, dass die Sicherungsmedien sicher gespeichert sind.</p>			
<p><b>9.6</b> Stellen Sie die physische Sicherheit aller Medien sicher.</p>	<p><b>9.6</b> Überprüfen Sie, ob die Verfahren zum Schutz von Karteninhaberdaten Kontrollen zur physischen Sicherheit aller Medien (einschließlich, aber nicht beschränkt auf Computer, elektronische Wechselmedien sowie physische Quittungen, Berichte und Faxe) umfassen.</p>			
<p><b>9.7</b> Führen Sie strikte Kontrollen der internen bzw. externen Verteilung jeglicher Art von Medien mit Karteninhaberdaten, einschließlich Folgender, durch:</p>	<p><b>9.7</b> Überprüfen Sie, ob eine Richtlinie zur Kontrolle der Verteilung von Medien vorhanden ist und ob diese Richtlinie sämtliche Medien abdeckt (d. h. auch die, die an Einzelpersonen verteilt wurden).</p>			
<p><b>9.7.1</b> Klassifizieren Sie die Medien, sodass die Sensibilität der Daten bestimmt werden kann.</p>	<p><b>9.7.1</b> Überprüfen Sie, ob alle Medien klassifiziert sind, damit die Sensibilität der Daten bestimmt werden kann.</p>			
<p><b>9.7.2</b> Versenden Sie die Medien über einen sicheren Kurier oder eine andere Liefermethode, die genau verfolgt werden kann.</p>	<p><b>9.7.2</b> 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.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>9.8</b> Stellen Sie sicher, dass das Management den Transfer sämtlicher Medien aus einem geschützten Bereich genehmigt (insbesondere, wenn die Medien an einzelne Personen weitergegeben werden).</p>	<p><b>9.8</b> Überprüfen Sie bei aktuellen und an mehreren Tagen genommenen Stichproben aus den Protokollen zur Standortverfolgung von Medien, ob alle wichtigen Details protokolliert wurden und die Genehmigung durch das Management vorlag.</p>			
<p><b>9.9</b> Führen Sie strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien durch.</p>	<p><b>9.9</b> Untersuchen Sie die Richtlinie zur Kontrolle der Aufbewahrung und Verwaltung sämtlicher Medien, und prüfen Sie, ob darin eine regelmäßige Inventur der vorhandenen Medien vorgesehen ist.</p>			
<p><b>9.9.1</b> Stellen Sie eine ordnungsgemäße Verwaltung von Medieninventurlisten und die Durchführung mindestens einer jährlichen Medieninventur sicher.</p>	<p><b>9.9.1</b> Untersuchen Sie das Medien-Inventurprotokoll, und achten Sie darauf, dass eine Inventur der vorhandenen Medien mindestens einmal pro Jahr stattfindet.</p>			
<p><b>9.10</b> Vernichten Sie Medien, wenn diese nicht mehr zu geschäftlichen oder juristischen Zwecken benötigt werden, wie folgt:</p>	<p><b>9.10</b> Prüfen Sie die Richtlinie zur regelmäßigen Vernichtung von Medien, und überprüfen Sie, ob diese Richtlinie für sämtliche Medien, gilt. Gehen Sie dabei wie folgt vor:</p>			
<p><b>9.10.1</b> Setzen Sie Aktenvernichter für Papiausdrucke ein, sodass keine Karteninhaberdaten wiederhergestellt werden können.</p>	<p><b>9.10.1.a</b> Überprüfen Sie, ob Papiausdrucke mit einem Aktenvernichter entsorgt werden und mit absoluter Sicherheit ausgeschlossen werden kann, dass diese Dokumente wiederhergestellt werden.</p>			
	<p><b>9.10.1.b</b> Überprüfen Sie, ob Container zur Aufbewahrung von Informationen, die gelöscht werden sollen, geschützt sind. Achten Sie beispielsweise darauf, dass ein Container mit zu vernichtenden Akten mit einem Schloss gesichert ist.</p>			
<p><b>9.10.2</b> Löschen von Karteninhaberdaten auf elektronischen Medien in einer Art und Weise, die eine Wiederherstellung der Daten ausschließt.</p>	<p><b>9.10.2</b> 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).</p>			

