



# Zahlungskartenbranche (PCI) Datensicherheitsstandard

---

## Anforderungen und Sicherheitsbeurteilungsverfahren

Version 3.2  
April 2016

## Dokumentänderungen

Datum	Version	Beschreibung	Seiten
Oktober 2008	1.2	Einführung von PCI-DSS v1.2 als „PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren“ zur Beseitigung von Redundanzen zwischen verschiedenen Dokumenten und zur Vornahme sowohl allgemeiner als auch spezifischer Änderungen seit dem PCI-DSS-Sicherheitsprüfverfahren v1.1. Ausführliche Informationen finden Sie in der Übersicht über die Änderungen von PCI-DSS-Version 1.1 auf 1.2.	
Juli 2009	1.2.1	Fügen Sie den Satz ein, der fälschlicherweise zwischen 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. Siehe <i>PCI-DSS – Änderungsübersicht von PCI-DSS-Version 1.2.1 auf 2.0</i> .	
November 2013	3.0	Aktualisierung von v2.0. Siehe <i>PCI-DSS – Änderungsübersicht von PCI-DSS-Version 2.0 auf 3.0</i> .	
April 2015	3.1	Aktualisieren von PCI-DSS v2.0. Details zu den Änderungen finden Sie unter <i>PCI-DSS – Änderungsübersicht von PCI-DSS Version 3.0 auf 3.1</i> .“	
April 2016	3.2	Aktualisieren von PCI-DSS v3.1. Details zu den Änderungen finden Sie unter <i>PCI-DSS – Änderungsübersicht von PCI-DSS Version 3.1 auf 3.2</i> .“	

# Inhalt

<b>April 2016</b> .....	<b>2</b>
<b>Dokumentänderungen</b> .....	<b>2</b>
<b>Einführung und Überblick über den PCI-Datensicherheitsstandard</b> .....	<b>5</b>
<i>Ressourcen zum PCI-DSS</i> .....	6
<b>Informationen zur PCI DSS-Anwendbarkeit</b> .....	<b>7</b>
<b>Beziehung zwischen PCI-DSS und PA-DSS</b> .....	<b>9</b>
<i>Anwendbarkeit von PCI-DSS auf PA-DSS-Anwendungen</i> .....	9
<i>Anwendbarkeit des PCI-DSS auf die Anbieter von Zahlungsanwendungen</i> .....	9
<b>Geltungsbereich von PCI-DSS-Anforderungen</b> .....	<b>10</b>
<i>Netzwerksegmentierung</i> .....	11
<i>Drahtlos</i> .....	12
<i>Ausgliederung an Drittanbieter</i> .....	12
<b>Bewährte Verfahren zur Umsetzung des PCI-DSS in Standardbetriebsverfahren</b> .....	<b>13</b>
<b>Für Prüfer: Stichprobenkontrolle von Unternehmenseinrichtungen/ Systemkomponenten</b> .....	<b>15</b>
<b>Kompensationskontrollen</b> .....	<b>16</b>
<b>Anweisungen und Inhalt des Konformitätsberichts</b> .....	<b>17</b>
<b>Prozess zur PCI-DSS-Untersuchung</b> .....	<b>17</b>
<b>PCI-DSS-Versionen</b> .....	<b>18</b>
<b>Ausführliche PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren</b> .....	<b>19</b>
<b>Erstellung und Wartung sicherer Netzwerke und Systeme</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> .....	30
<b>Schutz von Karteninhaberdaten</b> .....	<b>37</b>
<i>Anforderung 3: Schutz gespeicherter Karteninhaberdaten</i> .....	37
<i>Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze</i> .....	51
<b>Unterhaltung eines Anfälligkeits-Managementprogramms</b> .....	<b>54</b>
<i>Anforderung 5: Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen</i> .....	54
<i>Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen</i> .....	57
<b>Implementierung starker Zugriffskontrollmaßnahmen</b> .....	<b>73</b>

Anforderung 7:	Beschränkung des Zugriffs auf Karteninhaberdaten je nach betrieblichem Informationsbedarf .....	73
Anforderung 8:	Zugriff auf Systemkomponenten identifizieren und authentifizieren .....	77
Anforderung 9:	Physischen Zugriff auf Karteninhaberdaten beschränken .....	89
<b>Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken .....</b>		<b>100</b>
Anforderung 10:	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten .....	100
Anforderung 11:	Regelmäßiges Testen der Sicherheitssysteme und -prozesse .....	111
<b>Befolgung einer Informationssicherheitsrichtlinie .....</b>		<b>122</b>
Anforderung 12:	Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal .....	122
<b>Anhang A: Zusätzliche PCI DSS Anforderungen .....</b>		<b>136</b>
Anhang A1:	Zusätzliche PCI-DSS-Anforderungen für von mehreren Benutzern gemeinsam genutzte Hosting-Anbieter .....	137
Anhang A2:	Zusätzliche PCI-DSS-Anforderungen für Einheiten, die SSL/eine frühe Version von TLS verwenden .....	139
Anhang A3:	Ergänzende Überprüfung bestimmter Einheiten (Designated Entities Supplemental Validation, DESV) .....	143
<b>Anhang B: Kompensationskontrollen .....</b>		<b>158</b>
<b>Anhang C: Arbeitsblatt – Kompensationskontrollen .....</b>		<b>160</b>
<b>Anhang D: Segmentierung und Stichprobenkontrolle von Unternehmenseinrichtungen/Systemkomponenten .....</b>		<b>163</b>

## Einführung und Überblick über den PCI-Datensicherheitsstandard

Der Zahlungskartenbranche Datensicherheitsstandard (PCI DSS) wurde entwickelt, um die Sicherheit von Karteninhaberdaten 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 Kontodaten. Der PCI-DSS gilt für **alle** Einrichtungen, die an der Verarbeitung von Zahlungskarten beteiligt sind—einschließlich Vertragsunternehmen, EDV-Dienstleistern, abrechnenden Stellen, Kartennemittenten und Dienstleistern. Der PCI-DSS gilt außerdem für **alle** anderen Einrichtungen, die Karteninhaberdaten (CHD) und/oder Vertrauliche Authentifizierungsdaten (SAD) speichern, verarbeiten oder übertragen. Im Folgenden finden Sie eine übergeordnete Übersicht über die zwölf PCI DSS-Anforderungen.

### Überblick über den PCI-Datensicherheitsstandard

<b>Erstellung und Wartung sicherer Netzwerke und Systeme</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>Unterhaltung eines Anfälligkeits-Managementprogramms</b>	<ol style="list-style-type: none"> <li>5. Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen</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. Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten</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>Pflege einer Informationssicherheitsrichtlinie</b>	<ol style="list-style-type: none"> <li>12. Pflegen Sie eine Informationssicherheitsrichtlinie 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 der PCI-DSS-Konformitätsbeurteilungen im Rahmen 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 Testverfahren beginnen auf Seite 15.

Der PCI-DSS enthält Mindestanforderungen zum Schutz von Kontodaten; er kann um zusätzliche Kontrollen und Verfahren erweitert werden, um mögliche Risiken zu minimieren und den lokal, regional oder branchenweit geltenden Gesetzen und Regelungen zu entsprechen. Ferner können die gesetzlichen oder regulatorischen Anforderungen konkrete Schutzmaßnahmen für persönliche Daten oder andere Datenelemente (z. B. den Namen des Karteninhabers) fordern. Der PCI-DSS ersetzt keine lokalen oder regionalen Gesetze, behördliche Regulierungen oder andere gesetzlichen Bestimmungen.

### **Ressourcen zum PCI-DSS**

Auf der Website des PCI Security Standards Council (PCI SSC) ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) finden Sie eine Anzahl zusätzlicher Ressourcen rund um die PCI-DSS-Bewertungen und -Validierungen, wie z. B.:

- Dokumentbibliothek mit folgendem Inhalt:
  - *PCI-DSS – Übersicht über die Änderungen von PCI-DSS-Version 2.0 auf 3.0*
  - *PCI-DSS-Kurzübersicht*
  - *PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme*
  - *Ergänzungen und Richtlinien*
  - *Priorisierter Ansatz zum PCI-DSS*
  - *Berichtsvorlage und Anweisungen zum ROC (Report on Compliance, Konformitätsbericht)*
  - *SAQs (Self-Assessment Questionnaires, Selbstbewertungs-Fragebogen mit Anleitungen und Richtlinien)*
  - *AOCs (Attestations of Compliance, Konformitätsbescheinigungen)*
- Häufig gestellte Fragen (FAQs)
- Website zu PCI für kleine Händler
- PCI-Schulungskurse und Informations-Webinare
- Liste der QSAs (Qualified Security Assessors, Qualifizierte Sicherheitsprüfer) und ASVs (Approved Scanning Vendors, Zugelassene Scanninganbieter)
- Liste der für PTS zugelassenen Geräte und der für den PA-DSS validierten Zahlungsanwendungen

**Hinweis:** Die Zusatzinformationen ergänzen den PCI-DSS und benennen zusätzliche Aspekte und Empfehlungen zur Einhaltung der PCI-DSS-Anforderungen – sie treten nicht an die Stelle des PCI-DSS oder seiner Anforderungen und stellen auch keine Erweiterung des Standards dar.

Informationen zu diesen und weiteren Ressourcen finden Sie unter [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

## Informationen zur PCI DSS-Anwendbarkeit

Der PCI-DSS gilt für **alle** Einrichtungen, die mit Zahlungskarten arbeiten—einschließlich Vertragsunternehmen, EDV-Dienstleistern, abrechnenden Stellen, Kartenemittenten und Dienstleistern. Der PCI-DSS gilt außerdem für **alle** anderen Einrichtungen, die Karteninhaberdaten und/oder vertrauliche Authentifizierungsdaten speichern, verarbeiten oder übertragen.

Karteninhaberdaten und vertrauliche Authentifizierungsdaten sind wie folgt definiert:

Kontodaten	
Zu den Karteninhaberdaten zählen:	Zu den vertraulichen Authentifizierungsdaten zählen:
<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 Verfolgungsdaten (Magnetstreifendaten oder gleichwertige Daten auf einem Chip)</li> <li>▪ CAV2/CVC2/CVV2/CID</li> <li>▪ PINs/PIN-Blöcke</li> </ul>

**Die PAN (Primary Account Number, Primäre Kontonummer) ist der ausschlaggebende Faktor in Bezug auf die Karteninhaberdaten.**

Wenn der Name des Inhabers, der Servicecode und/oder das Ablaufdatum zusammen mit der PAN gespeichert, verarbeitet oder weitergegeben werden oder anderweitig innerhalb der Karteninhaberdaten-Umgebung (CDE) vorhanden sind, müssen diese Daten gemäß den PCI-DSS-Anforderungen geschützt werden.

Die PCI-DSS-Anforderungen gelten für Organisationen, in denen Kontodaten (CHD und/oder SAD) gespeichert, verarbeitet oder weitergegeben werden. Einige Anforderungen des PCI-DSS gelten unter Umständen auch für Organisationen, die die Zahlungsabwicklung bzw. das CDE-Management ausgegliedert haben<sup>1</sup>. Darüber hinaus tragen die Organisationen, die die Zahlungsabwicklung bzw. das CDE-Management an Fremdfirmen ausgegliedert haben, die Verantwortung für den Schutz der Kontodaten bei den Fremdfirmen gemäß den Anforderungen des PCI-DSS.

Die Tabelle auf der folgenden Seite führt häufig verwendete Elemente an Karteninhaberdaten und vertraulichen Authentifizierungsdaten auf. 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.

<sup>1</sup> Im Einklang mit den Konformitätsprogrammen der einzelnen Kartenunternehmen

		<b>Datenelement</b>	<b>Speichern zulässig</b>	<b>Gespeicherte Daten werden gemäß Anforderung 3.4 unleserlich gemacht.</b>
<b>Kontodaten</b>	<b>Karteninhaberdaten</b>	Primary Account Number (PAN)	Ja	Ja
		Name des Karteninhabers	Ja	Nein
		Servicecode	Ja	Nein
		Ablaufdatum	Ja	Nein
	<b>Vertrauliche Authentifizierungsdaten<sup>2</sup></b>	Vollständige Verfolgungsdaten <sup>3</sup>	Nein	Kann gemäß Anforderung 3.2 nicht gespeichert werden
		CAV2/CVC2/CVV2/CID <sup>4</sup>	Nein	Kann gemäß Anforderung 3.2 nicht gespeichert werden
		PIN/PIN-Block <sup>5</sup>	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.

Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung (auch im verschlüsselten Zustand) nicht gespeichert werden. Dies gilt auch dann, wenn keine PAN in der Umgebung vorliegt. Organisationen müssen sich direkt an den Acquirer bzw. die einzelnen Kartenunternehmen wenden, wenn sie wissen möchten, ob und wie lange SAD vor der Autorisierung gespeichert werden können und ob weitere Anforderungen im Hinblick auf Nutzung oder Schutz bestehen.

<sup>2</sup> Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung (auch im verschlüsselten Zustand) nicht gespeichert werden.

<sup>3</sup> Vollständige Verfolgungsdaten vom Magnetstreifen, gleichwertige Daten auf dem Chip oder einem anderen Speicherort

<sup>4</sup> Die drei- bzw. vierstellige Zahl auf der Vorder- bzw. Rückseite der Zahlungskarte

<sup>5</sup> Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht

## Beziehung zwischen PCI-DSS und PA-DSS

### **Anwendbarkeit von PCI-DSS auf PA-DSS-Anwendungen**

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.

Die PCI-DSS-Bewertung einer Einheit umfasst alle Anwendungen, in denen Karteninhaberdaten gespeichert, verarbeitet oder weitergegeben werden – einschließlich der Anwendungen, für die eine PA-DSS-Validierung durchgeführt wurde. Bei der PCI-DSS-Bewertung sollte geprüft werden, ob die nach PA-DSS validierte Zahlungsanwendung ordnungsgemäß konfiguriert und gemäß den PCI-DSS-Anforderungen sicher implementiert wurde. Wenn die Zahlungsanwendung individuell angepasst wurde, ist bei der PCI-DSS-Bewertung eine gründlichere Überprüfung erforderlich, da die Anwendung möglicherweise nicht mehr der Version entspricht, für die eine PA-DSS-Validierung durchgeführt wurde.

Die Anforderungen für den PA-DSS leiten sich aus den *PCI-DSS-Anforderungen und -Sicherheitsbeurteilungsverfahren* ab (die im vorliegenden Dokument definiert sind). Der PA-DSS gibt an, welche Elemente von einer Zahlungsanwendung unterstützt werden müssen, um Kunden die Einhaltung des PCI-DSS zu ermöglichen. Da sich auch Sicherheitsbedrohungen ständig weiterentwickeln, können Anwendungen, die nicht länger vom Hersteller unterstützt werden (z. B. vom Hersteller als “end of life (Ende der Lebensdauer)” bezeichnet), nicht dasselbe Maß an Sicherheit bieten, wie unterstützte Versionen.

Sichere Zahlungsanwendungen minimieren bei einer Implementierung in einer PCI-DSS-konformen Umgebung das Potenzial von Sicherheitsverletzungen, die zu einer Kompromittierung von PANs, vollständigen Verfolgungsdaten, 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.

Hinweise dazu, ob der PA-DSS für eine bestimmte Zahlungsanwendung gilt, finden Sie im PA-DSS-Programmleitfaden, der Ihnen unter [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) zur Verfügung steht.

### **Anwendbarkeit des PCI-DSS auf die Anbieter von Zahlungsanwendungen**

Der PCI-DSS gilt unter Umständen für einen Anbieter von Zahlungsanwendungen, wenn dieser Karteninhaberdaten speichert, verarbeitet oder weitergibt bzw. Zugriff auf die Karteninhaberdaten der Kunden hat (z. B. in der Rolle eines Diensteanbieters).

## Geltungsbereich von PCI-DSS-Anforderungen

Die PCI-DSS-Sicherheitsanforderungen gelten für alle Systemkomponenten, die sich in der CDE befinden oder daran angeschlossen sind. Die CDE (Cardholder Data Environment, Karteninhaberdatenumgebung) besteht aus Personen, Prozessen und Technologien, die Karteninhaberdaten oder vertrauliche Authentifizierungsdaten speichern, verarbeiten oder weitergeben. Unter dem Begriff „Systemkomponenten“ sind Netzwerkgeräte, Server, Rechengerte und Anwendungen zusammengefasst. Zu den Systemkomponenten zählen unter anderem:

- Systeme, die Sicherheitsservices bereitstellen (z. B. Authentifizierungsserver), die Segmentierung erleichtern (z. B. interne Firewalls) oder sich auf die Sicherheit der CDE auswirken (z. B. Namensauflösungs- oder Web-Umleitungsserver).
- Virtualisierungskomponenten wie beispielsweise virtuelle Rechner, virtuelle Switches/Router, virtuelle Appliances, virtuelle Anwendungen/Desktops und Hypervisoren.
- Netzwerkkomponenten wie z. B. Firewalls, Switches, Router, Zugriffspunkte für drahtlose Netzwerke, Netzwerk-Appliances und andere Sicherheits-Appliances.
- Servertypen wie zum Beispiel Web-, Anwendungs-, Datenbank-, Authentifizierungs-, Mail-, Proxy-, NTP- und DNS-Server.
- Anwendungen wie z. B. alle erworbenen und benutzerdefinierten Anwendungen, darunter auch interne und externe (z. B. Internet-) Anwendungen.
- Alle anderen in der CDE befindlichen oder damit verbundenen Komponenten oder Geräte.

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, sowie alle Systeme ermitteln, die mit dem CDE verbunden sind, oder im Falle einer Beeinträchtigung Auswirkungen darauf haben können, und sicherstellen, dass diese in dem PCI-DSS-Umfang enthalten sind. Alle Arten von Systemen und Standorten, einschließlich Standorte für Sicherheitskopien/Wiederherstellung und Systeme zur Ausfallsicherung sollten bei der Bestimmung des Umfangs berücksichtigt werden.

Führen Sie Folgendes durch, um die Richtigkeit des definierten CDE zu bestätigen,:

- Die betreffende Einheit identifiziert und dokumentiert sämtliche vorhandenen Karteninhaberdaten in ihrer Umgebung und stellt sicher, dass keine Karteninhaberdaten außerhalb der aktuell definierten CDE existieren.
- Sobald alle Speicherorte von Karteninhaberdaten identifiziert und dokumentiert sind, überprüft die betreffende Stelle aufgrund der Ergebnisse, 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 Einheit berücksichtigt sämtliche Karteninhaberdaten, die sich im Umfang der PCI-DSS-Untersuchung befinden und Teile der CDE sind. Falls die Einheit Daten ermittelt, die sich zurzeit nicht in der CDE befinden, müssen diese Daten sicher gelöscht oder in die aktuell definierte CDE migriert werden, oder die CDE muss so definiert werden, dass sie diese Daten umfasst.

Die Einheit dokumentiert die Verfahrensweise zur Bestimmung des Geltungsbereichs des PCI-DSS. Diese Dokumentation wird für Kontrollen durch den Bewerter und/oder als Referenz für den Bestätigungsvorgang des PCI-DSS-Geltungsbereichs im Folgejahr aufbewahrt.

Bei jeder PCI-DSS-Bewertung muss geprüft werden, ob der Geltungsbereich der Bewertung richtig definiert und dokumentiert ist.

## **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-Untersuchung
- Die Kosten der PCI-DSS-Untersuchung
- 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), unterliegt das gesamte Netzwerk der PCI-DSS-Untersuchung. Die Netzwerksegmentierung kann mithilfe einer Vielzahl von physischen oder logischen Mitteln erreicht werden, beispielsweise durch sachgerecht konfigurierte interne Netzwerk-Firewalls, Router mit umfassenden Zugriffssteuerungslisten oder andere Technologien, die den Zugriff auf ein bestimmtes Segment eines Netzwerks einschränken. Damit eine Systemkomponente als außerhalb des PCI-DSS-Geltungsbereichs liegend betrachtet wird, muss sie so von der CDE isoliert (segmentiert) werden, dass selbst eine Kompromittierung einer Systemkomponente außerhalb des Geltungsbereichs keinerlei Auswirkungen auf die Sicherheit der CDE hätte.

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 Beseitigung nicht erforderlicher Daten und die Konsolidierung erforderlicher Daten zur Beschränkung der Speicherung von Karteninhaberdaten auf möglichst wenig Orte durch die Beseitigung nicht erforderlicher Daten und die Konsolidierung erforderlicher Daten erfordert unter Umständen die Überarbeitung bewährter Unternehmensverfahren.

Das Dokumentieren von Karteninhaberdaten-Datenflüssen mithilfe eines Datenflussdiagramms erleichtert das vollständige Verständnis aller Karteninhaberdaten-Datenflüsse und gewährleistet, dass eine Netzwerksegmentierung die Karteninhaberdaten-Umgebung wirksam isoliert.

Wenn die Netzwerksegmentierung eingerichtet ist und verwendet wird, um den Umfang der PCI-DSS-Untersuchung zu verringern, muss der Prüfer bestätigen, 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 zu den Auswirkungen der Netzwerksegmentierung- und Stichprobenkontrolle auf den Umfang einer PCI-DSS-Untersuchung.*

## **Drahtlos**

Wenn drahtlose Technologie zum Speichern, Verarbeiten oder Weitergeben von Karteninhaberdaten (z. B. Point-Of-Sale-Transaktionen, „Line-Busting“) verwendet wird, oder wenn ein drahtloses Netzwerk (WLAN) mit der Karteninhaberdaten-Umgebung verbunden oder Bestandteil der Umgebung ist, gelten die PCI-DSS-Anforderungen für drahtlose Umgebungen (z. B. Anforderung 1.2.3, 2.1.1 und 4.1.1), und es müssen die entsprechenden Testverfahren ausgeführt werden. Bevor drahtlose Technologie implementiert wird, sollte das Unternehmen den Technologiebedarf sorgfältig gegen die Risiken abwägen. Der Einsatz drahtloser Technologie eignet sich nur für die Übertragung nichtvertraulicher Daten.

## **Ausgliederung an Drittanbieter**

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

Die Parteien geben klar an, welche Services und Systemkomponenten zum Umfang der PCI-DSS-Untersuchung des Dienstanbieters gehören. Außerdem ist zu klären, welche konkreten PCI-DSS-Anforderungen der Dienstanbieter erfüllt, welche Anforderungen dagegen im Verantwortungsbereich der Kunden des Dienstanbieters liegen und von diesen in eigenen PCI-DSS-Prüfungen zu berücksichtigen sind. So muss ein Anbieter von Aufnahmen von Managed-Hosting-Leistungen klar festlegen, welche IP-Adressen im Rahmen der vierteljährlichen Schwachstellenprüfungen getestet werden und welche IP-Adressen von dessen Kunden in ihre eigenen vierteljährlichen Prüfungen einbezogen werden müssen.

Dienstanbieter sind dafür verantwortlich, ihre PCI-PSS-Konformität nachzuweisen und können von Kartenunternehmen dazu aufgefordert werden. Dienstanbieter wenden sich an ihren Acquirer beziehungsweise ihr Kartenunternehmen, um eine geeignete Konformitätsüberprüfung zu bestimmen.

Es gibt zwei Möglichkeiten, mit denen Drittdienstleister die Konformität validieren können:

- 1) **Jährliche Beurteilung:** Dienstanbieter können sich selbst einer PCI-DSS-Untersuchung unterziehen und ihren Kunden die entsprechenden Konformitätsnachweise vorlegen; oder
- 2) **Mehrere Beurteilungen auf Abruf:** Falls sie sich nicht einer eigenen PCI-DSS-Untersuchung unterziehen, haben sich Dienstanbieter auf Anfrage ihrer Kunden einer Untersuchung zu unterziehen beziehungsweise an jeder PCI-DSS-Überprüfung ihrer Kunden teilzunehmen und die Ergebnisse jeder Überprüfung dem jeweiligen Kunden zur Verfügung zu stellen

Falls der Drittanbieter eine eigene PCI-DSS-Untersuchung vornimmt, belegt er den Kunden gegenüber in ausreichendem Umfang, dass die PCI-DSS-Untersuchung des Dienstanbieters die auf den Kunden zutreffenden Services umfasste und dass die relevanten PCI-DSS-Anforderungen geprüft wurden und eingehalten werden. In welcher Form der Dienstanbieter seinen Kunden gegenüber die Belege vorlegt, hängt von den Vereinbarungen/vertraglichen Regelungen zwischen den Parteien ab. So können die Informationen etwa ganz oder teilweise über das AOC und/oder relevante Abschnitte aus dem (im Hinblick auf den Schutz vertraulicher Informationen redigierten) ROC des Dienstanbieters bereitgestellt werden.

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

## Bewährte Verfahren zur Umsetzung des PCI-DSS in Standardbetriebsverfahren

Um die Sicherheitskontrollen dauerhaft richtig umzusetzen, muss der PCI-DSS im Rahmen einer allgemeinen Sicherheitsstrategie der Einheit als BAU-Aktivität (Business As Usual; Standardverfahren) definiert werden. Auf diese Weise kann das Unternehmen die Wirksamkeit der Sicherheitskontrollen fortwährend überwachen und dafür sorgen, dass die Umgebung auch zwischen zwei PCI-DSS-Bewertungen PCI-DSS-konform bleibt. Unter anderem kann der PCI-DSS wie in folgenden Beispielen in BAU-Aktivitäten eingebunden werden:

1. Überwachung der Sicherheitskontrollen – wie etwa Firewalls, IDS/IPS (Intrusion-Detection Systems/Intrusion-Prevention Systems, Systeme zur Erkennung und Verhinderung von Eindringversuchen), FIM (File Integrity Monitoring, Überwachung der Dateiintegrität), Antivirenprogramme, Zugriffskontrollen usw. –, damit die Kontrollen effektiv und wie beabsichtigt funktionieren.
2. Schnelle Erkennung und Behebung aller Ausfälle bei den Sicherheitskontrollen. Die Reaktion auf Ausfälle bei den Sicherheitskontrollen umfasst die folgenden Prozesse:
  - Wiederherstellung der Sicherheitskontrolle
  - Ermittlung der Ausfallursache
  - Ermittlung und Lösung von Sicherheitsproblemen, die während des Ausfalls der Sicherheitskontrolle aufgetreten sind
  - Umsetzung von Verfahren oder technischen Maßnahmen, mit denen das erneute Auftreten der Ausfallursache verhindert werden kann
  - Wiederaufnahme der Überwachung der Sicherheitskontrolle, unter Umständen mit vorübergehender Verstärkung der Überwachung, bis geklärt ist, ob die Kontrolle effektiv funktioniert
3. Prüfen von Veränderungen an der Umgebung (z. B. Ergänzung um neue Systeme, Änderungen an der System- bzw. Netzwerkkonfiguration) vor der konkreten Umsetzung der Veränderungen und Durchführung der folgenden Verfahren:
  - Bestimmen der potenziellen Auswirkungen auf den Geltungsbereich des PCI-DSS (so könnte beispielsweise eine neue Firewall-Regel, die eine Verbindung zwischen einem System in der CDE und einem anderen System zulässt, dafür sorgen, dass zusätzliche Systeme bzw. Netzwerke in den PCI-DSS-Geltungsbereich fallen).
  - Ermitteln der PCI-DSS-Anforderungen bei Systemen und Netzwerken, die von den Veränderungen betroffen sind (z. B. müsste ein System, das zusätzlich in den PCI-DSS-Geltungsbereich fällt, gemäß den Systemstandards – d. h. FIM, AV, Patches, Audit-Protokollierung usw. – konfiguriert und in den Plan für die vierteljährlichen Schwachstellenprüfung aufgenommen werden).
  - Aktualisieren des PCI-DSS-Geltungsbereichs und Umsetzung der entsprechenden Sicherheitskontrollen.
4. Änderungen der Organisationsstruktur (z. B. Unternehmensfusion oder -übernahme) führen zu einer formellen Prüfung der Auswirkungen auf den Geltungsbereich und die Anforderungen des PCI-DSS.
5. Durchführung und kommunizieren regelmäßiger Prüfungen darüber, ob die PCI-DSS-Anforderungen noch gelten, und ob sich das Personal an sichere Prozesse hält. Diese regelmäßigen Prüfungen beziehen sich auf sämtliche Einrichtungen und Standorte wie Einzelhandelsgeschäfte, Rechenzentren usw. und umfassen die Prüfung von Systemkomponenten (bzw. Stichproben davon) hinsichtlich der Frage, ob die PCI-DSS-Anforderungen noch gelten – beispielsweise, ob Konfigurationsstandards angewendet werden, Patches und AV auf dem neuesten Stand sind, Audit-Protokolle geprüft werden usw. Die Häufigkeit von regelmäßigen Prüfungen muss von der Einheit unter Berücksichtigung der Größe und Komplexität der Umgebung bestimmt werden.

Anhand dieser Prüfungen kann auch festgestellt werden, ob die entsprechenden Belege gespeichert werden – etwa Audit-Protokolle, Berichte von Schwachstellenprüfungen, Firewall-Prüfungen usw. Diese Informationen sind bei der Vorbereitung der nächsten Konformitätsbewertung hilfreich.

6. Prüfen der Hardware und Software mindestens einmal pro Jahr daraufhin, ob sie vom Anbieter noch unterstützt wird und die Sicherheitsanforderungen der Einheit (inklusive des PCI-DSS) noch erfüllt. Falls sich herausstellt, dass einzelne Technologien vom Anbieter nicht mehr unterstützt werden oder die Sicherheitsanforderungen des Unternehmens nicht erfüllen, erarbeitet das Unternehmen einen Plan zur Abhilfe, der bei Bedarf einen Austausch dieser Technologie vorsieht.

Neben den oben genannten Verfahren können Organisationen auch eine Abtrennung der Pflichten im Zusammenhang mit den Sicherheitsfunktionen in Erwägung ziehen. In diesem Fall werden die Sicherheits- und/oder Audit-Funktionen von den betrieblichen Funktionen abgetrennt. In Umgebungen, in denen eine einzige Person mehrere Funktionen erfüllt (z. B. die Administration und die Sicherheitsfunktionen), können die Pflichten so verteilt werden, dass niemand die durchgehende Kontrolle eines Prozesses ohne einen unabhängigen Kontrollpunkt innehat. Die Verantwortung für die Konfiguration und für die Genehmigung von Änderungen kann beispielsweise unterschiedlichen Personen zugewiesen werden.

**Hinweis:** Für einige Einrichtungen sind diese bewährten Verfahren auch Anforderungen, um die fortlaufende Konformität mit dem PCI DSS zu gewährleisten. Der PCI DSS enthält beispielsweise diese Prinzipien in einigen Anforderungen, ebenso erfordert die Ergänzende Überprüfung bestimmter Einheiten (PCI DSS Anhang A3), dass bestimmte Unternehmen diese Prinzipien validieren.

Alle Organisationen sollten die Implementierung dieser bewährten Verfahren in ihrer Umgebung berücksichtigen, selbst wenn die jeweilige Organisation zu deren Validierung nicht verpflichtet ist.

## Für Prüfer: Stichprobenkontrolle von Unternehmenseinrichtungen/ Systemkomponenten

Bei einer großen Zahl von Unternehmenseinrichtungen und/oder Systemkomponenten kann der Bewertungsprozess durch die Beschränkung auf Stichproben vereinfacht werden.

Ein Bewerter kann zwar im Rahmen der Prüfung eines Unternehmens auf PCI-DSS-Konformität Stichproben der Unternehmenseinrichtungen/Systemkomponenten untersuchen, doch darf das Unternehmen nicht die PCI-DSS-Anforderungen nur auf Stichproben der Umgebung anwenden (beispielsweise gelten die Anforderungen für die vierteljährlichen Schwachstellenprüfungen für sämtliche Systemkomponenten). Ebenso kann ein Bewerter die PCI-DSS-Konformitätsanforderungen nicht bloß stichprobenartig prüfen.

Nach Betrachtung des Gesamtumfangs und der Komplexität der zu bewertenden Umgebung kann der Prüfer unabhängig repräsentative Stichproben aus Unternehmenseinrichtungen/Systemkomponenten auswählen, um die Konformität des Unternehmens mit den PCI-DSS-Anforderungen zu überprüfen. Diese Stichproben müssen zunächst für Unternehmenseinrichtungen und anschließend für Systemkomponenten innerhalb der einzelnen ausgewählten Unternehmenseinrichtungen festgelegt werden. Die Stichproben müssen eine repräsentative Auswahl aller Arten und Standorte von Unternehmenseinrichtungen sowie der Arten 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.

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.

Der Prüfer kann sich beispielsweise in einer Stichprobe für eine Unternehmenseinrichtung auf Sun-Server mit Apache, Windows-Server mit Oracle, Mainframe-Systeme mit Legacy-Anwendungen zur Kartenverarbeitung, Datenübertragungsserver mit HP-UX und Linux-Server mit MySQL entscheiden. Wenn alle Anwendungen von einer einzelnen Version eines einzigen Betriebssystems (z. B. Windows 7 oder Solaris 10) ausgeführt werden, sollte die Stichprobe dennoch verschiedene Anwendungen (z. B. Datenbankserver, Webserver, Datenübertragungsserver) umfassen.

Beim unabhängigen 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, dem Prüfer die Sicherheit zu geben, dass alle Unternehmenseinrichtungen und Systemkomponenten gemäß den Standardprozessen aufgebaut sind. Der Bewerter muss überprüfen, ob die standardisierten und zentralisierten Kontrollen umgesetzt werden und effektiv funktionieren.

- 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, Unternehmenseinrichtungen/Systemkomponenten aller einzelnen Prozesstypen zu umfassen.
- 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 sicher sein kann, dass alle Unternehmenseinrichtungen/Systemkomponenten die PCI-DSS-Anforderungen korrekt umgesetzt haben.
- Stichproben von Systemkomponenten müssen sämtliche verwendeten Typen und Kombinationen umfassen. Wenn beispielsweise Stichproben von Anwendungen genommen werden, müssten für jede Anwendung sämtliche Versionen und Plattformen berücksichtigt werden.

Wenn Stichprobenkontrollen eingesetzt werden, muss der Prüfer immer:

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

**Siehe auch:** Anhang D: Segmentierung und Stichprobenkontrollen bei Unternehmenseinrichtungen/Systemkomponenten.

Die Prüfer müssen den Grund aller Stichprobenkontrollen für jede Untersuchung neu validieren. Wenn eine Stichprobenkontrolle durchgeführt wird, sind für jede Untersuchung verschiedene Stichproben von Unternehmenseinrichtungen und Systemkomponenten zu wählen.

## Kompensationskontrollen

Alle Kompensationskontrollen sind jährlich vom Prüfer gemäß *Anhang B: Kompensationskontrollen* und *Anhang C: Arbeitsblatt zu Kompensationskontrollen zu dokumentieren, zu prüfen und zu validieren und in den ROC aufzunehmen*.

Das Arbeitsblatt zu Kompensationskontrollen (*Anhang C*) **muss** für jede Kompensationskontrolle ausgefüllt werden. Darüber hinaus sollten Kompensationskontrollerggebnisse 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

Anweisungen und Inhalt für den ROC (Report On Compliance, Konformitätsbericht) finden sich in der *ROC-Berichtsvorlage für den PCI-DSS*.

Die *ROC-Berichtsvorlage für den PCI-DSS* ist als Vorlage zum Erstellen des *Konformitätsberichts* zu verwenden. Das untersuchte Unternehmen sollte die entsprechenden Reporting-Anforderungen jedes Kartenunternehmens befolgen, um zu gewährleisten, dass jedes Kartenunternehmen den Konformitätsstatus der Einheit anerkennt. Setzen Sie sich mit jedem Kartenunternehmen bzw. dem Acquirer in Verbindung, um Reporting-Anforderungen und Anweisungen zu ermitteln.

## Prozess zur PCI-DSS-Untersuchung

Der Prozess zur PCI-DSS-Untersuchung umfasst den Abschluss der folgenden Schritte:

1. Bestätigen Sie den Umfang der PCI-DSS-Untersuchung.
2. Führen Sie die PCI-DSS-Untersuchung der Umgebung aus, und befolgen Sie die Testverfahren für die einzelnen Anforderungen.
3. Füllen Sie den Bericht für die Bewertung aus (d. h. den SAQ (*Self-Assessment Questionnaire*, Selbstbeurteilungs-Fragebogen) oder den ROC (Report on Compliance, Konformitätsbericht)), und dokumentieren Sie sämtliche Kontrollen gemäß den PCI-Richtlinien und -Anweisungen.
4. Füllen Sie die Konformitätsbescheinigung je nachdem für Dienstanbieter oder Händler vollständig aus. Konformitätsbescheinigungen finden Sie auf der PCI-SSC-Website.
5. Reichen Sie den SAQ bzw. den ROC und die Konformitätsbescheinigung zusammen mit allen anderen erforderlichen Dokumenten – zum Beispiel den ASV-Scan-Berichten – beim Acquirer (für Händler) oder beim Kartenunternehmen oder einer anderen Anforderungsstelle (für Dienstanbieter) ein.
6. Führen Sie bei Bedarf Abhilfemaßnahmen durch, um Anforderungen zu erfüllen, die noch nicht implementiert wurden, und reichen Sie einen aktualisierten Bericht ein.

## PCI-DSS-Versionen

Mit Wirkung zum Veröffentlichungsdatum dieses Dokuments, ist der PCI DSS v3.1 gültig bis 31. Oktober 2016 und tritt nach diesem Datum außer Kraft. Alle PCI-DSS-Validierungen nach diesem Datum müssen gemäß PCI DSS v3.2 oder einer späteren Version erfolgen.

Die nachfolgende Tabelle bietet einen Überblick über die PCI-DSS-Versionen und deren Gültigkeitsdaten<sup>6</sup>.

Version	Veröffentlicht:	Außer Kraft:
PCI DSS v3.2 (Dieses Dokument)	April 2016	Noch festzulegen
PCI-DSS Version 3.1	April 2015	31. Oktober 2016

---

<sup>6</sup> Änderungen bei Veröffentlichung einer neuen Version des PCI DSS vorbehalten.

## Ausführliche PCI DSS-Anforderungen und Sicherheitsbeurteilungsverfahren

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

- **PCI-DSS-Anforderungen** – Diese Spalte definiert die Anforderungen an den Datensicherheitsstandard. Die PCI-DSS-Konformität wird anhand dieser Anforderungen validiert.
- **Testverfahren** – Diese Spalte zeigt Prozesse an, mit denen validiert wird, ob die PCI-DSS-Anforderungen gelten und eingehalten werden.
- **Anweisung** – In dieser Spalte ist der Zweck bzw. das Sicherheitsziel hinter jeder PCI-DSS-Anforderung angegeben. Diese Spalte dient lediglich zum besseren Verständnis der Anforderungen. Die Angaben in dieser Spalte sind kein Ersatz bzw. keine Erweiterung der PCI-DSS-Anforderungen und -Testverfahren.

**Hinweis:** Wenn Kontrollen noch nicht implementiert sind oder wenn die Implementierung für ein späteres Datum geplant ist, dürfen PCI-DSS-Anforderungen nicht als geltend betrachtet werden. Sobald offene bzw. noch nicht geltende Elemente von der Einheit überarbeitet wurden, validiert der Prüfer bei einer erneuten Bewertung, ob alle offenen Punkte geklärt wurden und alle Anforderungen erfüllt werden.

Bei der Dokumentation der PCI-DSS-Untersuchung stehen Ihnen auf der PCI-SSC-Website die folgenden Ressourcen zur Verfügung:

- Anweisungen zur Erstellung des ROC (Report On Compliance, Konformitätsbericht) finden Sie in der ROC-Berichtsvorlage für den PCI-DSS.
- Anweisungen zum Ausfüllen von SAQs finden Sie in der Anleitung und den Richtlinien zum PCI-DSS-Selbstbewertungsfragebogen.
- Weitere Anweisungen zur Übermittlung von Validierungsberichten zur PCI-DSS-Konformität finden Sie in den PCI-DSS-Konformitätsbescheinigungen.

## Erstellung und Wartung sicherer Netzwerke und Systeme

### 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 des internen vertrauenswürdigen Netzwerks einer Stelle kontrollieren. Die CDE ist ein Beispiel für einen sensibleren Bereich innerhalb des vertrauenswürdigen Netzwerks einer Einheit.

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 Systemkomponenten mit Firewall-Funktionen eingesetzt werden, vorausgesetzt, sie erfüllen die Mindestanforderungen für Firewalls gemäß Anforderung 1. Wenn andere Systemkomponenten mit Firewall-Funktionalitäten innerhalb der CDE eingesetzt werden, müssen diese Geräte in den Umfang und die Bewertung nach Anforderung 1 aufgenommen werden.