## 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 oder sogar gar nicht ermitteln.

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

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>10.2.6</b> Initialisierung der Audit-Protokolle	<b>10.2.6</b> Prüfen Sie, ob die Initialisierung der Audit-Protokolle protokolliert wird.			
<b>10.2.7</b> Erstellen und Löschen von Objekten auf Systemebene	<b>10.2.7</b> Prüfen Sie, ob das Erstellen und Löschen von Objekten auf Systemebene protokolliert wird.			
<b>10.3</b> Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf:	<b>10.3</b> Führen Sie mittels Gesprächen und eigenen Beobachtungen zu jedem zu protokollierenden Ereignis (aus 10.2) Folgendes durch:			
<b>10.3.1</b> Benutzeridentifizierung	<b>10.3.1</b> Prüfen Sie, ob die Benutzer-ID in den Protokolleinträgen enthalten ist.			
<b>10.3.2</b> Ereignistyp	<b>10.3.2</b> Prüfen Sie, ob die Art des Ereignisses in den Protokolleinträgen enthalten ist.			
<b>10.3.3</b> Datum und Uhrzeit	<b>10.3.3</b> Prüfen Sie, ob die Datums- und Zeitangabe in den Protokolleinträgen enthalten ist.			
<b>10.3.4</b> Angabe von Erfolgen oder Fehlern	<b>10.3.4</b> Prüfen Sie, ob der Hinweis auf die erfolgreiche oder fehlgeschlagene Ausführung in den Protokolleinträgen enthalten ist.			
<b>10.3.5</b> Ereignisursprung	<b>10.3.5</b> Prüfen Sie, ob der Ursprung des Ereignisses in den Protokolleinträgen enthalten ist.			
<b>10.3.6</b> Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen.	<b>10.3.6</b> Überprüfen Sie, ob die Identität oder der Name der betroffenen Daten, Systemkomponenten oder Ressourcen in den Protokolleinträgen enthalten ist.			
<b>10.4</b> Synchronisieren Sie mit Technologien zur Zeitsynchronisierung alle wichtigen Systemuhren und -zeiten und stellen Sie sicher, dass	<b>10.4.a</b> Überprüfen Sie, ob eine Technologie zur Zeitsynchronisierung implementiert ist und diese entsprechend der PCI-DSS-Anforderungen 6.1 und 6.2. auf dem neuesten Stand gehalten wird.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p>folgende Elemente zur Ermittlung, Weitergabe und Speicherung der richtigen Zeit implementiert sind:</p> <p><b>Hinweis:</b> Eine Zeitsynchronisierungstechnologie ist beispielsweise das Network Time Protocol (NTP).</p>	<p><b>10.4.b</b> Prüfen Sie den Prozess zum Ermitteln, zur Weitergabe und Speicherung der richtigen Zeit innerhalb der Organisation und überprüfen Sie stichprobenartig die zeitbedingten Systemparametereinstellungen bei Systemkomponenten. Überprüfen Sie, ob folgende Elemente im Prozess enthalten und implementiert sind:</p>			
<p><b>10.4.1</b> Wichtige Systeme zeigen die richtige und gleichbleibende Uhrzeit an.</p>	<p><b>10.4.1.a</b> Überprüfen Sie, ob ausschließlich ausgewählte zentrale Zeitserver Zeitsignale von externen Quellen empfangen und ob die Zeitsignale von externen Quellen auf der Internationalen Atomzeit bzw. der Koordinierten Weltzeit (UTC) basieren.</p>			
	<p><b>10.4.1.b</b> Überprüfen Sie, ob die ausgewählten zentralen Zeitserver im Austausch untereinander für eine höchstmögliche Genauigkeit sorgen und andere interne Server die Uhrzeit nur von den zentralen Zeitservern empfangen.</p>			
<p><b>10.4.2</b> Zeitinformationen sind geschützt.</p>	<p><b>10.4.2.a</b> Überprüfen Sie die Systemkonfigurationen und Einstellungen der Zeitsynchronisierung, um sicherzustellen, dass der Zugriff auf Zeitinformationen ausschließlich Mitarbeitern vorbehalten ist, die den Zugriff auf Zeitinformationen aus geschäftlichen Gründen benötigen.</p>			
	<p><b>10.4.2.b</b> Überprüfen Sie die Systemkonfigurationen und Einstellungen sowie Prozesse der Zeitsynchronisierung, um sicherzustellen, dass jegliche Änderungen an den Zeiteinstellungen auf wichtigen Systemen protokolliert, überwacht und überprüft werden.</p>			
<p><b>10.4.3</b> Zeiteinstellungen werden von branchenüblichen Zeitquellen empfangen.</p>	<p><b>10.4.3</b> Überprüfen Sie, ob die Zeitserver Zeitaktualisierungen von spezifischen, branchenüblichen externen Quellen zulassen (um zu verhindern, dass die Uhr von einer Einzelperson manipuliert werden kann). Diese Zeitaktualisierungen können mit einem symmetrischen Schlüssel verschlüsselt werden. Außerdem können Zugriffskontrolllisten erstellt werden, aus denen die IP-Adressen der Client Rechner hervorgehen, die die Zeitaktualisierungen in Anspruch nehmen. (Hierdurch wird die Nutzung nicht autorisierter interner Zeitserver verhindert.)</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>10.5</b> Schützen Sie Audit-Trails vor Veränderungen.	<b>10.5</b> Ermitteln Sie in Gesprächen mit dem Systemadministrator und durch die Untersuchung von Berechtigungen, ob Audit-Trails so geschützt sind, dass sie nicht geändert werden können. Gehen Sie wie folgt vor:			
<b>10.5.1</b> Beschränken Sie die Anzeige der Audit-Trails auf Personen, die aus geschäftlichen Gründen darauf zugreifen müssen.	<b>10.5.1</b> Überprüfen Sie, ob nur Einzelpersonen Zugriff auf Audit-Trail-Dateien haben, die aus geschäftlichen Gründen darauf zugreifen müssen.			
<b>10.5.2</b> Schützen Sie Audit-Trail-Dateien vor nicht autorisierten Änderungen.	<b>10.5.2</b> Überprüfen Sie, ob die Dateien des aktuellen Audit-Trails mit Zugriffssteuerungssystemen, räumlicher Trennung und/oder Netzwerktrennung vor unbefugten Änderungen geschützt werden.			
<b>10.5.3</b> Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.	<b>10.5.3</b> Überprüfen Sie, ob Dateien des aktuellen Audit-Trails sofort auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen, gesichert werden.			
<b>10.5.4</b> Erstellen von Protokollen für nach außen gerichtete Technologien auf einem Protokollserver im internen LAN.	<b>10.5.4</b> 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.			
<b>10.5.5</b> 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).	<b>10.5.5</b> 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.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>10.6</b> Überprüfen Sie die Protokolle für alle Systemkomponenten mindestens einmal täglich. Protokollüberprüfungen müssen die Server mit Sicherheitsfunktionen wie Intrusion Detection System (IDS) und Authentication, Authorization and Accounting (AAA)-Protokollserver (z. B. RADIUS) umfassen.</p> <p><i>Hinweis: Zur Konformität mit Anforderung 10.6 können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.</i></p>	<p><b>10.6.a</b> Untersuchen Sie Sicherheitsrichtlinien und -verfahren daraufhin, ob sie Verfahren zur mindestens täglichen Prüfung von Sicherheitsprotokollen enthalten und dass Ausnahmen zwingend überprüft werden müssen.</p>			
	<p><b>10.6.b</b> Prüfen Sie durch Gespräche und eigene Beobachtungen, ob regelmäßig die Protokolle sämtlicher Systemkomponenten geprüft werden.</p>			
<p><b>10.7</b> Bewahren Sie die Audit-Trail-Verlaufsdaten für mindestens ein Jahr auf. Zur Analyse müssen diese Daten für einen Zeitraum von mindestens drei Monaten direkt zur Verfügung stehen (beispielsweise online, archiviert oder aus einer Sicherung wiederherstellbar).</p>	<p><b>10.7.a</b> Untersuchen Sie die Sicherheitsrichtlinien und -verfahren daraufhin, ob sie Aufbewahrungsrichtlinien für das Audit-Protokoll mit einer mindestens einjährigen Aufbewahrungsfrist enthalten.</p>			
	<p><b>10.7.b</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 Analyse zur Verfügung stehen.</p>			

### 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 nur so eine effektive Sicherheit in einer sich ändernden Umgebung erzielt werden kann.

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>11.1</b> Stellen Sie mithilfe von Tests fest, ob Zugriffspunkte für drahtlose Netzwerke vorhanden sind und suchen Sie vierteljährlich nach eventuellen nicht autorisierten Zugriffspunkten für drahtlose Netzwerke.</p> <p><i><b>Hinweis:</b> Methoden, die sich hierfür anbieten, sind unter anderen Scans zur Feststellung drahtloser Netzwerke, physische/logische Überprüfungen der Systemkomponenten und Infrastruktur, Network Access Control (NAC) oder Wireless IDS/IPS-Systeme.</i></p> <p><i>Welche Methode auch immer verwendet wird, sie muss ausreichend sein, um jegliche nicht autorisierten Geräte zu erkennen und zu identifizieren.</i></p>	<p><b>11.1.a</b> Überprüfen Sie, ob die Stelle über einen dokumentierten Prozess zur vierteljährlichen Erkennung und Identifizierung von Zugriffspunkten für drahtlose Netzwerke verfügt.</p>			
	<p><b>11.1.b</b> Überprüfen Sie, ob die angewandte Methodik ausreichend ist, um jegliche nicht autorisierten Zugriffspunkte für drahtlose Netzwerke, einschließlich mindestens folgender Elemente, zu erkennen und zu identifizieren:</p> <ul style="list-style-type: none"> <li>▪ In Systemkomponenten eingefügte WLAN-Karten</li> <li>▪ An Systemkomponenten angeschlossene tragbare Drahtlosgeräte (z. B. durch USB usw.)</li> <li>▪ An einen Netzwerkport oder ein Netzwerkgerät angeschlossene Drahtlosgeräte</li> </ul>			
	<p><b>11.1.c</b> Überprüfen Sie, ob der dokumentierte Prozess zur Identifizierung nicht autorisierter Zugriffspunkte für drahtlose Netzwerke mindestens vierteljährlich auf allen Systemkomponenten und an allen Stellen durchgeführt wird.</p>			
	<p><b>11.1.d</b> Wenn eine automatische Überwachung eingesetzt wird (z. B. ein Wireless IDS/IPS-System, NAC usw.) überprüfen Sie, ob in der Konfiguration Alarmmeldungen für das Personal vorgesehen sind.</p>			
	<p><b>11.1.e</b> Überprüfen Sie, ob im Vorfalreaktionsplan (Anforderung 12.9) eine Reaktion für den Fall definiert ist, dass nicht autorisierte Drahtlosgeräte entdeckt werden.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>11.2</b> 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).</p> <p><i><b>Hinweis:</b> 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><b>11.2</b> Überprüfen Sie, ob die internen und externen Schwachstellenprüfungen wie folgt ausgeführt werden:</p>			
<p><b>11.2.1</b> Führen Sie vierteljährlich interne Schwachstellenprüfungen durch.</p>	<p><b>11.2.1.a</b> Überarbeiten Sie die Prüfungsberichte und stellen Sie sicher, dass vier vierteljährliche interne Prüfungen in den letzten 12 Monaten stattgefunden haben.</p>			
	<p><b>11.2.1.b</b> Überarbeiten Sie die Prüfungsberichte und stellen Sie sicher, dass der Prüfungsprozess erneute Prüfungen vorsieht, bis der gefundene Fehler behoben wurde oder alle „schwerwiegenden“ Sicherheitslücken wie in der PCI-DSS-Anforderung 6.2 dargelegt gelöst wurden.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
	<p><b>11.2.1.c</b> Überprüfen Sie, ob die Prüfung von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt wurde und gegebenenfalls, ob der Tester für eine unabhängige Organisation tätig ist (es muss sich nicht um einen QSA oder ASV handeln).</p>			
<p><b>11.2.2</b> Führen Sie vierteljährlich externe Schwachstellenprüfungen über einen Scanninganbieter (ASV) durch, der vom Payment Card Industry Security Standards Council (PCI-SSC) zugelassen wurde.</p> <p><i>Hinweis: Vierteljährliche externe Schwachstellenprüfungen müssen von einem Scanninganbieter (ASV) durchgeführt werden, der vom Payment Card Industry Security Standards Council (PCI-SSC) zugelassen wurde. Nach Netzwerkänderungen durchgeführte Scans können vom internen Personal ausgeführt werden.</i></p>	<p><b>11.2.2.a</b> Überprüfen Sie die Ergebnisse der externen Schwachstellenprüfungen der vier letzten Quartale und stellen Sie sicher, dass in den letzten 12 Monaten vier vierteljährliche interne Prüfungen stattgefunden haben.</p>			
	<p><b>11.2.2.b</b> Überprüfen Sie die Ergebnisse der letzten vierteljährlichen Prüfung und stellen Sie sicher, dass sie die Anforderungen des ASV-Programmführers erfüllen (z. B. keine Schwachstellen, die vom CVSS eine Klassifizierung höher als 4.0 erhalten haben und keine automatischen Ausfälle).</p>			
	<p><b>11.2.2.c</b> Überprüfen Sie die Schwachstellenprüfungen, um sicherzustellen, dass die Tests von einem vom PCI-SSC zugelassenen Scanninganbieter durchgeführt wurden.</p>			