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
1.1 Festlegen von Standards für die Firewall- und Router-Konfiguration, die Folgendes beinhalten:	1.1 Prüfen Sie die Standards für die Firewall- und Router-Konfiguration und anderer, unten angegebener Dokumentation daraufhin, ob die Standards vollständig und in Anwendung sind.	Firewalls und Router sind zentrale Komponenten in der Architektur, die den Ein- und Ausgang des Netzwerks kontrollieren. Diese Einrichtungen sind Softwareprogramme oder Hardware-Geräte, die ungewünschte Zugriffe blockieren und zulässige ein- und ausgehende Zugriffe des Netzwerkes verwalten.  Konfigurationsstandards und Verfahren stellen sicher, dass die erste Verteidigungslinie eines Unternehmens in Sachen Datenschutz stark bleibt.
1.1.1 Förmlicher Prozess zur Genehmigung und zum Testen aller Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration	1.1.1.a Untersuchen Sie dokumentierte Verfahren daraufhin, ob es einen formalen Test- und Genehmigungsprozess für folgende Elemente gibt: <ul style="list-style-type: none"> <li>• Sämtliche Netzwerkverbindungen</li> <li>• Sämtliche Änderungen an den Firewall- und Router-Konfigurationen</li> </ul>	Ein dokumentierter und eingeführter Prozess zur Genehmigung und zum Test aller Verbindungen und Änderungen an Firewalls und Routern helfen dabei, Sicherheitsprobleme durch Fehlkonfigurationen des Netzwerks, des Routers oder der Firewall zu vermeiden.
	1.1.1.b Eine Stichprobe der Netzwerkverbindungen erhalten	Ohne förmliche Genehmigung und ohne Test der Änderungen werden die Datensätze zu den

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p>Sie, wenn Sie mit dem verantwortlichen Personal sprechen und anhand von Datensätzen prüfen, ob die Netzwerkverbindungen genehmigt und getestet wurden.</p>	<p>Änderungen unter Umständen nicht aktualisiert. Dies könnte zu Widersprüchen zwischen der Netzwerkdokumentation und der tatsächlichen Konfiguration führen.</p>
	<p><b>1.1.1.c</b> Legen Sie eine Stichprobe mit tatsächlich an den Firewall- und Router-Konfigurationen vorgenommenen Änderungen fest, vergleichen Sie die Daten mit den Änderungsdatensätzen, und stellen Sie im Gespräch mit dem zuständigen Personal fest, ob die Änderungen genehmigt waren und getestet wurden.</p>	
<p><b>1.1.2</b> Ein aktuelles Netzwerkdiagramm mit allen Verbindungen zwischen der CDE und anderen Netzwerken, einschließlich aller drahtlosen Netzwerke</p>	<p><b>1.1.2.a</b> Überprüfen Sie die Diagramme und Netzwerkkonfigurationen daraufhin, ob ein aktuelles Netzwerkdiagramm vorhanden ist und alle Verbindungen mit Karteninhaberdaten dokumentiert, einschließlich aller drahtlosen Netzwerke.</p> <p><b>1.1.2.b</b> Klären Sie durch Befragung des zuständigen Personals, ob das Diagramm auf dem neuesten Stand gehalten wird.</p>	<p>Aus Netzwerkdiagrammen sind die Konfiguration von Netzwerken und die Standorte der einzelnen Netzwerkgeräte ersichtlich.</p> <p>Ohne aktuelle Netzwerkdiagramme können Geräte übersehen und unwissentlich nicht in die im Sinne des PCI-DSS implementierten Sicherheitskontrollen eingeschlossen werden. Das macht die Geräte anfällig für Sicherheitsrisiken.</p>
<p><b>1.1.3</b> Aktuelles Diagramm mit den system- und netzwerkübergreifenden Flüssen von Karteninhaberdaten</p>	<p><b>1.1.3</b> Untersuchen Sie das Datenflussdiagramm, und prüfen Sie das Diagramm im Gespräch mit den Mitarbeitern darauf hin, ob es:</p> <ul style="list-style-type: none"> <li>• die system- und netzwerkübergreifenden Flüsse von Karteninhaberdaten umfasst.</li> <li>• auf dem neuesten Stand gehalten und bei Änderungen in der Umgebung entsprechend aktualisiert wird .</li> </ul>	<p>Anhand von Flussdiagrammen für Karteninhaberdaten lässt sich der Speicherort von allen gespeicherten, verarbeiteten oder im Netzwerk weitergegebenen Karteninhaberdaten ermitteln.</p> <p>Netzwerk- und Datenflussdiagramme helfen Organisationen dabei, den Datenfluss von Karteninhaberdaten im Netzwerk und zwischen einzelnen Geräten abzubilden, um den Umfang ihrer Umgebung vollends zu erfassen.</p>
<p><b>1.1.4</b> Einrichtung einer Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone</p>	<p><b>1.1.4.a</b> Überprüfen Sie, ob alle Standards für die Firewall-Konfiguration eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone fordern.</p> <p><b>1.1.4.b</b> Überprüfen Sie, ob das aktuelle Netzwerkdiagramm den Standards für die Firewall-Konfiguration entspricht.</p> <p><b>1.1.4.c</b> Überprüfen Sie die Netzwerkkonfigurationen darauf,</p>	<p>Mit einer Firewall an jeder eingehenden (und ausgehenden) Netzwerkverbindung sowie zwischen DMZ und internem Netzwerk kann ein Unternehmen den Zugriff überwachen und kontrollieren und damit weitestgehend verhindern, dass sich eine böswillige Person Zugriff auf das interne Netzwerk verschafft.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p>ob sich gemäß den dokumentierten Konfigurationsstandards und Netzwerkdiagrammen eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone befindet.</p>	
<p><b>1.1.5</b> Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die Verwaltung der Netzwerkkomponenten</p>	<p><b>1.1.5.a</b> Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration eine Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die Verwaltung der Netzwerkkomponenten enthalten.</p> <p><b>1.1.5.b</b> Prüfen Sie durch eine Befragung des für das Management der Netzwerkkomponenten verantwortlichen Personals, ob die Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen sind.</p>	<p>Aufgrund dieser Beschreibung der Rollen und der Zuweisung von Verantwortlichkeiten ist allen Mitarbeitern klar, wer für die Sicherheit aller Netzwerkkomponenten verantwortlich ist, und diese Personen sind sich ihrer Pflicht auch bewusst. Falls Rollen und Verantwortlichkeiten nicht formal zugewiesen sind, kann es vorkommen, dass Geräte nicht verwaltet werden.</p>
<p><b>1.1.6</b> Dokumentation der Begründung und Genehmigung für den Einsatz aller zulässigen Services, Protokolle und Ports, einschließlich der Dokumentation von Sicherheitsfunktionen für die Protokolle, die als unsicher gelten.</p>	<p><b>1.1.6.a</b> Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration eine dokumentierte Liste aller Dienste, Protokolle und Ports, einschließlich einer Begründung und Genehmigung für den Einsatz dieser, enthalten.</p> <p><b>1.1.6.b</b> Identifizieren Sie zulässige unsichere Services, Protokolle und Ports, und überprüfen Sie, dass Sicherheitsfunktionen für jeden Dienst dokumentiert wurden.</p> <p><b>1.1.6.c</b> Überprüfen Sie die Firewall- und Router-Konfiguration daraufhin, ob die dokumentierten Sicherheitsfunktionen für jeden unsicheren Dienst, jedes unsichere Protokoll und jeden unsicheren Port implementiert wurden.</p>	<p>Sicherheitsverletzungen treten häufig durch unbenutzte oder unsichere Dienste und Ports auf, da diese oft bekannte Sicherheitsrisiken aufweisen und viele Unternehmen nicht mithilfe von Patches für eine die Behebung derartiger Sicherheitsrisiken in ungenutzten Diensten, Protokollen und Ports (obwohl diese Sicherheitsrisiken weiterhin bestehen).</p> <p>Organisationen können durch die eindeutige Definition und Dokumentation der für ihre Geschäfte erforderlichen Dienste, Protokolle und Ports dafür sorgen, dass alle übrigen Dienste, Protokolle und Ports deaktiviert oder gelöscht werden.</p> <p>Genehmigungen sollten von Mitarbeitern erteilt werden, die unabhängig von den Mitarbeitern sind, welche die Konfiguration verwalten.</p> <p>Wenn unsichere Dienste, Protokolle oder Ports für ein Unternehmen wichtig sind, muss das Risiko, das aus der Nutzung dieser Protokolle erwächst, vom Unternehmen akzeptiert werden. Außerdem muss die Nutzung des Protokolls begründet und Sicherheitsfunktionen dokumentiert und implementiert werden, die eine sichere Nutzung dieser Protokolle gewährleisten. Wenn diese unsicheren Dienste, Protokolle oder Ports für ein</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
		<p>Unternehmen nicht wesentlich sind, sollten sie deaktiviert oder gelöscht werden.</p> <p>Informationen zu den als unsicher eingestuften Diensten, Protokollen oder Ports finden Sie in den Branchenstandards und Anleitungen (z. B. NIST, ENISA, OWASP, etc.).</p>
<p><b>1.1.7</b> Prüfung der Firewall- und Router-Regelsätze mindestens alle sechs Monate</p>	<p><b>1.1.7.a</b> Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration mindestens alle sechs Monate eine Prüfung von Firewall- und Router-Regelsätzen erfordern.</p> <p><b>1.1.7.b</b> Prüfen Sie die Regelsatz-Dokumentation, und fragen Sie das zuständige Personal, ob die Regelsätze mindestens alle sechs Monate überprüft werden.</p>	<p>Diese Überprüfung bietet dem Unternehmen die Gelegenheit, mindestens alle sechs Monate unnötige, veraltete oder fehlerhafte Regeln zu entfernen und dafür zu sorgen, dass alle Regelsätze nur autorisierte Dienste und Ports zulassen, die den dokumentierten betrieblichen Begründungen entsprechen.</p> <p>Bei Organisationen, die zahlreiche Änderungen an den Regelsätzen für Firewalls und Router vornehmen, empfiehlt es sich unter Umständen, diese Prüfung häufiger vorzunehmen, damit die Regelsätze stets den geschäftlichen Anforderungen entsprechen.</p>
<p><b>1.2</b> Aufbau von Firewall- und Router-Konfigurationen, die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der CDE einschränken.</p> <p><b>Hinweis:</b> Ein „nicht vertrauenswürdiges Netzwerk“ ist jedes Netzwerk, das außerhalb der Netzwerke liegt, die zu der geprüften Einheit gehören und/oder das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Einheit liegt.</p>	<p><b>1.2</b> Prüfen Sie bei Firewall- und Router-Konfigurationen wie folgt, ob Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der CDE eingeschränkt werden:</p>	<p>Es muss ein Netzwerkschutz zwischen dem internen, vertrauenswürdigen Netzwerk und anderen, nicht vertrauenswürdigen Netzwerken, die extern aufgestellt und/oder nicht von der betreffenden Einheit kontrolliert oder verwaltet werden können, installiert werden. Falls diese Maßnahme nicht korrekt implementiert wird, setzt sich die Einheit der Gefahr von unerlaubten Zugriffen durch böswillige Personen oder schädliche Softwares aus.</p> <p>Damit die Firewall effektiv funktionieren kann, muss sie so konfiguriert werden, dass der Datenverkehr in das und aus dem Netzwerk der Einheit gesteuert und/oder begrenzt werden kann.</p>
<p><b>1.2.1</b> Beschränken des ein- und ausgehenden Datenverkehrs auf das für die CDE notwendige Maß und ausdrückliche Ablehnung des</p>	<p><b>1.2.1</b> Untersuchen Sie die Standards für die Firewall- und Router-Konfiguration daraufhin, ob der für die CDE notwendige ein- und ausgehende Datenverkehr identifiziert wird.</p>	<p>Die Untersuchung aller eingehenden und ausgehenden Verbindungen bietet Gelegenheit zur Prüfung und Einschränkung von Datenverkehr auf der Basis der Quell- bzw. Zieladresse, damit</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
gesamten sonstigen Datenverkehrs.	<b>1.2.1.b</b> Untersuchen Sie die Firewall- und Router-Konfigurationen daraufhin, ob der ein- und ausgehende Datenverkehr auf das für die CDE absolut notwendige Mindestmaß beschränkt wird.	<p>es nicht zu ungefilterten Zugriffen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Umgebungen kommt. Dadurch wird verhindert, dass böswillige Personen auf das Netzwerk der Einheit über unerlaubte IP-Adressen zugreifen oder Dienste, Protokolle oder Ports auf missbräuchliche Art und Weise nutzen (z. B. indem sie Daten, an die sie über das Netzwerk der Einheit gelangt sind, an einen nicht vertrauenswürdigen Server senden).</p> <p>Mit einer Regel zur Unterbindung des gesamten nicht ausdrücklich erforderlichen eingehenden sowie ausgehenden Datenverkehrs werden unbeabsichtigte Sicherheitslücken vermieden, die sämtlichen unerwünschten und möglicherweise schädlichen Datenverkehr zuließen.</p>
	<b>1.2.1.c</b> Überprüfen Sie in den Firewall- und Router-Konfigurationen, ob jeder andere ein- und ausgehende Verkehr konkret abgelehnt wird, z. B. durch die Verwendung einer ausdrücklichen „Alle ablehnen“-Anweisung oder einer impliziten Anweisung, bei der alles abgelehnt wird, was nicht ausdrücklich zugelassen wurde.	
1.2.2 Sichern und Synchronisieren von Router-Konfigurationsdateien.	<b>1.2.2.a</b> Überprüfen Sie, ob die Dateien zur Router-Konfiguration vor unbefugtem Zugriff geschützt sind.	<p>Die aktiven Router-Konfigurationsdateien enthalten die aktuellen, sicheren Einstellungen. Die beim Neustart oder Booten der Router verwendeten Dateien müssen jedoch aktualisiert werden, damit die Sicherheitseinstellungen bei der Ausführung der Startkonfiguration angewendet werden.</p> <p>Da diese Start-Konfigurationsdateien nur ab und zu ausgeführt werden, geraten sie häufig in Vergessenheit und werden nicht aktualisiert. Wenn ein Router aufgrund einer fehlenden Aktualisierung nicht mit den Sicherheitseinstellungen der aktiven Konfigurationsdateien neu gestartet wird, können daraus schwächere Regeln resultieren, die böswilligen Personen den Zugriff auf das Netzwerk ermöglichen.</p>
	<b>1.2.2.b</b> Überprüfen Sie, ob Router-Konfigurationsdateien synchronisiert sind. So sollte beispielsweise die laufende (oder aktive) Konfiguration der Startkonfiguration (für den Geräteneustart) entsprechen.	
1.2.3 Installieren von Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der CDE und Konfigurieren dieser Firewalls, sodass der gesamte Verkehr zwischen der	<b>1.2.3.a</b> Prüfen Sie bei Firewall- und Router-Konfigurationen, ob Umkreis-Firewalls zwischen allen Drahtlos-Netzwerken und der CDE installiert sind.	<p>Die bekannte (oder nicht bekannte) Implementierung und Ausnutzung von Drahtlostechnologie in einem Netzwerk ist eine altbewährte Methode für böswillige Individuen, um sich Zugriff zu einem Netzwerk und zu</p>
	<b>1.2.3.b</b> Prüfen Sie, ob der gesamte Verkehr zwischen der drahtlosen Umgebung und der CDE von den Firewalls	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>drahtlosen Umgebung und der CDE abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten und für die Geschäftszwecke notwendigen Datenverkehr handelt.</p>	<p>abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten und für die Geschäftszwecke notwendigen Datenverkehr handelt.</p>	<p>Karteninhaberdaten zu verschaffen. Wenn ein drahtloses Gerät oder Netzwerk ohne das Wissen einer Einheit installiert wird, könnte sich eine böswillige Person mühelos und „heimlich“ Zugang zum Netzwerk verschaffen. Wenn Firewalls nicht den Zugriff von drahtlosen Netzwerken auf die CDE einschränken, könnten sich böswillige Individuen, die sich unerlaubten Zugang zum drahtlosen Netzwerk verschafft haben, mit der CDE verbinden und Kontoinformationen gefährden.</p> <p>Firewalls müssen zwischen allen drahtlosen Netzwerken und der Karteninhaberdaten-Umgebung installiert sein, unabhängig von der Aufgabe der Umgebung, mit der das drahtlose Netzwerk verbunden ist. Darunter fallen unter anderem Unternehmensnetzwerke, Einzelhandelsgeschäfte, Gast-Netzwerke, Lagerumgebungen usw.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>1.3</b> Verboten des direkten öffentlichen Zugriffs zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung.</p>	<p><b>1.3</b> Überprüfen Sie die Firewall- und Router-Konfigurationen – inklusive des Choke Routers im Internet, des DMZ-Routers und der Firewall, des DMZ-Karteninhabersegments, des Perimeter-Routers und des internen Karteninhabernetzwerksegments, und bestimmen Sie wie folgt, dass kein direkter Zugriff zwischen dem Internet und den Systemkomponenten im internen Karteninhabernetzwerksegment besteht:</p>	<p>Auch wenn es möglicherweise legitime Gründe zum Gestatten nicht vertrauenswürdiger Verbindungen mit DMZ-Systemen gibt (um beispielsweise öffentlichen Zugang zu einem Webserver zu ermöglichen), dürfen solche Verbindungen niemals zu Systemen im internen Netzwerk gewährt werden. Der Zweck einer Firewall besteht darin, alle Verbindungen zwischen öffentlichen und internen Systemen zu verwalten und zu steuern. Dies gilt insbesondere für Systeme, in denen Karteninhaberdaten gespeichert, verarbeitet oder weitergeleitet werden. Wenn Direktzugriffe zwischen öffentlichen Systemen und der CDE zugelassen werden, kann der von der Firewall gebotene Schutz umgangen werden, was Systemkomponenten mit Karteninhaberdaten unter Umständen gefährdet.</p>
<p><b>1.3.1</b> Implementieren einer DMZ, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene, öffentlich zugängliche Dienste, Protokolle und Ports anbieten.</p>	<p><b>1.3.1</b> Überprüfen Sie in der Firewall- und Router-Konfiguration, ob eine DMZ implementiert ist, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene, öffentlich zugängliche Dienste, Protokolle und Ports anbieten.</p>	<p>Die DMZ ist der Teil des Netzwerks, das die Verbindungen zwischen dem Internet (oder anderen nicht vertrauenswürdigen Netzwerken) und Diensten, die ein Unternehmen der Öffentlichkeit zur Verfügung stellen muss (beispielsweise ein Webserver), verwaltet.</p>
<p><b>1.3.2</b> Beschränken des eingehenden Internetverkehrs auf IP-Adressen innerhalb der DMZ.</p>	<p><b>1.3.2</b> Überprüfen Sie in der Konfiguration der Firewall und des Routers, ob der eingehende Internetverkehr auf IP-Adressen innerhalb der DMZ beschränkt wird.</p>	<p>Diese Funktion soll verhindern, dass böswillige Personen auf das interne Netzwerk des Unternehmens über das Internet zugreifen oder Dienste, Protokolle oder Ports auf missbräuchliche Art und Weise nutzen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>1.3.3</b> Implementierung von Anti-Spoofing-Maßnahmen zur Erkennung und Blockierung gefälschter Quell-IP-Adressen, über die auf das Netzwerk zugegriffen wird.</p> <p>(So kann beispielsweise der Datenverkehr blockiert werden, der trotz einer internen Quelladresse über das Internet zuzugreifen versucht.)</p>	<p><b>1.3.3</b> Überprüfen Sie in der Konfiguration der Firewall und des Routers, dass Anti-Spoofing-Maßnahmen umgesetzt wurden, so dass z. B. interne Adressen nicht aus dem Internet in die DMZ übergeben werden können.</p>	<p>Normalerweise enthält ein Paket die IP-Adresse des Computers, von dem das Paket stammt, damit andere Computer im Netzwerk die Herkunft kennen. Böswillige Personen versuchen häufig, die IP-Adresse des Absenders so zu fälschen (oder nachzuahmen), dass das Zielsystem glaubt, das Paket stamme aus einer vertrauenswürdigen Quelle.</p> <p>Indem Sie die Pakete filtern, die in Ihr Netzwerk gelangen, können Sie unter anderem dafür sorgen, dass die Pakete nicht so verfälscht sind, dass sie den Anschein erwecken, sie kämen aus Ihrem eigenen internen Netzwerk.</p>
<p><b>1.3.4</b> Unterbindung von nicht autorisiertem ausgehenden Datenverkehr von der CDE zum Internet.</p>	<p><b>1.3.4</b> Überprüfen Sie in der Konfiguration der Firewall und des Routers, ob ausgehender Datenverkehr von der CDE zum Internet ausdrücklich zugelassen ist.</p>	<p>Der gesamte von der CDE ausgehende Datenverkehr muss daraufhin untersucht werden, ob er den implementierten, zugelassenen Regeln entspricht. Die Verbindungen sollten daraufhin überprüft werden, dass sie den Datenverkehr auf zugelassene Kommunikationen beschränken (z. B. indem Quell-/Ziel-Adressen bzw. Ports eingeschränkt und/oder Inhalte blockiert werden).</p>
<p><b>1.3.5</b> Lassen Sie nur "etablierte" Verbindungen zum Netzwerk zu.</p>	<p><b>1.3.5</b> Überprüfen Sie in der Konfiguration der Firewall und des Routers, ob die Firewall ausschließlich etablierte Verbindungen zum internen Netzwerk zulässt und eingehende Verbindungen, die nicht mit einer zuvor etablierten Sitzung zusammenhängen, zurückweist.</p>	<p>Eine Firewall, die den Status für jede Verbindung über die Firewall festhält weiß, ob es sich bei den Antworten auf eine vorangegangene Verbindung tatsächlich um gültige und autorisierte Antworten (weil der Status jeder einzelnen Verbindung festgehalten wird) oder um schädlichen Datenverkehr handelt, der versucht, die Firewall zu täuschen, damit sie die Verbindung zulässt.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>1.3.6</b> Speichern von Systemkomponenten mit Karteninhaberdaten (z. B. Datenbank) in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauenswürdigen Netzwerken getrennt ist.</p>	<p><b>1.3.6</b> Überprüfen Sie in der Konfiguration der Firewall und des Routers, ob sich die Systemkomponenten mit Karteninhaberdaten in einer internen Netzwerkzone befinden, die sowohl von der DMZ als auch von anderen nicht vertrauenswürdigen Netzwerken getrennt ist.</p>	<p>Wenn sich Karteninhaberdaten innerhalb einer DMZ befinden, ist es wegen der geringeren Zahl an zu durchdringenden Schichten für einen externen Angreifer einfacher, auf diese Informationen zuzugreifen. Der Schutz von Systemkomponenten mit Karteninhaberdaten in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauenswürdigen Netzwerken durch eine Firewall getrennt ist, kann verhindern, dass nicht autorisierter Netzwerkverkehr die Systemkomponente erreicht.</p> <p><b>Hinweis:</b> Diese Anforderung gilt nicht für die temporäre Speicherung von Karteninhaberdaten in einem flüchtigen Speicher.</p>
<p><b>1.3.7</b> Vermeidung der Weitergabe privater IP-Adressen und Routing-Informationen an unbefugte Dritte.</p> <p><b>Hinweis:</b> Zu den Methoden zum Verbergen von IP-Adressen zählen unter anderem:</p> <ul style="list-style-type: none"> <li>• Network Address Translation (NAT);</li> <li>• Platzieren von Servern mit Karteninhaberdaten hinter Proxy-Servern/Firewalls;</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>1.3.7.a</b> Überprüfen Sie in der Konfiguration der Firewall und des Routers, ob Methoden implementiert wurden, mit denen die Offenlegung privater IP-Adressen und Routing-Informationen von internen Netzwerken an das Internet verhindert wird.</p> <p><b>1.3.7.b</b> Befragen Sie das Personal und prüfen Sie in der Dokumentation, ob die Offenlegung privater IP-Adressen und Routing-Informationen an externe Einheiten zugelassen ist.</p>	<p>Die Offenlegung privater bzw. interner IP-Adressen muss unbedingt eingeschränkt werden, damit Hacker nicht die IP-Adressen des internen Netzwerkes in Erfahrung bringen können und sich auf diese Weise Zugriff auf das Netzwerk verschaffen.</p> <p>Auf welche Methode dieses Ziel am besten erreicht wird, hängt von der konkreten Netzwerktechnologie ab. Beispielweise müssen in IPv4-Netzwerken andere Kontrollen als in IPv6-Netzwerken eingesetzt werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>1.4</b> Installieren von persönlicher Firewall-Software oder einer gleichwertige Funktion auf allen mobilen und/oder den Mitarbeitern gehörenden Geräten, die außerhalb des Netzwerks auf das Internet zugreifen (z. B. Laptops, die von Mitarbeitern verwendet werden) und die auch für den Zugriff auf das CDE eingesetzt werden. Firewall (oder gleichwertige Funktion) Konfigurationen umfassen:</p> <ul style="list-style-type: none"> <li>• Spezifische Konfigurationseinstellungen sind definiert.</li> <li>• Die persönliche Firewall (oder gleichwertige Funktion) ist aktiv.</li> <li>• Die persönliche Firewall (oder gleichwertige Funktion) kann nicht von Benutzern des mobilen Computergerätes geändert werden.</li> </ul>	<p><b>1.4.a</b> Überprüfen Sie die Richtlinien und Konfigurationsstandards auf Folgendes:</p> <ul style="list-style-type: none"> <li>• Eine persönliche Firewall-Software oder eine gleichwertige Funktion ist auf allen mobilen und/oder den Mitarbeitern gehörenden Geräten erforderlich, die außerhalb des Netzwerks auf das Internet zugreifen (z. B. Laptops, die von Mitarbeitern verwendet werden) und die auch für den Zugriff auf das CDE eingesetzt werden.</li> <li>• Für persönliche Firewall-Software (oder gleichwertige Funktionen) werden spezielle Konfigurationseinstellungen festgelegt.</li> <li>• Die persönliche Firewall (oder gleichwertige Funktion) ist so konfiguriert, dass diese aktiv läuft.</li> <li>• Die persönliche Firewall (oder gleichwertige Funktion) ist so konfiguriert, dass diese nicht von Benutzern des mobilen Computergerätes geändert werden kann.</li> </ul> <p><b>1.4.b</b> Untersuchen Sie stichprobenartig die im Besitz von Mitarbeitern oder des Unternehmens befindlichen Geräte auf folgende Punkte:</p> <ul style="list-style-type: none"> <li>• Die persönliche Firewall (oder gleichwertige Funktion) wird gemäß den konkreten Konfigurationseinstellungen der Organisation installiert und konfiguriert.</li> <li>• Die persönliche Firewall (oder gleichwertige Funktion) ist aktiv.</li> <li>• Die persönliche Firewall (oder gleichwertige Funktion) kann nicht von Benutzern des mobilen Computergerätes geändert werden.</li> </ul>	<p>Tragbare Computer und Geräte, die außerhalb der Unternehmens-Firewall eine Verbindung zum Internet herstellen dürfen, sind Bedrohungen aus dem Internet stärker ausgesetzt. Durch eine Firewall (z. B. persönliche Firewall-Software oder Hardware) können Geräte vor Angriffen aus dem Internet geschützt werden, bei denen das Gerät bei späteren Netzwerkverbindungen für den Zugriff auf die Systeme und Daten der Organisation missbraucht werden kann.</p> <p>Wie die Firewall im konkreten Fall konfiguriert werden muss, wird von der Organisation festgelegt.</p> <p><b>Hinweis:</b> Diese Anforderung gilt für mobile Computergeräte, die sich im Besitz eines Mitarbeiters oder des Unternehmens befinden. Systeme, die nicht mittels Unternehmensrichtlinien verwaltet werden können, stellen Schwächen dar und bieten böswilligen Personen Angriffsmöglichkeiten. Wenn nicht vertrauenswürdige Systeme eine Verbindung zum CDE einer Organisation herstellen dürfen, könnten sich Angreifer und andere böswillige Benutzer Zugriff auf das Netzwerk verschaffen.</p>
<p><b>1.5</b> Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung der Firewalls müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>	<p><b>1.5</b> Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung der Firewalls Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Sie sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	<p>Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit Firewalls und Router dauerhaft einen nicht autorisierten Zugriff auf das Netzwerk verhindern.</p>

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

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

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>2.1</b> Änderung der Standardeinstellungen des Anbieters und Entfernung bzw. Deaktivierung unnötiger Standardkonten stets <b>vor</b> der Installation eines Systems im Netzwerk.</p> <p>Dies gilt für SÄMTLICHE Standardkennwörter wie etwa die von Betriebssystemen, Sicherheitssoftware, Anwendungs- und Systemkonten, POS (Point of Sale, Verkaufsstelle)-Terminals, SNMP (Simple Network Management Protocol)-Community-Zeichenfolgen usw.</p>	<p><b>2.1.a</b> Wählen Sie eine Stichprobe aus Systemkomponenten aus, 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 (z. B. für Betriebssysteme, Sicherheitssoftware, Anwendungs- und Systemkonten, POS-Terminals und SNMP-Community-Zeichenfolgen) geändert wurden. (Konten/Kennwörter von Anbietern finden Sie in den entsprechenden Handbüchern und im Internet.)</p> <p><b>2.1.b</b> Prüfen Sie bei der Stichprobe der Systemkomponenten, ob sämtliche nicht benötigten Standardkonten (wie etwa vom Betriebssystem, von der Sicherheitssoftware, von Anwendungen, Systemen, POS-Terminals oder SNMP verwendete Konten) entfernt oder deaktiviert wurden.</p> <p><b>2.1.c</b> Klären Sie durch Befragungen des Personals und durch Prüfung der Dokumentation Folgendes:</p> <ul style="list-style-type: none"> <li>• SÄMTLICHE Standardkennwörter, wie etwa die von Betriebssystemen, Sicherheitssoftware, Anwendungs- und Systemkonten, POS (Point of Sale, Verkaufsstelle)-Terminals, SNMP (Simple Network Management Protocol)-Community-Zeichenfolgen usw. wurden geändert, bevor ein System im Netzwerk installiert wird.</li> <li>• Nicht benötigte Standardkonten (wie etwa vom Betriebssystem, von der Sicherheitssoftware, von Anwendungen, Systemen, POS-Terminals oder SNMP verwendete Konten) wurden entfernt oder deaktiviert, bevor ein System im Netzwerk installiert wird.</li> </ul>	<p>Böswillige Personen (Externe gleichermaßen wie Unternehmensangehörige) greifen häufig mit Standardeinstellungen, -kontonamen und -kennwörtern von Anbietern auf Systeme zu und schädigen die Betriebssystemsoftware sowie Anwendungen und die zugehörigen Systeme. Da diese Standardeinstellungen häufig öffentlich zugänglich und in der Hacker-Szene gut bekannt sind, müssen diese Einstellungen geändert werden, damit Ihr System weniger anfällig gegenüber Angriffen wird.</p> <p>Selbst wenn ein Standardkennwort nicht verwendet werden soll, empfiehlt es sich, zuerst ein sicheres und eindeutiges Kennwort festzulegen und das Konto anschließend zu deaktivieren. Auf diese Weise wird verhindert, dass böswillige Personen das Konto reaktivieren und über das Standardkennwort Zugriff erlangen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>2.1.1</b> Ändern SÄMTLICHER Standardeinstellungen der Anbieter von Drahtlossystemen, einschließlich der Standard-Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen bei drahtlosen Umgebungen, die mit der CDE verbunden sind oder Karteninhaberdaten übertragen.</p>	<p><b>2.1.1.a</b> Klären Sie durch Befragungen des Personals und durch Prüfung der Dokumentation Folgendes:</p> <ul style="list-style-type: none"> <li>• Die Standardwerte der Verschlüsselungsschlüssel wurden zum Zeitpunkt der Installation geändert.</li> <li>• Die Verschlüsselungsschlüssel werden jedes Mal geändert, wenn ein Mitarbeiter, der die Schlüssel kennt, das Unternehmen verlässt oder die Position wechselt.</li> </ul>	<p>Wenn Drahtlosnetzwerke nicht mit ausreichenden Sicherheitskonfigurationen (einschließlich der Änderung von Standardeinstellungen) implementiert werden, können Wireless-Sniffer den Datenverkehr belauschen, Daten und Kennwörter leicht erfassen, sich Zugriff auf Ihr Netzwerk verschaffen und es schädigen.</p> <p>Darüber hinaus wurde das Schlüsselaustauschprotokoll der älteren 802.11x-Verschlüsselung (WEP) geknackt und die Verschlüsselung somit nutzlos gemacht. Die Firmware für Geräte muss so aktualisiert werden, dass sie sichere Protokolle unterstützt.</p>
	<p><b>2.1.1.b</b> Klären Sie durch eine Überprüfung der Dokumentation und Verfahren sowie durch eine Befragung des Personals Folgendes ab:</p> <ul style="list-style-type: none"> <li>• Müssen Standard-SNMP-Community-Zeichenfolgen bei der Installation geändert werden?</li> <li>• Müssen Standardkennwörter/-kennsätze an Zugriffspunkten bei der Installation geändert werden?</li> </ul>	
	<p><b>2.1.1.c</b> Prüfen Sie durch eine Untersuchung der Anbieterdokumentation sowie durch eine Anmeldung an Wireless-Geräten (mit Unterstützung des Systemadministrators) Folgendes:</p> <ul style="list-style-type: none"> <li>• Werden Standard-SNMP-Community-Zeichenfolgen nicht verwendet?</li> <li>• Werden Standardkennwörter/-sätze an Zugriffspunkten nicht verändert?</li> </ul>	
	<p><b>2.1.1.d</b> Prüfen Sie in der Anbieterdokumentation und in der Drahtlos-Konfiguration, ob Firmware auf drahtlosen Geräten so aktualisiert wird, dass eine starke Verschlüsselung für die folgenden Funktionen unterstützt wird:</p> <ul style="list-style-type: none"> <li>• Authentifizierung über Drahtlosnetzwerke</li> <li>• Übertragung über Drahtlosnetzwerke</li> </ul>	
	<p><b>2.1.1.e</b> Prüfen Sie in der Anbieterdokumentation und in der Drahtlos-Konfiguration, ob gegebenenfalls andere sicherheitsbezogene Standardeinstellungen des Anbieters des Drahtlossystems geändert wurden.</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<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.</p> <p>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>In vielen Betriebssystemen, Datenbanken und Firmenanwendungen gibt es bekannte Schwachstellen, welche mithilfe bestimmter Konfigurationen behoben werden können. Um jenen zu helfen, die keine Sicherheitsexperten sind, haben eine Reihe von Sicherheitsunternehmen Empfehlungen zur Korrektur dieser Schwächen erarbeitet.</p> <p>Beispiele für Empfehlungen zu Konfigurationsstandards finden Sie unter anderem auf den folgenden Websites: <a href="http://www.nist.gov">www.nist.gov</a>, <a href="http://www.sans.org">www.sans.org</a>, <a href="http://www.cisecurity.org">www.cisecurity.org</a> und <a href="http://www.iso.org">www.iso.org</a> sowie bei den Anbietern entsprechender Produkte.</p> <p>Systemkonfigurationsstandards müssen auf dem neuesten Stand gehalten werden, damit neu entdeckte Sicherheitslücken geschlossen werden, bevor ein System im Netzwerk installiert wird.</p>
	<p><b>2.2.b</b> Überprüfen Sie durch die Untersuchung von Richtlinien und die Befragung des Personals, ob die Systemkonfigurationsstandards gemäß Anforderung 6.1 aktualisiert werden, sobald neue Schwachstellen identifiziert werden.</p>	
	<p><b>2.2.c</b> Überprüfen Sie durch die Untersuchung von Richtlinien und die Befragung des Personals, ob die Systemkonfigurationsstandards bei der Konfiguration neuer Systeme angewendet und umgesetzt werden, bevor ein System im Netzwerk installiert wird.</p>	
	<p><b>2.2.d</b> Überprüfen Sie, ob die Systemkonfigurationsstandards die folgenden Verfahren für alle Arten von Systemkomponenten enthalten:</p> <ul style="list-style-type: none"> <li>• Ändern sämtlicher Standards der Anbieter und Löschen unnötiger Standardkonten</li> <li>• Implementieren von nur einer primären Funktion pro Server, um zu vermeiden, dass auf einem Server Funktionen mit verschiedenen Sicherheitsniveauanforderungen vorhanden sind</li> <li>• Aktivieren der Dienste, Protokolle, Daemons usw., die für die Systemfunktion unbedingt erforderlich sind</li> <li>• Implementieren zusätzlicher Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden</li> <li>• Konfigurieren von Systemsicherheitsparametern zur Missbrauchsvermeidung</li> <li>• Entfernen aller unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver</li> </ul>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<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 Sicherheitsniveaunanforderungen 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 in den Systemkonfigurationen für eine Stichprobe von Systemkomponenten, ob nur eine primäre Funktion pro Server implementiert ist.</p> <p><b>2.2.1.b</b> Wenn Virtualisierungstechnologien eingesetzt werden, überprüfen Sie in der Systemkonfiguration, ob pro virtuelle Systemkomponente oder Gerät nur eine primäre Funktion implementiert ist.</p>	<p>Wenn sich auf dem gleichen Server Funktionen mit anderen Sicherheitsanforderungen befinden, könnten die höheren Anforderungen aufgrund der Funktionen mit den niedrigeren Anforderungen nicht erfüllt werden. Darüber hinaus können Serverfunktionen mit geringerem Sicherheitsniveau zu Schwachstellen bei anderen Funktionen auf dem gleichen Server führen. Indem die Organisationen die Sicherheitsanforderungen unterschiedlicher Serverfunktionen als Bestandteil der Systemkonfigurationsstandards sowie zugehöriger Verfahren betrachten, können sie dafür sorgen, dass Funktionen mit unterschiedlichen Sicherheitsniveaus nicht auf demselben Server untergebracht werden.</p>
<p><b>2.2.2</b> Ausschließliches Aktivieren notwendiger Dienste, Protokolle, Daemons usw. entsprechend dem Bedarf der Systemfunktion.</p>	<p><b>2.2.2.a</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob nur notwendige Systemdienste, Daemons und Protokolle aktiviert sind.</p> <p><b>2.2.2.b</b> Suchen Sie nach aktivierten unsicheren Diensten, Daemons oder Protokollen, und prüfen Sie durch Befragung des Personals, ob Aktivierung nach den dokumentierten Konfigurationsstandards gerechtfertigt ist.</p>	<p>Wie bereits in der Anforderung 1.1.6 erwähnt gibt es zahlreiche Protokolle, die ein Unternehmen unter Umständen benötigt (oder standardmäßig aktivieren muss) und die häufig von böswilligen Personen ausgenutzt werden, um ein Netzwerk zu beschädigen. Damit ausschließlich notwendige Dienste und Protokolle aktiviert werden, muss diese Anforderung in die Konfigurationsstandards und zugehörigen Prozesse der Organisation aufgenommen werden.</p>
<p><b>2.2.3</b> Implementieren Sie zusätzliche Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden.</p> <p><b>Hinweis:</b> Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 erfüllt werden.</p>	<p><b>2.2.3.a</b> Überprüfen Sie in den Konfigurationseinstellungen, ob Sicherheitsfunktionen für jeden unsicheren Dienst, jeden unsicheren Daemon und jedes unsichere Protokoll dokumentiert und implementiert wurden.</p> <p><b>2.2.3.b</b> Falls SSL/eine frühe Version von TLS verwendet wird, führen Sie die Prüfverfahren aus Anhang A2 durch: Zusätzliche PCI-DSS-Anforderungen für Einheiten, die SSL/eine frühe Version von TLS verwenden.</p>	<p>Wenn Sicherheitsfunktionen schon vor der Bereitstellung von neuen Servern aktiviert werden, können Server mit unsicheren Konfigurationen nicht in der Umgebung installiert werden.</p> <p>Wenn sämtliche unsicheren Dienste, Protokolle und Daemons durch entsprechende Sicherheitsmerkmale wirksam geschützt sind, wird böswilligen Benutzern die Ausnutzung bekannter Schwachpunkte in einem Netzwerk erschwert.</p> <p>Informationen zu starker Kryptographie und sicheren Protokollen finden Sie in den Branchenstandards und bewährten Verfahren (z. B. NIST SP 800-52 and SP 800-57, OWASP, etc.).</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>2.2.4</b> Konfigurieren von Systemsicherheitsparametern zur Missbrauchsvermeidung.</p>	<p><b>2.2.4.a</b> Prüfen Sie in Gesprächen mit Systemadministratoren und/oder Sicherheitsbeauftragten, ob diese die gängigen Sicherheitsparametereinstellungen für Systemkomponenten kennen.</p>	<p>Systemkonfigurationsstandards und zugehörige Prozesse sollten insbesondere jene Sicherheitseinstellungen und Parameter ansprechen, die sich bekanntermaßen auf die Sicherheit aller verwendeten Systeme auswirken.</p> <p>Damit Systeme sicher konfiguriert werden können, muss das für die Konfiguration und/oder Administration der Systeme zuständige Personal die für das System wichtigen Sicherheitsparameter und -einstellungen kennen.</p>
	<p><b>2.2.4.b</b> Überprüfen Sie, ob gängige Sicherheitsparametereinstellungen in den Systemkonfigurationsstandards enthalten sind.</p>	
	<p><b>2.2.4.c</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob gängige Sicherheitsparameter angemessen und in Übereinstimmung mit den Konfigurationsstandards festgelegt sind.</p>	
<p><b>2.2.5</b> Entfernen aller unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver.</p>	<p><b>2.2.5.a</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob alle unnötigen Funktionen (z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme usw.) aus der Konfiguration entfernt wurden.</p>	<p>Unnötige Funktionen bieten böswilligen Personen zusätzliche Möglichkeiten für einen Zugriff auf ein System. Wenn sie unnötige Funktionen entfernen, können sich Organisationen darauf konzentrieren, die wirklich notwendigen Funktionen sicher zu machen und so das Risiko eines Missbrauchs unbekannter Funktionen zu senken.</p> <p>Die Einbindung dieser Überlegungen in Standards zur Absicherung von Servern und Prozessen behebt die besonderen Sicherheitsfragen, die sich aus unnötigen Funktionen ergeben (z. B. indem der FTP- oder der Webserver gelöscht/deaktiviert wird, wenn der Server diese Funktionen nicht nutzt).</p>
	<p><b>2.2.5.b</b> Überprüfen Sie in der Dokumentation und den Sicherheitsparametern, ob aktivierte Funktionen dokumentiert sind und eine sichere Konfiguration unterstützen.</p>	
	<p><b>2.2.5.c</b> Überprüfen Sie in der Dokumentation und in den Sicherheitsparametern, ob auf den Systemkomponenten der Stichprobe ausschließlich dokumentierte Funktionen vorhanden sind.</p>	
<p><b>2.3</b> Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs mithilfe einer starken Kryptographie.</p> <p><b>Hinweis:</b> Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 erfüllt werden.</p>	<p><b>2.3</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob der nicht über die Konsole erfolgte Verwaltungszugriff durch folgende Maßnahmen verschlüsselt ist:</p>	<p>Wenn die nicht über die Konsole erfolgte Verwaltung (inklusive Remote-Administration) nicht mit einer sicheren Authentifizierung und verschlüsselter Kommunikation erfolgt, können vertrauliche Informationen auf Verwaltungs- oder Betriebsebene (wie etwa Administrator-IDs und -Kennwörter) unter Umständen abgefangen werden. Ein Angreifer könnte diese Informationen nutzen, um sich Zugang zum Netzwerk zu verschaffen, sich als Administrator auszugeben und Daten zu entwenden.</p> <p>Bei Klartextprotokollen (wie HTTP, Telnet usw.) werden weder der Datenverkehr noch die Anmeldedaten verschlüsselt. Dies erleichtert das</p>
	<p><b>2.3.a</b> Beobachten Sie den Anmeldevorgang eines Administrators an jedem System und überprüfen Sie in den Systemkonfigurationen, ob eine starke Verschlüsselungsmethode aufgerufen wird, bevor das Administrator Kennwort angefordert wird.</p>	
	<p><b>2.3.b</b> Vergewissern Sie sich bei den Diensten und Parameterdateien auf Systemen, dass Telnet und andere unsichere Remote-Anmeldebefehle nicht für den Zugriff</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	ohne Konsole verfügbar sind.	Abfangen dieser Informationen.  <i>(Fortsetzung auf der nächsten Seite)</i>
	<p><b>2.3.c</b> Überprüfen Sie bei Administratoranmeldungen an den einzelnen Systemen, ob der Administratorzugriff auf webbasierte Managementschnittstellen mit einer starken Kryptographie verschlüsselt ist.</p> <p><b>2.3.d</b> Überprüfen Sie anhand der Anbieterdokumentation und durch Befragung des Personals, ob für die verwendete Technologie eine starke Kryptographie gemäß den bewährten Branchenverfahren und/oder Anbieterempfehlungen implementiert wird.</p> <p><b>2.3.e</b> Falls SSL/eine frühe Version von TLS verwendet wird, führen Sie die Prüfverfahren aus <i>Anhang A2 durch: Zusätzliche PCI-DSS-Anforderungen für Einheiten, die SSL/eine frühe Version von TLS verwenden.</i></p>	Eine „starke Kryptographie“ liegt nur vor, wenn branchenweit anerkannte Protokolle mit angemessen sicherer Verschlüsselung und Schlüsselverwaltung nach Bedarf für die eingesetzte Technologie verwendet werden. (Siehe "Starke Kryptographie" im <i>PCI DSS und PA-DSS Glossar für Abkürzungen und Akronyme</i> und den Branchenstandards und bewährten Verfahren wie NIST SP 800-52 and SP 800-57, OWASP, etc.)
<b>2.4</b> Pflege eines Bestands an Systemkomponenten für den PCI-DSS.	<p><b>2.4.a</b> Überprüfen Sie im Systembestand, ob eine Liste der Hardware- und Softwarekomponenten mit einer Beschreibung der einzelnen Funktionen/Einsatzgebiete geführt wird.</p> <p><b>2.4.b</b> Klären Sie durch Befragung des zuständigen Personals, ob die Bestandsdokumentation auf dem neuesten Stand gehalten wird.</p>	Anhand einer aktuellen Liste aller Systemkomponenten kann eine Organisation genau und effizient den Umfang der Umgebung für die Implementierung von PCI-DSS-Kontrollen festlegen. Ohne eine Bestandsübersicht könnte es vorkommen, dass einige Systemkomponenten vergessen und versehentlich aus den Konfigurationsstandards der Organisation ausgenommen werden.
<b>2.5</b> Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung von Anbieterstandards und sonstigen Sicherheitsparametern müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	<p><b>2.5</b> Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung von Anbieterstandards Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Die Richtlinien und Verfahren sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit Anbieterstandards und andere Sicherheitsparameter dauerhaft verwaltet und unsichere Konfigurationen verhindert werden.