<p><b>11.2.3</b> Führen Sie nach jeder wesentlichen Änderung interne und externe Scans durch.</p> <p><i>Hinweis: Nach Änderungen durchgeführte Scans können vom internen Personal ausgeführt werden.</i></p>	<p><b>11.2.3.a</b> Überprüfen Sie die Änderungskontrolldokumentation und Prüfungsberichte, um sicherzustellen, dass Systemkomponenten, an denen wesentliche Änderungen vorgenommen wurden, gescannt wurden.</p>			
	<p><b>11.2.3.b</b> Überprüfen Sie die Prüfungsberichte und stellen Sie sicher, dass der Scan-Vorgang so lange durchgeführt wird, bis:</p> <ul style="list-style-type: none"> <li>▪ Bei externen Scans keine Sicherheitslücken mehr vorhanden sind, die vom CVSS mit einer Klassifizierung höher als 4.0 bewertet wurden,</li> <li>▪ Bei internen Scans der Fehler behoben wurde oder alle „schwerwiegenden“ Sicherheitslücken wie in der PCI-DSS-Anforderung 6.2 dargelegt gelöst wurden.</li> </ul>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
	<p><b>11.2.3.c</b> Überprüfen Sie, ob die Prüfung von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt wurde und gegebenenfalls, ob der Tester für eine unabhängige Organisation tätig ist (es muss sich nicht um einen QSA oder ASV handeln).</p>			
<p><b>11.3</b> 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 in der Umgebung). Diese Penetrationstests müssen Folgendes enthalten:</p>	<p><b>11.3.a</b> 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.</p>			
	<p><b>11.3.b</b> Überprüfen Sie, ob bekannte ausnutzbare Schwachstellen korrigiert wurden und ob anschließend ein erneuter Test durchgeführt wurde.</p>			
	<p><b>11.3.c</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>			
<p><b>11.3.1</b> Penetrationstests auf Netzwerkebene</p>	<p><b>11.3.1</b> Überprüfen Sie, ob der Penetrationstest auch Tests auf Netzwerkebene umfasst. Die Tests müssen Komponenten enthalten, die Netzwerkfunktionen und Betriebssysteme unterstützen.</p>			
<p><b>11.3.2</b> Penetrationstests auf Anwendungsebene</p>	<p><b>11.3.2</b> Überprüfen Sie, ob der Penetrationstest auch Penetrationstests auf Anwendungsebene umfasst. In den Tests sollten mindestens die in der Anforderung 6.5 aufgeführten Schwachstellen überprüft werden.</p>			
<p><b>11.4</b> Nutzung von Systemen zur Erkennung und/oder Verhinderung von Angriffsversuchen zur Überwachung des kompletten Datenverkehrs in der Umgebung, in der sich Karteninhaberdaten befinden, sowie kritischer Punkte innerhalb der Karteninhaberdaten-Umgebung und Alarmierung des Personals bei</p>	<p><b>11.4.a</b> Überprüfen Sie die Nutzung von Systemen zur Erkennung und/oder Verhinderung von Angriffsversuchen und dass der gesamte Datenverkehr in der Umgebung, in der sich Karteninhaberdaten befinden, sowie kritische Punkte innerhalb der Karteninhaberdaten-Umgebung überwacht werden.</p>			
	<p><b>11.4.b</b> Überprüfen Sie, ob IDS und/oder IPS so konfiguriert sind, dass das Personal bei mutmaßlichen Sicherheitsverletzungen alarmiert wird.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p>mutmaßlichen Sicherheitsverletzungen. Ständige Aktualisierung der Angriffserfassungs- und -vorbeugungssysteme, Ausgangseinstellungen und Signaturen.</p>	<p><b>11.4.c</b> 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.</p>			
<p><b>11.5</b> Setzen Sie Tools zur Überwachung der Dateiintegrität ein, die das Personal über nicht autorisierte Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien alarmieren, und konfigurieren Sie die Software so, dass sie mindestens wöchentlich Vergleiche wichtiger Dateien herstellt.</p> <p><i><b>Hinweis:</b> 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 Dienstleister) beurteilt und definiert werden.</i></p>	<p><b>11.5.a</b> Überprüfen Sie die Nutzung von Tools zur Überwachung der Dateiintegrität innerhalb der Umgebung mit Karteninhaberdaten, indem Sie die Systemeinstellungen und die überwachten Dateien sowie Ergebnisse aus der Aktivitätsüberwachung untersuchen.</p> <p>Beispiele für Dateien, die überwacht werden sollten:</p> <ul style="list-style-type: none"> <li>▪ Ausführbare Systemdateien</li> <li>▪ Ausführbare Anwendungsdateien</li> <li>▪ Konfigurations- und Parameterdateien</li> <li>▪ Zentral gespeicherte Protokoll- und Audit-Dateien (alt oder archiviert)</li> </ul> <p><b>11.5.b</b> Überprüfen Sie, ob die Tools konfiguriert sind, das Personal über nicht zulässige Änderungen wichtiger Dateien zu alarmieren und mindestens einmal wöchentlich Vergleiche wichtiger Dateien herzustellen.</p>			

## Befolgung einer Informationssicherheits-Richtlinie

### **Anforderung 12: Befolgung einer Informationssicherheits-Richtlinie für das gesamte Personal.**

Eine strenge Sicherheitsrichtlinie gibt den Takt für die gesamte Stelle vor und dient dem Personal als Richtschnur dazu, was von ihm verlangt wird. Alle Mitarbeiter sollten sich darüber im Klaren sein, dass Daten Gefahren ausgesetzt sind und dass sie für deren Schutz verantwortlich sind. Zum Zwecke der Anforderung 12 bezieht sich der Begriff „Mitarbeiter“ hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter, Subunternehmer und Berater, die am Standort der jeweiligen Stelle „ansässig“ sind oder anderweitig Zugriff auf die Karteninhaberdaten-Umgebung haben.

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<b>12.1</b> Festlegen, Veröffentlichen, Verwalten und Verbreiten einer Sicherheitsrichtlinie mit den folgenden Zielen:	<b>12.1</b> Untersuchen Sie die Datensicherheitsrichtlinie, und prüfen Sie, ob die Richtlinie veröffentlicht und an alle relevanten Mitarbeiter (einschließlich Subunternehmer und Geschäftspartner) weitergeleitet wurde.			
<b>12.1.1</b> Umfasst sämtliche PCI-DSS-Anforderungen.	<b>12.1.1</b> Überprüfen Sie, ob die Richtlinie sämtliche PCI-DSS-Anforderungen umfasst.			
<b>12.1.2</b> Umfasst einen jährlichen Prozess zur Ermittlung von Bedrohungen und Anfälligkeiten, der zu einer offiziellen Risikobeurteilung führt. (Beispiele von Risikobewertungsmethoden sind unter anderen OCTAVE, ISO 27005 und NIST SP 800-30.)	<b>12.1.2.a</b> Überprüfen Sie, ob der jährliche Prozess zur Ermittlung von Bedrohungen und Anfälligkeiten, der zu einer offiziellen Risikobeurteilung führt, dokumentiert ist.			
	<b>12.1.2.b</b> Überprüfen Sie die Risikobewertungsdokumentation, um sicherzustellen, dass der Risikobewertungsprozess mindestens einmal jährlich durchgeführt wird.			
<b>12.1.3</b> Umfasst eine mindestens jährliche Überprüfung sowie Aktualisierungen bei Umgebungsänderungen.	<b>12.1.3</b> Überprüfen Sie, ob die Richtlinie zur Informationssicherheit mindestens einmal im Jahr überarbeitet und an die geänderten Geschäftsziele bzw. Risiken angepasst wird.			
<b>12.2</b> Entwickeln von Routineverfahren für die Betriebssicherheit, die den Anforderungen in dieser Spezifikation entsprechen (z. B. Benutzerkonto-Wartungsverfahren und Protokollüberprüfungsverfahren).	<b>12.2</b> 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
<b>12.3</b> Entwickeln Sie Verwendungsrichtlinien für wichtige Technologien (z. B. Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, PDAs, E-Mail-Programme und Internet), und beschreiben Sie die korrekte Verwendung dieser Technologien. Die Verwendungsrichtlinien umfassen folgende Punkte:	<b>12.3</b> Untersuchen Sie die Verwendungsrichtlinien auf wichtige Technologien und führen Sie Folgendes durch:			
<b>12.3.1</b> Ausdrückliche Genehmigung durch autorisierte Parteien	<b>12.3.1</b> Überprüfen Sie, ob in den Verwendungsrichtlinien eine ausdrückliche Genehmigung dritter Parteien für die Verwendung dieser Technologien festgelegt ist.			
<b>12.3.2</b> Authentifizierung zur Verwendung der Technologie	<b>12.3.2</b> 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.			
<b>12.3.3</b> Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff	<b>12.3.3</b> Überprüfen Sie, ob laut Verwendungsrichtlinie eine Liste sämtlicher Geräte und der zur Verwendung der Geräte befugten Personen angelegt werden muss.			
<b>12.3.4</b> Etikettierung von Geräten, um Eigner, Kontaktinformationen und Zweck zu bestimmen	<b>12.3.4</b> Überprüfen Sie, ob die Verwendungsrichtlinie eine Etikettierung von Geräten erfordert, um ihnen den entsprechenden Eigner, Kontaktinformationen und Zweck zuzuordnen.			
<b>12.3.5</b> Akzeptable Verwendung der Technologie	<b>12.3.5</b> Überprüfen Sie, ob in den Verwendungsrichtlinien festgelegt ist, dass von der Technologie eine angemessene Verwendung gemacht werden muss.			
<b>12.3.6</b> Akzeptable Netzwerkkarte für die Technologien	<b>12.3.6</b> Überprüfen Sie, ob in den Verwendungsrichtlinien festgelegt ist, dass für die Technologie angemessene Netzwerkkarte eingerichtet werden müssen.			
<b>12.3.7</b> Liste der vom Unternehmen zugelassenen Produkte	<b>12.3.7</b> Überprüfen Sie, ob in den Verwendungsrichtlinien eine Liste mit vom Unternehmen zugelassenen Produkten vorgeschrieben ist.			
<b>12.3.8</b> Automatisches Trennen von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität	<b>12.3.8</b> Überprüfen Sie, ob in den Verwendungsrichtlinien eine automatische Trennung von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität festgelegt ist.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>12.3.9</b> Aktivierung von Remotezugriff-Technologien für Anbieter und Geschäftspartner nur, wenn bei Anbietern und Geschäftspartnern ein dringender Bedarf besteht und die Technologie nach der Nutzung gleich wieder deaktiviert wird</p>	<p><b>12.3.9</b> Überprüfen Sie, ob die Verwendungsrichtlinien eine Aktivierung von Remotezugriff-Technologien für Anbieter und Geschäftspartner nur im Bedarfsfall und mit sofortiger Deaktivierung nach der Verwendung vorsieht.</p>			
<p><b>12.3.10</b> Untersagen Sie Mitarbeitern, die auf Karteninhaberdaten per Remotezugriff zugreifen, Karteninhaberdaten auf lokale Festplatten und elektronische Wechselmedien zu kopieren, zu verschieben oder zu speichern, sofern nicht ausdrücklich aufgrund bekannter Geschäftsbedürfnisse gestattet.</p>	<p><b>12.3.10.a</b> Überprüfen Sie, ob in den Verwendungsrichtlinien festgelegt ist, dass Karteninhaberdaten über Remotezugriff-Technologien nicht auf lokale Festplatten und elektronische Wechselmedien kopiert, verschoben oder gespeichert werden dürfen.</p>			
	<p><b>12.3.10.b</b> Überprüfen Sie, ob die Verwendungsrichtlinien für Mitarbeiter mit entsprechenden Befugnissen den Schutz der Karteninhaberdaten gemäß den PCI-DSS-Anforderungen voraussetzen.</p>			
<p><b>12.4</b> Stellen Sie sicher, dass die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter beinhalten.</p>	<p><b>12.4</b> Überprüfen Sie, ob die Sicherheitsrichtlinien eine klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter enthalten.</p>			
<p><b>12.5</b> Weisen Sie einer Einzelperson oder einem Team folgende Managementverantwortungsbereiche in puncto Informationssicherheit zu:</p>	<p><b>12.5</b> 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:</p>			