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>2.6</b> Anbieter von gemeinsam genutzten Hosting-Services müssen die gehostete Umgebung und Karteninhaberdaten aller Einheiten schützen. Diese Anbieter müssen bestimmte Anforderungen erfüllen, wie in <i>Anhang A1: Zusätzliche PCI DSS-Anforderungen für gemeinsam verwendete Hosting-Provider</i> dargestellt.</p>	<p><b>2.6</b> Überprüfen Sie für PCI-DSS-Untersuchungen gemeinsam verwendeter Hosting-Anbieter mit den Testverfahren <b>A.1</b> bis <b>A.1.4</b>, die in <i>Anhang A1</i> ausgeführt werden: <i>Zusätzliche PCI-DSS-Anforderungen für Anbieter von gemeinsam genutzten Hosting-Services</i> zur Sicherstellung, dass gemeinsam verwendete Hosting-Anbieter die gehostete Umgebung und die Daten ihrer Einheiten (Händler und Dienstanbieter) schützen.</p>	<p>Dies gilt für Hosting-Anbieter, die von mehreren Clients auf demselben Server genutzte Hosting-Umgebungen anbieten. Wenn sich alle Daten auf demselben Server befinden und von einer einzigen Umgebung gesteuert werden, lassen sich die Einstellungen auf diesen gemeinsam genutzten Servern oftmals nicht von einem einzigen Client verwalten. Dies erlaubt den Clients, unsichere Funktionen und Skripts hinzuzufügen, die die Sicherheit anderer Client-Umgebungen beeinträchtigen können und es somit einem Angreifer leicht machen, die Daten eines Clients zu beschädigen und sich anschließend Zugriff auf die Daten aller anderen Clients zu verschaffen. Details zu den Anforderungen finden Sie in <i>Anhang A1</i>.</p>

## Schutz von Karteninhaberdaten

### Anforderung 3: Schutz gespeicherter Karteninhaberdaten

Schutzmethoden wie Verschlüsselung, Abkürzung, Maskierung und Hashing sind kritische Bestandteile des Schutzes von Karteninhaberdaten. Wenn ein Eindringling andere Sicherheitskontrollen umgeht und Zugriff auf verschlüsselte Daten ohne die entsprechenden kryptographischen Schlüssel erlangt, sind die Daten nicht lesbar und für diese Person unbrauchbar. Andere effektive Methoden zum Schutz gespeicherter Daten sollten als Möglichkeit zur Risikoabschwächung ebenfalls in Betracht gezogen 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 im *Glossar für Begriffe, Abkürzungen und Akronyme für PCI-DSS und DA-DSS*.

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>3.1</b> Beschränkung der Speicherung von Karteninhaberdaten auf ein Minimum durch Implementierung von Richtlinien und Verfahren zur Datenaufbewahrung und -löschung, die zumindest folgende Punkte für die Speicherung von Karteninhaberdaten umfassen:</p> <ul style="list-style-type: none"> <li>• Begrenzen der Speichermenge und der Aufbewahrungszeit auf die für rechtliche, gesetzliche und/oder geschäftliche Zwecke festgelegten Vorgaben.</li> <li>• Spezifische Aufbewahrungsanforderungen für Karteninhaberdaten</li> <li>• Prozesse zum Löschen von Daten,</li> </ul>	<p><b>3.1.a</b> Prüfen Sie, ob die Richtlinien und Verfahren zur Datenaufbewahrung und -löschung für den Speicher aller Karteninhaberdaten mindestens folgende Elemente enthalten:</p> <ul style="list-style-type: none"> <li>• Begrenzen der Speichermenge und der Aufbewahrungszeit auf die für rechtliche, gesetzliche und/oder geschäftliche Zwecke festgelegten Vorgaben.</li> <li>• Spezielle Anforderungen an die Aufbewahrung von Karteninhaberdaten (Karteninhaberdaten müssen z. B. für den Zeitraum X aus den Geschäftsgründen Y aufbewahrt werden)</li> <li>• Prozesse zum sicheren Löschen von Karteninhaberdaten, wenn sie nicht mehr zu juristischen, gesetzlichen oder geschäftlichen Zwecken benötigt werden.</li> <li>• Ein vierteljährlicher Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten, die den festgelegten Aufbewahrungszeitraum überschritten haben</li> </ul>	<p>In einer formalen Datenaufbewahrungsrichtlinie wird festgelegt, welche Daten aufbewahrt werden müssen und wo sich diese Daten befinden, damit diese sicher vernichtet oder gelöscht werden können, sobald sie nicht mehr erforderlich sind.</p> <p>Die einzigen Karteninhaberdaten, die auch nach der Autorisierung gespeichert werden können, sind die primäre Kontonummer oder auch PAN genannt (in unleserlicher Form), Ablaufdatum, Name des Karteninhabers und der Servicecode.</p> <p>Es muss bekannt sein, wo die Karteninhaberdaten gespeichert werden, damit sie ordnungsgemäß aufbewahrt bzw. (nach Ende der Nutzung) gelöscht werden können. Um angemessene Aufbewahrungsanforderungen zu definieren, muss sich ein Unternehmen sich</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>sobald diese nicht mehr benötigt werden.</p> <ul style="list-style-type: none"> <li>Ein vierteljährlicher Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten, die den festgelegten Aufbewahrungszeitraum überschritten haben.</li> </ul>	<p><b>3.1.b</b> Klären Sie durch Befragung des zuständigen Personals Folgendes:</p> <ul style="list-style-type: none"> <li>Die Speicherorte der Karteninhaberdaten sind Teil der Prozesse zur Datenaufbewahrung und -löschung.</li> <li>Es besteht ein vierteljährlicher automatischer oder manueller Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten.</li> <li>Dieser vierteljährliche automatische bzw. manuelle Prozess wird an allen Speicherorten von Karteninhaberdaten ausgeführt.</li> </ul>	<p>zunächst über seine eigenen Betriebsbedürfnisse und gesetzlichen oder behördlichen Pflichten im Klaren sein, die für seine Branche beziehungsweise den jeweiligen Datentyp gelten.</p> <p style="text-align: right;"><i>(Fortsetzung auf der nächsten Seite)</i></p>
	<p><b>3.1.c</b> Gehen Sie für eine Stichprobe von Systemkomponenten mit Karteninhaberdaten wie folgt vor:</p> <ul style="list-style-type: none"> <li>Vergewissern Sie sich in den Dateien und Systemdatensätzen, dass die gespeicherten Daten nicht den in der Datenaufbewahrungsrichtlinie festgelegten Zeitraum überschreiten.</li> <li>Überprüfen Sie die Löschmechanismen daraufhin, ob die Daten sicher gelöscht werden.</li> </ul>	<p>Mit der Ermittlung und Löschung von Daten, deren Aufbewahrungsfrist überschritten wurde, wird verhindert, dass nicht mehr benötigte Daten unnötig aufbewahrt werden. Der Prozess kann automatisch ablaufen oder manuell gesteuert werden oder aus einer Kombination aus beidem bestehen. Es könnte beispielsweise eine (automatisch oder manuell ausgelöste) Programmprozedur zur Suche und Entfernung von Daten beziehungsweise eine manuelle Prüfung der Datenspeicherbereiche durchgeführt werden.</p> <p>Der Einsatz sicherer Verfahren zum Löschen von Daten gewährleistet, dass diese nicht mehr aufgerufen werden können, wenn dafür kein Bedarf mehr besteht.</p> <p><b><u>Denken Sie daran – wenn nicht benötigt, nicht speichern!</u></b></p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>3.2</b> Speichern Sie keine vertraulichen Authentifizierungsdaten nach der Autorisierung (auch wenn diese verschlüsselt sind). Falls vertrauliche Authentifizierungsdaten empfangen werden, sind sämtliche Daten nach Abschluss des Autorisierungsprozesses so zu löschen, dass sie nicht wiederhergestellt werden können.</p> <p><i>Kartenaussteller und Unternehmen, die Kartenausstellungsdienste unterstützen, dürfen in den folgenden Fällen vertrauliche Authentifizierungsdaten speichern:</i></p> <ul style="list-style-type: none"> <li>• wenn es eine geschäftliche Begründung gibt</li> <li>• wenn die Daten sicher gespeichert werden</li> </ul> <p>Vertrauliche Authentifizierungsdaten umfassen die Daten, die in den folgenden Anforderungen 3.2.1 bis 3.2.3 aufgeführt sind:</p>	<p><b>3.2.a</b> Prüfen Sie bei Kartenausstellern und/oder Unternehmen, die Kartenausstellungsdienste unterstützen und vertrauliche Authentifizierungsdaten speichern, durch Betrachtung der Richtlinien und Befragung des Personals, ob für die Speicherung von vertraulichen Authentifizierungsdaten eine dokumentierte Begründung vorliegt.</p>	<p>Vertrauliche Authentifizierungsdaten umfassen vollständige Verfolgungsdaten, Kartenausstellungsdaten oder -werte und PIN-Daten. Die Speicherung vertraulicher Authentifizierungsdaten ist nach der Autorisierung nicht zulässig! Diese Daten sind für Personen mit böswilligen Absichten von großem Wert, da sie ihnen ermöglichen, gefälschte Zahlungskarten zu generieren und betrügerische Transaktionen zu erstellen.</p>
	<p><b>3.2.b</b> Prüfen Sie bei Kartenausstellern und/oder Unternehmen, die Kartenausstellungsdienste unterstützen und vertrauliche Authentifizierungsdaten speichern, durch Untersuchung der Datenspeicher und Systemkonfigurationen, ob die vertraulichen Authentifizierungsdaten sicher gespeichert werden.</p>	<p>Unternehmen, die Zahlungskarten ausstellen bzw. Kartenausstellungsdienste erbringen oder unterstützen, erstellen und v verwahren im Rahmen der Kartenausstellung häufig vertrauliche Authentifizierungsdaten. Unternehmen, die Kartenausstellungsdienste anbieten, fördern oder unterstützen, dürfen vertrauliche Authentifizierungsdaten NUR speichern, WENN für die Speicherung dieser Daten eine betriebliche Begründung vorliegt.</p>
	<p><b>3.2.c</b> Alle anderen Unternehmen befolgen beim Empfang von vertraulichen Authentifizierungsdaten die Richtlinien und Verfahren und vergewissern sich in den Systemkonfigurationen, dass die Daten nach der Autorisierung nicht gespeichert werden.</p>	<p>Hierbei sei angemerkt, dass für Kartenaussteller alle PCI-DSS-Anforderungen gelten, und dass die einzige Ausnahme darin besteht, dass Kartenaussteller und zugehörige Dienstleister vertrauliche Authentifizierungsdaten speichern dürfen, wenn hierfür berechnete Gründe vorliegen. Ein berechneter Grund ist, dass der Kartenaussteller die Daten zwingend für eine ordnungsgemäße Erfüllung seiner Funktion und nicht nur für eine bequemere Ausführung der Arbeit benötigt. Diese Daten müssen sicher und gemäß dem PCI-DSS sowie den konkreten Anforderungen der Kartenaussteller gespeichert werden.</p>
	<p><b>3.2.d</b> Alle anderen Unternehmen befolgen beim Empfang von vertraulichen Authentifizierungsdaten die Verfahren und vergewissern sich in den Prozessen zur sicheren Datenlöschung, dass die Daten nicht wiederherstellbar sind.</p>	<p>Einheiten, die keine Zahlungskarten ausstellen, dürfen vertrauliche Authentifizierungsdaten nach der Autorisierung nicht speichern.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>3.2.1</b> Speichern Sie nach der Autorisierung nicht den gesamten Inhalt einer Spur (auf dem Magnetstreifen auf der Kartenrückseite, in einem Chip oder an anderer Stelle). Diese Daten werden auch als Spurdaten, Full-Track-, Track-, Track-1-, Track-2- und Magnetstreifendaten bezeichnet.</p> <p><b>Hinweis:</b> Beim normalen Geschäftsverlauf müssen möglicherweise 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 betrieblich benötigten Datenelemente.</p>	<p><b>3.2.1</b> Vergewissern Sie sich anhand einer Stichprobe von Systemkomponenten in den Datenquellen (einschließlich den nachstehend aufgeführten Datenquellen), dass die vollständigen Inhalte einer beliebigen Spur vom Magnetstreifen auf der Kartenrückseite oder vergleichbare 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>• Datenbankinhalte</li> </ul>	<p>Wenn vollständige Verfolgsdaten gespeichert werden, sind Angreifer, die auf diese Daten zugreifen können, in der Lage, Zahlungskarten zu reproduzieren und betrügerische Transaktionen durchzuführen.</p>
<p><b>3.2.2</b> Speichern Sie nach der Autorisierung 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> Vergewissern Sie sich für eine Stichprobe von Systemkomponenten in den Datenquellen (einschließlich der folgenden), dass der drei- bzw. vierstelligen Kartenprüfcode oder -wert auf der Vorderseite der Karte oder dem Unterschriftenfeld (CVV2, CVC2, CID, CAV2) nach der Autorisierung 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>• Datenbankinhalte</li> </ul>	<p>Der Zweck des Kartvalidierungscode ist der Schutz von Transaktionen, bei denen weder der Kunde anwesend ist noch die Karte vorliegt, d. h. bei Auftragsabwicklungen über das Internet oder per Post/Telefon.</p> <p>Wenn diese Daten entwendet werden, sind Betrüger in der Lage, Transaktionen über das Internet und per Post/Telefon abzuwickeln.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>3.2.3</b> Speichern Sie nach der Autorisierung keine persönlichen Identifizierungsnummern (PIN) oder verschlüsselten PIN-Blöcke.</p>	<p><b>3.2.3</b> Vergewissern Sie sich für eine Stichprobe von Systemkomponenten in den Datenquellen (einschließlich der folgenden), dass PINs und verschlüsselte PIN-Blöcke nach der Autorisierung 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>• Datenbankinhalte</li> </ul>	<p>Diese Werte sollten ausschließlich dem Karteninhaber und der Bank, die die Karte ausgestellt hat, bekannt sein. Wenn diese Daten entwendet werden, sind Betrüger in der Lage, PIN-basierte Lastschriften auszuführen (z. B. Abhebungen an Geldautomaten).</p>
<p><b>3.3</b> Maskieren Sie die PAN bei der Anzeige (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden), so dass nur Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/die letzten vier Ziffern der PAN einsehen können.</p> <p><b>Hinweis:</b> Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten – z. B. bei juristischen Anforderungen und Anforderungen der Kreditkartenunternehmen an POS-Belege.</p>	<p><b>3.3.a</b> Untersuchen Sie die schriftlich fixierten Richtlinien und Verfahren zur Maskierung der PAN-Anzeige, und prüfen Sie Folgendes:</p> <ul style="list-style-type: none"> <li>• Eine Liste der Rollen, die auf die Anzeige von mehr als den ersten sechs/letzten vier Ziffern der PAN angewiesen sind, ist zusammen mit dem rechtmäßigen geschäftlichen Grund dieses Zugriffs dokumentiert.</li> <li>• Die PAN muss bei der Anzeige so maskiert sein, dass nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können.</li> <li>• Bei sämtlichen anderen nicht explizit für die Anzeige der PAN autorisierten Rollen werden ausschließlich maskierte PANs angezeigt.</li> </ul> <p><b>3.3.b</b> Vergewissern Sie sich in den Systemkonfigurationen, dass die vollständige PAN nur bei Benutzern/Rollen mit dokumentierten geschäftlichen Gründen angezeigt und die PAN bei allen anderen Anforderungen maskiert wird.</p>	<p>Die Anzeige der vollständigen PAN beispielweise auf Computerbildschirmen, Zahlungsbestätigungen, Faxmitteilungen oder Berichten in Papierform kann dazu führen, dass diese Daten in die Hände von unbefugten Personen gelangen, die diese dann in betrügerischer Absicht nutzen. Ist sichergestellt, dass die PAN nur für Personen, die die vollständige PAN aus rechtmäßigen geschäftlichen Gründen einsehen müssen, in voller Länge sichtbar ist, verringert sich das Risiko eines unbefugten Zugriffs auf PAN-Daten.</p> <p>Der Ansatz zur Maskierung sollte immer sicherstellen, dass nur die Mindestanzahl der zum Durchführen einer bestimmten Geschäftsfunktion notwendigen Ziffern dargestellt wird. Wenn beispielsweise nur die letzten vier Ziffern zum Durchführen einer Geschäftsfunktion benötigt</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p><b>3.3</b> Vergewissern Sie sich bei einer Untersuchung der PAN-Anzeige (z. B. auf dem Bildschirm, auf Papierbelegen), dass PANs beim Anzeigen von Karteninhaberdaten verborgen werden und dass nur Personen mit rechtmäßigen geschäftlichen Gründen mehr als die ersten sechs/letzten vier Ziffern der PAN einsehen können.</p>	<p>werden, maskieren Sie die PAN so, dass die Person, die die Funktion durchführt, nur die letzten vier Ziffern sehen kann. Ein weiteres Beispiel: Wenn eine Funktion zu Routing-Zwecken Zugriff auf die Bankleitzahl (bank identification number, BIN) benötigt, decken Sie während dieser Funktion nur die BIN-Ziffern (üblicherweise die ersten sechs) auf.</p> <p>Diese Anforderung bezieht sich auf den Schutz von PANs, die auf Bildschirmen, Belegen usw. <u>abgebildet</u> sind und darf nicht mit der Anforderung 3.4 zum Schutz der in Dateien, Datenbanken usw. <u>gespeicherten</u> PANs verwechselt werden.</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 (Hashing kann nicht verwendet werden, um das abgekürzte Segment der PAN zu ersetzen);</li> <li>• Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden);</li> <li>• Starke Kryptographie mit entsprechenden Schlüsselverwaltungsprozessen 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-</p>	<p><b>3.4.a</b> Vergewissern Sie sich in der Dokumentation über das System zum Schutz der PAN (einschließlich des Anbieters, des System-/Prozesstyps und ggf. der Verschlüsselungsalgorithmen), dass die PAN auf eine der folgenden Methoden unleserlich gemacht wird:</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> <p><b>3.4.b</b> Überprüfen Sie mehrere Tabellen oder Dateien aus einer Stichprobe aus Daten-Repositorys daraufhin, ob die PAN unlesbar gemacht wurde (d. h. nicht als normaler Text gespeichert wurde).</p> <p><b>3.4.c</b> Vergewissern Sie sich in einer Stichprobe von Wechseldatenträgern (z. B. Sicherungsbändern), dass die PAN nicht lesbar ist.</p> <p><b>3.4.d</b> Vergewissern Sie sich in einer Stichprobe von Prüfprotokollen einschließlich der Protokolle von Zahlungsanwendungen, dass die PAN unlesbar gemacht wurde und nicht in den Protokollen vorhanden ist.</p>	<p>PANs, die in einem Hauptspeicher (Datenbanken oder einfache Dateien, wie etwa Textdateien oder Tabellen) oder auch in Nicht-Hauptspeichern (Sicherungskopien, Audit-Protokolle, Ausnahme- oder Fehlerbehebungsprotokolle) gespeichert werden, müssen geschützt werden.</p> <p>Karteninhaberdaten können mit unidirektionalen Hash-Funktionen, die auf einer starken Kryptographie basieren, unleserlich gemacht werden. Hash-Funktionen eignen sich, wenn die ursprüngliche Nummer nicht mehr abgerufen werden muss (unidirektionale Hashes können nicht rückgängig gemacht werden). Es wird empfohlen, vor dem Hashing die Karteninhaberdaten um eine zufällig generierte Zahl zu ergänzen. Dadurch wird es einem Angreifer erschwert, die Daten mit vorab berechneten Hash-Werten zu vergleichen und daraus die PAN abzuleiten. Diese Empfehlung ist zurzeit jedoch noch keine offizielle Anforderung.</p> <p>Bei einer Abkürzung wird ein Bereich der PAN-Daten dauerhaft entfernen, so dass nur ein Teil (nicht mehr als die ersten sechs und die letzten vier Ziffern) der PAN gespeichert wird.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><i>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, damit die originale PAN nicht durch den Vergleich von gehashten und abgekürzten Versionen rekonstruiert werden kann.</i></p>	<p><b>3.4.e</b> Wenn die gehashte und die abgekürzte Version derselben PAN in der Umgebung derselben Stelle nebeneinander bestehen, prüfen Sie die eingerichteten Kontrollen darauf hin, dass gehashte und abgekürzte Versionen nicht verglichen werden können, um die originale PAN zu rekonstruieren.</p>	<p>Ein Index-Token ist ein kryptographisches Token, das die PAN anhand eines bestimmten Indexes ersetzt und so einen unvorhersehbaren Wert liefert. Ein One-Time-Pad ist ein System, bei dem ein per Zufallsgenerator erstellter privater Schlüssel nur einmal benutzt wird, um eine Nachricht zu verschlüsseln, die anschließend mit einem entsprechenden One-Time-Pad und Schlüssel wieder entschlüsselt wird.</p> <p>Das Ziel der starken Kryptographie (gemäß der Definition im <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>) ist es, die Verschlüsselung auf der Grundlage branchenbewährter und akzeptierter Algorithmen (keine firmeneigenen oder selbst entwickelten Algorithmen) mit starken kryptographischen Schlüsseln vorzunehmen.</p> <p>Wenn ein Angreifer die gehashte und die abgekürzte Version einer bestimmten PAN miteinander vergleicht, kann er leicht den ursprünglichen PAN-Wert ableiten. Damit die ursprüngliche PAN dauerhaft nicht gelesen werden kann, helfen Kontrollen, die verhindern, dass diese Daten einander zugeordnet werden.</p>
<p><b>3.4.1</b> Wenn Festplattenverschlüsselung verwendet wird (anstelle der Datenbankverschlüsselung auf Datei- oder Spaltenebene), muss der logische Zugriff unabhängig von nativen Authentifizierungs- und Zugriffskontrollmechanismen des Betriebssystems verwaltet werden (z. B. indem lokale Benutzerkontodatenbanken und allgemeine Netzwerkanmeldedaten nicht verwendet werden). Dechiffrierschlüssel dürfen nicht mit</p>	<p><b>3.4.1.a</b> Überprüfen Sie bei Festplattenverschlüsselung durch Untersuchung der Konfiguration und Beobachtung des Authentifizierungsprozesses, ob der logische Zugriff auf verschlüsselte Dateisysteme über einen Mechanismus implementiert wird, der vom nativen Authentifizierungsmechanismus des Betriebssystems (z. B. keine Verwendung lokaler Benutzerkontodatenbanken bzw. allgemeiner Netzwerkanmeldedaten) getrennt ist.</p> <p><b>3.4.1.b</b> Überprüfen Sie durch Beobachtung der Prozesse und Befragung von Personal, ob kryptographische Schlüssel sicher gespeichert sind (z. B. auf Wechseldatenträgern, die durch starke Zugriffskontrollen entsprechend geschützt sind).</p>	<p>Diese Anforderung betrifft die Annehmbarkeit von Festplattenverschlüsselungen, mit denen Karteninhaberdaten unleserlich gemacht werden, ein. Bei der Festplattenverschlüsselung werden auf einer Festplatte/Partition eines Computers gespeicherte Daten verschlüsselt und automatisch entschlüsselt, wenn ein autorisierter Benutzer dies anfordert. Zahlreiche Systeme zur Festplattenverschlüsselung fangen Lese- und Schreibvorgänge des Betriebssystems ab und führen die entsprechenden kryptographischen Umwandlungen ohne jegliches Zutun des Benutzers, außer der Eingabe eines Kennworts</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>Benutzerkonten verbunden werden.</p> <p><b>Hinweis:</b> Diese Anforderung gilt zusätzlich zu allen anderen PCI-DSS-Anforderungen und Schlüsselverwaltungsanforderungen.</p>	<p><b>3.4.1.c</b> Überprüfen Sie in den Konfigurationen und Prozessen, ob Karteninhaberdaten auf Wechseldatenträgern unabhängig vom Speicherort verschlüsselt sind.</p> <p><b>Hinweis:</b> Wenn keine Festplattenverschlüsselung zur Verschlüsselung von Wechseldatenträgern eingesetzt wird, müssen die auf diesen Datenträgern gespeicherten Daten mithilfe einer anderen Methode unlesbar gemacht werden.</p>	<p>oder Kennsatzes beim Systemstart oder zu Beginn der Sitzung, aus. Basierend auf den Eigenschaften der Festplattenverschlüsselung darf die jeweilige Methode, soll sie dieser Anforderung entsprechen, folgende Elemente nicht aufweisen:</p> <ol style="list-style-type: none"> <li>1) Die gleiche Benutzerkonten-Authentifizierung wie für das Betriebssystem verwenden.</li> <li>2) Einen Dechiffrierschlüssel einsetzen, der mit der lokalen Benutzerkonten-Datenbank des Systems bzw. allgemeinen Netzwerkanmeldedaten verknüpft ist oder daraus abgeleitet wird.</li> </ol> <p>Die vollständige Festplattenverschlüsselung trägt zum Schutz von Daten beim Verlust einer Festplatte bei und eignet sich daher zum Beispiel für tragbare Geräte mit Karteninhaberdaten.</p>
<p><b>3.5</b> Dokumentieren und implementieren Sie Verfahren zum Schutz von Schlüsseln, die für die Sicherheit gespeicherter Karteninhaberdaten eingesetzt werden, vor Weitergabe und Missbrauch:</p> <p><b>Hinweis:</b> Diese Anforderung gilt für Schlüssel zum Verschlüsseln gespeicherter Karteninhaberdaten und auch für Schlüsselverschlüsselungsschlüssel, die zum Schutz von Datenverschlüsselungsschlüsseln verwendet werden. Diese Schlüsselverschlüsselungsschlüssel müssen mindestens so sicher wie der Datenverschlüsselungsschlüssel sein.</p>	<p><b>3.5</b> Überprüfen Sie in den Schlüsselmanagementrichtlinien und -verfahren, ob Prozesse zum Schutz von Schlüsseln für die Verschlüsselung von Karteninhaberdaten vor Weitergabe und Missbrauch angegeben sind und mindestens folgende Punkte umfassen:</p> <ul style="list-style-type: none"> <li>• Der Zugriff auf Schlüssel ist auf die unbedingt notwendige Anzahl von Personen beschränkt.</li> <li>• Die Schlüsselverschlüsselungsschlüssel sind mindestens so sicher wie die Datenverschlüsselungsschlüssel, zu deren Schutz sie eingesetzt werden.</li> <li>• Schlüsselverschlüsselungsschlüssel werden getrennt von Datenverschlüsselungsschlüsseln aufbewahrt.</li> <li>• Die Schlüssel werden sicher und an so wenigen Orten und in so wenigen Formen wie möglich aufbewahrt.</li> </ul>	<p>Kryptographische Schlüssel müssen streng geschützt werden, da Personen, die in deren Besitz gelangen, in der Lage sind, Daten zu entschlüsseln.</p> <p>Schlüsselverschlüsselungsschlüssel müssen, falls sie verwendet werden, mindestens so sicher wie Datenverschlüsselungsschlüssel sein, damit sowohl der Datenverschlüsselungsschlüssel als auch die Daten, die mit diesem Schlüssel verschlüsselt wurden, angemessen geschützt sind.</p> <p>Die Anforderung, Schlüssel vor Weitergabe und Missbrauch zu schützen, gilt sowohl für Schlüssel zum Verschlüsseln von Daten als auch für Schlüssel zum Verschlüsseln von Schlüsseln. Da ein Schlüssel zum Verschlüsseln von Schlüsseln Zugriff auf eine Vielzahl von Schlüsseln zum Verschlüsseln von Daten ermöglicht, ist es notwendig, die Schlüssel zum Verschlüsseln von Schlüsseln mithilfe strenger Schutzvorkehrungen zu sichern.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>3.5.1 Zusätzliche Anforderung nur für Dienstanbieter:</b> Pflegen Sie eine dokumentierte Beschreibung der kryptographischen Architektur, die folgende Elemente enthält:</p> <ul style="list-style-type: none"> <li>• Details aller Algorithmen, Protokolle und Schlüssel, einschließlich der Schlüssellänge und dem Ablaufdatum, die für den Schutz der Karteninhaberdaten verwendet werden</li> <li>• Beschreibung der Verwendung für jeden Schlüssel</li> <li>• Bestand eines HSM und anderen SCD, die für die Schlüsselverwaltung verwendet werden</li> </ul> <p><i>Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</i></p>	<p><b>3.5.1</b> Vergewissern Sie sich durch Befragung der verantwortlichen Mitarbeiter und Überprüfung der Dokumentation, dass ein Dokument zur Beschreibung der kryptographischen Architektur vorhanden ist, das folgende Elemente enthält:</p> <ul style="list-style-type: none"> <li>• Details aller Algorithmen, Protokolle und Schlüssel, einschließlich der Schlüssellänge und dem Ablaufdatum, die für den Schutz der Karteninhaberdaten verwendet werden</li> <li>• Beschreibung der Verwendung für jeden Schlüssel</li> <li>• Bestand eines HSM und anderen SCD, die für die Schlüsselverwaltung verwendet werden</li> </ul>	<p><b>Hinweis:</b> Diese Anforderung muss nur beachtet werden, wenn es sich bei der zu bewertenden Einheit um einen Dienstanbieter handelt.</p> <p>Die Pflege einer aktuellen Dokumentation der kryptographischen Architektur ermöglicht einem Unternehmen, die Algorithmen, Protokolle und kryptographischen Schlüssel, zu verstehen, die zum Schutz von Karteninhaberdaten und der Geräte verwendet werden, die die Schlüssel generieren, verwenden und schützen. Dies ermöglicht einem Unternehmen, mit den sich weiterentwickelnden Bedrohungen für ihre Architektur Schritt zu halten und Aktualisierungen entsprechend den sich ändernden Sicherheitsanforderungsstufen von verschiedenen Algorithmen/Schlüsselstärken zu planen. Die Pflege einer solchen Dokumentation ermöglicht einem Unternehmen außerdem, verlorene oder fehlende Schlüssel oder Geräte zur Schlüsselverwaltung zu ermitteln und nicht autorisierte Hinzufügungen zu ihrer kryptographischen Architektur zu erkennen.</p>
<p><b>3.5.2</b> Einschränken des Zugriff auf kryptographische Schlüssel auf die unbedingt notwendige Anzahl von Personen.</p>	<p><b>3.5.2</b> Prüfen Sie in den Benutzerzugriffslisten, ob der Zugriff auf Schlüssel auf möglichst wenige Personen beschränkt ist.</p>	<p>Es sollten möglichst wenige Personen Zugriff auf die kryptographischen Schlüssel haben und üblicherweise ausschließlich Personen, die als Schlüsselwächter eingesetzt werden. Auf diese Weise lässt sich das Risiko, dass Karteninhaberdaten von nicht autorisierten Parteien eingesehen werden können, deutlich reduzieren.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>3.5.3</b> Geheime und private Schlüssel zur Ver- und Entschlüsselung von Karteninhaberdaten müssen stets in einer (oder mehreren) der folgenden Formen gespeichert werden:</p> <ul style="list-style-type: none"> <li>• Verschlüsselung mit einem Schlüsselverschlüsselungsschlüssel, der mindestens so sicher wie der Datenverschlüsselungsschlüssel ist und separat von diesem gespeichert wird</li> <li>• Speicherung in einem sicheren kryptographischen System (wie einem HSM (Host Security Module, Host-Sicherheitsmodul) oder einem für PTS zugelassenen POI-Gerät (Point Of Interaction, Interaktionspunkt)</li> <li>• Speicherung gemäß branchenweit akzeptierter Methoden in mindestens zwei Schlüsselkomponenten voller Länge oder in Schlüssel-Shares</li> </ul> <p><b>Hinweis:</b> Öffentliche Schlüssel müssen nicht in dieser Form gespeichert werden.</p>	<p><b>3.5.3.a</b> Vergewissern Sie sich anhand dokumentierter Verfahren, dass Schlüssel zur Ver- und Entschlüsselung von Karteninhaberdaten stets nur in einer (oder mehreren) der folgenden Formen gespeichert werden:</p> <ul style="list-style-type: none"> <li>• Verschlüsselung mit einem Schlüsselverschlüsselungsschlüssel, der mindestens so sicher wie der Datenverschlüsselungsschlüssel ist und separat von diesem gespeichert wird</li> <li>• Speicherung in einem sicheren kryptographischen System (wie einem HSM (Host Security Module, Host-Sicherheitsmodul) oder einem für PTS zugelassenen POI-Gerät (Point Of Interaction, Interaktionspunkt)</li> <li>• Speicherung gemäß branchenweit akzeptierter Methoden in Schlüsselkomponenten oder Schlüssel-Shares</li> </ul> <p><b>3.5.3.b</b> Vergewissern Sie sich in Systemkonfigurationen und an Schlüsselspeicherorten, dass kryptographische Schlüssel zur Ver- und Entschlüsselung von Karteninhaberdaten stets nur in einer (oder mehreren) der folgenden Formen vorhanden sind:</p> <ul style="list-style-type: none"> <li>• Verschlüsselung mit einem Schlüsselverschlüsselungsschlüssel</li> <li>• Speicherung in einem sicheren kryptographischen System (wie einem HSM (Host Security Module, Host-Sicherheitsmodul) oder einem für PTS zugelassenen POI-Gerät (Point Of Interaction, Interaktionspunkt)</li> <li>• Speicherung gemäß branchenweit akzeptierter Methoden in Schlüsselkomponenten oder Schlüssel-Shares</li> </ul> <p><b>3.5.3.c</b> Überprüfen Sie bei Verwendung von Schlüsselverschlüsselungsschlüsseln Folgendes in den Systemkonfigurationen und an den Schlüsselspeicherorten:</p> <ul style="list-style-type: none"> <li>• Die Schlüsselverschlüsselungsschlüssel müssen mindestens so sicher sein wie die Datenverschlüsselungsschlüssel, zu deren Schutz sie eingesetzt werden.</li> <li>• Schlüsselverschlüsselungsschlüssel werden getrennt von Datenverschlüsselungsschlüsseln aufbewahrt.</li> </ul>	<p>Kryptographische Schlüssel müssen sicher gespeichert werden, damit nicht autorisierter oder unnötiger Zugriff, der zur Preisgabe von Karteninhaberdaten führen könnte, verhindert wird.</p> <p>Es ist nicht vorgesehen, dass Schlüsselverschlüsselungsschlüssel selbst verschlüsselt werden, allerdings müssen auch sie gemäß Anforderung 3.5 vor Weitergabe und Missbrauch geschützt werden. Durch das Speichern von Schlüsselverschlüsselungsschlüsseln an physisch und/oder logisch von Datenverschlüsselungsschlüsseln getrennten Speicherorten kann das Risiko unerlaubter Zugriffe auf beide Schlüssel reduziert werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>3.5.4</b> Speichern kryptographischer Schlüssel an möglichst wenigen Speicherorten.</p>	<p><b>3.5.4</b> Prüfen Sie an den Speicherorte von Schlüsseln und in Prozessen, ob die Schlüssel an so wenigen Orten wie möglich aufbewahrt werden.</p>	<p>Organisationen, die kryptographische Schlüssel an so wenigen Orten wie möglich speichern, haben weniger Probleme mit der Protokollierung und Überwachung aller Schlüssel Speicherorte und bieten eine geringere Angriffsfläche für den unbefugten Zugriff auf die Schlüssel.</p>
<p><b>3.6</b> Vollständige Dokumentation und Implementierung aller Schlüsselverwaltungsprozesse und -verfahren für kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, wie z. B.:</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 Zusätzliches Testverfahren nur für die Beurteilung von Dienstleistern:</b> Wenn der Dienstleister Schlüssel gemeinsam mit seinen Kunden für die Übertragung oder Speicherung von Karteninhaberdaten verwendet, überprüfen Sie, ob die vom Dienstleister für die Kunden bereitgestellte Dokumentation Anweisungen zur sicheren Übertragung, Speicherung und Aktualisierung von Kundenschlüsseln gemäß den Anforderungen 3.6.1 bis 3.6.8 unten enthält.</p> <p><b>3.6.b</b> Überprüfen Sie die Schlüsselverwaltungsverfahren und die Prozesse für Schlüssel zur Verschlüsselung von Karteninhaberdaten, und führen Sie Folgendes durch:</p>	<p>Die Art und Weise, in der kryptographische Schlüssel verwaltet werden, spielt in der Sicherheit der Verschlüsselungslösung eine wichtige Rolle. Ein guter Schlüsselverwaltungsprozess – ganz gleich, ob es sich um einen manuellen oder automatischen Bestandteil des Verschlüsselungsprodukts handelt –, basiert auf Branchenstandards und geht auf alle in 3.6.1 bis 3.6.8 aufgeführten Schlüsselemente ein.</p> <p>Durch die Bereitstellung von Anweisungen für Kunden zur sicheren Weitergabe, Speicherung und Aktualisierung von kryptographischen Schlüsseln wird dazu beigetragen, dass Schlüssel ordnungsgemäß verwaltet und nicht an Unbefugte weitergegeben werden.</p> <p>Diese Anforderung gilt für Schlüssel, die zur Verschlüsselung gespeicherter Karteninhaberdaten dienen, sowie für sämtliche zugehörigen Schlüsselverschlüsselungsschlüssel.</p> <p><i>Hinweis: Das Testverfahren 3.6.a ist ein zusätzliches Verfahren, das nur dann Anwendung findet, wenn es sich bei der zu bewertenden Einheit um einen Dienstleister handelt.</i></p>
<p><b>3.6.1</b> Erstellung starker kryptographischer Schlüssel</p>	<p><b>3.6.1.a</b> Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung festgelegt ist, wie starke Schlüssel erstellt werden.</p> <p><b>3.6.1.b</b> Prüfen Sie, ob mit dem Verfahren zum Erstellen von Schlüsseln starke Schlüssel generiert werden.</p>	<p>Die Verschlüsselungslösung muss in der Lage sein, starke Schlüssel entsprechend „Erstellung kryptografischer Schlüssel“ im <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i> zu generieren. Der Einsatz starker kryptographischer Schlüssel erhöht die Sicherheit verschlüsselter Karteninhaberdaten deutlich.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<b>3.6.2</b> Sichere Verteilung kryptographischer Schlüssel	<b>3.6.2.a</b> Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung festgelegt ist, wie Schlüssel sicher verteilt werden.	Die Verschlüsselungslösung muss sicher Schlüssel verteilen können, d. h., dass Schlüssel nie in Klartext und nur an die in 3.5.1 festgelegten Personen verteilt werden dürfen.
	<b>3.6.2.b</b> Prüfen Sie, ob mit der Schlüsselverteilungsmethode die Schlüssel sicher verteilt werden.	
<b>3.6.3</b> Sicheres Speichern kryptographischer Schlüssel	<b>3.6.3.a</b> Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung festgelegt ist, wie Schlüssel sicher gespeichert werden.	Die Verschlüsselungslösung muss Schlüssel sicher speichern können (z. B. indem diese mit einem Schlüsselverschlüsselungsschlüssel verschlüsselt werden). Die Speicherung von Schlüsseln ohne angemessenen Schutz könnte dazu führen, dass Angreifer auf die Schlüssel zugreifen und Karteninhaberdaten entschlüsseln.
	<b>3.6.3.b</b> Prüfen Sie, ob mit der Schlüsselspeicherungsmethode die Schlüssel sicher gespeichert werden.	
<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.a</b> Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die Schlüsseländerungen nach Ablauf einer für die einzelnen Schlüsseltypen festgelegten Schlüssellebensdauer erfordern.	Die Schlüssellebensdauer beschreibt die Zeitspanne, in der ein bestimmter kryptographischer Schlüssel für den ihm vorbestimmten Zweck eingesetzt werden kann. Bei der Bestimmung der Schlüssellebensdauer müssen unter anderem die Stärke des zugrundeliegenden Algorithmus, die Größe oder Länge des Schlüssels, das Risiko für eine Kompromittierung des Schlüssels und die Vertraulichkeit der zu verschlüsselnden Daten berücksichtigt werden.  Das regelmäßige Ändern der Verschlüsselungsschlüssel nach Ablauf der Schlüssellebensdauer ist zur Minimierung des Risikos unerlässlich, dass sich Unbefugte Zugriff auf Verschlüsselungsschlüssel verschaffen und damit Daten entschlüsseln.
<b>3.6.4.b</b> Befragen Sie das Personal, ob Schlüssel nach Ablauf der angegebenen Schlüssellebensdauer geändert werden.		