<p><b>12.5.1</b> Festlegen, Dokumentieren und Verteilen von Sicherheitsrichtlinien und -verfahren.</p>	<p><b>12.5.1</b> Überprüfen Sie, ob die Verantwortlichkeit zur Erstellung und Verteilung von Sicherheitsrichtlinien und -verfahren formal festgelegt wurde.</p>			
<p><b>12.5.2</b> Überwachen und analysieren Sie Sicherheitsalarme und -informationen und verteilen Sie sie an das entsprechende Personal.</p>	<p><b>12.5.2</b> Überprüfen Sie, ob die Verantwortlichkeit für die Überwachung und Analyse von Sicherheitsalarmen sowie für die Weitergabe von Informationen formal an das zuständige Personal zugewiesen wurde.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
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 Sie Benutzerkonten, einschließlich Ergänzungen, Löschungen und Änderungen	12.5.4 Überprüfen Sie, ob die Verantwortlichkeit für die Verwaltung von Benutzerkonten und für das Authentifizierungsmanagement formal geregelt wurde.			
12.5.5 Überwachen und kontrollieren Sie den gesamten Datenzugriff.	12.5.5 Überprüfen Sie, ob die Verantwortlichkeiten zur Überwachung und Kontrolle des gesamten Datenzugriffs formal zugewiesen wurden.			
12.6 Implementieren Sie ein offizielles Sicherheitsbewusstseinsprogramm, durch das 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 Führen Sie Mitarbeiterschulungen bei der Einstellung und danach mindestens einmal im Jahr ein.  <i>Hinweis: Die Methoden sind abhängig von der Funktion der Mitarbeiter und deren Zugriffsrechte auf Karteninhaberdaten.</i>	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, Meetings und Sonderaktionen).			
	12.6.1.b Überprüfen Sie, ob die Mitarbeiter zur Einstellung und danach mindestens einmal im Jahr an entsprechenden Schulungen teilnehmen.			
12.6.2 Fordern Sie von den Mitarbeitern mindestens einmal pro Jahr eine schriftliche Bestätigung, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens gelesen und verstanden haben.	12.6.2 Überprüfen Sie, ob im Sicherheitsbewusstseinsprogramm festgelegt ist, dass die Mitarbeiter mindestens einmal im Jahr schriftlich oder elektronisch bestätigen müssen, dass sie die Datensicherheitsrichtlinie gelesen und verstanden haben.			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>12.7</b> Überprüfen Sie potentielle neue Mitarbeiter, um das Risiko von Angriffen durch interne Quellen zu minimieren. (Beispiele für Hintergrundinformationen sind frühere Tätigkeiten, eventuelle Vorstrafen, die finanzielle Situation und Referenzen bisheriger Arbeitgeber.)</p> <p><i><b>Hinweis:</b> Für potentielle neue Mitarbeiter wie z. B. Kassierer, die nur Zugriff auf jeweils eine Kartennummer gleichzeitig haben, wenn eine Transaktion durchgeführt wird, ist diese Anforderung lediglich eine Empfehlung.</i></p>	<p><b>12.7</b> 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.</p>			
<p><b>12.8</b> Wenn Karteninhaberdaten gemeinsam mit Dienstanbietern genutzt werden, müssen Richtlinien und Verfahren zur Verwaltung von Dienstanbietern umgesetzt und eingehalten werden. Hierunter fallen die folgenden Punkte:</p>	<p><b>12.8</b> Wenn die betreffende Stelle Karteninhaberdaten an Dienstanbieter (z. B. Einrichtungen für die Aufbewahrung von Sicherungsbändern, Anbieter verwalteter Dienste wie Webhosting-Unternehmen und Sicherheitsdienstleister 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:</p>			
<p><b>12.8.1</b> Stellen Sie eine Liste der Dienstanbieter auf.</p>	<p><b>12.8.1</b> Überprüfen Sie, ob eine Liste mit Dienstanbietern geführt wird.</p>			
<p><b>12.8.2</b> Unterhalten Sie eine schriftliche Vereinbarung mit einer Bestätigung, dass der Dienstanbieter für die Sicherheit der Karteninhaberdaten in seinem Besitz haftet.</p>	<p><b>12.8.2</b> Überprüfen Sie, ob eine schriftliche Vereinbarung existiert, die eine Bestätigung umfasst, dass die Dienstanbieter für die Sicherheit der Karteninhaberdaten haften.</p>			
<p><b>12.8.3</b> Festlegung eines eindeutigen Verfahrens für die Inanspruchnahme von Dienstanbietern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht.</p>	<p><b>12.8.3</b> Überprüfen Sie, ob Richtlinien und Verfahren für die Auswahl von Dienstanbietern vorliegen und ob bei der Wahl des Anbieters die erforderliche Sorgfalt beachtet wurde.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>12.8.4</b> Richten Sie ein Programm zur mindestens einmal jährlichen Überwachung der Dienstleister-Konformität mit dem PCI-Datensicherheitsstandard ein.</p>	<p><b>12.8.4</b> Überprüfen Sie, ob an der betreffenden Stelle ein Programm zur mindestens einmal jährlichen Überwachung der Dienstleister-Konformität mit dem PCI-Datensicherheitsstandard vorliegt.</p>			
<p><b>12.9</b> Implementieren Sie einen Vorfalldaktionsplan. Bereiten Sie sich auf eine sofortige Reaktion auf Sicherheitsverletzungen im System vor.</p>	<p><b>12.9</b> Untersuchen Sie den Vorfalldaktionsplan sowie zugehörige Verfahren, und führen Sie Folgendes durch:</p>			
<p><b>12.9.1</b> Erstellen Sie den Vorfalldaktionsplan, der im Falle einer Sicherheitsverletzung im System eingesetzt wird. Stellen Sie sicher, dass der Plan mindestens die folgenden Punkte umfasst:</p> <ul style="list-style-type: none"> <li>▪ Rollen, Verantwortungsbereiche und Kommunikations- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken</li> <li>▪ Konkrete Verfahren für die Reaktion auf Vorfälle</li> <li>▪ Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs</li> <li>▪ Verfahren zur Datensicherung</li> <li>▪ Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen</li> <li>▪ Abdeckung sämtlicher wichtigen Systemkomponenten</li> <li>▪ Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle</li> </ul>	<p><b>12.9.1.a</b> Überprüfen Sie, ob der Vorfalldaktionsplan Folgendes umfasst:</p> <ul style="list-style-type: none"> <li>▪ Rollen, Verantwortungsbereiche und Kommunikationsstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken:</li> <li>▪ Konkrete Verfahren für die Reaktion auf Vorfälle</li> <li>▪ Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs</li> <li>▪ Verfahren zur Datensicherung</li> <li>▪ 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).</li> <li>▪ Abdeckung sämtlicher wichtigen Systemkomponenten</li> <li>▪ Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle</li> </ul> <p><b>12.9.1.b</b> Überprüfen Sie die Dokumentation einer in der Vergangenheit gemeldeten Sicherheitsverletzung oder Warnmeldung, um sicherzustellen, dass der dokumentierte Vorfalldaktionsplan und die entsprechenden Verfahren befolgt wurden.</p>			

PCI-DSS-Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>12.9.2</b> Testen Sie den Plan mindestens einmal im Jahr.</p>	<p><b>12.9.2</b> Überprüfen Sie, ob der Plan mindestens einmal im Jahr getestet wird.</p>			
<p><b>12.9.3</b> Stellen Sie sicher, dass rund um die Uhr Mitarbeiter eingesetzt sind, die auf mögliche Warnmeldungen reagieren.</p>	<p><b>12.9.3</b> 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><b>12.9.4</b> Führen Sie Schulungen für Mitarbeiter ein, die für die Reaktion auf Sicherheitsverletzungen verantwortlich sind.</p>	<p><b>12.9.4</b> Überprüfen Sie durch Beobachtung und Untersuchung von Richtlinien, dass die Mitarbeiter, die für die Reaktion auf Sicherheitsverletzungen verantwortlich sind, regelmäßig an Schulungen teilnehmen.</p>			
<p><b>12.9.5</b> Achten Sie hierbei auch auf Alarme aus Systemen zur Erkennung und/oder Verhinderung von Angriffsversuchen und zur Überwachung der Dateintegrität.</p>	<p><b>12.9.5</b> Überprüfen Sie durch Beobachtung und Untersuchung der Prozesse, ob die Überwachung und die Reaktion auf Alarme von Sicherheitssystemen, einschließlich die Erkennung unbefugter WLAN-Zugriffspunkte, im Vorfallreaktionsplan enthalten sind.</p>			
<p><b>12.9.6</b> Entwickeln Sie einen Prozesses zur Änderung und Weiterentwicklung des Vorfallreaktionsplans entsprechend Ihrer eigenen Erfahrungen und integrieren Sie Branchenentwicklungen.</p>	<p><b>12.9.6</b> Überprüfen Sie durch Beobachtung und Untersuchung von Richtlinien, ob ein Prozess zur Änderung und Weiterentwicklung des Vorfallreaktionsplans nach den eigenen Erfahrungen und unter Einbeziehung von Branchenentwicklungen vorhanden ist.</p>			