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><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) oder Grund zur Annahme besteht, dass bestimmte Schlüssel beschädigt sind.</p> <p><i><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.</i></p>	<p><b>3.6.5.a</b> Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung Prozesse für die folgenden Punkte festgelegt sind:</p> <ul style="list-style-type: none"> <li>• Wenn die Integrität eines Schlüssels gefährdet ist, wird er entfernt oder ausgetauscht.</li> <li>• Schlüssel, bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden, werden ausgetauscht.</li> <li>• Nach der Entfernung bzw. dem Austausch aufbewahrte Schlüssel werden nicht mehr für Verschlüsselungsvorgänge eingesetzt.</li> </ul> <p><b>3.6.5.b</b> Befragen Sie die Mitarbeiter, ob die folgenden Prozesse implementiert sind:</p> <ul style="list-style-type: none"> <li>• Wenn die Integrität eines Schlüssels gefährdet ist, wird er entfernt oder ausgetauscht. Dies gilt auch für Fälle, in denen ein Mitarbeiter mit Kenntnissen über den Schlüssel das Unternehmen verlässt.</li> <li>• Schlüssel, bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden, werden ausgetauscht.</li> <li>• Nach der Entfernung bzw. dem Austausch aufbewahrte Schlüssel werden nicht mehr für Verschlüsselungsvorgänge eingesetzt.</li> </ul>	<p>Schlüssel, die nicht mehr genutzt oder gebraucht werden bzw. bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden, sind aus dem Verkehr zu ziehen beziehungsweise zu vernichten, damit sie nicht mehr eingesetzt werden. Falls solche Schlüssel aufbewahrt werden müssen (z. B. zur Unterstützung archivierter, verschlüsselter Daten), sind sie mittels strenger Sicherheitsvorkehrungen zu schützen.</p> <p>Die Verschlüsselungslösung sollte einen Prozess umfassen und unterstützen, mit dem Schlüssel ersetzt werden können, deren Ersetzung fällig ist bzw. bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden.</p>
<p><b>3.6.6</b> Bei einer manuellen Verwaltung kryptographischer Klartext-Schlüssel gilt das Prinzip der geteilten Kenntnis und doppelten Kontrollen.</p> <p><i><b>Hinweis:</b> Zu den manuellen Verfahren zur Schlüsselverwaltung zählen unter anderen das Generieren, Übertragen, Laden, Speichern und Vernichten von Schlüsseln.</i></p>	<p><b>3.6.6.a</b> Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung Prozesse für die folgenden Punkte festgelegt sind:</p> <ul style="list-style-type: none"> <li>• Die Schlüsselkomponenten befinden sich in der Kontrolle von mindestens zwei Personen, die jeweils nur Kenntnisse zu ihrer Komponente haben, UND</li> <li>• Die Schlüssel werden doppelt kontrolliert, d. h. das Schlüsselmanagement muss von mindestens zwei Personen durchgeführt werden, wobei diese Personen nicht auf die Authentifizierungsdaten des jeweils anderen (z. B. Kennwörter oder Schlüssel) zugreifen können.</li> </ul>	<p>Mit geteiltem Wissen und dualen Schlüsselkontrollen wird verhindert, dass eine Person Zugriff auf den vollständigen Schlüssel hat. Diese Kontrolle gilt für die manuelle Schlüsselverwaltung bzw. für Verschlüsselungsprodukte, die keine Schlüsselverwaltung bieten.</p> <p>Geteiltes Wissen bedeutet, dass die Komponenten eines Schlüssels auf mindestens zwei Personen aufgeteilt werden. Jede Person kennt nur die eigene Komponente, und der</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p><b>3.6.6 b</b> Prüfen Sie durch Befragung des Personals und/oder Beobachtung von Prozessen, ob bei einer manuellen Verwaltung von Klartextschlüsseln folgende Prinzipien gelten:</p> <ul style="list-style-type: none"> <li>• Geteiltes Wissen UND</li> <li>• Doppelte Kontrolle</li> </ul>	<p>ursprüngliche kryptographische Schlüssel kann mithilfe der einzelnen Komponenten rekonstruiert werden.</p> <p>Nach dem Prinzip der doppelten Kontrolle sind mindestens zwei Personen für die Durchführung einer Aufgabe erforderlich, und keine Person kann die Authentifizierungsunterlagen einer anderen Person aufrufen oder verwenden.</p>
<p><b>3.6.7</b> Verhindern der unbefugten Ersetzung kryptographischer Schlüssel.</p>	<p><b>3.6.7.a</b> Überprüfen Sie, ob in Verfahren zur Schlüsselverwaltung Prozesse zur Vermeidung der unbefugten Schlüsselersetzung festgelegt sind.</p>	<p>Die Verschlüsselungslösung sollte keine Auswechselungen von Schlüsseln autorisieren, die aus nicht zugelassenen Quellen oder unerwarteten Prozessen stammen.</p>
	<p><b>3.6.7 b</b> Prüfen Sie durch Befragung des Personals und/oder Beobachtung von Prozessen, ob die nicht autorisierte Ersetzung von Schlüsseln verhindert wird.</p>	
<p><b>3.6.8</b> Aufbewahrer kryptographischer Schlüssel müssen formal bestätigen, dass sie ihre Verantwortung als Aufbewahrer verstehen und annehmen.</p>	<p><b>3.6.8.a</b> Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung Prozesse festgelegt sind, nach denen die Schlüsselwächter (entweder in schriftlicher oder elektronischer Form) bestätigen, dass sie ihre Verantwortlichkeiten verstehen und akzeptieren.</p>	<p>Dieser Prozess gewährleistet, dass sich Personen, die als Schlüsselwächter fungieren, an ihre Rolle als Schlüsselwächter halten und die damit verbundenen Verantwortlichkeiten verstehen.</p>
	<p><b>3.6.8.b</b> Überprüfen Sie die entsprechende Dokumentation oder andere Unterlagen, in denen die Schlüsselwächter (entweder schriftlich oder elektronisch) bestätigen, dass sie ihre Verantwortung als Schlüsselwächter verstehen und akzeptieren.</p>	
<p><b>3.7</b> Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz gespeicherter Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>	<p><b>3.7</b> Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz gespeicherter Karteninhaberdaten Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Die Richtlinien und Verfahren sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	<p>Das Personal muss die folgenden Sicherheitsrichtlinien und dokumentierten betrieblichen Verfahren kennen und befolgen, damit die Karteninhaberdaten dauerhaft sicher gespeichert werden.</p>

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

Über Netzwerke, auf die böswillige Personen mühelos zugreifen können, sind vertrauliche Informationen verschlüsselt zu übertragen. Falsch konfigurierte drahtlose Netzwerke und Sicherheitslücken bei der Legacy-Verschlüsselung und Authentifizierungsprotokollen sind auch weiterhin Ziele böswilliger Personen, die diese Sicherheitslücken ausnutzen, um sich privilegierten Zugriff auf Karteninhaberdaten-Umgebungen zu verschaffen.

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>4.1</b> Verwenden starker Kryptographie und Sicherheitsprotokolle zum Schutz sensibler Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke:</p> <ul style="list-style-type: none"> <li>• Es werden ausschließlich vertrauenswürdige Schlüssel und Zertifikate akzeptiert.</li> <li>• Das verwendete Protokoll unterstützt ausschließlich sichere Versionen oder Konfigurationen.</li> <li>• Für die verwendete Verschlüsselungsmethode wird die richtige Verschlüsselungsstärke verwendet.</li> </ul> <p><i><b>Hinweis:</b> Wenn SSL/ eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 erfüllt werden.</i></p> <p><i>Zu den offenen, öffentlichen Netzwerken zählen unter anderem:</i></p> <ul style="list-style-type: none"> <li>• Das Internet</li> <li>• Drahtlose Technologien wie 802.11 und Bluetooth</li> <li>• Mobilfunktechnologien wie GSM (Global System for Mobile Communications) und CDMA (Code Division Multiple Access)</li> </ul>	<p><b>4.1.a</b> Ermitteln Sie sämtliche Orte, an denen Karteninhaberdaten über offene, öffentliche Netzwerke übertragen oder empfangen werden. Untersuchen Sie die dokumentierten Standards und vergleichen Sie sie mit den Systemkonfigurationen. So können Sie prüfen, ob an allen Standorten Sicherheitsprotokolle und eine starke Kryptographie eingesetzt werden.</p> <p><b>4.1.b</b> Prüfen Sie in den dokumentierten Richtlinien und Verfahren, ob Prozesse für Folgendes festgelegt wurden:</p> <ul style="list-style-type: none"> <li>• Werden ausschließlich vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert?</li> <li>• Unterstützt das verwendete Protokoll ausschließlich sichere Versionen und Konfigurationen?</li> <li>• Wird für die verwendete Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet?</li> </ul> <p><b>4.1.c</b> Wählen Sie eine Stichprobe aus ein- und ausgehenden Transaktionen (z. B. durch Beobachten von Systemprozessen oder des Netzwerkdatenverkehrs) aus, und prüfen Sie bei der Beobachtung der Stichproben, ob sämtliche Karteninhaberdaten während der Übertragung stark verschlüsselt werden.</p> <p><b>4.1.d</b> Überprüfen Sie, ob nur vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert werden.</p> <p><b>4.1.e</b> Überprüfen Sie in der Systemkonfiguration, ob das Protokoll so implementiert ist, dass ausschließlich sichere Konfigurationen verwendet und unsichere Versionen bzw. Konfigurationen nicht unterstützt werden.</p>	<p>Vertrauliche Informationen müssen während der Übertragung über öffentliche Netzwerke verschlüsselt werden, da böswillige Personen Daten während der Übertragung mühelos abfangen und/oder umleiten können.</p> <p>Eine sichere Übertragung von Karteninhaberdaten setzt die Verwendung vertrauenswürdiger Schlüssel/Zertifikate, eines sicheren Übertragungsprotokolls und eine starke Verschlüsselung der Karteninhaberdaten voraus. Bei Verbindungsanfragen von Systemen, die erforderliche Verschlüsselungsstärke nicht unterstützen und daher zu einer unsicheren Verbindung führen würden, sollten nicht akzeptiert werden.</p> <p>Beachten Sie, dass einige Protokollimplementierungen (z. B. SSL, SSH v1.0 und frühe Versionen von TLS) bekannte Sicherheitsrisiken aufweisen, über die ein Angreifer die Kontrolle über das betroffene System erlangen könnte. Welche Sicherheitsprotokoll auch verwendet wird, stellen Sie sicher, dass nur sichere Versionen und Konfigurationen verwendet werden, um unsichere Verbindungen zu verhindern—beispielsweise indem diese ausschließlich vertrauenswürdige Zertifikate verwenden und eine starke Verschlüsselung unterstützen (keine schwächeren, unsicheren Protokolle oder Methoden unterstützen).</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<ul style="list-style-type: none"> <li>• <i>General Packet Radio Service (GPRS)</i></li> <li>• <i>Satellitenverbindungen</i></li> </ul>	<p><b>4.1.f</b> Überprüfen Sie in der Systemkonfiguration, ob für die eingesetzte Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet wird. (Schlagen Sie Anbieterempfehlungen/bewährte Verfahren nach.)</p>	<p>Zur Integrität der sicheren Verbindung kann eine Prüfung auf die Vertrauenswürdigkeit des Zertifikats beitragen (z. B. darf das Zertifikat nicht abgelaufen sein und muss von einer vertrauenswürdigen Quelle ausgestellt worden sein).</p> <p style="text-align: right;"><i>(Fortsetzung auf der nächsten Seite)</i></p>
	<p><b>4.1.g</b> Prüfen Sie bei TLS-Implementierungen in den Systemkonfigurationen, ob TLS bei jeder Übertragung bzw. bei jedem Empfang von Karteninhaberdaten aktiviert wird. Bei browserbasierten Implementierungen ist beispielsweise Folgendes zu prüfen:</p> <ul style="list-style-type: none"> <li>• Wird „HTTPS“ als Bestandteil des Browser-URL-Protokolls angezeigt?</li> <li>• Werden Karteninhaberdaten nur angefordert, wenn die URL die Komponente „HTTPS“ enthält?</li> </ul>	<p>Im Allgemeinen beginnt die URL der Website mit „HTTPS“, und im Browser-Fenster wird ein Vorhängeschloss-Symbol angezeigt. Bei zahlreichen Anbieter von TLS-Zertifikaten wird auch ein deutlich sichtbares Prüfsymbol (bisweilen auch als „Sicherheitssymbol“, „Symbol für sichere Websites“ oder „Symbol für vertrauenswürdige Website“ bezeichnet) angezeigt. Wenn Sie auf dieses Symbol klicken, werden Informationen zur Website aufgerufen.</p>
	<p><b>4.1.h</b> Falls SSL/eine frühe Version von TLS verwendet wird, führen Sie die Prüfverfahren aus <i>Anhang A2</i> durch: <i>Zusätzliche PCI-DSS-Anforderungen für Einheiten, die SSL/eine frühe Version von TLS verwenden.</i></p>	<p>Schlagen Sie zu starker Kryptographie und sicheren Protokollen (z. B. NIST SP 800-52 and SP 800-57, OWASP, etc.) in Branchenstandards und bewährten Verfahren nach</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>4.1.1</b> Stellen Sie sicher, dass drahtlose Netzwerke, die Karteninhaberdaten übertragen oder mit der CDE verbunden sind, mittels bewährter Branchenverfahren eine starke Verschlüsselung für die Authentifizierung und Übertragung implementieren.</p>	<p><b>4.1.1</b> Ermitteln Sie sämtliche Drahtlosnetzwerke, die Karteninhaberdaten übertragen oder mit der CDE verbunden sind. Untersuchen Sie dokumentierte Standards, und vergleichen Sie sie mit den Systemkonfigurationseinstellungen. Prüfen Sie hierbei die folgenden Punkte für alle ermittelten Drahtlosnetzwerke:</p> <ul style="list-style-type: none"> <li>• Es werden bewährte Branchenverfahren eingesetzt, um eine starke Verschlüsselung bei der Authentifizierung und Übertragung zu implementieren.</li> <li>• Eine schwache Verschlüsselung (z. B. WEP, SSL) wird nicht als Sicherheitskontrolle für die Authentifizierung oder Übertragung eingesetzt.</li> </ul>	<p>Böswillige Personen verwenden kostenlose und allseits verfügbare Tools, um Drahtloskommunikationen zu belauschen. Einsatz von starker Kryptographie kann die Weitergabe vertraulicher Informationen über Drahtlosnetzwerke einschränken.</p> <p>Um zu vermeiden, dass sich böswillige Benutzer Zugriff auf das Drahtlosnetzwerk verschaffen oder über die Drahtlosnetzwerke andere interne Netzwerke oder Daten erreichen, ist eine Kryptographie bei der Authentifizierung und Übertragung von Karteninhaberdaten erforderlich.</p>
<p><b>4.2</b> Versenden Sie niemals ungeschützte PANs über Messaging-Technologien für Endbenutzer (z. B. E-Mail, Instant Messaging, SMS, Chat usw.).</p>	<p><b>4.2.a</b> Wenn Karteninhaberdaten über Messaging-Technologien für Endbenutzer übermittelt werden, vergewissern Sie sich in den Prozessen zur PAN-Versendung und stichprobenartig in den ausgehenden Verbindungen, dass die PAN unleserlich gemacht oder mittels einer starken Kryptographie gesichert wurde.</p>	<p>E-Mail, Instant Messaging, SMS und Chats können in internen und öffentlichen Netzwerken während der Übertragung mithilfe von Paket-Sniffing leicht abgefangen werden. Nutzen Sie diese Messaging-Tools nicht zur Versendung von PANs, sofern sie nicht für starke Verschlüsselung konfiguriert sind.</p>
	<p><b>4.2.b</b> Vergewissern Sie sich in den schriftlich fixierten Richtlinien, dass ungeschützte PANs nicht über Messaging-Technologien für Endbenutzer gesendet werden dürfen.</p>	<p>Wenn eine Einrichtung darüber hinaus eine PAN über Messaging-Technologien für Endbenutzer anfordert, muss die Einrichtung ein Tool oder eine Methode mit starker Kryptographie zum Schutz dieser PAN bieten, oder die PAN vor der Übertragung unleserlich machen.</p>
<p><b>4.3</b> Sicherheitsrichtlinien und betriebliche Verfahren zur Verschlüsselung der Übertragung von Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>	<p><b>4.3</b> Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zur Verschlüsselung der Übertragung von Karteninhaberdaten Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Die Richtlinien und Verfahren sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	<p>Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit die Karteninhaberdaten dauerhaft sicher übertragen werden.</p>

## Unterhaltung eines Anfälligkeits-Managementprogramms

### **Anforderung 5: Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen**

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

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>5.1</b> Implementieren von Antivirensoftware auf allen Systemen, die häufig von böswilliger Software befallen werden (insbesondere Personal Computer und Server).</p>	<p><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.</p>	<p>Es gibt fortlaufend Angriffe unter Ausnutzung bekannter Sicherheitslücken. Bei diesen häufig als „0-Day“-Angriffe bezeichneten Angriffen werden ansonsten gesicherte Systeme über bislang unbekannte Sicherheitslücken angegriffen. Ohne eine regelmäßig aktualisierte Antivirensoftware sind diese neuen Arten von Malware in der Lage, Ihre Systeme anzugreifen, ein Netzwerk zu deaktivieren oder Daten zu beschädigen.</p>
<p><b>5.1.1</b> Sorgen Sie dafür, dass die Antivirenprogramme in der Lage sind, alle bekannten Malware-Typen zu erkennen, zu entfernen und davor zu schützen.</p>	<p><b>5.1.1</b> Überprüfen Sie Folgendes in der Anbieterdokumentation und den Antiviren-Konfigurationen:</p> <ul style="list-style-type: none"> <li>• Werden alle bekannten Arten von Malware erkannt?</li> <li>• Werden alle bekannten Arten von Malware entfernt?</li> <li>• Werden die Systeme vor allen bekannten Arten von Malware geschützt?</li> </ul> <p><i>Unter den Begriff „Malware“ fallen beispielsweise Viren, Würmer, Trojaner (trojanische Pferde), Würmer, Spyware, Adware und Rootkits.</i></p>	<p>Es ist wichtig, sich gegen <b>ALLE</b> Arten und Formen von Malware zu schützen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>5.1.2</b> Bei Systemen, die in der Regel nicht von Malware befallen sind, muss regelmäßig geprüft werden, ob sich die Malware-Bedrohung erhöht hat oder weiterhin keine Antivirensoftware auf diesen Systemen installiert werden muss.</p>	<p><b>5.1.2</b> Befragen Sie bei Systemen, die in der Regel nicht von Malware befallen sind, die Mitarbeiter, ob potenzielle Malware-Bedrohungen überwacht und analysiert werden, bevor festgelegt wird, dass weiterhin keine Antivirensoftware auf diesen Systemen installiert werden muss.</p>	<p>Zurzeit sind Mainframes, Mid-Range-Computer (wie z. B. AS/400) und vergleichbare Systeme in der Regel keine Malware-Ziele. Die Trends bei Malware ändern sich jedoch schnell. Daher müssen sich Organisationen immer bewusst sein, dass neue Malware ihre Systeme betreffen könnte. Aus diesem Grund sollten Sicherheitshinweise der Anbieter und Informationen aus Antiviren-Newsgruppen intensiv verfolgt werden, damit Gefahren aus neuer Malware frühzeitig erkannt werden.</p> <p>Die Malware-Trends müssen bei der Identifizierung neuer Sicherheitsrisiken berücksichtigt werden. Ebenso sollten Methoden zur Korrektur neuer Trends je nach Bedarf in die Konfigurationsstandards und Schutzmechanismen eines Unternehmens aufgenommen werden.</p>
<p><b>5.2</b> Bei sämtlichen Antivirensysteme muss Folgendes beachtet werden:</p> <ul style="list-style-type: none"> <li>• Die Systeme müssen auf dem neuesten Stand gehalten werden.</li> <li>• Es müssen regelmäßige Suchläufe stattfinden.</li> <li>• Es sind Prüfprotokolle zu erstellen, die gemäß PCI-DSS-Anforderung 10.7 aufbewahrt werden müssen.</li> </ul>	<p><b>5.2.a</b> Prüfen Sie in den Richtlinien und Verfahren, ob Antivirensoftware und Virendefinitionen immer auf dem neuesten Stand gehalten werden müssen.</p> <p><b>5.2.b</b> Untersuchen Sie die Antiviren-Konfigurationen einschließlich der Master-Installationen der Software auf folgende Punkte:</p> <ul style="list-style-type: none"> <li>• Werden die Antivirensysteme automatisch aktualisiert?</li> <li>• Finden regelmäßig Suchläufe statt?</li> </ul> <p><b>5.2.c</b> Überprüfen Sie für eine Stichprobe von Systemkomponenten, einschließlich aller Betriebssystemtypen, die häufig von Malware befallen werden, folgende Punkte:</p> <ul style="list-style-type: none"> <li>• Sind die Antivirensoftware und die Definitionen auf dem neuesten Stand?</li> <li>• Finden regelmäßig Suchläufe statt?</li> </ul> <p><b>5.2.d</b> Untersuchen Sie die Antiviren-Konfigurationen einschließlich der Master-Installation der Software sowie eine Stichprobe der Systemkomponenten auf folgende Punkte:</p> <ul style="list-style-type: none"> <li>• Ist die Protokollerstellung in der Antivirensoftware aktiviert?</li> <li>• Werden die Protokolle gemäß PCI-DSS-Anforderung 10.7 aufbewahrt?</li> </ul>	<p>Selbst die besten Antivirenlösungen funktionieren nur eingeschränkt, wenn sie nicht gepflegt und mit Sicherheits-Updates, Signaturdateien und Malware-Schutz auf dem neuesten Stand gehalten werden.</p> <p>Audit-Protokolle ermöglichen die Überwachung der Viren- und Malware-Aktivität und der Reaktion der Anti-Malware-Systeme. Folglich muss die Anti-Malware-Software so konfiguriert werden, dass sie Prüfprotokolle generiert und diese Protokolle gemäß Anforderung 10 verwaltet werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>5.3</b> Stellen Sie sicher, dass die Antivirensysteme aktiv ausgeführt werden und von den Benutzern weder deaktiviert noch verändert werden können, sofern keine fallweise Ausnahmegenehmigung der Geschäftsführung für einen beschränkten Zeitraum vorliegt.</p> <p><i><b>Hinweis:</b> Antivirenlösungen dürfen nur dann vorübergehend deaktiviert werden, wenn es einen triftigen technischen Grund dafür gibt. Hierzu ist für jeden Einzelfall die Genehmigung der Geschäftsführung einzuholen. Wenn der Virenschutz aus bestimmten Gründen deaktiviert werden muss, ist hierfür eine förmliche Autorisierung erforderlich. Möglicherweise sind außerdem für den Zeitraum, in dem der Virenschutz nicht aktiv ist, zusätzliche Sicherheitsmaßnahmen zu treffen.</i></p>	<p><b>5.3.a</b> Untersuchen Sie die Antiviren-Konfigurationen einschließlich der Master-Installationen der Software sowie eine Stichprobe der Systemkomponenten daraufhin, ob die Antivirensoftware aktiv ausgeführt wird.</p> <p><b>5.3.b</b> Untersuchen Sie die Antiviren-Konfigurationen einschließlich der Master-Installationen der Software sowie eine Stichprobe der Systemkomponenten darauf hin, dass die Antivirensoftware nicht von den Benutzern deaktiviert oder geändert werden kann.</p> <p><b>5.3.c</b> Vergewissern Sie sich durch Befragung der zuständigen Mitarbeiter und Beobachtung von Prozessen, dass die Antivirensoftware von den Benutzern weder deaktiviert noch verändert werden kann, sofern die Änderungen nicht fallweise für einen beschränkten Zeitraum von der Geschäftsführung genehmigt wurden.</p>	<p>Den besten Schutz vor Malware bietet Antivirensoftware, die ununterbrochen ausgeführt wird und nicht geändert werden kann.</p> <p>Die Verwendung richtliniengestützter Kontrollen auf allen Systemen sorgt dafür, dass der Malware-Schutz nicht verändert oder deaktiviert werden kann. So wird verhindert, dass Malware Systemschwachstellen ausnutzt.</p> <p>Möglicherweise sind außerdem für den Zeitraum, in dem der Virenschutz nicht aktiv ist, zusätzliche Sicherheitsmaßnahmen zu treffen. Hierunter fallen beispielsweise das Trennen des ungeschützten Systems vom Internet, solange der Virenschutz deaktiviert ist, und eine vollständige Systemprüfung, nachdem der Schutz wiederhergestellt wurde.</p>
<p><b>5.4</b> Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz von Systemen vor Malware müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>	<p><b>5.4</b> Klären Sie durch Überprüfung der Dokumentation und Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz der Systeme vor Malware Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Sie sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	<p>Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit die Systeme dauerhaft vor Malware geschützt sind.</p>

## 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 Systeme müssen mit den neuesten Versionen der entsprechenden Software-Patches für den Schutz vor Ausnutzung und Gefährdung von Karteninhaberdaten durch böswillige Personen und Malware versehen sein.