## Anhang A: Zusätzliche PCI-DSS-Anforderungen für von mehreren Benutzern gemeinsam genutzten Hosting-Anbieter

### 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	Impleme-ntiert	Nicht impleme-ntiert	Zieldatum/Anmer-kungen
<p><b>A.1</b> Schutz der gehosteten Umgebung und der Daten jeder Stelle (d. h. Händler, Dienstleister oder eine andere Stelle) gemäß A.1.1 bis A.1.4:</p> <p>Ein Hosting-Anbieter muss diese Anforderungen sowie die anderen relevanten Abschnitte des PCI-Datensicherheitsstandards erfüllen.</p> <p><i><b>Hinweis:</b> 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><b>A.1</b> 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>			

Anforderungen	Prüfverfahren	Implementiert	Nicht implementiert	Zieldatum/Anmerkungen
<p><b>A.1.1</b> Stellen Sie sicher, dass an den einzelnen Stellen nur Prozesse ausgeführt werden, die Zugriff auf die Karteninhaberdaten-Umgebung dieser Stelle haben.</p>	<p><b>A.1.1</b> 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: 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.</p>			
<p><b>A.1.2</b> Schränken Sie den Zugriff und die Berechtigungen aller Stellen auf ihre eigene Karteninhaberdaten-Umgebung ein.</p>	<p><b>A.1.2.a</b> Überprüfen Sie, ob die Benutzer-ID eines Anwendungsprozesses nicht über besondere Rechte (root/admin) verfügt.</p>			
	<p><b>A.1.2.b</b> Überprüfen Sie, ob die einzelnen Stellen (Händler, Dienstleister) Lese-, Schreib- und Ausführungsberechtigungen nur für eigene Dateien und Verzeichnisse oder für notwendige Systemdateien (eingeschränkt durch Dateisystemberechtigungen, Zugriffssteuerungslisten, chroot, jailshell usw.) besitzen. <b>Wichtig:</b> Die Dateien einer Stelle können nicht von einer Gruppe gemeinsam genutzt werden.</p>			
	<p><b>A.1.2.c</b> Stellen Sie sicher, dass die Benutzer einer Stelle keinen Schreibzugriff auf gemeinsam genutzte Systemdateien besitzen.</p>			
	<p><b>A.1.2.d</b> Überprüfen Sie, ob die Anzeige von Protokolleinträgen auf die protokollbesitzende Stelle beschränkt ist.</p>			
	<p><b>A.1.2.e</b> 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 können, überprüfen Sie, ob für die folgenden Systemressourcen Beschränkungen gelten:</p> <ul style="list-style-type: none"> <li>▪ Festplattenkapazität</li> <li>▪ Bandbreite</li> <li>▪ Arbeitsspeicher</li> <li>▪ Prozessor</li> </ul>			

Anforderungen	Prüfverfahren	Impleme ntiert	Nicht impleme ntiert	Zieldatum/Anmer kungen
<p><b>A.1.3</b> Stellen Sie sicher, dass eindeutige, mit der PCI-DSS-Anforderung 10 konforme, Protokollierungs- und Audit-Trails für die Karteninhaberdaten-Umgebung jeder Stelle aktiviert sind.</p>	<p><b>A.1.3</b> Überprüfen Sie, ob der gemeinsame Hosting-Anbieter die Protokollierung für jede einzelne Händler- und Dienstanbieterumgebung wie folgt aktiviert hat:            Protokolle werden für gängige Anwendungen von Drittanbietern aktiviert.            Protokolle sind standardmäßig aktiviert.            Protokolle können von der Stelle, die sie besitzt, eingesehen werden.            Die Besitzer der Protokolle erhalten eine Mitteilung zum genauen Speicherort der Protokolle.</p>			
<p><b>A.1.4</b> Aktivieren Sie Prozesse für eine rechtzeitige gerichtliche Untersuchung im Falle einer Sicherheitsverletzung bei einem gehosteten Händler oder Dienstanbieter.</p>	<p><b>A.1.4</b> 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.</p>			

## 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. (Der Zweck der 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. Zum Beispiel müssen Kennwörter für den nicht über die Konsole vorgenommenen Administratorzugriff verschlüsselt versendet werden, damit Administratorkennwörter 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. Zum Beispiel kann ein Unternehmen 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 haben 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. <b>Einschränkungen</b>	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	
2. <b>Ziel</b>	Definieren Sie das Ziel der ursprünglichen Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	
3. <b>Ermitteltes Risiko</b>	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	
4. <b>Definition der Kompensationskontrollen</b>	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	
5. <b>Validierung der Kompensationskontrollen</b>	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	
6. <b>Verwaltung</b>	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	

## Arbeitsblatt zu Kompensationskontrollen – Beispiel

Mit diesem Arbeitsblatt können Sie Kompensationskontrollen für sämtliche Anforderungen definieren, die mittels Kompensationskontrollen als „implementiert“ gekennzeichnet wurden.

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

	<b>Erforderliche Informationen</b>	<b>Erklärung</b>
<b>1. Einschränkungen</b>	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>
<b>2. Ziel</b>	Definieren Sie das Ziel der ursprünglichen 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>
<b>3. Ermitteltes Risiko</b>	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>
<b>4. Definition der Kompensationskontrollen</b>	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>
<b>5. Validierung der Kompensationskontrollen</b>	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>
<b>6. Verwaltung</b>	Legen Sie Prozesse und	<i>Unternehmen XYZ demonstriert Prozesse</i>

	Kontrollen zur Verwaltung der Kompensationskontrollen fest.	<i>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: Segmentierung und Stichprobenkontrolle von Unternehmenseinrichtungen/Systemkomponenten