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

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>6.1</b> Einrichtung eines Prozesses zur Ermittlung von Sicherheitsrisiken auf der Grundlage verlässlicher Quellen und Einteilung neu ermittelter Sicherheitsrisiken in verschiedene Risikostufen (hoch/mittel/niedrig).</p> <p><b>Hinweis:</b> Die Risikostufen sollten auf den bewährten Verfahren der Branche beruhen und die potenziellen Auswirkungen berücksichtigen. So könnten der CVSS-Basiswert und/oder die Klassifizierung durch den Anbieter sowie die Art der betroffenen Systeme als Kriterien für die Einteilung der Sicherheitsrisiken in verschiedene Stufen dienen.</p> <p>Die Methoden zur Bewertung der Sicherheitsrisiken und zur Einteilung in Sicherheitsstufen hängen von der Unternehmensumgebung und der Strategie zur Risikobewertung ab. Bei der Risikoeinstufung müssen zumindest die Sicherheitsrisiken ermittelt werden, die als „hohes Risiko“ für die Umgebung gelten. Zusätzlich zu der Risikoeinstufung können einzelne Sicherheitsrisiken als „kritisch“ betrachtet werden, falls sie eine unmittelbare Bedrohung der Umgebung darstellen, sich auf wichtige Systeme auswirken und/oder eine potenzielle Gefährdung darstellen, wenn</p>	<p><b>6.1.a</b> Prüfen Sie in den Richtlinien und Verfahren, ob Prozesse für Folgendes festgelegt wurden:</p> <ul style="list-style-type: none"> <li>• Ermittlung neuer Sicherheitsrisiken</li> <li>• Zuweisung von Risikostufen für Sicherheitsrisiken mit der Ermittlung sämtlicher „hohen“ und „kritischen“ Risiken</li> <li>• Nutzung verlässlicher externer Quellen von Informationen zu Sicherheitsrisiken</li> </ul> <p><b>6.1.b</b> Klären Sie durch eine Befragung des Personals und die Beobachtung von Prozessen Folgendes ab:</p> <ul style="list-style-type: none"> <li>• Neue Sicherheitsrisiken werden ermittelt.</li> <li>• Die Sicherheitsrisiken werden verschiedenen Risikostufen zugeordnet, und alle „hohen Risiken“ und „kritischen“ Schwachstellen werden ermittelt.</li> <li>• Bei den Prozessen zur Ermittlung neuer Sicherheitsrisiken werden verlässliche externe Quellen berücksichtigt.</li> </ul>	<p>Der Zweck dieser Anforderung besteht darin, dass ein Unternehmen stets auf dem neuesten Stand bezüglich Sicherheitsrisiken ist, die seine Umgebung gefährden könnten.</p> <p>Die Quellen für Informationen zu Sicherheitsrisiken sollten vertrauenswürdig sein. Häufig zählen die Websites von Anbietern, Branchen-Newsgruppen, Mailinglisten und RSS-Feeds ebenso dazu.</p> <p>Sobald ein Unternehmen ein Sicherheitsrisiko entdeckt, das seine Umgebung beeinträchtigen könnte, muss es das Risiko bewerten und einstufen. Voraussetzung hierfür ist, dass das Unternehmen über eine einheitliche Methode zur Analyse und Bewertung von Sicherheitsrisiken verfügt. Dies wird nicht durch einen ASV-Scan oder eine interne Risikoprüfung erreicht. Vielmehr ist ein Prozess erforderlich, mit dem die Branchenquellen von Risikoinformationen aktiv überwacht werden.</p> <p>Die Einstufung von Risiken (z. B. als „hoch“, „mittel“ oder „niedrig“) erlaubt Organisationen, schneller die größten Risiken zu erkennen und zu beheben und somit die Wahrscheinlichkeit zu reduzieren, dass die größten Sicherheitsrisiken tatsächlich ausgenutzt werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><i>nicht auf sie eingegangen wird. Beispiele für wichtige Systeme sind Sicherheitssysteme, öffentlich zugängliche Geräte und Systeme, Datenbanken und andere Systeme, in denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden.</i></p>		
<p><b>6.2</b> Alle Systemkomponenten und Softwareanwendungen müssen vor bekannten Sicherheitsrisiken mithilfe der neuesten Sicherheitspatches des jeweiligen Anbieters geschützt werden. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden.</p> <p><b>Hinweis:</b> Kritische Sicherheitspatches müssen gemäß dem in Anforderung 6.1 festgelegten Prozess zur Risikoeinstufung ermittelt werden.</p>	<p><b>6.2.a</b> Prüfen Sie in den Richtlinien und Verfahren im Zusammenhang mit Sicherheitspatches, ob Prozesse für Folgendes festgelegt wurden:</p> <ul style="list-style-type: none"> <li>• Kritische Sicherheitspatches der Anbieter müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden.</li> <li>• Alle sonstigen geltenden Sicherheitspatches der Anbieter müssen innerhalb eines angemessenen Zeitraums (z. B. innerhalb von drei Monaten) installiert werden.</li> </ul> <p><b>6.2.b</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, und überprüfen Sie Folgendes:</p> <ul style="list-style-type: none"> <li>• Werden kritische Sicherheitspatches der Anbieter innerhalb eines Monats nach ihrer Veröffentlichung installiert?</li> <li>• Werden alle sonstigen anwendbaren Sicherheitspatches der Anbieter innerhalb eines angemessenen Zeitraums (z. B. innerhalb von drei Monaten) installiert?</li> </ul>	<p>Es gibt fortlaufend Angriffe unter Ausnutzung bekannter Sicherheitslücken. Bei diesen häufig als „0-Day“-Angriffe bezeichneten Angriffen werden ansonsten gesicherte Systeme über bislang unbekannte Sicherheitslücken angegriffen. Wenn nicht immer so bald wie möglich die neuesten Patches auf wichtigen Systemen implementiert werden, kann sich eine böswillige Personen dieser Verfahren bedienen, um ein System anzugreifen bzw. zu deaktivieren oder sich Zugang zu vertraulichen Daten zu verschaffen.</p> <p>Durch die Festlegung von Prioritäten für Patches zu kritischen Infrastrukturen werden Systeme und Geräte mit hoher Priorität so schnell wie möglich nach der Patch-Veröffentlichung vor Sicherheitsrisiken geschützt. Erwägen Sie, Prioritäten für die Patch-Installationen festzulegen, sodass wichtige Sicherheitspatches auf wichtigen oder gefährdeten Systemen innerhalb von 30 Tagen und andere weniger risikoreiche Änderungen innerhalb von 2 bis 3 Monaten installiert werden.</p> <p>Diese Anforderung gilt für sämtliche anwendbaren Patches zu allen installierten Softwareanwendungen, einschließlich Zahlungsanwendungen (sowohl PA-DSS-validierte als auch nicht validierte).</p>
<p><b>6.3</b> Sichere Entwicklung von Softwareanwendungen (interne und externe, inklusive Web-Administrationszugriff auf die</p>	<p><b>6.3.a</b> Überprüfen Sie, ob die schriftlich festgehaltenen Softwareentwicklungsprozesse auf Branchenstandards und/oder bewährten Praktiken basieren.</p>	<p>Ohne die Einbindung von Informationssicherheitsmaßnahmen während der Definition der Anforderungen sowie der Design-,</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>Anwendungen) unter Berücksichtigung der folgenden Punkte:</p> <ul style="list-style-type: none"> <li>• Werden Softwareanwendungen gemäß dem PCI-DSS entwickelt (z. B. sichere Authentifizierung und Protokollierung)?</li> <li>• Basieren die Entwicklungsprozesse auf Branchenstandards und/oder bewährten Verfahren?</li> <li>• Ist die Informationssicherheit während des gesamten Softwareentwicklungszyklus integriert?</li> </ul> <p><b>Hinweis:</b> Diese Anforderungen gelten für alle intern entwickelten Softwareanwendungen sowie individuell von Drittanbietern entwickelte Software.</p>	<p><b>6.3.b</b> Untersuchen Sie in den schriftlichen Softwareentwicklungsprozessen, ob die Informationssicherheit während des gesamten Lebenszyklus enthalten ist.</p> <p><b>6.3.c</b> Überprüfen Sie in den schriftlichen Softwareentwicklungsprozessen, ob die Softwareanwendungen gemäß den PCI-DSS-Anforderungen entwickelt werden.</p> <p><b>6.3.d</b> Überprüfen Sie durch eine Befragung von Softwareentwicklern, ob die schriftlich festgehaltenen Softwareentwicklungsprozesse implementiert wurden.</p>	<p>Analyse- und Testphasen in der Softwareentwicklung können Sicherheitslücken ungewollt oder in böswilliger Absicht in die Produktionsumgebung eingeschleust werden.</p> <p>Wenn Sie wissen, wie vertrauliche Daten von der Anwendung behandelt werden – etwa bei Speicherung, Übertragung und Aufbewahrung –, können Sie ermitteln, an welcher Stelle die Daten geschützt werden müssen.</p>
<p><b>6.3.1</b> Löschen Sie Konten, Benutzer-IDs und Kennwörter für Entwicklung, Tests und/oder individuelle Anwendungen, bevor die Anwendungen aktiv oder für Kunden freigegeben werden.</p>	<p><b>6.3.1</b> Vergewissern Sie sich durch Untersuchung von Softwareentwicklungsverfahren und Befragung der verantwortlichen Mitarbeiter, dass Vorproduktions- und/oder individuelle Anwendungskonten, Benutzer-IDs und/oder Kennwörter entfernt werden, bevor die Anwendung in Produktion geht oder für Kunden freigegeben wird.</p>	<p>Entwicklungs-, Test- und individuelle Anwendungskonten, Benutzer-IDs und Kennwörter müssen aus dem Produktionscode gelöscht werden, bevor die Anwendung aktiviert oder für die Kunden freigegeben wird, da diese Elemente Informationen über die Funktionsweise der Anwendung preisgeben können. Personen, die in den Besitz derartiger Informationen gelangen, könnten die Anwendung sowie zugehörige Karteninhaberdaten gefährden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>6.3.2</b> Prüfung des individuellen Programmcodes vor der Freigabe für Produktion oder Kunden (entweder mithilfe manueller oder automatischer Prozesse) auf alle potenziellen Sicherheitsrisiken; dabei sind mindestens die folgenden Punkte zu berücksichtigen:</p> <ul style="list-style-type: none"> <li>• Codeänderungen werden von anderen Personen geprüft als dem ursprünglichen Ersteller des Codes, außerdem von Personen, die mit Verfahren zur Codeprüfung und sicheren Codierungsverfahren vertraut sind.</li> <li>• Mit Codeprüfungen wird sichergestellt, dass der Code gemäß sicheren Codierungsrichtlinien erstellt wird.</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> <p><i>(Fortsetzung auf der nächsten Seite)</i></p>	<p><b>6.3.2.a</b> Überprüfen Sie die schriftlich festgehaltenen Softwareentwicklungsverfahren, und vergewissern Sie sich durch die Befragung der zuständigen Mitarbeiter, dass sämtliche Änderungen am individuellen Anwendungscode (mit manuellen oder automatischen Prozessen) wie folgt geprüft werden:</p> <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>	<p>Sicherheitslücken in benutzerspezifischen Codes werden von böswilligen Individuen häufig ausgenutzt, um sich Zugriff auf ein Netzwerk zu verschaffen und Karteninhaberdaten zu kompromittieren.</p> <p>In den Überprüfungsprozess ist eine kompetente und erfahrene Person einzubinden. Code-Überprüfungen müssen von einer anderen Person als dem Entwickler des Codes vorgenommen werden, damit eine unabhängige und objektive Überprüfung stattfindet. Anstelle von manuellen Überprüfungen können auch automatisierte Tools bzw. Prozesse eingesetzt werden. Dabei ist jedoch zu beachten, dass sich mit automatisierten Tools in der Regel Codeprobleme schwer oder gar nicht erkennen lassen.</p> <p>Die Behebung von Codierungsfehlern vor der Bereitstellung in einer Produktionsumgebung bzw. vor der Freigabe für die Kunden verhindert, dass Umgebungen durch Codefehlern gefährdet werden. Nach der Bereitstellung bzw. Freigabe des Codes in Produktionsumgebungen ist es außerdem viel schwieriger und kostspieliger, Codefehler zu beheben.</p> <p>Eine offizielle Prüfung und Genehmigung durch die Geschäftsführung vor der Freigabe helfen sicherzustellen, dass der Code in Übereinstimmung mit den Richtlinien und Verfahren entwickelt wurde und zugelassen wird.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>Hinweis:</b> Diese Vorschrift von Code-Prüfungen gilt für den gesamten benutzerdefinierten (internen und öffentlichen) Code im Rahmen des Systementwicklungszyklus.</p> <p>Code-Prüfungen können durch qualifiziertes internes Personal oder durch Dritte ausgeführt werden. Für die Öffentlichkeit bestimmte Webanwendungen unterliegen auch zusätzlichen Kontrollen, um laufende Bedrohungen und Sicherheitsrisiken nach der Implementierung gemäß der Definition in PCI DSS-Anforderung 6.6 anzugehen.</p>	<p><b>6.3.2.b</b> Wählen Sie eine Stichprobe aus kürzlich vorgenommenen Änderungen an individuellen Anwendungen aus und überprüfen Sie, ob der individuelle Anwendungscode gemäß Punkt 6.3.2.a oben geprüft wird.</p>	
<p><b>6.4</b> Befolgen von Änderungskontrollprozessen und -verfahren für alle Änderungen an Systemkomponenten. Die Prozesse müssen Folgendes umfassen:</p>	<p><b>6.4</b> Überprüfen Sie Richtlinien und Verfahren daraufhin, ob Folgendes ist:</p> <ul style="list-style-type: none"> <li>• Die Entwicklungs-/Testumgebungen sind von den Produktionsumgebungen getrennt, auch ist zur Durchsetzung dieser Trennung ist Zugriffskontrolle implementiert.</li> <li>• Es besteht eine Trennung der Aufgaben zwischen Mitarbeitern, die den Entwicklungs-/Testumgebungen zugewiesen sind, und Mitarbeitern, die der Produktionsumgebung zugeteilt sind.</li> <li>• Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet.</li> <li>• Testdaten und -konten werden gelöscht, bevor ein Produktionssystem aktiv wird.</li> <li>• Änderungskontrollverfahren im Hinblick auf die Implementierung von Sicherheitspatches und Softwareänderungen sind dokumentiert.</li> </ul>	<p>Ohne ordnungsgemäß dokumentierte und implementierte Änderungskontrollen können Sicherheitsfunktionen ungewollt oder wissentlich ausgelassen oder gar funktionsunfähig gemacht werden. Außerdem könnten Unregelmäßigkeiten in der Verarbeitung auftreten oder schädliche Codes eingeführt werden.</p>
<p><b>6.4.1</b> Trennung der Entwicklungs-/Testumgebungen von der Produktionsumgebung und Durchsetzung dieser Trennung mittels Zugriffskontrolle.</p>	<p><b>6.4.1.a</b> Vergewissern Sie sich in der Netzwerkdokumentation und der Konfiguration der Netzwerkgeräte, dass die Entwicklungs-/Testumgebungen von den Produktionsumgebungen getrennt sind.</p>	<p>Aufgrund des sich fortwährend ändernden Status von Entwicklungs- und Testumgebungen sind sie oft unsicherer als die Produktionsumgebung. Ohne eine angemessene Trennung der Umgebungen ist es</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p><b>6.4.1.b</b> Vergewissern Sie sich in den Zugriffskontrolleinstellungen, dass die Trennung der Entwicklungs-/Testumgebungen von den Produktionsumgebungen erzwungen wird.</p>	<p>möglich, dass die Produktionsumgebung und die Karteninhaberdaten aufgrund von zu wenig stringenten Sicherheitskonfigurationen und von möglichen Sicherheitsrisiken in einer Test- oder Entwicklungsumgebung gefährdet sind.</p>
<p><b>6.4.2</b> Trennung der Aufgaben zwischen Entwicklungs-, Test- und Produktionsumgebungen</p>	<p><b>6.4.2</b> Vergewissern Sie sich durch die Beobachtung von Prozessen und die Befragung der Mitarbeiter von Entwicklungs-/Testumgebungen einerseits und den Produktionsumgebungen andererseits, dass eine Trennung der Aufgaben zwischen den Mitarbeitern besteht.</p>	<p>Die Einschränkung der Personenzahl, die Zugriff auf die Produktionsumgebung und die Karteninhaberdaten hat, minimiert das Risiko und hilft sicherstellen, dass der Zugriff auf Personen mit betrieblichen Informationsbedarf beschränkt ist.</p> <p>Der Zweck dieser Anforderung liegt in der Trennung der Entwicklungs-/Testfunktionen von den Produktionsfunktionen. Ein Entwickler könnte beispielsweise in der Entwicklungsumgebung ein Konto auf Administratorebene mit erweiterten Rechten nutzen und ein separates Konto mit Zugriff auf Benutzerebene für die Produktionsumgebung verwenden.</p>
<p><b>6.4.3</b> Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet</p>	<p><b>6.4.3.a</b> Vergewissern Sie sich durch Beobachtung der Testverfahren und Befragung der Mitarbeiter, dass keine Produktionsdaten (Live-PANs) zum Testen oder zur Entwicklung verwendet werden.</p>	<p>In der Test- bzw. Entwicklungsumgebung sind die Sicherheitskontrollen normalerweise weniger streng. Die Verwendung von Produktionsdaten bietet böswilligen Personen die Gelegenheit, sich unbefugten Zugriff auf Produktionsdaten (Karteninhaberdaten) zu verschaffen.</p>
	<p><b>6.4.3.b</b> Vergewissern Sie sich in Stichproben von Testdaten, dass keine Produktionsdaten (Live-PANs) zum Testen oder zur Entwicklung verwendet werden.</p>	
<p><b>6.4.4</b> Löschung von Testdaten und -konten aus Systemkomponenten, bevor das System aktiv wird / in Produktion geht.</p>	<p><b>6.4.4</b> Vergewissern Sie sich durch Beobachtung von Testverfahren und Befragung von Mitarbeitern, dass Testdaten und -konten gelöscht werden, bevor ein Produktionssystem aktiv wird.</p>	<p>Testdaten und -konten müssen gelöscht werden, bevor die Systemkomponente aktiviert wird (in Produktion), da diese Elemente Informationen über die Funktionsweise der Anwendung preisgeben können. Personen, die in den Besitz dieser Informationen gelangen, könnten die Anwendung sowie zugehörige Karteninhaberdaten gefährden.</p>
	<p><b>6.4.4.b</b> Überprüfen Sie in einer Stichprobe der Daten und Konten aus den kürzlich installierten oder aktualisierten Produktionssystemen, ob Testdaten und -konten vor der Systemaktivierung gelöscht werden.</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>6.4.5</b> Verfahren zur Änderungskontrolle müssen folgende Elemente beinhalten:</p>	<p><b>6.4.5.a</b> Untersuchen Sie die dokumentierten Änderungskontrollverfahren und prüfen Sie, ob Verfahren für die folgenden Punkte definiert sind:</p> <ul style="list-style-type: none"> <li>• Dokumentation der Auswirkungen</li> <li>• Dokumentierte Genehmigung von Änderungen durch autorisierte Parteien</li> <li>• Testen der Funktionalität, damit die Änderung nicht die Sicherheit des Systems beeinträchtigt.</li> <li>• Back-Out-Verfahren</li> </ul> <p><b>6.4.5.b</b> Befragen Sie zuständige Mitarbeiter, um aktuelle Änderungen für eine Stichprobe von Systemkomponenten festzulegen. Verfolgen Sie diese Änderungen zurück zur entsprechenden Dokumentation der Änderungskontrolle. Führen Sie für jede untersuchte Änderung die folgenden Schritte aus:</p>	<p>Wird die Verwaltung nicht ordnungsgemäß durchgeführt, sind die Auswirkungen von Systemänderungen — wie Hard- oder Softwareupdates und die Installation von Sicherheitspatches — möglicherweise nicht vollständig bekannt, und könnten unbeabsichtigte Folgen nach sich ziehen.</p>
<p><b>6.4.5.1</b> Dokumentation der Auswirkungen.</p>	<p><b>6.4.5.1</b> Überprüfen Sie, ob die Dokumentation der Auswirkungen in der Änderungskontrolldokumentation für jede Änderung in der Stichprobe enthalten ist.</p>	<p>Die Auswirkungen der Änderung sollten dokumentiert werden, sodass alle betroffenen Parteien Prozessänderungen entsprechend vorausplanen können.</p>
<p><b>6.4.5.2</b> Dokumentierte Genehmigung von Änderungen durch autorisierte Parteien.</p>	<p><b>6.4.5.2</b> Überprüfen Sie, ob für jede Änderung aus der Stichprobe eine dokumentierte Genehmigung durch autorisierte Parteien vorhanden ist.</p>	<p>Die Genehmigung durch eine autorisierte Partei zeigt, dass es sich um eine zulässige und von dem Unternehmen genehmigte Änderung handelt.</p>
<p><b>6.4.5.3</b> Testen der Funktionalität, damit die Änderung nicht die Sicherheit des Systems beeinträchtigt.</p>	<p><b>6.4.5.3.a</b> Vergewissern Sie sich mit Funktionalitätstests für jede Änderung in der Stichprobe, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt.</p> <p><b>6.4.5.3.b</b> Überprüfen Sie bei individuellen Codeänderungen, dass alle Aktualisierungen vor der Implementierung in der Produktionsumgebung auf ihre Konformität mit der PCI-DSS-Anforderung 6.5 getestet wurden.</p>	<p>Es sollten eingehende Tests durchgeführt werden, um sicherzustellen, dass die Sicherheit durch diese Änderung nicht herabgesetzt wird. Die Tests sollten überprüfen, ob alle vorhandenen Sicherheitsvorkehrungen bestehen bleiben, durch ebenso starke Kontrollen ersetzt werden oder nach Änderungen in der Umgebung intensiviert werden müssen.</p>
<p><b>6.4.5.4</b> Back-Out-Verfahren.</p>	<p><b>6.4.5.4</b> Überprüfen Sie, ob für jede Änderung in der Stichprobe Back-Out-Verfahren erstellt werden.</p>	<p>Für alle Änderungen müssen Verfahren etabliert sein, um die Änderung – für den Fall, dass sie fehlschlägt oder die Sicherheit einer Anwendung oder eines Systems beeinträchtigt – rückgängig zu machen und den vorherigen Zustand wiederherzustellen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>6.4.6</b> Nach Abschluss einer signifikanten Änderung müssen alle relevanten PCI-DSS-Anforderungen auf allen neuen oder veränderten Systemen und Netzwerken implementiert, und die Dokumentation entsprechend aktualisiert sein.</p> <p><i><b>Hinweis:</b> Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</i></p>	<p><b>6.4.6</b> Untersuchen Sie für eine Stichprobe der signifikanten Änderungen die Änderungsdokumentation, befragen Sie Mitarbeiter und beobachten Sie die betroffenen Systeme/Netzwerke, um sicherzustellen, dass alle anwendbaren PCI-DSS-Anforderungen implementiert wurden und die Dokumentation als Teil der Änderung aktualisiert wurde.</p>	<p>Prozesse zur Analyse signifikanter Änderungen helfen dabei sicherzustellen, dass auf allen Systemen oder Netzwerken, die innerhalb der Umgebung hinzugefügt oder verändert wurden, alle entsprechenden PCI-DSS-Kontrollen angewendet werden.</p> <p>Die Integration dieser Validierung in die Change-Management-Prozesse hilft dabei sicherzustellen, dass die Standards für Gerätebestände und -konfiguration aktuell gehalten und Sicherheitskontrollen wo nötig angewendet werden.</p> <p>Ein Change-Management-Prozess sollte unterstützende Beweise dafür enthalten, dass PCI-DSS-Anforderungen implementiert oder über das iterative Verfahren erhalten wurden. Beispiele für PCI-DSS-Anforderungen, die betroffen sein könnten, sind unter anderem:</p> <ul style="list-style-type: none"> <li>• Das Netzwerkdiagramm wird zur Wiedergabe der Änderungen aktualisiert.</li> <li>• Die Systeme sind gemäß Konfigurationsstandard konfiguriert, alle Standardkennwörter wurden geändert und nicht benötigte Dienste deaktiviert.</li> <li>• Die Systeme sind durch die erforderlichen Kontrollen geschützt—z. B. Tools zur Überwachung der Dateintegrität (FIM), Antivirus, Patches, Audit-Protokollierung.</li> <li>• Vertrauliche Authentifizierungsdaten (SAD) werden nicht gespeichert, und alle Speicher von Karteninhaberdaten (CHD) sind dokumentiert und fester Bestandteil der Richtlinien und Verfahren zur Datenspeicherung</li> <li>• Neue Systeme werden in die vierteljährlichen Schwachstellenprüfungen mit einbezogen.</li> </ul>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>6.5</b> Gehen Sie häufige Sicherheitsrisiken in Softwareentwicklungsprozessen an, einschließlich der folgenden Punkte:</p> <ul style="list-style-type: none"> <li>• Entwickler müssen mindestens jährlich auf aktuelle Techniken zur sicheren Programmierung, einschließlich dem Vorbeugen häufiger Schwachstellen, geschult werden.</li> <li>• Entwicklung von Anwendungen aufgrund sicherer Programmierungsrichtlinien.</li> </ul> <p><b>Hinweis:</b> Die unter 6.5.1 bis 6.5.10 aufgeführten Sicherheitsrisiken entsprechen zum Zeitpunkt der Veröffentlichung dieser Version des PCI-DSS den bewährten Verfahren der Branche. Da jedoch die bewährten Verfahren der Branche beim Management von Sicherheitsrisiken aktualisiert werden (z. B. der OWASP Leitfaden, SANS CWE Top 25, CERT Secure Coding usw.), sind für diese Anforderungen die jeweils gültigen bewährten Verfahren zu verwenden.</p>	<p><b>6.5.a</b> Vergewissern Sie sich durch Untersuchung von Richtlinien und Verfahren für die Softwareentwicklung, dass aktuelle Schulungen zu sicheren Programmierverfahren für Entwickler auf Basis der bewährten Verfahren der Branche sowie Anweisungen mindestens einmal jährlich vorgeschrieben werden.</p> <p><b>6.5.b</b> Überprüfen Sie in Schulungsunterlagen, ob die Softwareentwickler mindestens einmal jährlich in aktuellen Techniken zur Erstellung sicherer Codes und zur Vermeidung häufiger Sicherheitsrisiken geschult werden.</p> <p><b>6.5.c</b> Vergewissern Sie sich, dass Anwendungen durch entsprechende Prozesse mindestens vor den folgenden Sicherheitsrisiken geschützt sind:</p>	<p>Die Anwendungsschicht ist einem hohen Risiko ausgesetzt und ist sowohl durch interne als auch externe Bedrohungen gefährdet.</p> <p>Die Mindestkontrollen werden durch die Anforderungen 6.5.1 bis 6.5.10 festgelegt. Ein Unternehmen sollte je nach der Technologie, die es einsetzt, entsprechende sichere Programmierverfahren implementieren.</p> <p>Anwendungsentwickler müssen ordnungsgemäß geschult sein, damit sie Probleme im Zusammenhang mit diesen (und anderen) gängigen Programmier Risiken erkennen und lösen können. Wenn die Mitarbeiter mit sicheren Programmiermethoden vertraut sind, kann die Anzahl der Sicherheitsrisiken, die durch unzulängliche Programmierverfahren eingeschleust werden, auf ein Minimum reduziert werden. Schulungen für Entwickler können intern oder von Drittanbietern für die jeweils verwendete Technik angeboten werden.</p> <p>Da sich die von der Branche akzeptierten Verfahrensweisen zur sicheren Programmierung im Laufe der Zeit ändern können, sind die Programmierpraktiken in der Organisation und die Schulungen der Entwickler ebenfalls an neue Bedrohungen wie etwa Memory-Scraping-Angriffe anzupassen.</p> <p>Die in den Punkten 6.5.1 bis 6.5.10 aufgeführten Sicherheitsrisiken stellen eine Mindestanforderung dar. Es ist Aufgabe der Unternehmen, bei Sicherheitstrends auf dem neuesten Stand zu bleiben und angemessene Maßnahmen für eine sichere Programmierung zu ergreifen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<b>Hinweis:</b> Die Anforderungen 6.5.1 bis 6.5.6 gelten für alle Anwendungen (intern oder extern):		
<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> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob Injektionsfehlern mit u. a. den folgenden Programmiertechniken begegnet wird:</p> <ul style="list-style-type: none"> <li>• Validierung der Eingabe, damit Benutzerdaten nicht die Bedeutung von Befehlen und Abfragen ändern können</li> <li>• Verwendung von parametrisierten Abfragen</li> </ul>	<p>Injektionsfehler, insbesondere die SQL-Injektion, sind eine häufige Methode zur Beschädigung von Anwendungen. Injektionen treten auf, wenn vom Benutzer übermittelte Daten als Teil eines Befehls oder einer Anfrage an einen Interpreter gesendet werden. Die schädlichen Daten des Angreifers verleiten den Interpreter unwissentlich dazu, Befehle auszuführen oder Daten zu ändern, was es dem Angreifer ermöglicht, die Komponenten im Netzwerk über die Anwendung anzugreifen, Angriffe wie beispielsweise Pufferüberläufe einzuleiten oder sowohl vertrauliche Informationen als auch Anwendungsfunktionen des Servers zu enthüllen.</p> <p>Die Informationen müssen vor der Weiterleitung an die Anwendung validiert werden – beispielsweise werden sie auf das Vorhandensein von Buchstaben, alphanumerischen Zeichen usw. untersucht.</p>
<p><b>6.5.2</b> Pufferüberläufe</p>	<p><b>6.5.2</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob Pufferüberläufen mit u. a. den folgenden Programmiertechniken begegnet wird:</p> <ul style="list-style-type: none"> <li>• Validierung von Puffergrenzen</li> <li>• Kürzung der eingegebenen Zeichenfolgen</li> </ul>	<p>Pufferüberläufe treten auf, wenn eine Anwendung auf ihrem Pufferspeicherplatz nicht über eine geeignete Bereichseingrenzung verfügt. Das kann dazu führen, dass die Informationen in dem Puffer aus dem Pufferspeicherplatz auf einen ausführbaren Speicherbereich verdrängt werden. In diesem Fall ist der Angreifer in der Lage, schädlichen Code an das Ende eines Puffers zu hängen und diesen Code anschließend, indem der Puffer zum Überlaufen gebracht wird, in einen ausführbaren Speicherbereich einzuschleusen. Der schädliche Code wird dann ausgeführt und gewährt dem Angreifer den Fernzugriff auf die Anwendung beziehungsweise das betroffene System.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<b>6.5.3</b> Unsicherer kryptographischer Speicher	<b>6.5.3</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob unsicherem kryptographischem Speicher mit u. a. den folgenden Programmieretechniken begegnet wird: <ul style="list-style-type: none"> <li>• Verhindern Sie kryptographische Fehler.</li> <li>• Nutzung starker kryptographischer Algorithmen und Schlüssel</li> </ul>	Anwendungen, die beim Speichern der Daten die starken kryptographischen Funktionen nicht richtig einsetzen, sind einem erhöhten Risiko der Kompromittierung und der Gefährdung der Authentifizierungsinformationen und/oder Karteninhaberdaten ausgesetzt. Wenn ein Angreifer schwache kryptographische Prozesse ausnutzen kann, ist er unter Umständen auch in der Lage, auf verschlüsselte Daten im Klartext zuzugreifen.
<b>6.5.4</b> Unsichere Mitteilungen	<b>6.5.4</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob unsicheren Mitteilungen mit Programmieretechniken begegnet wird, bei denen sämtliche vertraulichen Datenübertragungen authentifiziert und verschlüsselt werden.	Anwendungen, die den Netzwerkdatenverkehr nicht mithilfe einer starken Kryptographie angemessen verschlüsseln, sind einem erhöhten Risiko für Kompromittierungen und Gefährdungen ihrer Karteninhaberdaten ausgesetzt. Wenn ein Angreifer schwache kryptographische Prozesse ausnutzen kann, ist er unter Umständen auch in der Lage, die Herrschaft über eine Applikation zu gewinnen oder sogar auf verschlüsselte Daten im Klartext zuzugreifen.
<b>6.5.5</b> Inkorrekte Fehlerhandhabung	<b>6.5.5</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob inkorrekte Fehlerhandhabung mit Programmierverfahren, die keine Informationen über Fehlermeldungen preisgeben (indem beispielsweise keine konkreten Fehlerdetails, sondern nur allgemeine Angaben zurückgegeben werden), verhindert wird.	Anwendungen können durch unangemessene Methoden zur Fehlerhandhabung Informationen über ihre Konfiguration oder internen Abläufe bzw. vertrauliche Informationen preisgeben. Angreifer nutzen diese Schwachstellen aus, um vertrauliche Informationen zu entwenden oder das gesamte System zu gefährden. Wenn eine böswillige Person Fehler einbauen kann, die die Anwendung anschließend nicht richtig behebt, ist sie auch in der Lage, an ausführliche Informationen über das System zu gelangen, Denial-of-Service-Unterbrechungen hervorzurufen, das Sicherheitssystem zum Scheitern oder den Server zum Abstürzen zu bringen. Durch die Meldung „falsches Kennwort“ erfährt ein Angreifer beispielsweise, dass die Benutzer-ID korrekt war und er seine Anstrengungen nun auf das Kennwort konzentrieren kann. Es wird empfohlen, allgemeinere Meldungen zu verwenden, wie z. B. „Die Daten konnten nicht verifiziert werden.“

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>6.5.6</b> Alle „schwerwiegenden“ Sicherheitsrisiken werden entsprechend dem Identifikationsprozess ermittelt (wie in der PCI-DSS-Anforderung 6.1 definiert).</p>	<p><b>6.5.6</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob die Programmierverfahren auf alle „hohen“ Sicherheitsrisiken eingehen, die die Anwendung beeinträchtigen könnten – entsprechend der PCI-DSS-Anforderung 6.1.</p>	<p>Alle Sicherheitsrisiken, die vom Unternehmensprozess zur Risikoeinstufung (in der PCI-DSS-Anforderung 6.1 definiert) als „hohes Risiko“ eingestuft werden und die die Anwendung beeinträchtigen könnten, müssen während der Anwendungsentwicklung ermittelt und behoben werden.</p>
<p><b>Hinweis:</b> Die nachstehenden Anforderungen 6.5.7 bis 6.5.10 gelten für Webanwendungen und Anwendungsschnittstellen (intern oder extern):</p>		<p>Webanwendungen sowohl intern als auch extern (öffentlich) sind aufgrund ihrer Architektur sowie der relativ einfachen Erstellung und der Häufigkeit von Angriffen besonderen Sicherheitsrisiken ausgesetzt.</p>
<p><b>6.5.7</b> Siteübergreifendes Scripting (XSS)</p>	<p><b>6.5.7</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob siteübergreifendem Scripting mit u. a. den folgenden Programmier Techniken begegnet wird:</p> <ul style="list-style-type: none"> <li>• Validierung aller Parameter vor der Einbindung</li> <li>• Nutzung einer kontextabhängigen Außerkräftsetzungsfunktion</li> </ul>	<p>XSS-Fehler treten auf, wenn eine Anwendung vom Benutzer übermittelte Daten an einen Webbrowser sendet, ohne diese zuvor zu überprüfen oder deren Inhalt zu verschlüsseln. XSS ermöglicht es Angreifern im Browser eines betroffenen Benutzers, Skripts auszuführen, wodurch unter anderem Benutzer-Sitzungen übernommen, Websites unleserlich gemacht und möglicherweise Würmer eingeschleust werden können.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>6.5.8</b> Kontrolle unangemessener Zugriffe (z. B. unsichere direkte Objektverweise, fehlende Einschränkung des URL-Zugriffs, Directory Traversal und fehlende Einschränkung des Benutzerzugriffs auf bestimmte Funktionen).</p>	<p><b>6.5.8</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob auf eine ungenügende Zugriffskontrolle – beispielsweise unsichere direkte Objektverweise, unterlassene Einschränkung des URL-Zugriffs und Directory Traversal – mit folgenden Programmierverfahren eingegangen wird:</p> <ul style="list-style-type: none"> <li>• Ordnungsgemäße Benutzerauthentifizierung</li> <li>• Bereinigung der Eingaben</li> <li>• Keine Preisgabe interner Objektverweise an Benutzer</li> <li>• Benutzeroberflächen, die keinen Zugriff auf nicht autorisierte Funktionen zulassen</li> </ul>	<p>Ein direkter Objektverweis liegt vor, wenn ein Entwickler einen Verweis einem internen Implementierungsobjekt, wie etwa einer Datei, einem Verzeichnis, einem Datensatz in einer Datenbank oder einem Schlüssel, in Form einer URL oder eines Formularparameters zugänglich macht. Angreifer können diese Verweise manipulieren, um unerlaubt auch auf andere Objekte zuzugreifen.</p> <p>Setzen Sie die Zugriffskontrolle einheitlich in der Präsentationsebene und der Geschäftslogik für alle URLs durch. Oft schützt eine Anwendung eine empfindliche Funktion nur, indem sie verhindert, dass Links oder URLs unbefugten Benutzern angezeigt werden. Angreifer können diese Schwachstelle ausnutzen, indem sie diese URLs direkt aufrufen und sich Zugriff verschaffen und nicht autorisierte Operationen ausführen.</p> <p>Ein Angreifer ist unter Umständen in der Lage, die Verzeichnisstruktur einer Website aufzulisten und zu durchsuchen (Directory Traversal) und sich somit Zugriff auf nicht autorisierte Informationen zu verschaffen sowie tiefere Einblicke in die Funktionsweise der Site für spätere Angriffe zu gewinnen.</p> <p>Falls Benutzeroberflächen den Zugriff auf nicht autorisierte Funktionen ermöglichen, könnten sich unbefugte Personen Zugriff auf vertrauliche Anmeldeinformationen oder Karteninhaberdaten verschaffen. Nur autorisierte Benutzer dürfen in der Lage sein, über direkte Objektverweise auf vertrauliche Ressourcen zuzugreifen. Die Einschränkung des Zugriffs auf Datenressourcen trägt dazu bei, dass Karteninhaberdaten nicht von Unbefugten aufgerufen werden können.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<b>6.5.9</b> Cross-Site Request Forgery (CSRF)	<b>6.5.9</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob CSRF (Cross-site Request Forgery, websiteübergreifende Anfragenfälschung) mit Programmierverfahren begegnet wird, so dass Anwendungen keine Autorisierungsinformationen und Token verwenden, die automatisch von Browsern gesendet werden.	Ein CSRF-Angriff zwingt den Browser eines angemeldeten Benutzers, eine noch nicht authentifizierte Anfrage an eine gefährdete Webanwendung zu senden, wodurch der Angreifer beliebige statusverändernde Vorgänge ausführen kann, zu denen der Benutzer autorisiert ist (beispielsweise das Aktualisieren von Kontodetails, Einkäufe oder sogar die Authentifizierung der Anwendung).
<b>6.5.10</b> Umgang mit geknackten Authentifizierungen und Sitzungen	<b>6.5.10</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob geknackten Authentifizierungen und Sitzungen mit u. a. den folgenden Programmiertechniken begegnet wird: <ul style="list-style-type: none"> <li>• Kennzeichnung von Sitzungstoken (zum Beispiel Cookies) als „sicher“</li> <li>• Keine Anzeige von Sitzungs-IDs in der URL</li> <li>• Berücksichtigung angemessener Timeouts und Rotation der Sitzungs-IDs nach erfolgreicher Anmeldung</li> </ul>	Eine sichere Authentifizierungs- und Sitzungsverwaltung verhindert, dass unbefugte Personen zulässige Kontoanmeldeinformationen, Schlüssel oder Sitzungstoken gefährden, mit denen ein Angreifer die Identität eines autorisierten Benutzers annehmen könnte.

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>6.6</b> Kontinuierliche Betrachtung neuer Bedrohungen und Sicherheitsrisiken bei öffentlichen Webanwendungen Schutz dieser Anwendungen vor bekannten Angriffen mithilfe einer der folgenden Methoden:</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> </ul> <p><b>Hinweis:</b> Diese Bewertung ist nicht mit den für Anforderung 11.2 durchgeführten Schwachstellenprüfungen identisch.</p> <ul style="list-style-type: none"> <li>• Installation einer automatischen technischen Lösung zur Erkennung und Verhinderung webbasierter Angriffe (z. B. eine Webanwendungs-Firewall) bei öffentlichen Webanwendungen zur kontinuierlichen Prüfung des Datenverkehrs</li> </ul>	<p><b>6.6</b> Achten Sie bei <i>öffentlichen</i> Webanwendungen darauf, dass <i>eine</i> der folgenden Methoden implementiert ist:</p> <ul style="list-style-type: none"> <li>• Überprüfen Sie durch die Untersuchung dokumentierter Prozesse, die Befragung von Mitarbeitern und die Untersuchung von Unterlagen zur Bewertung der Anwendungssicherheit, ob öffentliche Webanwendungen wie folgt geprüft werden (mit manuellen oder automatisierten Tools oder Methoden zur Bewertung 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>– In den Bewertungen sollten mindestens die in der Anforderung 6.5 aufgeführten Sicherheitsrisiken überprüft werden.</li> <li>– Dass alle Sicherheitslücken geschlossen werden</li> <li>– Dass die Anwendung nach den Korrekturen erneut bewertet wird</li> </ul> </li> <li>• Überprüfen Sie durch die Untersuchung der Einstellungen in der Systemkonfiguration und die Befragung von zuständigen Mitarbeitern, ob eine automatisierte technische Lösung wie folgt implementiert ist, mit der sich webbasierte Angriffe erkennen und verhindern lassen (z. B. mit einer Webanwendungs-Firewall): <ul style="list-style-type: none"> <li>– Die Lösung befindet sich vor öffentlichen Webanwendungen und dient dazu, webbasierte Angriffe zu erkennen und zu verhindern.</li> <li>– Die Lösung wird aktiv ausgeführt und auf dem neuesten Stand gehalten.</li> <li>– In der Lösung werden Prüfprotokolle erstellt.</li> <li>– Die Lösung ist so konfiguriert, dass webbasierte Angriffe abgeblockt werden oder ein Alarm ausgelöst wird, der sofort untersucht wird.</li> </ul> </li> </ul>	<p>Öffentliche Webanwendungen sind primäre Ziele für Angreifer. Schlecht programmierte Webanwendungen sind ein Einfallstor für Angreifer, die sich Zugriff auf vertrauliche Daten und Systeme verschaffen wollen. Die Anforderung zur Überprüfung von Anwendungen oder zur Installation von Webanwendungs-Firewalls soll die Anzahl der Gefährdungen öffentlicher Webanwendungen reduzieren, durch die häufig Karteninhaberdaten gefährdet werden.</p> <ul style="list-style-type: none"> <li>• Manuelle oder automatisierte Tools oder Methoden zur Bewertung der Anwendungssicherheit dienen zur Prüfung bzw. zum Test der Anwendung auf Sicherheitsrisiken.</li> <li>• Web Application Firewalls filtern und blockieren unnötigen Datenverkehr auf Anwendungsebene. Zusammen mit einer netzwerkbasierten Firewall kann eine angemessen konfigurierte Web Application Firewall Angriffe auf Anwendungsebene verhindern, sofern die Anwendungen entsprechend codiert oder konfiguriert sind. Dies kann durch eine Kombination von Technologie und Prozessen erreicht werden. Prozessorientierte Lösungen müssen Mechanismen umfassen, die eine zeitnahe Reaktion auf Alarmmeldungen ermöglichen, um den Zweck dieser Anforderung, nämlich der Verhinderung von Angriffen, zu erfüllen.</li> </ul> <p><b>Hinweis:</b> „Ein Unternehmen, das auf Anwendungssicherheit spezialisiert ist“, kann ein Drittunternehmen oder eine interne Organisation sein, sofern sich die Prüfer auf Anwendungssicherheit spezialisieren und die Unabhängigkeit vom Entwicklungsteam nachweisen können.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>6.7</b> Die Sicherheitsrichtlinien und betriebliche Verfahren zum Aufbau und zur Wahrung sicherer Systeme und Anwendungen müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>	<p><b>6.7</b> Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zur Entwicklung und Pflege von Sicherheitssystemen und -anwendungen Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Die Richtlinien und Verfahren sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	<p>Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit die Systeme und Anwendungen dauerhaft sicher entwickelt und werden können und vor Sicherheitsrisiken geschützt sind.</p>

## Implementierung starker Zugriffskontrollmaßnahmen

### **Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach betrieblichem Informationsbedarf**

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

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

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>7.1</b> Beschränken des Zugriffs auf Systemkomponenten und Karteninhaberdaten auf die Personen, deren Tätigkeit diesen Zugriff erfordert.</p>	<p><b>7.1</b> Überprüfen Sie, ob die schriftlich fixierte Richtlinie für die Zugriffskontrolle die Anforderungen 7.1.1 bis 7.1.4 wie folgt erfüllt:</p> <ul style="list-style-type: none"> <li>• Jeder Rolle werden Zugriffsanforderungen und -berechtigungen zugewiesen.</li> <li>• Der Zugriff für Benutzer-IDs ist auf Mindestberechtigungen beschränkt, die zum Ausüben der tätigkeitsbezogenen Verpflichtungen erforderlich sind.</li> <li>• Die Zuweisung von Zugriffsberechtigungen erfolgt gemäß der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter.</li> <li>• Genehmigungen (in schriftlicher oder elektronischer Form) durch autorisierten Parteien sind für alle Zugriffsberechtigungen einschließlich einer Liste der genehmigten Berechtigungen zu dokumentieren.</li> </ul>	<p>Je mehr Personen Zugriff auf die Karteninhaberdaten haben, desto höher ist das Risiko, dass das Konto eines Benutzers in böser Absicht ausgenutzt wird. Die Beschränkung des Zugriffs auf Personen, die aus betrieblichen Gründen Einsicht benötigen, kann einem Unternehmen helfen, falschen Umgang von Karteninhaberdaten aus Unerfahrenheit oder Böswilligkeit zu verhindern.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>7.1.1</b> Definition der Zugriffsanforderungen für die einzelnen Rollen unter Berücksichtigung der folgenden Aspekte:</p> <ul style="list-style-type: none"> <li>• Systemkomponenten und Datenressourcen, die für die Ausführung der tätigkeitsbezogenen Funktionen benötigt werden</li> <li>• Erforderliche Berechtigungsstufe (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen</li> </ul>	<p><b>7.1.1</b> Bestimmen Sie eine Stichprobe aus Rollen, und prüfen Sie, ob die Zugriffsanforderungen für die einzelnen Rollen definiert sind und die folgenden Punkte umfassen:</p> <ul style="list-style-type: none"> <li>• Systemkomponenten und Datenressourcen, die für die Ausführung der tätigkeitsbezogenen Funktionen benötigt werden</li> <li>• Ermittlung der für die Durchführung der tätigkeitsbezogenen Funktionen der Rolle erforderliche Berechtigungen</li> </ul>	<p>Damit der Zugriff auf Karteninhaberdaten auf diejenigen Personen beschränkt bleibt, die tatsächlich auf die Daten zugreifen müssen, ist zuerst für die Systeme/Geräte/Daten zu definieren, inwieweit die einzelnen Rollen (Systemadministrator, Callcenter-Personal, Filialmitarbeiter usw.) darauf zugreifen müssen, und welche Berechtigungsstufe für eine effektive Ausführung der zugewiesenen Aufgaben erforderlich ist. Sind die Rollen und die zugehörigen Zugriffsberechtigungen definiert, können die Berechtigungen den einzelnen Benutzern zugewiesen werden.</p>
<p><b>7.1.2</b> Beschränkung des Zugriffs für Benutzer-IDs auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind.</p>	<p><b>7.1.2.a</b> Überprüfen Sie durch Gespräche mit den für die Zugriffszuweisung zuständigen Mitarbeitern, dass für den Zugriff auf die privilegierten Benutzer-IDs Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Die Zugriffsrechte werden nur Rollen zugewiesen, die diesen privilegierten Zugriff konkret benötigen.</li> <li>• Die Zugriffsrechte sind auf Mindestberechtigungen beschränkt, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind.</li> </ul>	<p>Bei der Zuweisung von IDs mit Berechtigungen dürfen den einzelnen Personen nur die Rechte zugewiesen werden, die sie zur Ausführung ihrer Aufgaben benötigen (die „Mindestberechtigungen“). So dürfen dem Datenbank- bzw. Backup-Administrator nicht die gleichen Berechtigungen wie dem allgemeinen Systemadministrator zugewiesen werden.</p> <p style="text-align: right;"><i>(Fortsetzung auf der nächsten Seite)</i></p>
	<p><b>7.1.2.b</b> Überprüfen Sie an stichprobenartig zusammengestellten Benutzer-IDs mit privilegiertem Zugriff und durch Gespräche mit den für die Verwaltung zuständigen Mitarbeitern, dass für die zugewiesenen Berechtigungen Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Die Berechtigungen sind für die tätigkeitsbezogenen Aufgaben der Person erforderlich.</li> <li>• Die Zugriffsrechte sind auf Mindestberechtigungen beschränkt, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind.</li> </ul>	<p>Das Zuweisen von Mindestberechtigungen trägt dazu bei zu verhindern, dass Benutzer ohne ausreichende Anwendungskennntnisse fälschlicherweise oder versehentlich die Anwendungskonfiguration oder ihre Sicherheitseinstellungen ändern. Die Durchsetzung der Mindestberechtigung minimiert auch das Ausmaß des Schadens, der entstehen kann, wenn eine nicht autorisierte Person Zugriff auf eine Benutzer-ID erhält.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>7.1.3</b> Zuweisung von Zugriffsberechtigungen aufgrund der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter.</p>	<p><b>7.1.3</b> Überprüfen Sie an stichprobenartig zusammengestellten Benutzer-IDs und durch Gespräche mit den für die Verwaltung zuständigen Mitarbeitern, dass die zugewiesenen Berechtigungen auf der Tätigkeitsklassifizierung und -funktion des jeweiligen Mitarbeiters basieren.</p>	<p>Sobald die Anforderungen für die einzelnen Benutzerrollen definiert sind (gemäß PCI-DSS-Anforderung 7.1.1), kann Einzelpersonen unter Verwendung der bereits erstellten Rollen problemlos der Zugriff gemäß Tätigkeitsklassifizierung und -funktion gewährt werden.</p>
<p><b>7.1.4</b> Die Genehmigung durch autorisierte Parteien, in der die erforderlichen Berechtigungen angegeben sind, muss dokumentiert werden.</p>	<p><b>7.1.4</b> Prüfen Sie für stichprobenartig ausgewählte Benutzer-IDs durch einen Vergleich mit dokumentierten Genehmigungen, dass Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Die Genehmigung der zugewiesenen Berechtigungen wurde dokumentiert.</li> <li>• Die Genehmigung wurde von autorisierten Parteien erteilt.</li> <li>• Die angegebenen Berechtigungen entsprechen den Rollen, die der Person zugewiesen sind.</li> </ul>	<p>Die (schriftliche oder elektronische) Dokumentation der Genehmigung stellt sicher, dass das Management die mit Zugriffsberechtigung und sonstigen Rechten ausgestatteten Personen kennt und dass der Zugriff für die Tätigkeitsfunktionen erforderlich ist.</p>
<p><b>7.2</b> Festlegen eines Zugriffskontrollsystems für Systemkomponenten, das den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird.</p> <p>Dieses Zugriffskontrollsystem muss Folgendes umfassen:</p>	<p><b>7.2</b> Prüfen Sie anhand von Systemeinstellungen und der Anbieterdokumentation, ob ein Zugriffskontrollsystem wie folgt implementiert ist:</p>	<p>Ohne einen Mechanismus, um den Zugriff von Benutzern entsprechend ihres Informationsbedarfs einzuschränken, könnte einem Benutzer unter Umständen ungewollt Zugriff auf Karteninhaberdaten gewährt werden. Zugriffskontrollsysteme automatisieren den Prozess zur Beschränkung des Zugriffs und zur Zuweisung von Berechtigungen. Darüber hinaus sorgt die Einstellung „Alle ablehnen“ dafür, dass niemandem Zugriff gewährt wird, solange keine Regel vorliegt, die einen Zugriff konkret gewährt. Einrichtungen können eine oder mehrere Zugriffskontrollen zur Verwaltung von Benutzerzugriffen besitzen.</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>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.</p>
<p><b>7.2.3</b> Standardeinstellung „Alle ablehnen“</p>	<p><b>7.2.3</b> Vergewissern Sie sich, dass die Zugriffskontrollsysteme die Standardeinstellung „Alle ablehnen“ aufweisen.</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>7.3</b> Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des Zugriffs auf Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>	<p><b>7.3</b> Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren für die Beschränkung des Zugriffs auf Karteninhaberdaten Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Sie sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	<p>Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit der Zugriff dauerhaft kontrolliert wird und auf Basis des Informationsbedarfs und der Mindestberechtigung erfolgt.</p>

## Anforderung 8: Zugriff auf Systemkomponenten identifizieren und authentifizieren

Durch die Zuweisung einer eindeutigen Kennung (ID) zu jeder Person mit Zugriff ist jede(r) Einzelne eindeutig 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 und Prozessen vorgenommen werden, und sämtliche Maßnahmen lassen sich auf den jeweiligen Initiator zurückführen.

Die Effektivität eines Kennworts hängt im Wesentlichen von der Konzeption und Umsetzung des Authentifizierungssystems ab – insbesondere davon, wie häufig Angreifer versuchen können, ein Kennwort einzugeben, und von den Sicherheitsmethoden zum Schutz von Benutzerkennwörtern bei der Eingabe, bei der Übertragung und bei der Speicherung.

**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. Hierunter fallen auch Konten, die von Anbietern und anderen Dritten (z. B. für Support oder Wartung) verwendet werden. Diese Anforderungen gelten nicht für die Konten von Verbrauchern (z. B. Karteninhaber).

Allerdings gelten die Anforderungen 8.1.1, 8.2, 8.5, 8.2.3 bis 8.2.5 und 8.1.6 bis 8.1.8 nicht für Benutzerkonten mit einer Point-of-Sale-Zahlungsanwendung, die nur auf eine Kartenummer auf einmal Zugriff haben, um einzelne Transaktionen zuzulassen (z. B. Kassierer-Konten).

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<b>8.1</b> Definition und Implementierung von Richtlinien und Verfahren zur geeigneten Benutzeridentifizierungsverwaltung für Nichtverbraucherbenutzer und Administratoren auf allen Systemkomponenten nach folgender Maßgabe:	<b>8.1.a</b> Vergewissern Sie sich, dass in den Verfahren Prozesse für die einzelnen unter 8.1.1 bis 8.1.8 aufgeführten Elemente definiert werden.	Indem sichergestellt wird, dass jeder Benutzer eindeutig identifiziert ist – anstatt einen Benutzernamen für mehrere Mitarbeiter zu verwenden – kann ein Unternehmen Einzelne für ihre Handlungen zur Rechenschaft ziehen und pro Mitarbeiter einen effektiven Audit-Trail erstellen. Dies hilft, die Problembewältigung und den Einsatz von Vorbeugungsmaßnahmen im Falle von Missbrauch oder böswilligen Absichten zu beschleunigen.
	<b>8.1.b</b> Überprüfen Sie auf folgende Weise, ob die Verfahren zur Benutzeridentifizierungsverwaltung implementiert wurden:	
<b>8.1.1</b> Zuweisen einer eindeutigen ID für alle Benutzer, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird.	<b>8.1.1</b> Vergewissern Sie sich durch Befragung des administrativen Personals, dass allen Benutzern eine eindeutige ID für den Zugriff auf Systemkomponenten oder Karteninhaberdaten zugewiesen wird.	
<b>8.1.2</b> Kontrollieren Sie die Vorgänge des Hinzufügens, Löschens und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsobjekten.	<b>8.1.2</b> Überprüfen Sie für eine Stichprobe von Benutzer-IDs mit besonderen Berechtigungen und von allgemeinen Benutzer-IDs durch Untersuchung der zugehörigen Autorisierungen und Beobachtung der Systemeinstellungen, ob den einzelnen Benutzer-IDs und den Benutzer-IDs mit besonderen Berechtigungen nur die Rechte zugewiesen wurden, deren Genehmigung dokumentiert wurde.	Damit der Zugriff auf Systeme nur Benutzern mit gültigen und anerkannten Benutzerkonten gewährt wird, müssen sämtliche Änderungen an den Benutzer-IDs und anderen Anmeldedaten (wie z. B. das Hinzufügen bzw. Ändern oder Löschen von Daten) von starken Prozessen übernommen werden

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>8.1.3</b> Sofortige Deaktivierung des Zugriffs ehemaliger Benutzer.</p>	<p><b>8.1.3.a</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 (für lokalen und Remote-Zugriff) gelöscht wurden.</p> <p><b>8.1.3.b</b> Überprüfen Sie, ob sämtliche Methoden zur physischen Authentifizierung – Smartcards, Tokens usw. zurückgegeben bzw. deaktiviert wurden.</p>	<p>Wenn ein Mitarbeiter, der das Unternehmen verlassen hat, weiterhin Zugriff auf das Netzwerk über dessen Benutzerkonto besitzt, kann es zu unnötigen oder böswilligen Zugriffen auf Karteninhaberdaten kommen – sowohl durch den früheren Mitarbeiter als auch durch nicht autorisierte Dritte, die das alte beziehungsweise nicht verwendete Benutzerkonto missbrauchen. Um einen nicht autorisierten Zugriff zu vermeiden, müssen Anmeldedaten und sonstige Authentifizierungsmethoden sofort (schnellstmöglich) nach Ausscheiden des Mitarbeiters deaktiviert werden.</p>
<p><b>8.1.4</b> Entfernen bzw. Deaktivieren inaktiver Benutzerkonten innerhalb von 90 Tagen.</p>	<p><b>8.1.4</b> Überprüfen Sie, ob seit mehr als 90 Tagen inaktive Konten entfernt oder deaktiviert werden.</p>	<p>Nicht regelmäßig genutzte Konten sind häufiger Ziel eines Angriffs, da es weniger wahrscheinlich ist, dass Änderungen (wie z. B. eine Kennwortänderung) auffallen. Daher können diese Konten einfacher missbraucht und zum Zugriff auf Karteninhaberdaten genutzt werden.</p>
<p><b>8.1.5</b> Beim Management von IDs, die von Dritten für den Zugriff, den Support oder die Wartung von Systemkomponenten per Remote-Zugriff verwendet werden, müssen folgende Aspekte berücksichtigt werden:</p> <ul style="list-style-type: none"> <li>• Sie werden nur in dem Zeitraum aktiviert, in dem sie benötigt werden, und anschließend wieder deaktiviert.</li> <li>• Verwendete IDs werden überwacht.</li> </ul>	<p><b>8.1.5.a</b> Vergewissern Sie sich durch Gespräche mit den Mitarbeitern und die Beobachtung der Prozesse Dritter für den Zugriff, den Support und die Wartung von Systemkomponenten, dass für die von Dritten für den Remote-Zugriff verwendeten Konten Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Nicht verwendete Konten werden deaktiviert.</li> <li>• Von Dritten benötigte Konten werden nur in dem Zeitraum aktiviert, in dem sie benötigt werden, und anschließend wieder deaktiviert.</li> </ul> <p><b>8.1.5.b</b> Überprüfen Sie durch Befragung der Mitarbeiter und die Beobachtung von Prozessen, ob der Remote-Kontenzugriff Dritter überwacht wird.</p>	<p>Wenn Sie Anbietern ermöglichen, durchgehend auf Ihr Netzwerk zuzugreifen, um bei Bedarf Arbeiten an Ihrem System vorzunehmen, erhöht sich das Risiko unbefugter Zugriffe entweder durch Benutzer aus der Umgebung des Anbieters oder durch eine böswillige Person, die diesen jederzeit verfügbaren externen Zugriffspunkt in Ihr Netzwerk ausnutzt. Wenn Sie den Zugriff ausschließlich auf die notwendigen Zeiträume beschränken und sofort deaktivieren, wenn er nicht mehr benötigen, können diese Verbindungen nicht mehr missbraucht werden.</p> <p>Durch eine Überwachung des Anbieterzugriffs sorgen Sie dafür, dass die Anbieter nur auf notwendige Systeme und nur innerhalb der genehmigten Zeiträume zugreifen.</p>
<p><b>8.1.6</b> Begrenzen der wiederholten Zugriffsversuche durch Sperren der Benutzer-ID nach spätestens sechs Versuchen.</p>	<p><b>8.1.6.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.</p>	<p>Ohne implementierte Mechanismen für Kontosperrungen kann ein Angreifer fortwährend versuchen, ein Kennwort über manuelle oder automatisierte Tools zu erraten (z. B. Kennwort-Cracking-Tools), bis er Erfolg hat und sich Zugriff</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p><b>8.1.6.b Zusätzliches Testverfahren nur für die Beurteilung von Dienstleistern:</b> Vergewissern Sie sich durch die Prüfung interner Prozesse und Kunden-/Benutzerdokumente sowie durch die Beobachtung der implementierten Prozesse, ob Konten von Nichtverbraucherbenutzern nach spätestens sechs ungültigen Anmeldeversuchen gesperrt werden.</p>	<p>auf das Konto eines Benutzers verschafft.</p> <p><b>Hinweis:</b> Das Testverfahren 8.1.6.b ist ein zusätzliches Verfahren, das nur dann Anwendung findet, wenn es sich bei der zu bewertenden Einheit um einen Dienstleister handelt.</p>
<p><b>8.1.7</b> Festlegen einer Aussperrdauer von mindestens 30 Minuten, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann.</p>	<p><b>8.1.7</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Systemkonfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass eine mindestens 30-minütige Aussperrdauer gilt, in der das Konto nur durch den Administrator zurückgesetzt werden kann.</p>	<p>Wenn ein Konto gesperrt wurde, weil eine Person versucht hat, ein Kennwort zu erraten, unterbinden Steuerungen zur Hinauszögerung der Reaktivierung dieser gesperrten Konten, dass ein Angreifer weiter versucht, das Kennwort zu erraten (während eines Zeitraums von mindestens 30 Minuten können sie keine weiteren Eingaben tätigen, bis das Konto erneut aktiviert wird.) Darüber hinaus kann der Administrator oder Helpdesk, sollte die erneute Aktivierung beantragt werden müssen, nachprüfen, ob die Reaktivierung tatsächlich vom Kontoinhaber beantragt wird.</p>
<p><b>8.1.8</b> Nach mehr als 15-minütiger Inaktivität müssen sich die Benutzer erneut authentifizieren und das Terminal oder die Sitzung reaktivieren.</p>	<p><b>8.1.8</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Systemkonfigurationseinstellungen daraufhin, ob die Sperre des Systems bzw. der Sitzung nach einer höchstens 15-minütigen Inaktivitätszeit eintritt.</p>	<p>Wenn sich ein Benutzer von seinem Rechner mit Zugriff auf wichtige Systemkomponenten oder Karteninhaberdaten entfernt, kann der Rechner von anderen in Abwesenheit des Benutzers dazu verwendet werden, sich unbefugten Zugriff auf dessen Konto zu verschaffen und/oder es missbräuchlich einzusetzen.</p> <p>Die erneute Authentifizierung kann entweder auf Systemebene (damit alle auf diesem Rechner ausgeführten Sitzungen geschützt sind) oder auf Anwendungsebene erfolgen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>8.2</b> Neben einer eindeutigen ID muss mindestens eine der folgenden Methoden zur Authentifizierung sämtlicher Benutzer zum Einsatz kommen, damit das Benutzerauthentifizierungsmanagement für Nichtverbraucherbenutzer und -Administratoren auf allen Systemkomponenten ordnungsgemäß verläuft:</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 oder -satz) für den Zugriff auf die CDE authentifiziert haben:</p> <ul style="list-style-type: none"> <li>• Untersuchen Sie Dokumente, aus denen hervorgeht, welche Authentifizierungsmethode(n) verwendet wurde(n).</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>	<p>Wenn diese Authentifizierungsmethoden zusammen mit eindeutigen Benutzer-IDs eingesetzt werden, sind die Benutzer-IDs besser vor Angriffen geschützt, da der Angreifer sowohl die eindeutige Benutzer-ID als auch das Kennwort (oder andere verwendete Authentifizierungselemente) kennen muss. Solange ein digitales Zertifikat für einen bestimmten Benutzer nur einmalig vergeben wird, ist es eine gute Option für eine Authentifizierung des Typs „Etwas, das Sie haben“.</p> <p>Da der erste Schritt eines Angreifers zur Beschädigung eines Systems in der Ausnutzung schwacher oder nicht vorhandener Kennwörter liegt, ist es von großer Bedeutung, zuverlässige Verfahren zur Authentifizierungsverwaltung zu implementieren.</p>
<p><b>8.2.1</b> Nicht entschlüsselbare Übertragung und Speicherung von Kennwörtern und -sätzen auf sämtlichen Systemkomponenten unter Verwendung einer sicheren Verschlüsselung.</p>	<p><b>8.2.1.a</b> Überprüfen Sie die Dokumentation und die Einstellungen der Systemkonfiguration, und prüfen Sie, ob alle Kennwörter bei jeder Übertragung und Speicherung mithilfe starker Kryptographie geschützt werden.</p> <p><b>8.2.1.b</b> Testen Sie stichprobenartig die Kennwortdateien von Systemkomponenten auf die Verschlüsselung von Kennwörtern bei der Speicherung.</p> <p><b>8.2.1.c</b> Testen Sie stichprobenartig die Datenübertragungen bei Systemkomponenten auf die Verschlüsselung von Kennwörtern.</p> <p><b>8.2.1.d <i>Zusätzliches Testverfahren nur für die Beurteilung von Dienstleistern:</i></b> Vergewissern Sie sich in den Kennwortdateien, dass die gespeicherten Nichtverbraucher-Kundenkennwörter nicht lesbar sind.</p> <p><b>8.2.1.e <i>Zusätzliches Testverfahren nur für die Beurteilung von Dienstleistern:</i></b> Vergewissern Sie sich bei Datenübertragungen, dass die Kundenkennwörter von Nichtverbrauchern während der Übertragung nicht lesbar sind.</p>	<p>Viele Netzwerkgeräte und -anwendungen übertragen unverschlüsselte und lesbare Kennwörter über das Netzwerk und/oder speichern Kennwörter unverschlüsselt. Ein Angreifer kann leicht die unverschlüsselten Kennwörter während der Übertragung mithilfe eines „Sniffers“ abfangen oder direkt auf die unverschlüsselte Kennwörter in Dateien zugreifen und sich mithilfe dieser Daten unbefugten Zugriff verschaffen.</p> <p><b>Hinweis:</b> Die Testverfahren 8.2.1.d und 8.2.1.e sind zusätzliche Verfahren, die nur dann Anwendung finden, wenn es sich bei der zu bewertenden Einheit um einen Dienstleister handelt.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>8.2.2</b> Vor der Änderung von Authentifizierungsdaten muss die Benutzeridentität geprüft werden – beispielsweise beim Zurücksetzen von Kennwörtern, bei der Bereitstellung neuer Tokens oder bei der Erstellung neuer Schlüssel.</p>	<p><b>8.2.2</b> Untersuchen Sie die Authentifizierungsverfahren zur Änderung von Authentifizierungsdaten, und beobachten Sie das Sicherheitspersonal. Vergewissern Sie sich dabei, dass bei Benutzeranforderungen zum Zurücksetzen des Kennworts, die telefonisch, per E-Mail oder über das Internet bzw. auf anderem nicht-persönlichen Weg eingehen, die Identität des Benutzers vor der Änderung der Authentifizierungsdaten überprüft wird.</p>	<p>Viele Angreifer bedienen sich „Social Engineering“-Techniken,— zum Beispiel, indem sie den Helpdesk kontaktieren und sich als der entsprechende Benutzer ausgeben – um ein Kennwort zu ändern, damit sie einen bestimmten Benutzernamen verwenden können. Erwägen Sie den Einsatz von Sicherheitsfragen, die ausschließlich der jeweilige Benutzer beantworten kann, damit Administratoren den Benutzer eindeutig identifizieren können, bevor sie sein Kennwort zurücksetzen oder ändern.</p>
<p><b>8.2.3</b> Kennwörter/Kennsätze müssen die folgenden Anforderungen erfüllen:</p> <ul style="list-style-type: none"> <li>• Die Mindestlänge beträgt sieben Zeichen.</li> <li>• Es müssen sowohl Ziffern als auch Buchstaben verwendet werden.</li> </ul> <p>Alternativ müssen die Komplexität und Stärke eines Kennworts/ Kennsatzes mindestens den oben angegebenen Parametern entsprechen.</p>	<p><b>8.2.3a</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Parameter für Kennwörter/Kennsätze so eingestellt sind, dass mindestens die folgende Kennwortstärke/-komplexität erforderlich ist:</p> <ul style="list-style-type: none"> <li>• Die Mindestlänge beträgt sieben Zeichen.</li> <li>• Es müssen sowohl Ziffern als auch Buchstaben verwendet werden.</li> </ul> <p><b>8.2.3.b <i>Zusätzliches Testverfahren nur für die Beurteilung von Dienstleistern:</i></b> Überprüfen Sie in internen Prozessen und in der Kunden-/Benutzerdokumentation, ob die folgenden Mindestanforderungen an die Stärke/Komplexität von Kennwörtern/Kennsätzen für Nichtverbraucherbenutzer gelten:</p> <ul style="list-style-type: none"> <li>• Die Mindestlänge beträgt sieben Zeichen.</li> <li>• Es müssen sowohl Ziffern als auch Buchstaben verwendet werden.</li> </ul>	<p>Starke Kennwörter/Kennsätze sind die erste Verteidigungslinie eines Netzwerks, da Angreifer oft zunächst versuchen, Konten mit schwachen oder nicht vorhandenen Kennwörtern ausfindig zu machen. Wenn Kennwörter kurz oder leicht zu erraten sind, ist es für einen Angreifer relativ einfach, diese schwachen Konten zu finden und unter dem Deckmantel einer gültigen Benutzer-ID ein Netzwerk zu beschädigen.</p> <p>Diese Anforderung legt fest, dass die Mindestlänge für Kennwörter/ Kennsätze sieben Zeichen ist, und dass sowohl Ziffern als auch Buchstaben verwendet werden müssen. Wenn diese Mindestanforderung aufgrund technischer Beschränkungen nicht erfüllt werden kann, können Einheiten zur Evaluierung der Alternative auf „gleichwertige Stärke“ setzen. Informationen zur Variabilität und Äquivalenz der Kennwortstärke (auch als Entropie bezeichnet) für Kennwörter/Kennsätze verschiedener Formate, finden Sie in den Branchenstandards (z. B. die aktuelle Version des NIST SP 800-63.)</p> <p><b>Hinweis:</b> Das Testverfahren 8.2.3.b ist ein zusätzliches Verfahren, das nur dann Anwendung findet, wenn es sich bei der zu bewertenden Einheit um einen Dienstleister handelt.</p>
<p><b>8.2.4</b> Änderung der Benutzerkennwörter/-sätze mindestens</p>	<p><b>8.2.4.a</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Parameter für Kennwörter/Kennsätze so</p>	<p>Wenn Kennwörter/Kennsätze über einen langen Zeitraum hinweg unverändert gültig sind, haben Angreifer länger Zeit, das Kennwort bzw. den</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
einmal alle 90 Tage.	<p>eingestellt sind, dass die Benutzer mindestens einmal alle 90 Tage ihr Kennwort ändern müssen.</p> <p><b>8.2.4.b Zusätzliches Testverfahren nur für die Beurteilung von Dienstleistern:</b> Überprüfen Sie interne Prozesse und die Kunden-/Benutzerdokumentation auf folgende Punkte:</p> <ul style="list-style-type: none"> <li>• Kennwörter/Kennsätze von Nichtverbraucherbenutzern müssen regelmäßig geändert werden; und</li> <li>• Nichtverbraucherbenutzer erhalten Hinweise dazu, wann und unter welchen Umständen Kennwörter/Kennsätze geändert werden müssen.</li> </ul>	<p>Kennsatz herauszufinden.</p> <p><b>Hinweis:</b> Das Testverfahren 8.2.4.b ist ein zusätzliches Verfahren, das nur dann Anwendung findet, wenn es sich bei der zu bewertenden Einheit um einen Dienstleister handelt.</p>
<p><b>8.2.5</b> Neue Kennwörter/Kennsätze müssen sich von den letzten vier Kennwörtern/Kennsätzen unterscheiden.</p>	<p><b>8.2.5.a</b> Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass sich ein neues Kennwort/Kennsatz von den letzten vier Kennwörtern/Kennsätzen unterscheiden muss.</p> <p><b>8.2.5.b Zusätzliches Testverfahren nur für die Beurteilung von Dienstleistern:</b> Vergewissern Sie sich in internen Prozessen und der Kunden-/Benutzerdokumentation, dass sich neue Kennwörter/Kennsätze von Nichtverbraucherbenutzern von den letzten vier Kennwörtern unterscheiden müssen.</p>	<p>Wenn der Kennwortverlauf nicht aufgezeichnet wird, sinkt die Wirksamkeit der erzwungenen Kennwortänderungen, da alte Kennwörter immer wieder neu verwendet werden können. Wenn Kennwörter über einen bestimmten Zeitraum hinweg nicht wiederverwendet werden dürfen, sinkt die Wahrscheinlichkeit, dass Kennwörter, die erraten oder mithilfe der Brute-Force-Methode ermittelt wurden, in der Zukunft wiederverwendet werden.</p> <p><b>Hinweis:</b> Das Testverfahren 8.2.5.b ist ein zusätzliches Verfahren, das nur dann Anwendung findet, wenn es sich bei der zu bewertenden Einheit um einen Dienstleister handelt.</p>
<p><b>8.2.6</b> Festlegen von Kennwörtern/Kennsätzen für die erste Verwendung bzw. nach dem Zurücksetzen des Kennworts auf einen eindeutigen Wert für jeden Benutzer, der sofort nach der ersten Verwendung geändert werden muss.</p>	<p><b>8.2.6</b> Vergewissern Sie sich bei einer Untersuchung des Kennwortverfahrens und durch die Beobachtung des Sicherheitspersonals, dass Kennwörter/Kennsätze neuer Benutzer für die erste Verwendung und zurückgesetzte Kennwörter/Kennsätze für vorhandene Benutzer auf einen eindeutigen Wert gesetzt und nach der ersten Nutzung geändert werden.</p>	<p>Wenn für jeden neuen Benutzer dasselbe Kennwort verwendet wird, könnte es einem internen Benutzer, einem früheren Mitarbeiter oder einem Angreifer bekannt sein bzw. von diesem in Erfahrung gebracht und zum Zugriff auf Konten eingesetzt werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>8.3</b> Sichern Sie alle Nichtkonsolen-Verwaltungszugriffe und Fernzugriffe auf das CDE durch Multi-Faktor-Authentifizierung.</p> <p><i><b>Hinweis:</b> Bei der Multi-Faktor-Authentifizierung müssen mindestens 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 Multi-Faktor-Authentifizierung.</i></p>		<p>Die Multi-Faktor-Authentifizierung erfordert, dass mindestens zwei voneinander getrennte Formen der Authentifizierung (beschrieben in Anforderung 8.2) vorgewiesen werden, bevor ein Zugriff gestattet wird.</p> <p>Die Multi-Faktor-Authentifizierung bietet zusätzliche Gewissheit über die Identität der Person, die versucht Zugriff zu erhalten. Bei der Multi-Faktor-Authentifizierung müsste ein Angreifer mindestens zwei verschiedene Mechanismen zur Authentifizierung kompromittieren, was die Schwierigkeit einer Kompromittierung erhöht und das Risiko dadurch verringert.</p> <p>Eine Multi-Faktor-Authentifizierung ist sowohl auf System- und Anwendungsebene nicht für eine bestimmte Systemkomponente erforderlich. Die Multi-Faktor-Authentifizierung kann entweder bei Authentifizierung im bestimmten Netzwerk oder der Systemkomponente durchgeführt werden.</p> <p>Beispiele für Technologien mit mehreren Faktoren sind unter anderem der Remote-Authentifizierungs- und Einwähldienst (RADIUS) mit Tokens; Terminal Access Controller Access Control System (TACACS) mit Tokens und andere Technologien, die eine Multi-Faktor-Authentifizierung ermöglichen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>8.3.1</b> Machen Sie die Multi-Faktor-Authentifizierung zum festen Bestandteil für alle Nichtkonsolen-Zugriffe auf das CDE durch Mitarbeiter mit Verwaltungszugriff.</p> <p><i>Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</i></p>	<p><b>8.3.1.a</b> Vergewissern Sie sich falls zutreffend durch Untersuchen der Netzwerk- und/oder Systemkonfigurationen, dass die Multi-Faktor-Authentifizierung für alle Nichtkonsolen-Verwaltungszugriffe auf das CDE erforderlich ist.</p> <p><b>8.3.1.b</b> Beobachten Sie stichprobenartig, wie sich die Verwaltungsmitarbeiter im CDE einloggen, und überprüfen Sie, ob hierfür mindestens zwei der drei Authentifizierungsmethoden verwendet werden.</p>	<p>Diese Anforderung gilt für alle Mitarbeiter mit Verwaltungszugriff auf das CDE. Diese Anforderung gilt ausschließlich für Mitarbeiter mit Verwaltungszugriff und nur für Nichtkonsolen-Zugriff auf das CDE; sie gilt nicht für Anwendungs- oder Systemkonten, die automatisierte Funktionen durchführen.</p> <p>Falls das CDE von der Einheit nicht durch Segmentierung vom Rest ihres Netzwerks isoliert wird, könnte ein Administrator die Multi-Faktor-Authentifizierung entweder zum Anmelden im CDE Netzwerk oder in einem System verwenden.</p> <p>Wenn das CDE vom Rest des Netzwerks der Einheit abgeschnitten ist, müsste ein Administrator die Multi-Faktor-Authentifizierung verwenden, um sich von einem nicht-CDE Netzwerk aus mit einem CDE-System zu verbinden. Multi-Faktor-Authentifizierung kann auf Netzwerk- oder auf System-/Anwendungsebene implementiert werden; es muss nicht beides sein. Wenn der Administrator MFA bei der Anmeldung in das CDE-Netzwerk verwendet, muss er zur Anmeldung an einem bestimmten System oder Anwendung innerhalb des CDE keine MFA mehr verwenden.</p>
<p><b>8.3.2</b> Integrieren Sie die Multi-Faktor-Authentifizierung als festen Bestandteil bei allen Fernzugriffen auf das Netzwerk durch interne Mitarbeiter (Benutzer und Administratoren) und Dritte von außerhalb des Netzwerkes (einschließlich Anbieterzugriff zu Support- oder Wartungszwecken).</p>	<p><b>8.3.2.a</b> Vergewissern Sie sich bei einer Untersuchung der Konfigurationen von Servern und Systemen für den Remote-Zugriff, dass die Multi-Faktor-Authentifizierung für folgende Fälle erforderlich ist:</p> <ul style="list-style-type: none"> <li>• Alle Remote-Zugriffe durch Mitarbeiter, sowohl Anwender, als auch Administratoren, und</li> <li>• Sämtlichen Remote-Zugriff von Dritten/Anbietern (einschließlich des Zugriffs auf Anwendungen und Systemkomponenten zu Support- und Wartungszwecken).</li> </ul> <p><b>8.3.2.b</b> Beobachten Sie stichprobenartig, wie die Mitarbeiter (z. B. Benutzer und Administratoren) eine Remote-Verbindung zum Netzwerk herstellen, und überprüfen Sie, ob hierfür mindestens zwei der drei Authentifizierungsmethoden verwendet werden.</p>	<p>Diese Anforderung gilt für Mitarbeiter (allgemeine Benutzer, Administratoren und Anbieter zu Support- und Wartungszwecken), die einen Remote-Zugriff auf das Netzwerk besitzen und bei denen über diesen Remote-Zugriff auch Zugang zur CDE besteht. Wenn per Remote-Zugriff das Netzwerk einer Einheit mit angemessener Segmentierung aufgerufen wird, können diese Remote-Benutzer nicht auf die CDE zugreifen oder diese gefährden. Folglich wäre für ein solches Netzwerk keine Multi-Faktor-Authentifizierung erforderlich. Nichtsdestotrotz ist eine Multi-Faktor-Authentifizierung für alle Remote-Zugriffe auf Netzwerke mit Zugang auf die Karteninhaberdaten-Umgebung erforderlich und empfehlenswert für alle</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>8.4</b> Dokumentation und Weitergabe der Richtlinien und Verfahren zur Authentifizierung an alle Benutzer unter Einschluss der folgenden Informationen:</p> <ul style="list-style-type: none"> <li>• Hinweise zur Auswahl starker Authentifizierungsinformationen</li> <li>• Hinweise zum Schutz der Authentifizierungsinformationen durch die Benutzer</li> <li>• Anweisungen zur Vermeidung wiederverwendeter Kennwörter</li> <li>• Anweisungen zur Änderung von Kennwörtern beim Verdacht einer Gefährdung</li> </ul>	<p><b>8.4.a</b> Vergewissern Sie sich durch eine Überprüfung der Verfahren sowie durch eine Befragung des Personals, dass die Verfahren und Richtlinien zur Authentifizierung an alle Benutzer verteilt werden.</p> <p><b>8.4.b</b> Vergewissern Sie sich, dass die an die Benutzer weitergegebenen Verfahren und Richtlinien zur Authentifizierung folgende Punkte enthalten:</p> <ul style="list-style-type: none"> <li>• Hinweise zur Auswahl starker Authentifizierungsinformationen</li> <li>• Hinweise zum Schutz der Authentifizierungsinformationen durch die Benutzer</li> <li>• Anweisungen zur Vermeidung wiederverwendeter Kennwörter</li> <li>• Anweisungen zur Änderung von Kennwörtern beim Verdacht einer Gefährdung</li> </ul> <p><b>8.4.c</b> Befragen Sie stichprobenartig einige Benutzer nach ihren Kenntnissen der Verfahren und Richtlinien zur Authentifizierung.</p>	<p>Remote-Zugriffe auf die Netzwerke der Einheit.</p> <p>Durch die Mitteilung von Verfahren und Richtlinien für Kennwörter/ die Authentifizierung an alle Benutzer sind diese in der Lage, die Richtlinien besser zu verstehen und sich an diese zu halten.</p> <p>Hinweise zur Auswahl starker Kennwörter können beispielsweise Vorschläge zur Festlegung eines schwer zu erratenden Kennworts umfassen, das keine Wörter aus dem Wörterbuch und keine Informationen über den Benutzer (wie etwa die Benutzer-ID, Namen von Familienangehörigen, Geburtsdaten usw.) enthält. Hinweise zum Schutz der Authentifizierungsinformationen können beispielsweise Vorschläge umfassen, Kennwörter nicht aufzuschreiben oder in unsicheren Dateien zu speichern und wachsam zu sein, dass keine Angreifer ihre Kennwörter ausnutzen (z. B. indem ein Mitarbeiter angerufen und nach seinem Kennwort gefragt wird, um ein vermeintliches Problem zu lösen).</p> <p>Indem die Benutzer angewiesen werden, ihr Kennwort zu ändern, sobald die Gefahr einer Sicherheitsverletzung besteht, kann verhindert werden, dass sich Angreifer mittels legitimer Kennwörter unbefugt Zugriff verschaffen.</p>
<p><b>8.5</b> Keine Verwendung von IDs und Kennwörtern für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder von anderen Authentifizierungsmethoden und Beachtung der folgenden Punkte:</p> <ul style="list-style-type: none"> <li>• Allgemeine Benutzer-IDs werden deaktiviert oder entfernt.</li> <li>• Es gibt keine gemeinsamen Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen.</li> <li>• Es werden keine gemeinsamen und</li> </ul>	<p><b>8.5.a</b> Vergewissern Sie sich bei einer Stichprobe von Systemkomponenten, dass für die Benutzer-ID-Listen Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Allgemeine Benutzer-IDs werden deaktiviert oder 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> <p><b>8.5.b</b> Vergewissern Sie sich in den Authentifizierungsrichtlinien und -verfahren, dass IDs und/oder Kennwörter für Gruppen bzw. mehrere Personen oder andere Authentifizierungsmethoden ausdrücklich untersagt sind.</p>	<p>Wenn mehrere Benutzer gemeinsam dieselben Authentifizierungsinformationen benutzen (z. B. Benutzerkonto und Kennwort), ist es nicht mehr möglich, Systemzugriffe und Aktivitäten hin zu einzelnen Personen zurückzuverfolgen. In diesem Fall kann eine Einheit nicht mehr Einzelne als Verantwortliche ausmachen und für ihre Aktionen zur Rechenschaft ziehen oder effektive Protokolle darüber zu führen, da die Aktion von jedem in der Gruppe, der die Authentifizierungsinformationen kennt, hätte durchgeführt werden können.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>allgemeinen Benutzer-IDs zur Administration von Systemkomponenten verwendet.</p>	<p><b>8.5.c</b> Vergewissern Sie sich durch Gespräche mit Systemadministratoren, dass selbst auf Anfrage keine Gruppen- bzw. gemeinsamen Kennwörter vergeben oder andere Authentifizierungsmethoden genutzt werden.</p>	
<p><b>8.5.1 Zusätzliche Anforderung nur für Dienstanbieter:</b> Dienstanbieter mit Remote-Zugriff auf Kundensysteme (z. B. für den Support von POS-Systemen oder -Servern) benötigen für jeden Kunden eindeutige Authentifizierungsinformationen (wie etwa ein Kennwort oder einen Kennsatz).</p> <p><i>Hinweis: Diese Anforderung gilt nicht für Anbieter von gemeinsam genutzten Hosting-Services, die auf ihre eigene Hosting-Umgebung, in der mehrere Kundenumgebungen gehostet werden, zugreifen möchten.</i></p>	<p><b>8.5.1 Zusätzliches Testverfahren nur für die Beurteilung von Dienstanbietern:</b> Vergewissern Sie sich durch die Untersuchung von Authentifizierungsrichtlinien und die Befragung von Mitarbeitern, dass für jeden Kundenzugriff andere Authentifizierungsinformationen verwendet werden.</p>	<p><b>Hinweis:</b> Diese Anforderung muss nur beachtet werden, wenn es sich bei der zu bewertenden Einheit um einen Dienstanbieter handelt.</p> <p>Um zu verhindern, dass mehrere Kunden durch die Verwendung der gleichen Anmeldeinformationen gefährdet werden, müssen Anbieter mit Konten für den Remote-Zugriff auf Kundenumgebungen unterschiedliche Authentifizierungsinformationen für die einzelnen Kunden verwenden.</p> <p>Dieser Anforderung kann auch mit Technologien, die bei jeder Verbindung eine eindeutige Komponente der Anmeldeinformationen bereitstellen (z. B. mittels eines Einmalkennworts), Genüge getan werden. Dies gilt etwa für die Multi-Faktor-Authentifizierung.</p>
<p><b>8.6</b> Bei Verwendung anderer Authentifizierungsmethoden (z. B. Tokens für die physische/logische Sicherheit, Smartcards, Zertifikate usw.) muss die folgende Zuweisung beachtet werden:</p> <ul style="list-style-type: none"> <li>Authentifizierungsinformationen müssen einem einzelnen Konto zugewiesen sein und dürfen nicht von mehreren Konten gemeinsam genutzt werden.</li> <li>Mit physischen und/oder logischen Kontrollen muss gewährleistet werden, dass der Zugriff nur über das Konto erfolgen kann, für das die Authentifizierungsinformationen gedacht sind.</li> </ul>	<p><b>8.6.a</b> Vergewissern Sie sich durch die Untersuchung von Authentifizierungsrichtlinien und -verfahren, dass die Verfahren zur Nutzung von Authentifizierungsmethoden, wie etwa Sicherheits-Tokens, Smartcards und Zertifikate, definiert sind und folgende Punkte umfassen:</p> <ul style="list-style-type: none"> <li>Authentifizierungsinformationen sind einem einzelnen Konto zugewiesen und werden nicht von mehreren Konten gemeinsam genutzt.</li> <li>Mit physischen und/oder logischen Kontrollen muss gewährleistet werden, dass der Zugriff nur über das Konto erfolgen kann, für das die Authentifizierungsinformationen gedacht sind.</li> </ul>	<p>Falls die Methoden zur Benutzerauthentifizierung, wie etwa Tokens, Smartcards und Zertifikate, von mehreren Konten genutzt werden können, lässt sich nicht mehr eindeutig feststellen, wer die Authentifizierungsmethode genutzt hat. Durch physische und/oder logische Kontrollen (wie etwa PIN, biometrische Daten oder Kennwörter) zur eindeutigen Identifizierung des Kontobenutzers wird verhindert, dass nicht autorisierte Benutzer über eine gemeinsam genutzte Authentifizierungsmethode Zugriff erhalten.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p><b>8.6.b</b> Vergewissern Sie sich durch eine Befragung des Sicherheitspersonals, dass die Authentifizierungsinformationen einem einzelnen Konto zugewiesen sind und nicht von mehreren Konten gemeinsam genutzt werden.</p>	
	<p><b>8.6.c</b> Vergewissern Sie sich durch eine Untersuchung der Einstellungen in der Systemkonfiguration und/oder der physischen Kontrollen, dass die Kontrollen implementiert sind und dass nur das gedachte Konto mit den Authentifizierungsinformationen Zugriff erlangt.</p>	
<p><b>8.7</b> Der gesamte Zugriff auf die Datenbank mit den Karteninhaberdaten (einschließlich des Zugriffs durch Anwendungen, Administratoren und alle anderen Benutzer) wird wie folgt beschränkt:</p> <ul style="list-style-type: none"> <li>• Sämtliche Zugriffe, Anfragen und Aktionen der Benutzer im Bezug auf die Datenbank erfolgen mittels programmierter Verfahren.</li> <li>• Nur Datenbankadministratoren können direkt auf die Datenbanken zugreifen und Abfragen durchführen.</li> <li>• Die Anwendungs-IDs für Datenbankanwendungen können nur von den Anwendungen (und nicht von Einzelbenutzern oder nicht zu den Anwendungen gehörenden Prozessen) verwendet werden.</li> </ul>	<p><b>8.7.a</b> Überprüfen Sie in den Konfigurationseinstellungen für Datenbank und Anwendungen, ob alle Benutzer vor dem Zugriff authentifiziert werden.</p> <p><b>8.7.b</b> Überprüfen Sie in den Konfigurationseinstellungen für Datenbank und Anwendungen, dass sämtliche Zugriffe, Anfragen und Aktionen der Benutzer im Bezug auf die Datenbank (z. B. Verschieben, Kopieren und Löschen) ausschließlich über programmierte Verfahren (z. B. gespeicherte Verfahren) erfolgen.</p> <p><b>8.7.c</b> Überprüfen Sie in den Zugriffskontrolleinstellungen für die Datenbank und die Konfigurationseinstellungen der Datenbankanwendung, ob der direkte Benutzerzugriff auf die oder Anfragen bezüglich der Datenbank ausschließlich Datenbankadministratoren vorbehalten ist.</p> <p><b>8.7.d</b> Vergewissern Sie sich bei den Zugriffskontrolleinstellungen für die Datenbank und den Konfigurationseinstellungen der Datenbankanwendung sowie den zugehörigen Anwendungs-IDs, dass die Anwendungs-IDs nur von den Anwendungen (und nicht von Einzelbenutzern oder anderen Prozessen) verwendet werden können.</p>	<p>Ohne eine Benutzerauthentifizierung für den Zugriff auf Datenbanken und Anwendungen erhöht sich das Risiko für unbefugte oder in böser Absicht getätigte Zugriffe. Darüber hinaus können diese Zugriffe nicht protokolliert werden, da sich der Benutzer nicht angemeldet hat und dem System folglich nicht bekannt ist. Auch der Zugriff auf Datenbanken sollte ausschließlich über programmierte Methoden gewährt werden (z. B. mittels gespeicherter Verfahren), anstatt durch einen direkten Zugriff auf die Datenbank durch Endbenutzer (mit Ausnahme von DBAs, die direkten Zugriff auf die Datenbank zur Erfüllung ihrer administrativen Aufgaben benötigen).</p>
<p><b>8.8</b> Sicherheitsrichtlinien und betriebliche Verfahren zur Identifizierung und Authentifizierung müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>	<p><b>8.8</b> Vergewissern Sie sich durch eine Überprüfung der Dokumentation und eine Befragung des Personals, dass für Sicherheitsrichtlinien und betriebliche Verfahren zur Identifizierung und Authentifizierung Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Sie sind dokumentiert,</li> <li>• werden verwendet und</li> </ul>	<p>Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren für ein dauerhaftes Management von Identifizierung und Authentifizierung kennen und befolgen.</p>

<b>PCI-DSS-Anforderungen</b>	<b>Prüfverfahren</b>	<b>Anweisung</b>
	<ul style="list-style-type: none"><li>• sind allen Beteiligten bekannt.</li></ul>	

### **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	Anweisung
<p><b>9.1</b> Verwenden angemessener Zugangskontrollen, um den physischen Zugriff auf Systeme in der CDE zu überwachen und zu beschränken.</p>	<p><b>9.1</b> Überprüfen Sie, ob für die einzelnen Computerräume, Rechenzentren und sonstigen Bereiche mit Systemen in der CDE physische Sicherheitskontrollen 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 in der Karteninhaberdaten-Umgebung abläuft, und überprüfen Sie, ob die Sperre zur Verhinderung der unbefugten Nutzung funktioniert.</li> </ul>	<p>Ohne physische Zugriffskontrollen wie Ausweissysteme und Türkontrollen können sich Unbefugte leicht Zugang zu Ihrer Einrichtung verschaffen und wichtige Systeme stören sowie Karteninhaberdaten entwenden, deaktivieren oder zerstören.</p> <p>Eine Sperre der Konsolen-Anmeldebildschirme verhindert, dass sich unbefugte Personen Zugriff auf vertrauliche Informationen verschaffen, die Systemkonfigurationen verändern, Sicherheitsrisiken in das System einschleusen oder Datensätze zerstören.</p>
<p><b>9.1.1</b> Überwachen des Zugangs zu zugangsbeschränkten Bereichen entweder mithilfe von Videokameras</p>	<p><b>9.1.1.a</b> Überprüfen Sie, ob der Zugang zu zugangsbeschränkten Bereichen entweder mithilfe von Videokameras oder Kontrollsystemen (oder beidem) überwacht wird.</p>	<p>Wenn Verletzungen der physischen Integrität untersucht werden, können diese Kontrollen dabei helfen, jene Personen ausfindig zu machen, die direkt</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>oder Kontrollsystemen (oder beidem). Überprüfen der gesammelten Daten und Korrelation mit anderen Daten. Speichern der Daten mindestens drei Monate lang, wenn dies gesetzlich zulässig ist.</p> <p><b>Hinweis:</b> „Sensible 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 öffentlichen Bereiche, in denen lediglich POS-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).</p>	<p><b>9.1.1.b</b> Überprüfen Sie, ob entweder Videokameras oder Kontrollsysteme (oder beide) vor Manipulation oder Deaktivierung geschützt sind.</p>	<p>auf diese zugangsbeschränkten Bereiche zugreifen, und festzustellen, wann sie auf die Bereiche zugegriffen und sie wieder verlassen haben.</p> <p>Kriminelle Angreifer, die versuchen, Zugang zu zugangsbeschränkten Bereichen zu erhalten, versuchen häufig, die Überwachungskontrollen zu deaktivieren oder zu umgehen. Um eine Manipulation an diesen Kontrollen zu verhindern, könnten Videokameras an einem unzugänglichen Ort installiert oder ihrerseits überwacht werden. Ebenso können Zugriffskontrollsysteme überwacht oder mit physischen Schutzvorrichtungen versehen werden, damit sie von Angreifern nicht beschädigt oder deaktiviert werden können.</p> <p style="text-align: right;"><i>(Fortsetzung auf der nächsten Seite)</i></p>
	<p><b>9.1.1.c</b> Überprüfen Sie, ob die Daten von Videokameras und/oder Kontrollsystemen überwacht werden und ob diese mindestens drei Monate lang gespeichert werden.</p>	<p>Solche zugangsbeschränkten Bereiche sind beispielsweise Serverräume für Unternehmensdatenbanken, Back-Office-Räume von Einzelhandelsgeschäften, in denen Karteninhaberdaten gespeichert werden, sowie Speichersysteme für große Mengen von Karteninhaberdaten. In jeder Organisation sollten zugangsbeschränkte Bereiche festgelegt werden, damit die angemessenen physischen Kontrollen implementiert werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>9.1.2</b> Implementierung physischer und/oder logischer Kontrollen zur Beschränkung des Zugriffs auf öffentlich zugängliche Netzwerkbuchsen.</p> <p><i>Beispielsweise sollte die Möglichkeit bestehen, Netzwerkbuchsen in für Besucher zugänglichen Bereichen zu deaktivieren und nur dann zu aktivieren, wenn der Netzwerkzugriff ausdrücklich zugelassen ist. Alternativ können auch Prozesse implementiert werden, mit denen Besucher jederzeit in Bereiche mit aktiven Netzwerkbuchsen geleitet werden.</i></p>	<p><b>9.1.2</b> Überprüfen Sie durch die Befragung der zuständigen Mitarbeiter und durch die Beobachtung von Orten, an denen sich öffentlich zugängliche Netzwerkbuchsen befinden, ob der Zugriff auf diese Netzwerkbuchsen durch physische und/oder logische Kontrollen beschränkt ist.</p>	<p>Durch Einschränkung des Zugriffs auf Netzwerkbuchsen wird verhindert, dass Angreifer über leicht zugängliche Netzwerkbuchsen auf interne Netzwerkressourcen zugreifen.</p> <p>Logische und/oder physische Kontrollen müssen so ausgelegt sein, dass Personen oder Geräte ohne ausdrückliche Autorisierung keine Verbindung zum Netzwerk herstellen können.</p>
<p><b>9.1.3</b> Beschränkung des physischen Zugriffs auf WLAN-Zugriffspunkte, Gateways, Handgeräte, Netzwerk- und Kommunikations-hardware und Telekommunikationsleitungen.</p>	<p><b>9.1.3</b> Überprüfen Sie, ob der physische Zugriff auf WLAN-Zugriffspunkte, Gateways, Handgeräte, Netzwerk- und Kommunikations-hardware und Telekommunikationsleitungen entsprechend eingeschränkt ist.</p>	<p>Wenn beim Zugriff auf drahtlose Komponenten und Geräte nicht für Sicherheit gesorgt wird, sind böswillige Benutzer unter Umständen in der Lage, mit unbeaufsichtigten Drahtlosgeräten Ihres Unternehmens auf Ihre Netzwerkressourcen zuzugreifen oder sogar eigene Geräte an Ihr drahtloses Netzwerk anzuschließen und sich unerlaubten Zugriff zu verschaffen. Darüber hinaus kann durch die Sicherung von Netzwerk- und Kommunikations-hardware verhindert werden, dass böswillige Benutzer den Netzwerkdatenverkehr abfangen oder ihre eigenen Geräte an Ihre kabelgebundenen Netzwerkressourcen anschließen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>9.2</b> Entwicklung von Verfahren mit den folgenden Elementen zur leichteren Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern:</p> <ul style="list-style-type: none"> <li>• Identifizierung von Besuchern und Mitarbeitern vor Ort (z. B. durch Vergabe von Ausweisen)</li> <li>• Änderungen bei den Zugangs- bzw. Zugriffsanforderungen</li> <li>• Rücknahme bzw. Beendigung der Identifizierung von Vor-Ort-Mitarbeitern und Besuchern (z. B. mittels Ausweis) bei Ablauf des Status</li> </ul>	<p><b>9.2.a</b> Prüfen Sie in den dokumentierten Prozessen, ob Verfahren zur Identifizierung und zur Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern definiert sind.</p> <ul style="list-style-type: none"> <li>• Die Verfahren müssen folgende Anforderungen erfüllen:</li> <li>• Identifizierung von Besuchern und Mitarbeitern vor Ort (z. B. durch Vergabe von Ausweisen),</li> <li>• Zugangs- bzw. Zugriffsanforderungen und</li> <li>• Rücknahme der Identifizierung (z. B. mittels Ausweis) von ehemaligen Vor-Ort-Mitarbeitern und Besuchern, deren Besuchstatus abgelaufen ist</li> </ul> <p><b>9.2.b</b> Untersuchen Sie die Methoden zur Identifizierung (wie ID-Ausweise) und prüfen Sie die Verfahren zur Identifizierung und zur Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern daraufhin, ob folgende Punkte erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Die Besucher werden eindeutig identifiziert.</li> <li>• Die Besucher lassen sich leicht von den Mitarbeitern vor Ort unterscheiden.</li> </ul> <p><b>9.2.c</b> Überprüfen Sie, ob der Zugriff auf den Identifizierungsprozess (z. B. ein Ausweissystem) befugtem Personal vorbehalten ist.</p>	<p>Indem Sie zugelassene Besucher anhand beispielsweise eines Ausweises kennzeichnen, damit sie leicht von den Mitarbeitern vor Ort unterschieden werden können, vermeiden Sie, dass unbefugten Besuchern Zugang auf Bereiche mit Karteninhaberdaten gewährt wird.</p>
<p><b>9.3</b> Kontrolle des Zugangs von Vor-Ort-Personal zu den zugangsbeschränkten Bereichen gemäß den folgenden Anforderungen:</p> <ul style="list-style-type: none"> <li>• Der Zugang muss autorisiert sein und auf der jeweiligen tätigkeitsbezogenen Aufgabe basieren.</li> <li>• Die Zugangsberechtigung wird sofort nach dem Ende der Beschäftigung zurückgenommen, und sämtliche physischen Zugangssysteme wie Schlüssel, Karten usw. werden zurückgegeben oder deaktiviert.</li> </ul>	<p><b>9.3.a</b> Vergewissern Sie sich für eine Stichprobe der Vor-Ort-Mitarbeiter mit Zugriff auf zugangsbeschränkte Bereiche durch die Befragung des zuständigen Personals und die Prüfung von Zugriffskontrolllisten, dass Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Der Zugriff auf den sensiblen Bereich ist autorisiert.</li> <li>• Der Zugriff ist für die jeweiligen tätigkeitsbezogenen Aufgaben erforderlich.</li> </ul> <p><b>9.3.b</b> Überprüfen Sie beim Zugriff des Personals auf zugangsbeschränkte Bereiche, ob alle Mitarbeiter autorisiert werden, bevor ihnen der Zugriff gewährt wird.</p> <p><b>9.3.c</b> Vergewissern Sie sich stichprobenartig in den Zugriffskontrolllisten bei Mitarbeitern, deren Beschäftigung kürzlich endete, dass die Mitarbeiter nicht mehr physisch auf zugangsbeschränkte Bereiche zugreifen können.</p>	<p>Eine Kontrolle des physischen Zugriffs auf zugangsbeschränkte Bereiche sorgt dafür, dass nur autorisiertem Personal mit legitimen geschäftlichen Anforderungen Zugriff gewährt wird.</p> <p>Wenn Mitarbeiter das Unternehmen verlassen, müssen alle physischen Zugangssysteme sofort (schnellstmöglich) nach dem Ausscheiden zurückgegeben oder deaktiviert werden, damit diese Personen nach dem Beschäftigungsende nicht mehr physisch auf die zugangsbeschränkten Bereiche zugreifen können.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>9.4</b> Implementierung von Verfahren zur Identifizierung und Autorisierung von Besuchern.</p> <p>Die Verfahren müssen Folgendes umfassen:</p>	<p><b>9.4</b> Überprüfen Sie, ob die Autorisierungs- und Zugriffskontrollen für Benutzer wie folgt umgesetzt werden:</p>	<p>Besucherkontrollen sind von zentraler Bedeutung, um das Risiko zu reduzieren, dass sich unbefugte Personen in böser Absicht Zugang zu Einrichtungen (und unter Umständen auch Karteninhaberdaten) verschaffen.</p>
<p><b>9.4.1</b> Besucher müssen vor dem Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder gepflegt werden, autorisiert und innerhalb dieser Bereiche jederzeit begleitet werden.</p>	<p><b>9.4.1.a</b> Vergewissern Sie sich durch die Überprüfung von Verfahren und die Befragung von Mitarbeitern, dass Besucher vor dem Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder gepflegt werden, autorisiert und innerhalb dieser Bereiche jederzeit begleitet werden.</p> <p><b>9.4.1.b</b> Prüfen Sie ob Besucherausweise oder sonstige Mittel zur Identifizierung genutzt werden, damit kein unbeaufsichtigter Zugang zu Bereichen gewährt wird, in denen Karteninhaberdaten verarbeitet oder gepflegt werden.</p>	<p>Besucherkontrollen sorgen außerdem dafür, dass Besucher als Besucher zu erkennen sind, damit das Personal deren Aktivitäten überwachen kann, und dass ihre Zugangsberechtigung nur für die Länge des genehmigten Besuchs gültig ist.</p> <p>Wenn Sie dafür sorgen, dass Besucherausweise nach Ablauf des Besuchsstatus bzw. nach Ende des Besuchs zurückgegeben werden, können sich Angreifer nicht mit der ursprünglichen Berechtigung nachträglich Zugang zum Gebäude verschaffen.</p>
<p><b>9.4.2</b> Die Besucher werden identifiziert und mit einem Ausweis oder einer sonstigen Identifizierung versehen, mit der sie sich deutlich von den Vor-Ort-Mitarbeitern unterscheiden lassen.</p>	<p><b>9.4.2.a</b> Überprüfen Sie, ob Personen innerhalb der Einrichtung, Besucherausweise oder andere Identifizierungsmöglichkeiten nutzen und sich leicht vom Personal vor Ort unterscheiden lassen.</p> <p><b>9.4.2.b</b> Überprüfen Sie, ob die Besucherausweise eine begrenzte Gültigkeit haben.</p>	<p>Ein Besucherprotokoll, das Mindestinformationen über den Besucher dokumentiert, ist einfach und kostengünstig zu verwalten und hilft bei der Identifizierung des Zugangs zu einem Gebäude oder Raum sowie des potenziellen Zugriffs auf Karteninhaberdaten.</p>
<p><b>9.4.3</b> Die Besucher werden um Rückgabe des Ausweises bzw. der Identifizierung gebeten, wenn die Besucher die Einrichtung verlassen oder die Erlaubnis ausläuft.</p>	<p><b>9.4.3</b> Beobachten Sie, ob Besucher den Ausweis bzw. die sonstige Identifizierung beim Verlassen der Einrichtung bzw. beim Auslaufen der Erlaubnis zurückgeben müssen.</p>	
<p><b>9.4.4</b> Die Aktivität der Besucher in der Einrichtung und in Computerräumen und Rechenzentren, in denen Karteninhaberdaten gespeichert oder übertragen werden, muss in einem Besucherprotokoll festgehalten werden.</p> <p>Dokumentieren Sie den Namen des Besuchers, den Firmennamen und den Namen des Mitarbeiters vor Ort, der</p>	<p><b>9.4.4.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>9.4.4.b</b> Vergewissern Sie sich, dass das Protokoll folgende Informationen enthält:</p> <ul style="list-style-type: none"> <li>• Name des Besuchers</li> <li>• Unternehmen, das der Besucher vertritt</li> <li>• Mitarbeiter vor Ort, der dem Besucher Zugang gewährt hat</li> </ul>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>dem Besucher Zugang gewährt. Aufbewahren des Besucherprotokolls für die Dauer von mindestens drei Monaten, wenn dies gesetzlich zulässig ist.</p>	<p><b>9.4.4.c</b> Überprüfen Sie, ob das Protokoll mindestens drei Monate lang aufbewahrt wird.</p>	
<p><b>9.5</b> Stellen Sie die physische Sicherheit aller Medien sicher.</p>	<p><b>9.5</b> Überprüfen Sie, ob die Verfahren zum Schutz von Karteninhaberdaten Kontrollen zur physischen Sicherheit aller Medien (Computer, elektronische Wechselmedien sowie Quittungen, Berichte und Faxsendungen usw.) umfassen.</p>	<p>Kontrollen zum physischen Schutz von Medien sollen verhindern, dass Unbefugte auf Karteninhaberdaten auf beliebigen Medien zugreifen. Karteninhaberdaten sind durch unbefugte Zugriffe, unerlaubtes Kopieren oder Scannen gefährdet, wenn sie, während sie sich auf auswechselbaren oder tragbaren Datenträgern befinden, ausgedruckt oder auf einem Schreibtisch unbeaufsichtigt gelassen werden, nicht durch entsprechende Schutzmaßnahmen gesichert sind.</p>
<p><b>9.5.1</b> Aufbewahren von Sicherungskopien an einem sicheren Ort, vorzugsweise in einer anderen Einrichtung, wie z. B. an einem Alternativ- oder Backup-Standort oder bei einem kommerziellen Anbieter von Speicherkapazitäten. Überprüfen der Sicherheit dieses Standorts mindestens einmal pro Jahr.</p>	<p><b>9.5.1</b> Kontrollieren Sie, ob der für die Speicherung gewählte Standort mindestens einmal im Jahr auf die Sicherheit der dort aufbewahrten Sicherungskopien überprüft wird.</p> <p><b>9.6</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>Wenn Sicherungskopien von Karteninhaberdaten in einer nicht gesicherten Einrichtung gespeichert werden, können die Daten leicht verloren gehen oder in böser Absicht entwendet oder kopiert werden.</p> <p>Durch eine regelmäßige Prüfung des Speicherorts können ermittelte Sicherheitsrisiken frühzeitig angegangen und die potenziellen Risiken so gering wie möglich gehalten werden.</p>
<p><b>9.6</b> Durchführung strikter Kontrollen der internen bzw. externen Verteilung jeglicher Art von Medien, einschließlich der folgenden:</p>	<p><b>9.6.1</b> Überprüfen Sie, ob alle Medien klassifiziert sind, sodass das Gefährdungspotenzial der Daten bestimmt werden kann.</p>	<p>Entsprechende Verfahren und Prozesse helfen dabei, Karteninhaberdaten auf Datenträgern zu schützen, wenn sie an interne und/oder externe Nutzer verteilt werden. Ohne solche Verfahren können Daten abhanden kommen oder entwendet und für betrügerische Zwecke eingesetzt werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>9.6.1</b> Klassifizieren Sie die Medien, sodass das Gefährdungspotenzial der Daten bestimmt werden kann.</p>	<p><b>9.6.2.a</b> Vergewissern Sie sich durch die Befragung der Mitarbeiter und die Überprüfung von Unterlagen, dass ein Protokoll über alle Medien, die diese Einrichtung verlassen, geführt wird, und dass dieser Versand per sicherem Kurier oder mit einer anderen Liefermethode, die präzise nachverfolgt werden kann, erfolgt.</p>	<p>Die Medien müssen unbedingt so gekennzeichnet werden, dass ihre Klassifizierung leicht erkennbar ist. Nicht als vertraulich gekennzeichnete Medien werden unter Umständen nicht hinreichend geschützt oder können abhanden kommen oder gestohlen werden.</p> <p><b>Hinweis:</b> Das bedeutet nicht, dass die Medien als „Vertraulich“ gekennzeichnet sein müssen. Vielmehr geht es darum, dass das Unternehmen die Medien, auf denen sich vertrauliche Daten befinden, identifiziert und entsprechend schützt.</p>
<p><b>9.6.2</b> Versenden Sie die Medien über einen sicheren Kurier oder eine andere Liefermethode, die präzise nachverfolgt werden kann.</p>	<p><b>9.6.2.b</b> Überprüfen Sie bei aktuellen und an mehreren Tagen genommenen Stichproben aus den Protokollen zur Standortverfolgung von Medien, ob alle für die Nachverfolgung wichtigen Details protokolliert wurden.</p> <p><b>9.6.3</b> Wählen Sie eine aktuelle und an mehreren Tagen genommene Stichproben aus den Protokollen zur Standortverfolgung von Medien aus. Prüfen Sie anhand von Protokollen und Gesprächen mit dem verantwortlichen Personal, ob eine ordnungsgemäße Autorisierung durch das Management erfolgt, wenn Medien aus einem geschützten Bereich verschoben werden (auch dann, wenn die Medien an einzelne Personen weitergegeben werden).</p>	<p>Datenträger können abhanden kommen oder entwendet werden, wenn sie mit einer nicht nachverfolgbaren Methode wie etwa per Post gesendet werden. Wenn Unternehmen Medien mit Karteninhaberdaten per sicherem Kurier verschicken, sind sie mit deren Sendungsverfolgungssystemen über den Bestand und den Standort der Sendungen stets auf dem Laufenden.</p>
<p><b>9.6.3</b> Das Management muss den Transfer sämtlicher Medien aus einem geschützten Bereich genehmigen (insbesondere, wenn die Medien an einzelne Personen weitergegeben werden).</p>	<p><b>9.7</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>Wenn kein klarer Prozess festgelegt ist, nach dem sämtliche Medienbewegungen genehmigt werden müssen, sobald Medien aus dem geschützten Bereich verschoben werden, ist keine Nachverfolgung und kein angemessener Schutz möglich. Da auch der Standort unbekannt ist, sind Verlust und Diebstahl von Medien Tür und Tor geöffnet.</p>
<p><b>9.7</b> Strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien.</p>	<p><b>9.7.1</b> Überprüfen Sie im Medien-Inventurprotokoll, ob mindestens einmal pro Jahr eine Inventur der vorhandenen Medien stattfindet.</p>	<p>Ohne sorgfältige Inventurmethode und Speicherkontrollen können entwendete oder abhanden gekommene Daten auf unbestimmte Zeit</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>9.7.1</b> Ordnungsgemäße Verwaltung von Medieninventurlisten und Durchführung von mindestens einer Medieninventur im Jahr.</p>	<p><b>9.8</b> Prüfen Sie die Richtlinie zur regelmäßigen Vernichtung von Medien, und überprüfen Sie, ob diese Richtlinie für sämtliche Medien gilt und ob Anforderungen für die folgenden Punkte definiert sind:</p> <ul style="list-style-type: none"> <li>• Ausdrücke müssen der Aktenvernichtung zugeführt werden, damit nach allgemeinem Ermessen ausgeschlossen werden kann, dass die Einzelteile wieder zusammengefügt werden.</li> <li>• Container zur Aufbewahrung von zu vernichtendem Material müssen geschützt werden.</li> <li>• Karteninhaberdaten auf elektronischen Medien müssen nach Branchenstandards z. B. über Secure Wipes (sichere Lösungsverfahren) in einen Zustand versetzt werden, in dem sie nicht wiederherstellbar sind. Ansonsten können auch die Medien physisch unbrauchbar gemacht werden.</li> </ul>	<p>unbemerkt bleiben.</p> <p>Wenn keine Bestandsaufnahme der Datenträger durchgeführt wird, können entwendete oder abhanden gekommene Daten auf unbestimmte Zeit oder womöglich für immer unentdeckt bleiben.</p>
<p><b>9.8</b> Vernichtung von Medien, die nicht mehr zu geschäftlichen oder juristischen Zwecken benötigt werden, nach folgenden Maßgaben:</p>	<p><b>9.8.1.a</b> Überprüfen Sie durch die Befragung der Mitarbeiter oder die Untersuchung von Verfahrensweisen, ob Papiausdrucke vernichtet werden und nach allgemeinem Ermessen ausgeschlossen werden kann, dass diese Dokumente wiederhergestellt werden können.</p>	<p>Wenn Informationen auf Festplatten, tragbaren Speichermedien, CD/DVDs oder Papier vor deren Entsorgung nicht vernichtet werden, sind Angreifer in der Lage, die Informationen von den entsorgten Datenträgern wieder herzustellen und die Datensicherheit zu gefährden. Beispielsweise könnten böswillige Personen die unter dem Namen „Dumpster Diving“ bekannte Technik einsetzen, bei der in Abfalleimern nach passenden Informationen gesucht wird, um einen Angriff zu starten.</p>
<p><b>9.8.1</b> Papiausdrucke müssen in einer Form vernichtet werden, dass keine Karteninhaberdaten wiederhergestellt werden können. Container zur Aufbewahrung von zu vernichtendem Material müssen geschützt werden.</p>	<p><b>9.8.1.b</b> Überprüfen Sie, ob Container zur Aufbewahrung von Informationen, die vernichtet werden sollen, geschützt sind.</p>	<p>Der Schutz von Containern zur Aufbewahrung von zu vernichtenden Materialien verhindert ein Abgreifen vertraulicher Informationen aus den zur Vernichtung gesammelten Materialien. So kann zum Beispiel ein Container mit zu vernichtenden Akten durch ein Schloss geschützt werden, damit niemand auf den Inhalt zugreifen kann.</p> <p>Methoden zur sicheren Vernichtung elektronischer Datenträger sind unter anderem Wiping-Tools, die Entmagnetisierung oder die Zerstörung des Mediums an sich (wie etwa Festplatten-Degausser oder Shredder).</p>
	<p><b>9.8.2</b> Überprüfen Sie, ob die Karteninhaberdaten auf elektronischen Medien nach Branchenstandards für Secure Wipes (sichere Lösungsverfahren) unbrauchbar und nicht wiederherstellbar gemacht werden bzw. dass die Medien physisch unbrauchbar gemacht werden.</p>	
<p><b>9.8.2</b> Löschen von Karteninhaberdaten auf elektronischen Medien in einer Art und Weise, die eine Wiederherstellung der Daten unmöglich macht.</p>	<p><b>9.9</b> Überprüfen Sie, ob in den dokumentierten Richtlinien und Verfahren folgende Punkte enthalten sind:</p> <ul style="list-style-type: none"> <li>• Führen einer Geräteliste</li> <li>• Regelmäßige Prüfung der Geräte auf Manipulations- oder Austauschversuche</li> <li>• Förderung des Bewusstseins der Mitarbeiter für verdächtiges Verhalten und Melden der Manipulation bzw. des Austauschs von Geräten</li> </ul>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>9.9</b> Manipulations- und Austauschschutz von Geräten zur Erfassung von Zahlungskartendaten über eine direkte physische Interaktion mit der Karte.</p> <p><b>Hinweis:</b> Diese Anforderungen gelten für Kartenlesegeräte, die bei Transaktionen eingesetzt werden, bei denen die Karte am Point-of-Sale vorliegt und durch das Gerät gezogen oder in das Gerät eingesteckt werden muss. Diese Anforderung gilt nicht für Komponenten zur manuellen Eingabe wie Computertastaturen und POS-Ziffernblöcke.</p>	<p><b>9.9.1.a</b> Prüfen Sie, ob die Liste der Geräte folgende Informationen enthält:</p> <ul style="list-style-type: none"> <li>• Fabrikat und Modell des Geräts</li> <li>• Standort des Geräts (zum Beispiel die Adresse des Standorts oder der Einrichtung, an der sich das Gerät befindet)</li> <li>• Seriennummer des Geräts oder andere Informationen zur eindeutigen Identifizierung.</li> </ul>	<p>Kriminelle versuchen an Karteninhaberdaten zu gelangen, indem sie die Kartenlesegeräte und -Terminals entwenden und/oder manipulieren. So versuchen sie beispielsweise Geräte zu entwenden, um in Erfahrung zu bringen, wie sie am besten „geknackt“ werden. Häufig wird auch versucht, die richtigen Geräte durch falsche zu ersetzen und bei jedem Einstecken einer Zahlungskarte Informationen über die Karte abzurufen. Bisweilen wird auch versucht, außen an den Geräten zusätzliche Geräte anzubringen, um Zahlungskarteninformationen abzufangen. Die Informationen werden in diesem Fall doppelt erfasst: einmal vom zusätzlich angebrachten Gerät und ein weiteres Mal von der Gerätekomponente, die eigentlich hierfür vorgesehen ist. Diese als „Skimming“ bezeichnete Technik führt dazu, dass die Transaktionen weiterhin unterbrechungsfrei abgeschlossen werden können und gleichzeitig unbemerkt die Karteninformationen ausgelesen werden.</p> <p>Diese Anforderung wird für Komponenten zur manuellen Eingabe wie Computertastaturen und POS-Ziffernblöcke empfohlen, ist jedoch nicht zwingend vorgeschrieben.</p> <p>Zusätzliche bewährte Verfahren zur Vermeidung von Skimming-Angriffen finden Sie auf der PCI-SSC-Website.</p>
<p><b>9.9.1</b> Führen einer aktuellen Geräteliste. Die Liste muss folgende Punkte enthalten:</p> <ul style="list-style-type: none"> <li>• Fabrikat und Modell des Geräts</li> <li>• Standort des Geräts (zum Beispiel die Adresse des Standorts oder</li> </ul>	<p><b>9.9.1.b</b> Wählen Sie stichprobenartig einige Geräte aus der Liste aus, und überprüfen Sie, ob die Geräte- und Standortangaben in der Liste korrekt und aktuell sind.</p> <p><b>9.9.1.c</b> Fragen Sie die Mitarbeiter, ob die Geräteliste aktualisiert wird, sobald Geräte hinzugefügt, an einen anderen Standort gebracht oder außer Betrieb genommen werden usw.</p>	<p>Mit einer aktuellen Liste der Geräte behält ein Unternehmen die Übersicht darüber, wo sich die Geräte befinden müssten, und kann schnell ermitteln, ob ein Gerät fehlt oder verloren gegangen ist.</p> <p>Die Methode zum Führen einer Geräteliste kann automatisiert werden (z. B. in einem</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>der Einrichtung, an der sich das Gerät befindet)</p> <ul style="list-style-type: none"> <li>• Seriennummer des Geräts oder andere Informationen zur eindeutigen Identifizierung.</li> </ul>	<p><b>9.9.2.a</b> Prüfen Sie in den dokumentierten Verfahren, ob Prozesse für folgende Punkte festgelegt wurden:</p> <ul style="list-style-type: none"> <li>• Verfahren zur Untersuchung von Geräten</li> <li>• Häufigkeit der Untersuchungen</li> </ul>	<p>Gerätemanagementsystem) oder manuell durchgeführt werden (z. B. in elektronischen oder ausgedruckten Unterlagen dokumentiert). Bei mobilen Geräten kann bei der Standortangabe der Name des Mitarbeiters, dem das Gerät zugewiesen ist, angegeben werden.</p>
<p><b>9.9.2</b> Regelmäßige Untersuchung der Geräte auf Spuren von Manipulation (z. B. Anbringen von Skimming-Technik) oder Austausch (stimmen beispielsweise die Seriennummer oder andere Gerätemerkmale, oder wurde das Gerät durch ein anderes ausgetauscht?).</p> <p><b>Hinweis:</b> Anzeichen für eine Manipulation oder den Austausch von Geräten sind zum Beispiel unerwartete Anbauten oder Kabel, fehlende oder geänderte Sicherheitssiegel, beschädigte oder andersfarbige Gehäuse bzw. Änderungen bei der Seriennummer oder anderen externen Kennzeichen.</p>	<p><b>9.9.2.b</b> Klären Sie durch eine Befragung des zuständigen Personals und die Beobachtung der Untersuchungsprozesse Folgendes ab:</p> <ul style="list-style-type: none"> <li>• Kennen die Mitarbeiter die Verfahren zur Untersuchung von Geräten?</li> <li>• Werden sämtliche Geräte regelmäßig auf Manipulations- oder Austauschversuche geprüft?</li> </ul> <p><b>9.9.3.a</b> Überprüfen Sie, ob das Schulungsmaterial für die Mitarbeiter an POS-Standorten die folgenden Punkte umfasst:</p> <ul style="list-style-type: none"> <li>• Prüfung der Identität von Dritten, die vorgeben, Reparatur- oder Wartungsarbeiten am Gerät vorzunehmen (diese Prüfung muss erfolgen, bevor diesen Personen erlaubt wird, an den Geräten zu arbeiten)</li> <li>• Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe</li> <li>• Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen)</li> <li>• Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter)</li> </ul>	<p>Regelmäßige Untersuchungen von Geräten helfen Unternehmen dabei, schneller Manipulationen oder den Austausch eines Geräts zu erkennen und damit die potenziellen Auswirkungen des Einsatzes falscher Geräte so gering wie möglich zu halten.</p> <p>Die Art der Untersuchung ist geräteabhängig. So können zum Beispiel Fotos von erwiesenermaßen sicheren Geräten herangezogen werden, um den aktuellen mit dem ursprünglichen Zustand zu vergleichen. Es besteht auch die Möglichkeit, die Oberfläche des Geräts beispielsweise mit einer nur unter UV-Licht erkennbaren Markierung zu versehen, damit Manipulationen und ein Geräteaustausch offensichtlich werden. Kriminelle nehmen häufig das Gehäuse eines Geräts ab, um die Manipulation zu verbergen. Mit den genannten Methoden kann ein derartiges Vorgehen besser erkannt werden.</p> <p>Geräteanbieter verfügen unter Umständen über eigene Sicherheitshinweise und Leitlinien zur Frage, wie sich Manipulationen am Gerät erkennen lassen.</p> <p>Die Häufigkeit der Untersuchungen hängt von verschiedenen Faktoren ab – etwa, wo sich das Gerät befindet und ob es beaufsichtigt oder unbeaufsichtigt ist. Im öffentlichen Raum aufgestellte Geräte ohne Überwachung durch die Mitarbeiter des Unternehmens müssen unter Umständen häufiger untersucht werden als Geräte in geschützten Bereichen bzw. Geräte, die öffentlich zugänglich sind, aber überwacht werden. Wie häufig welche Art der Untersuchung durchgeführt wird, legt der Händler im jährlichen Risikobewertungsprozess fest.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>9.9.3</b> Personalschulungen zur Förderung des Bewusstseins im Hinblick auf Manipulations- oder Austauschversuche. Die Schulungen sollten Folgendes umfassen:</p> <ul style="list-style-type: none"> <li>• Prüfung der Identität von Dritten, die vorgeben, Reparatur- oder Wartungsarbeiten am Gerät vorzunehmen (diese Prüfung muss erfolgen, bevor diesen Personen erlaubt wird, an den Geräten zu arbeiten).</li> <li>• Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe.</li> <li>• Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen).</li> <li>• Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter).</li> </ul>	<p><b>9.9.3.b</b> Befragen Sie stichprobenartig einen Teil der Mitarbeiter an den POS-Standorten danach, ob sie geschult wurden und ob ihnen die Verfahren für folgende Punkte bewusst sind:</p> <ul style="list-style-type: none"> <li>• Prüfung der Identität von Dritten, die vorgeben, Reparatur- oder Wartungsarbeiten am Gerät vorzunehmen (diese Prüfung muss erfolgen, bevor diesen Personen erlaubt wird, an den Geräten zu arbeiten)</li> <li>• Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe</li> <li>• Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen)</li> <li>• Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter)</li> </ul> <p><b>9.10</b> Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des Zugangs zu Karteninhaberdaten Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Sie sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	<p>Kriminelle verschaffen sich häufig Zugang zu POS-Geräten, indem sie sich als autorisierte Wartungsmitarbeiter ausweisen. Sämtliche Dritte, die auf die Geräte zugreifen wollen, müssen stets verifiziert werden, bevor ihnen der Zugriff gewährt wird. So kann beispielsweise beim Management nachgefragt werden oder die Wartungsfirma telefonisch um Bestätigung gebeten werden. Viele Kriminelle versuchen, durch entsprechende Kleidung den Anschein der Legitimität zu erwecken (z. B. durch Arbeitskleidung und Werkzeugkoffer). Außerdem versuchen sie häufig, die Mitarbeiter mit sehr guten Orts- und Gerätekenntnissen zu überrumpeln. Aus diesem Grund ist es unbedingt erforderlich, die Verfahrensweisen jederzeit einzuhalten.</p> <p>Ein anderer Trick besteht darin, dass die Kriminellen ein „neues“ POS-System (Point-of-Sale) mit Anweisungen zum Austausch und zur Rücksendung des eigentlichen Systems an eine bestimmte Adresse versenden. Manchmal ist den Schreibern sogar das Porto zur Rücksendung beigelegt. Vor der Installation und dem geschäftlichen Einsatz von Geräten müssen die Mitarbeiter stets mit ihrem Manager oder den Zulieferern klären, ob es sich um ein legitimes Gerät aus einer vertrauenswürdigen Quelle handelt.</p>
<p><b>9.10</b> Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des physischen Zugangs zu Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>		<p>Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren zur Beschränkung des physischen Zugangs zu Karteninhaberdaten und CDE-Systemen kennen und dauerhaft befolgen.</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	Anweisung
<b>10.1</b> Implementierung von Audit-Trails zur Verknüpfung des gesamten Zugriffs auf Systemkomponenten mit den einzelnen Benutzern.	<b>10.1</b> Prüfen Sie durch Beobachtungen und durch Befragung des Systemadministrators folgende Punkte: <ul style="list-style-type: none"> <li>• Sind Audit-Trails für die Systemkomponenten vorhanden und aktiv?</li> <li>• Ist der Zugriff auf Systemkomponenten mit den einzelnen Benutzern verknüpft?</li> </ul>	Es ist wichtig, über einen Prozess oder ein System zu verfügen, bei dem der Benutzerzugriff mit den aufgerufenen Systemkomponenten verknüpft ist. Ein solches System generiert Audit-Protokolle und ermöglicht es, verdächtige Aktivitäten bis zu dem Benutzer zurückzuverfolgen, von dem diese ausgehen.
<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 Prüfprotokolleinstellungen Folgendes durch:	Indem Audit-Trails über verdächtige Aktivitäten erstellt werden, wird der Systemadministrator aufmerksam gemacht, es werden Daten an weitere Überwachungsmechanismen (wie etwa Eindringlingserfassungsmechanismen) gesendet und es wird ein Verlaufs-Trail für die Überprüfung im Anschluss des Vorfalls geliefert. Die Protokollierung der folgenden Ereignisse versetzt ein Unternehmen in die Lage, potentiell schädliche Aktivitäten zu erkennen und nachzuverfolgen.
<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.	Böswillige Individuen könnten Kenntnis über ein Benutzerkonto mit Zugriff auf Systeme in der CDE nehmen oder sie könnten ein neues, nicht genehmigtes Konto einrichten, um sich Zugriff auf die Karteninhaberdaten zu verschaffen. Einträge über alle einzelnen Zugriffe auf Karteninhaberdaten können Aufschluss darauf geben, welche Konten möglicherweise gefährdet oder missbräuchlich eingesetzt worden sind.

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>10.2.2</b> Alle von einer Einzelperson mit Root- oder Administratorrechten vorgenommene Aktionen</p>	<p><b>10.2.2</b> Prüfen Sie, ob alle von einer Einzelperson mit Root- oder Administratorrechten vorgenommenen Aktionen protokolliert werden.</p>	<p>Konten mit erweiterten Rechten, wie etwa das Administrator- oder Root-Konto, können die Sicherheit und die betriebliche Funktionalität eines Systems ernstlich gefährden. Ohne ein Protokoll über die durchgeführten Aktivitäten kann ein Unternehmen Probleme, die durch einen Fehler des Administrators oder durch den Missbrauch von Rechten entstanden sind, nicht bis zu der entsprechenden Aktion oder der verantwortlichen Person zurückverfolgen.</p>
<p><b>10.2.3</b> Zugriff auf alle Audit-Trails</p>	<p><b>10.2.3</b> Prüfen Sie, ob der Zugriff auf alle Audit-Trails protokolliert wird.</p>	<p>Böswillige Personen versuchen nicht selten, Audit-Protokolle zu verfälschen, um ihre Aktionen zu verbergen. Doch mittels eines Zugriffsprotokolls kann ein Unternehmen sämtliche Widersprüche oder potenziellen Manipulationen der Protokolle bis zu einem einzelnen Konto zurückverfolgen. Durch den Zugriff auf Protokolle, aus denen Änderungen, Ergänzungen und Löschungen hervorgehen, lassen sich die Schritte unbefugter Benutzer nachverfolgen.</p>
<p><b>10.2.4</b> Ungültige logische Zugriffsversuche</p>	<p><b>10.2.4</b> Prüfen Sie, ob ungültige logische Zugriffsversuche protokolliert werden.</p>	<p>Angriffe werden häufig mehrere Versuche unternehmen, um auf die gewünschten Systeme zuzugreifen. Mehrere ungültige Anmeldeversuche können ein Hinweis darauf sein, dass ein unbefugter Benutzer versucht, das Kennwort über einen „Brute Force“-Angriff herauszufinden oder zu erraten.</p>
<p><b>10.2.5</b> Verwendung der sowie Änderungen an Identifizierungs- und Authentifizierungsmechanismen (u. a. bei der Erstellung neuer Konten, Heraufstufung von Rechten usw.) und sämtliche Änderungen, Ergänzungen und Löschungen an bzw. von Konten mit „root“- oder Administratorrechten</p>	<p><b>10.2.5.a</b> Prüfen Sie, ob die Verwendung von Identifizierungs- und Authentifizierungssystemen protokolliert wird.</p>	<p>Wenn nicht bekannt ist, wer zu dem Zeitpunkt eines Vorfalles angemeldet war, ist es unmöglich, zu erkennen, welche Konten zu diesem Zweck benutzt werden konnten. Außerdem könnten Angreifer versuchen, die Authentifizierungskontrollen zu manipulieren, um sie entweder zu umgehen oder um sich als der Benutzer eines bestimmten gültigen Kontos auszugeben.</p>
	<p><b>10.2.5.b</b> Überprüfen Sie, ob sämtliche Heraufstufungen von Rechten protokolliert werden.</p>	
	<p><b>10.2.5.c</b> Prüfen Sie, ob alle Änderungen, Ergänzungen oder Löschungen an einem Konto mit Root- oder Administratorrechten protokolliert werden.</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<b>10.2.6</b> Initialisieren, Beenden oder Anhalten der Prüfprotokolle	<b>10.2.6</b> Überprüfen Sie, ob Folgendes protokolliert wird: <ul style="list-style-type: none"> <li>• Initialisierung der Prüfprotokolle</li> <li>• Beenden bzw. Anhalten der Prüfprotokolle</li> </ul>	Das Ausschalten (oder Anhalten) der Prüfprotokolle vor der Ausführung illegaler Aktivitäten ist eine beliebte Methode von Angreifern, die nicht entdeckt werden möchten. Die Initialisierung von Prüfprotokollen könnte darauf hinweisen, dass eine Protokollfunktion von einem Benutzer deaktiviert wurde, um seine Aktivitäten zu verbergen.
<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.	Schädliche Software, wie etwa Malware, erstellt oder ersetzt oft Objekte auf Systemebene im Zielsystem, um eine bestimmte Funktion oder einen Vorgang in diesem System zu steuern. Wenn der Zeitpunkt der Erstellung oder Löschung von Objekten auf Systemebene, z. B. Datenbanktabellen oder gespeicherte Verfahren, protokolliert wird, kann einfacher festgestellt werden, ob solche Änderungen genehmigt waren.
<b>10.3</b> Aufzeichnung von mindestens den folgenden Audit-Trail-Einträgen für alle Systemkomponenten zu jedem Ereignis:	<b>10.3</b> Führen Sie mittels Gesprächen und eigenen Beobachtungen der Prüfprotokolle zu jedem zu protokollierenden Ereignis (aus 10.2) Folgendes durch:	Indem diese Details für die protokollierenden Ereignisse unter 10.2 erfasst werden, kann eine potentielle Gefährdung schnell und mit Informationen zu dem Wer, Was, Wo, Wann und Wie erkannt werden.
<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 Fehlschlägen	<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.	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>10.3.6</b> Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen.</p>	<p><b>10.3.6</b> Überprüfen Sie, ob die Identität oder der Name der betroffenen Daten, Systemkomponenten oder Ressourcen in den Protokolleinträgen enthalten ist.</p>	
<p><b>10.4</b> Synchronisieren Sie mit Technologien zur Zeitsynchronisierung alle wichtigen Systemuhren und -zeiten und stellen Sie sicher, dass 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> Überprüfen Sie in den Konfigurationsstandards und -prozessen, 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.</p>	<p>Technologien zur Zeitsynchronisierung werden verwendet, um die Uhren mehrerer Systeme zu synchronisieren. Wenn Uhren nicht angemessen synchronisiert werden, wird es schwierig, wenn nicht sogar unmöglich, Protokolldateien unterschiedlicher Systeme miteinander zu vergleichen und eine exakte Abfolge der Ereignisse zu ermitteln (ein Punkt von entscheidender Bedeutung bei Ursachenanalysen im Falle eines Verstoßes). Für Ursachenanalyseteams sind die Genauigkeit und Einheitlichkeit der Uhrzeit auf allen Systemen sowie die Uhrzeit der einzelnen Aktivitäten von zentraler Bedeutung, wenn es darum geht, festzustellen, wie die Systeme angegriffen wurden.</p>
<p><b>10.4.1</b> Auf wichtigen Systeme ist die Uhrzeit korrekt und einheitlich.</p>	<p><b>10.4.1.a</b> Untersuchen Sie den Prozess zur Erfassung, Verteilung und Speicherung der richtigen Uhrzeit im Unternehmen, und überprüfen Sie dabei folgende Punkte:</p> <ul style="list-style-type: none"> <li>• Ausschließlich die festgelegten zentralen Zeitserver empfangen Zeitsignale von externen Quellen, und diese Zeitsignale basieren auf der Internationalen Atomzeit bzw. der Koordinierten Weltzeit (UTC).</li> <li>• Wenn es mehrere festgelegte Zeitserver gibt, bestimmen diese Server untereinander die richtige Uhrzeit.</li> <li>• Die Zeitinformationen auf den Systemen stammen ausschließlich von den festgelegten zentralen Zeitservern.</li> </ul>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p><b>10.4.1.b</b> Untersuchen Sie für eine Stichprobe der Systemkomponenten die zeitbezogenen Systemparametereinstellungen, und überprüfen Sie Folgendes:</p> <ul style="list-style-type: none"> <li>• Ausschließlich die festgelegten zentralen Zeitserver empfangen Zeitsignale von externen Quellen, und diese Zeitsignale basieren auf der Internationalen Atomzeit bzw. der Koordinierten Weltzeit (UTC).</li> <li>• Wenn es mehrere festgelegte Zeitserver gibt, bestimmen die festgelegten zentralen Zeitserver untereinander die richtige Uhrzeit.</li> <li>• Die Zeitinformationen auf den Systemen stammen ausschließlich von den festgelegten zentralen Zeitservern.</li> </ul>	
<p><b>10.4.2</b> Zeitinformationen sind geschützt.</p>	<p><b>10.4.2.a</b> Untersuchen Sie die Systemkonfigurationen und Einstellungen der Zeitsynchronisierung, und prüfen Sie, ob 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 Protokolle und Prozesse der Zeitsynchronisierung, und vergewissern Sie sich, 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 in den Systemkonfigurationen, ob die Zeitserver Zeitaktualisierungen von bestimmten, 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	Anweisung
<p><b>10.5</b> Schutz der Audit-Trails vor Veränderungen.</p>	<p><b>10.5</b> Ermitteln Sie in Gesprächen mit den Systemadministratoren und durch die Untersuchung von Systemkonfigurationen und Berechtigungen, ob Audit-Trails mit den folgenden Maßnahmen geschützt sind, dass sie nicht geändert werden können:</p>	<p>Oft wird ein Angreifer, der sich Zugriff auf das Netzwerk verschafft hat, versuchen, die Audit-Protokolle zu bearbeiten, um die von ihm ausgeführten Vorgänge zu verbergen. Ohne entsprechende Schutzmaßnahmen für die Audit-Protokolle kann deren Vollständigkeit, Genauigkeit und Integrität nicht garantiert werden und darüber hinaus können die Audit-Protokolle als Überprüfungs-Tool nach einem Vorfall unbrauchbar gemacht werden.</p>
<p><b>10.5.1</b> Beschränkung der Anzeige der Audit-Trails auf Personen, die aus geschäftlichen Gründen darauf zugreifen müssen.</p>	<p><b>10.5.1</b> Auf Audit-Trail-Dateien haben nur einzelne Personen Zugriff, die aus geschäftlichen Gründen darauf zugreifen müssen.</p>	<p>Ein angemessener Schutz der Audit-Protokolle impliziert eine strenge Zugriffskontrolle (beschränken Sie den Zugriff auf Protokolle auf Personen mit einem geschäftlichen Informationsbedarf) und eine physische Trennung und Netzwerktrennung (damit die Protokolle schwerer zu finden und abzuändern sind).</p>
<p><b>10.5.2</b> Schutz von Audit-Trail-Dateien vor nicht autorisierten Änderungen.</p>	<p><b>10.5.2</b> Die Dateien des aktuellen Audit-Trails werden mit Zugriffskontrollsystemen, räumlicher Trennung und/oder Netzwerktrennung vor unbefugten Änderungen geschützt.</p>	<p>Eine sofortige Sicherung der Protokolle auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen, sorgt für einen Schutz der Protokolle selbst für den Fall, dass das System, von dem die Protokolle erzeugt werden, Ziel eines Angriffs wird.</p>
<p><b>10.5.3</b> Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.</p>	<p><b>10.5.3</b> Die Dateien des aktuellen Audit-Trails werden sofort auf einem zentralen Protokollserver oder auf Medien gesichert, die sich nur schwer ändern lassen.</p>	<p>Durch das Schreiben von Protokollen über nach außen gerichtete Technologien wie etwa Drahtlostechnologien, Firewalls, DNS und Mail-Server wird das Risiko des Verlusts oder Diebstahls der Protokolle reduziert, da sie innerhalb des internen Netzwerks wesentlich sicherer sind.</p>
<p><b>10.5.4</b> Erstellung von Protokollen für nach außen gerichtete Technologien auf sicheren zentralen und internen Protokollservern oder Medien.</p>	<p><b>10.5.4</b> Protokolle für nach außen gerichtete Technologien (z. B. Wireless-Systeme, Firewalls, DNS, E-Mail) werden auf sicheren, zentralen und internen Protokollservern oder Medien abgelegt.</p>	<p>Protokolle können direkt in den sicheren internen Systemen bzw. Medien geschrieben oder von externen Systemen dorthin verschoben bzw. kopiert werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>10.5.5</b> Mithilfe von Software zur Dateiintegritätsüberwachung und zur Erfassung von Änderungen in Protokollen muss dafür gesorgt werden, dass bei der Änderung von bestehenden Protokoll Daten ein Alarm ausgelöst wird (nicht jedoch bei der Eingabe neuer Daten).</p>	<p><b>10.5.5</b> Vergewissern Sie sich durch die Untersuchung der Systemeinstellungen, der überwachten Dateien sowie der Ergebnisse der Überwachung, dass die Software zur Dateiintegritätsüberwachung und Änderungserfassung für Protokolle eingesetzt wird.</p>	<p>Systeme zur Überwachung der Dateiintegrität erkennen Änderungen an wichtigen Dateien und geben entsprechende Warnmeldungen aus. Um die Integrität von Dateien zu überwachen, überprüft eine Stelle normalerweise Dateien, die nur selten geändert werden und auf einen möglichen Angriff hinweisen, wenn tatsächlich eine Änderung vorgenommen wurde.</p>
<p><b>10.6</b> Überprüfung von Protokollen und Systemereignissen für alle Systemkomponenten auf Unregelmäßigkeiten oder verdächtige Aktivitäten.</p> <p><i>Hinweis: Zur Einhaltung dieser Anforderung können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.</i></p>	<p><b>10.6</b> Führen Sie Folgendes durch:</p>	<p>Viele Verstöße erstrecken sich über Tage oder Monate, bevor sie entdeckt werden. Regelmäßige Protokollprüfungen durch Mitarbeiter oder automatisierte Systeme ermöglichen die Ermittlung und frühzeitige Bekämpfung von nicht autorisiertem Zugriff auf die CDE.</p> <p>Der Protokollüberprüfungsprozess muss nicht manuell durchgeführt werden. Der Einsatz von Protokoll-Harvesting-, -Analyse- und Alarmtools kann die Ermittlung von genauer zu prüfenden Protokollereignissen erleichtern.</p>
<p><b>10.6.1</b> Prüfen Sie mindestens einmal täglich die folgenden Punkte:</p> <ul style="list-style-type: none"> <li>• Sämtliche Sicherheitsereignisse</li> <li>• Protokolle aller Systemkomponenten, die CHD und/oder SAD speichern, verarbeiten oder übertragen</li> <li>• Die Protokolle aller wichtigen Systemkomponenten</li> <li>• Die Protokolle aller Server- und Systemkomponenten, die Sicherheitsfunktionen ausführen</li> </ul>	<p><b>10.6.1.a</b> Prüfen Sie in den Sicherheitsrichtlinien und Verfahren, ob Verfahren für eine mindestens tägliche Prüfung der folgenden Elemente (manuell oder mittels Protokolltools) festgelegt sind:</p> <ul style="list-style-type: none"> <li>• Sämtliche Sicherheitsereignisse</li> <li>• Protokolle aller Systemkomponenten, die CHD und/oder SAD speichern, verarbeiten oder übertragen</li> <li>• Die Protokolle aller wichtigen Systemkomponenten</li> <li>• Die Protokolle aller Server- und Systemkomponenten, die Sicherheitsfunktionen ausführen (z. B. Firewalls, Systeme zur Erkennung/Verhinderung von Eindringversuchen (IDS/IPS), Authentifizierungsserver, E-Commerce-Umleitungsserver usw.)</li> </ul>	<p>Durch das tägliche Kontrollieren der Protokolle können die Gefährdung und der Zeitraum, über den möglicherweise eine Sicherheitsverletzung stattfindet, reduziert werden.</p> <p>Die tägliche Prüfung von Sicherheitsereignissen – etwa Benachrichtigungen oder Warnmeldungen bei verdächtigen Aktivitäten oder Unregelmäßigkeiten – sowie der Protokolle von wichtigen Systemkomponenten und von Systemen, die Sicherheitsfunktionen ausführen (wie Firewalls, IDS/IPS, FIM-Systemen zur Überwachung der Dateiintegrität usw.), ist zur</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
(z. B. Firewalls, Systeme zur Erkennung/Verhinderung von Eindringversuchen (IDS/IPS), Authentifizierungsserver, E-Commerce-Umleitungsserver usw.)	<p><b>10.6.1.b</b> Vergewissern Sie sich durch die Beobachtung von Prozessen und die Befragung von Mitarbeitern, dass folgende Elemente mindestens einmal täglich geprüft werden:</p> <ul style="list-style-type: none"> <li>• Sämtliche Sicherheitsereignisse</li> <li>• Protokolle aller Systemkomponenten, die CHD und/oder SAD speichern, verarbeiten oder übertragen</li> <li>• Die Protokolle aller wichtigen Systemkomponenten</li> <li>• Die Protokolle aller Server- und Systemkomponenten, die Sicherheitsfunktionen ausführen (z. B. Firewalls, Systeme zur Erkennung/Verhinderung von Eindringversuchen (IDS/IPS), Authentifizierungsserver, E-Commerce-Umleitungsserver usw.)</li> </ul>	Ermittlung potenzieller Probleme notwendig. Welche Ereignisse als „Sicherheitsereignisse“ betrachtet werden, ist von Unternehmen zu Unternehmen unterschiedlich und hängt unter Umständen auch davon ab, ob die Art der Technologie, der Standort und die Funktion des Geräts ebenfalls berücksichtigt werden. Unter Umständen legen die Unternehmen auch eine Basis für den „normalen“ Datenverkehr fest, um von dieser Normalität abweichendes Verhalten besser zu erkennen.
<p><b>10.6.2</b> Regelmäßige Prüfung der Protokolle aller anderen Systemkomponenten auf der Grundlage der Richtlinien und der Risikomanagementstrategie des Unternehmens und gemäß der jährlichen Risikobewertung des Unternehmens.</p>	<p><b>10.6.2.a</b> Prüfen Sie in den Sicherheitsrichtlinien und Verfahren, ob Verfahren für eine regelmäßige Prüfung der Protokolle aller anderen Systemkomponenten (manuell oder mittels Protokolltools) auf der Grundlage der Richtlinien und der Risikomanagementstrategie des Unternehmens festgelegt sind:</p>	<p>Die Protokolle aller anderen Systemkomponenten müssen ebenfalls regelmäßig daraufhin untersucht werden, ob es Anzeichen für potenzielle Probleme oder Zugriffsversuche auf zugangsbeschränkte Systeme über weniger stark gesicherte Systeme gibt. Wie häufig diese Prüfungen durchgeführt werden sollen, wird in der jährlichen Risikobewertung der Einheit festgelegt.</p>
	<p><b>10.6.2.b</b> Vergewissern Sie sich durch die Prüfung der Risikobewertungsdokumentation des Unternehmens und durch die Befragung von Mitarbeitern, dass die Prüfungen in Übereinstimmung mit den Richtlinien und der Risikomanagementstrategie des Unternehmens durchgeführt werden.</p>	
<p><b>10.6.3</b> Nachverfolgung von bei der Prüfung ermittelten Ausnahmen und Unregelmäßigkeiten.</p>	<p><b>10.6.3.a</b> Prüfen Sie in den Sicherheitsrichtlinien und Verfahren, ob Prozesse für eine Nachverfolgung von bei der Prüfung ermittelten Ausnahmen und Unregelmäßigkeiten festgelegt wurden:</p>	<p>Wenn bei der Prüfung ermittelte Ausnahmen und Unregelmäßigkeiten nicht weiter untersucht werden, bemerkt die Einheit unter Umständen nicht einmal, wenn nicht autorisierte und potenziell böswillige Aktivitäten im eigenen Netzwerk stattfinden.</p>
	<p><b>10.6.3.b</b> Klären Sie durch eine Befragung des Personals und die Beobachtung von Prozessen ab, ob bei Ausnahmen und Unregelmäßigkeiten eine Nachverfolgung stattfindet.</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>10.7</b> Aufbewahrung der Audit-Trail-Verlaufsdaten für mindestens ein Jahr. 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> Prüfen Sie, ob in den Sicherheitsrichtlinien und Verfahren Prozesse für Folgendes festgelegt wurden:</p> <ul style="list-style-type: none"> <li>• Richtlinien zur Aufbewahrung von Prüfprotokollen</li> <li>• Verfahren zur Aufbewahrung von Prüfprotokollen für die Dauer von mindestens einem Jahr, wobei mindestens drei Monate online verfügbar sind.</li> </ul> <p><b>10.7.b</b> Vergewissern Sie sich durch die Befragung von Mitarbeitern und die Untersuchung von Prüfprotokollen, dass die Prüfprotokolle für mindestens ein Jahr lang gespeichert werden.</p> <p><b>10.7.c</b> Vergewissern Sie sich durch die Befragung von Mitarbeitern und die Beobachtung von Prozessen, dass zumindest die Protokolle der letzten drei Monaten sofort zu Analyse Zwecken zur Verfügung stehen.</p>	<p>Indem Protokolle mindestens ein Jahr aufbewahrt werden, wird der Tatsache Rechnung getragen, dass es oft eine Zeitlang dauert, bis eine bereits geschehene oder aktuelle Sicherheitsverletzung entdeckt wird. Außerdem ermöglicht der ausführliche Protokollverlauf es Prüfern, zu ermitteln, seit wann die Sicherheitsverletzung besteht und welche/s System/e möglicherweise betroffen ist/sind. Wenn Protokolle über mehrere Monate direkt verfügbar sind, kann eine Stelle schnell einen Verstoß gegen die Datensicherheit erkennen und die möglichen Konsequenzen minimieren. Das Speichern von Protokollen an Offline-Standorten hat zur Folge, dass die Daten nicht sofort verfügbar sind und ihre Wiederherstellung, die Durchführung von Analysen sowie die Identifizierung betroffener Systeme oder Daten wesentlich länger dauert.</p>
<p><b>10.8 Zusätzliche Anforderung nur für Dienstleister:</b> Implementieren Sie einen Prozess zur baldigen Ermittlung und Meldung von Ausfällen wichtiger Sicherheitskontrollsystemen, einschließlich Ausfälle der Folgenden:</p> <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Antivirus</li> <li>• Physische Zugangskontrollen</li> <li>• Logische Zugriffskontrollen</li> <li>• Mechanismen zur Audit-</li> </ul>	<p><b>10.8.a</b> Vergewissern Sie sich in dokumentierten Richtlinien und Verfahren, dass Prozesse für die baldige Ermittlung und Meldung von Ausfällen wichtiger Sicherheitskontrollsystemen festgelegt wurden, einschließlich Ausfälle der Folgenden:</p> <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Antivirus</li> <li>• Physische Zugangskontrollen</li> <li>• Logische Zugriffskontrollen</li> <li>• Mechanismen zur Audit-Protokollierung</li> <li>• Segmentierungskontrollen (falls verwendet)</li> </ul>	<p><b>Hinweis:</b> Diese Anforderung muss nur beachtet werden, wenn es sich bei der zu bewertenden Einheit um einen Dienstleister handelt.</p> <p>Ohne offizielle Prozesse zur Ermittlung und Alarmierung von Ausfällen wichtiger Sicherheitskontrollen könnten Ausfälle für eine längere Zeitspanne unentdeckt bleiben und Angreifern genügend Zeit zur Kompromittierung der Systeme und dem Diebstahl sensibler Daten aus der Karteninhaberdaten-Umgebung bieten. Die bestimmten Arten von Ausfällen können abhängig von der Funktion des Gerätes und der verwendeten Technologie variieren. Ein typischer</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>Protokollierung</p> <ul style="list-style-type: none"> <li>Segmentierungskontrollen (falls verwendet)</li> </ul> <p><i>Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</i></p>	<p><b>10.8.b</b> Klären Sie durch eine Überprüfung der Prozesse zur Ermittlung und Alarmierung und eine Befragung des Personals, ob alle Prozesse für alle wichtigen Sicherheitskontrollen implementiert wurden, und ob ein Ausfall dieser zu einem Alarm führen.</p>	<p>Ausfall wäre beispielsweise ein System, dessen Sicherheitsfunktion nicht mehr oder nicht mehr wie vorgesehen funktioniert; z. B. eine Firewall, die ihre gesamten Regeln löscht oder offline geht.</p>
<p><b>10.8.1 Zusätzliche Anforderung nur für Dienstanbieter:</b> Reagieren Sie zügig auf Ausfälle wichtiger Sicherheitskontrollen. Die Reaktion auf Ausfälle bei den Sicherheitskontrollen muss die folgenden Prozesse umfassen:</p> <ul style="list-style-type: none"> <li>Wiederherstellung der Sicherheitsfunktionen</li> <li>Ermittlung und Dokumentierung der Dauer (Datum und Zeit von Anfang bis Ende) des Sicherheitsausfalls</li> <li>Ermittlung und Dokumentierung der Ursache(n) des Ausfalls, einschließlich der Fehlerursache, und Dokumentierung der erforderlichen Maßnahmen zur Behebung der Fehlerursache</li> </ul>	<p><b>10.8.1.a</b> Vergewissern Sie sich in dokumentierten Richtlinien und Verfahren, dass Prozesse zur Reaktion auf den Ausfall von Sicherheitskontrollen festgelegt und implementiert wurden, und diese die folgenden Elemente beinhalten:</p> <ul style="list-style-type: none"> <li>Wiederherstellung der Sicherheitsfunktionen</li> <li>Ermittlung und Dokumentierung der Dauer (Datum und Zeit von Anfang bis Ende) des Sicherheitsausfalls</li> <li>Ermittlung und Dokumentierung der Ursache(n) des Ausfalls, einschließlich der Fehlerursache, und Dokumentierung der erforderlichen Maßnahmen zur Behebung der Fehlerursache</li> <li>Ermittlung und Lösung von Sicherheitsproblemen, die während des Ausfalls aufgetreten sind</li> <li>Durchführung einer Risikobeurteilung zur Feststellung, ob weitere Maßnahmen als Folge des Sicherheitsausfalls erforderlich sind</li> <li>Implementierung von Kontrollen zur Verhinderung eines Wiederauftretens der Fehlerursache</li> <li>Wiederaufnahme der Überwachung von Sicherheitskontrollen</li> </ul>	<p><i>Hinweis: Diese Anforderung muss nur beachtet werden, wenn es sich bei der zu bewertenden Einheit um einen Dienstanbieter handelt.</i></p> <p>Wenn auf Alarme aufgrund von Ausfällen wichtiger Sicherheitskontrollen nicht schnell und wirksam reagiert wird, könnten Angreifer diese Zeit nutzen, um Schadsoftware einzuschleusen, Zugriff auf ein System zu erlangen oder Daten aus der Umgebung der Einheit zu stehlen.</p> <p>Dokumentierte Belege (z. B. Aufzeichnungen in einem Problemmanagement-System) müssen die vorhandenen Prozesse und Verfahren zur Reaktion auf Sicherheitsausfälle unterstützen. Des weiteren müssen sich die Mitarbeiter ihrer Verantwortung im Falle eines Ausfalles kennen. Maßnahmen und Reaktionen auf den Ausfall sind</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<ul style="list-style-type: none"> <li>• Ermittlung und Lösung von Sicherheitsproblemen, die während des Ausfalls aufgetreten sind</li> <li>• Durchführung einer Risikobeurteilung zur Feststellung, ob weitere Maßnahmen als Folge des Sicherheitsausfalls erforderlich sind</li> <li>• Implementierung von Kontrollen zur Verhinderung eines Wiederauftretens der Fehlerursache</li> <li>• Wiederaufnahme der Überwachung von Sicherheitskontrollen</li> </ul> <p><i>Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</i></p>	<p><b>10.8.1.b</b> Vergewissern Sie sich durch eine Überprüfung der Aufzeichnungen, dass Ausfälle von Sicherheitskontrollen dokumentiert sind, und die folgenden Elemente enthalten:</p> <ul style="list-style-type: none"> <li>• Ermittlung der Ursache(n) des Ausfalls, einschließlich der Fehlerursache</li> <li>• Dauer (Datum und Zeit von Anfang bis Ende) des Sicherheitsausfalls</li> <li>• Details zu den erforderlichen Maßnahmen zur Behebung der Fehlerursache</li> </ul>	<p>in den dokumentierten Belegen zu erfassen.</p>
<p><b>10.9</b> Sicherheitsrichtlinien und betriebliche Verfahren zur Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>	<p><b>10.9</b> Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zur Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Sie sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	<p>Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren zur Überwachung des Zugriffs auf alle Netzwerkressourcen und Karteninhaberdaten kennen und dauerhaft befolgen.</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	Anweisung
<p><b>11.1</b> Implementierung von Prozessen, mit denen getestet wird, ob Zugriffspunkte für drahtlose Netzwerke (802.11) vorhanden sind, und vierteljährlich alle autorisierten und nicht autorisierten Zugriffspunkte für drahtlose Netzwerke gesucht werden.</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>Sie können sich für eine beliebige Methode entscheiden, solange damit autorisierte und nicht autorisierte Geräte erkannt und identifiziert werden können.</i></p>	<p><b>11.1.a</b> Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren, ob Prozesse zur vierteljährlichen Erkennung und Identifizierung von autorisierten und nicht autorisierten Zugriffspunkten für drahtlose Netzwerke definiert sind.</p>	<p>Die Implementierung und/oder Ausnutzung von Drahtlostechnologie in einem Netzwerk ist eine altbewährte Methode, mit der sich Angreifer Zugriff zu einem Netzwerk und zu Karteninhaberdaten verschaffen. Wenn ein drahtloses Gerät oder Netzwerk ohne das Wissen eines Unternehmens installiert wird, könnte sich ein Angreifer mühelos und „heimlich“ Zugang zum Netzwerk verschaffen. Nicht zugelassene Drahtlosgeräte können in einem Computer oder einer anderen Systemkomponente versteckt oder daran angeschlossen sein oder direkt an einen Netzwerk-Port oder ein Netzwerkgerät, wie etwa einen Schalter oder einen Router, angeschlossen werden. Diese Geräte könnten als nicht zugelassener Zugriffspunkt in die Umgebung fungieren.</p> <p>Wenn Administratoren wissen, welche Drahtlosgeräte autorisiert sind, können sie schnell die nicht autorisierten Geräte erkennen. Eine schnelle Reaktion auf identifizierte nicht autorisierte WLAN-Zugriffspunkte hilft Ihnen dabei, die CDE frühzeitig vor Angriffen zu schützen.</p> <p>Aufgrund der Einfachheit, mit der ein drahtloser Zugriffspunkt an ein Netzwerk angeschlossen werden kann, dessen extrem komplizierter Erkennung und dem hohen Risiko durch nicht genehmigte Drahtlosgeräte, müssen diese Prozesse selbst dann ausgeführt werden, wenn eine Richtlinie implementiert ist, die die Nutzung von Drahtlostechnologien komplett untersagt.</p> <p>Die Größe und Komplexität einer bestimmten Umgebung geben Hinweise auf die erforderlichen</p>
	<p><b>11.1.b</b> Überprüfen Sie, ob mit der angewandten Methodik nicht autorisierte WLAN-Zugriffspunkte erkannt und identifiziert werden können. Dazu zählen mindestens die folgenden Elemente:</p> <ul style="list-style-type: none"> <li>• In Systemkomponenten eingefügte WLAN-Karten</li> <li>• An Systemkomponenten angeschlossene tragbare Geräte (z. B. durch USB), mit denen ein WLAN-Zugriffspunkt eingerichtet wird</li> <li>• an einen Netzwerkport oder ein Netzwerkgerät angeschlossene Drahtlosgeräte.</li> </ul>	
	<p><b>11.1.c</b> Wenn Wireless-Scans verwendet werden, prüfen Sie, ob für die zuletzt durchgeführten Scan-Vorgänge Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Es werden autorisierte und nicht autorisierte WLAN-Zugriffspunkte gefunden.</li> <li>• Der Scan findet mindestens einmal vierteljährlich auf allen Systemkomponenten und in allen Einrichtungen statt.</li> </ul>	
	<p><b>11.1.d</b> Überprüfen Sie bei automatischer Überwachung (z. B. Wireless IDS/IPS-System oder NAC), ob in der Konfiguration Alarmmeldungen für das Personal vorgesehen sind.</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
		<p>Tools und Prozesse, die eingesetzt werden müssen, um ausreichend Sicherheit dahingehend zu bieten, dass in der Umgebung kein unbefugter drahtloser Zugriffspunkt installiert wurde.</p> <p>(Fortsetzung auf der nächsten Seite)</p>
<p><b>11.1.1</b> Inventarisierung von autorisierten WLAN-Zugriffspunkten mit dokumentierter geschäftlicher Begründung.</p>	<p><b>11.1.1</b> Überprüfen Sie durch eine Untersuchung der Dokumentation, ob die autorisierten WLAN-Zugriffspunkten inventarisiert werden und ob zu jedem Zugriffspunkt eine geschäftliche Begründung dokumentiert ist.</p>	<p><b>Beispiel:</b> Im Falle eines einzelnen Verkaufskiosk in einem Einkaufszentrum, bei dem sich alle Kommunikations-komponenten innerhalb eines manipulationssicheren und sicherheitsverpackten Gehäuses befinden, mag eine physische Kontrolle des Kiosks ausreichend sein, um sicherzustellen, dass keine schädlichen drahtlosen Zugriffspunkte installiert oder angeschlossen wurden. In einer Umgebung mit mehreren Knoten (wie in einem großen Einzelhandelsgeschäft, Callcenter, Serverraum oder Rechenzentrum) gestaltet sich die physische Untersuchung schwierig. In diesem Fall bietet es sich an, mehrere Methoden miteinander zu kombinieren, um die Anforderung zu erfüllen, beispielsweise indem physische Systemüberprüfungen durchgeführt und mit den Ergebnissen eines Analysators für drahtlose Netzwerke kombiniert werden.</p>
<p><b>11.1.2</b> Implementierung von Vorfalreaktionsverfahren für den Fall, dass nicht autorisierte WLAN-Zugriffspunkte entdeckt werden.</p>	<p><b>11.1.2.a</b> Überprüfen Sie, ob im Vorfalreaktionsplan (Anforderung 12.10) eine Reaktion für den Fall definiert ist, dass ein nicht autorisierter WLAN-Zugriffspunkt entdeckt wird.</p> <p><b>11.1.2.b</b> Vergewissern Sie sich durch die Befragung der zuständigen Mitarbeiter und/oder die Untersuchung von aktuellen Scans auf Drahtlosgeräte sowie die zugehörigen Reaktionen, dass beim Auffinden von WLAN-Zugriffspunkten Maßnahmen ergriffen werden.</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>11.2</b> Ausführen interner und externer Netzwerkanfälligkeitsscans mindestens einmal pro Quartal und nach jeder wesentlichen Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Änderung der Firewall-Regeln, Produkt-Upgrades).</p> <p><b>Hinweis:</b> Um beim vierteljährlichen Scan sämtliche Systeme und alle möglichen Sicherheitsrisiken zu berücksichtigen, können mehrere Scan-Berichte miteinander kombiniert werden. Es ist unter Umständen zusätzliche Dokumentation erforderlich, um zu belegen, dass bei noch nicht behobenen Sicherheitsrisiken erste Schritte unternommen wurden.</p> <p>Es ist für die anfängliche PCI DSS-Konformität nicht erforderlich, dass vier vierteljährliche Scans bestanden sein müssen, wenn der Prüfer feststellt, 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 in den Scan-Ergebnissen festgestellten Sicherheitsrisiken nachweislich korrigiert wurden. Für die Folgejahre nach der ersten PCI-DSS-Prüfung müssen vier bestandene vierteljährliche Scans vorliegen.</p>	<p><b>11.2</b> Überprüfen Sie in den Scan-Berichten und der zugehörigen Dokumentation, ob die internen und externen Scans auf Sicherheitsrisiken wie folgt durchgeführt werden:</p>	<p>Ein Scan auf Sicherheitsrisiken ist eine Kombination automatischer oder manueller Tools, Techniken und/oder Methoden, die auf externen und internen Netzwerkgeräten und -servern ausgeführt werden und dazu dienen, potentielle Sicherheitsrisiken in Netzwerken aufzudecken, die von böswilligen Personen erkannt und ausgenutzt werden könnten.</p> <p>Für den PCI-DSS sind drei Arten von Scans auf Sicherheitsrisiken erforderlich:</p> <ul style="list-style-type: none"> <li>• Interne vierteljährliche Scans, die von qualifizierten Mitarbeitern durchgeführt werden müssen (die Beauftragung eines vom PCI SSC zugelassenen ASV (Approved Scanning Vendor, zugelassener Sicherheitsprüfer) ist nicht erforderlich)</li> <li>• Externe vierteljährliche Scans, die von einem ASV durchgeführt werden müssen</li> <li>• Bedarfsweise nach wesentlichen Änderungen vorgenommene interne und externe Scans</li> </ul> <p>Sobald diese Sicherheitsrisiken erkannt wurden, werden von der Einheit Korrekturmaßnahmen ergriffen. Anschließend wird bei einem erneuten Scan geprüft, ob die Sicherheitsrisiken tatsächlich behoben wurden.</p> <p>Die rechtzeitige Erkennung und Korrektur von Schwachstellen reduziert die Wahrscheinlichkeit, dass eine solche Sicherheitslücke ausgenutzt wird und eine Systemkomponente oder Karteninhaberdaten gefährdet werden.</p>
<p><b>11.2.1</b> Führen Sie vierteljährlich interne Schwachstellenprüfungen durch. Beheben Sie Schwachstellen und führen</p>	<p><b>11.2.1.a</b> Vergewissern Sie sich durch die Überprüfung der Scan-Berichte, dass in den letzten zwölf Monaten vier vierteljährliche interne Scans stattgefunden haben.</p>	<p>Ein etablierter Prozess zur Erkennung von Sicherheitsrisiken in internen Systemen setzt voraus, dass vierteljährliche Scans durchgeführt</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>Sie erneute Scans durch, um sicherzustellen, dass alle „hohen“ Sicherheitsrisiken gemäß der Risikogruppen der Einrichtung behoben wurden (gemäß Anforderung 6.1). Scans müssen von qualifizierten Mitarbeitern durchgeführt werden.</p>	<p><b>11.2.1.b</b> Vergewissern Sie sich durch die Prüfung der Scan-Berichte, dass alle Schwachstellen mit „hohem Risiko“ behoben wurden, und dass der Prozess erneute Scans vorsieht, bis alle „hohen“ Sicherheitsrisiken (gemäß PCI-DSS-Anforderung 6.1) beseitigt wurden.</p> <p><b>11.2.1.c</b> Überprüfen Sie durch die Befragung von Mitarbeitern, ob der Scan von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Drittanbieter durchgeführt wurde, und gegebenenfalls, ob der Tester organisatorisch unabhängig ist (es muss sich nicht um einen QSA oder ASV handeln).</p>	<p>werden. Jenen Sicherheitsrisiken, die ein besonders hohes Risiko für die Umgebung darstellen (z. B. Sicherheitsrisiken, die gemäß Anforderung 6.1 als „hoch“ eingestuft werden), sollte höchste Priorität eingeräumt werden.</p> <p>Interne Scans können von qualifiziertem internem Personal durchgeführt werden, das möglichst nicht direkt für die zu scannenden Systemkomponenten zuständig ist (z. B. sollte ein Firewall-Administrator nicht damit beauftragt werden, die Firewall zu scannen). Darüber hinaus bietet sich einer Einheit die Option, interne Scans von einem Unternehmen, das auf Sicherheitsrisiko-Scans spezialisiert ist, durchführen zu lassen.</p>
<p><b>11.2.2</b> Vierteljährliche externe Scans auf Sicherheitsrisiken, die von einem vom PCI SSC zugelassenen ASV durchgeführt werden. Nach Bedarf müssen erneute Scans durchgeführt werden, bis das Ergebnis „bestanden“ lautet.</p> <p><b>Hinweis:</b> Vierteljährliche externe Schwachstellenprüfungen müssen von einem Scanninganbieter (Approved Scanning Vendor, ASV) durchgeführt werden, der vom Payment Card Industry Security Standards Council (PCI SSC) zugelassen wurde.</p> <p>Informationen zu den Scan-Kunden-Zuständigkeiten, der Scan-Vorbereitung usw. finden Sie im ASV-Programmführer auf der PCI-SSC-Website.</p>	<p><b>11.2.2.a</b> Überprüfen Sie die Ergebnisse der externen Scans der letzten vier Quartale, und vergewissern Sie sich, dass in den letzten 12 Monaten vier vierteljährliche externe Scans stattgefunden haben.</p> <p><b>11.2.2.b</b> Überprüfen Sie die Ergebnisse der einzelnen vierteljährlichen Scans und eventueller erneuter Scans, und prüfen Sie, ob die Anforderungen des ASV-Programmführers erfüllt werden (z. B. keine Sicherheitsrisiken, 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 in den Scan-Berichten, ob die Tests von einem vom PCI SSC zugelassenen ASV durchgeführt wurden.</p>	<p>Da externe Netzwerke eher durch Angriffe gefährdet sind, muss vierteljährlich ein externer Anfälligkeits-Scan von einem vom PCI-SSC zugelassenen Scanninganbieter (ASV) durchgeführt werden.</p> <p>Ein robustes Scan-Programm gewährleistet, dass die Scans zeitnah durchgeführt und Schwachstellen behoben werden.</p>
<p><b>11.2.3</b> Führen Sie nach jeder wesentlichen Änderung interne und externe Scans und nach Bedarf erneute Scans durch. Scans müssen von</p>	<p><b>11.2.3.a</b> Vergewissern Sie sich in der Änderungskontrolldokumentation und den Scan-Berichten, dass Systemkomponenten, an denen wesentliche Änderungen vorgenommen wurden, gescannt wurden.</p>	<p>Welche Änderungen als wesentlich zu betrachten sind, hängt im hohem Maße von der Konfiguration einer bestimmten Umgebung ab. Sofern eine Aktualisierung oder Änderung den Zugriff auf die</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>qualifizierten Mitarbeitern durchgeführt werden.</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 Sicherheitsrisiken mehr vorhanden sind, die vom CVSS mit einer Klassifizierung höher als 4.0 bewertet wurden.</li> <li>• ... bei internen Scans alle „hohen“ Sicherheitsrisiken gemäß PCI-DSS-Anforderung 6.1 beseitigt wurden.</li> </ul>	<p>Karteninhaberdaten ermöglicht oder sich auf die Sicherheit der CDE auswirkt, kann sie als wesentlich betrachtet werden.</p> <p>Durch das Scannen einer Umgebung nach der Durchführung signifikanter Änderungen wird gewährleistet, dass die Änderungen vollständig abgeschlossen wurden und die Sicherheit der Umgebung durch die Änderungen nicht herabgesetzt wurde. Es müssen alle von der Änderung betroffenen Systemkomponenten gescannt werden.</p>
<p><b>11.3</b> Implementierung einer Methodik für Penetrationstests, die die folgenden Elemente umfasst:</p> <ul style="list-style-type: none"> <li>• Die Methodik basiert auf branchenweit akzeptierten Verfahren für Penetrationstests (z. B. NIST SP800-115).</li> <li>• Die Methodik umfasst die gesamte Umgebung der CDE und wichtige Systeme.</li> <li>• Es werden Tests innerhalb und außerhalb des Netzwerks durchgeführt.</li> <li>• Bei den Tests werden auch Kontrollen zur Segmentierung und zur Reduktion des Umfangs validiert.</li> <li>• Bei der Definition von Penetrationstests auf Anwendungsebene müssen mindestens die in Anforderung 6.5</li> </ul>	<p><b>11.3</b> Überprüfen Sie durch die Untersuchung der Methodik für Penetrationstests und durch die Befragung der zuständigen Mitarbeiter, ob eine Methodik mit den folgenden Elementen implementiert ist:</p> <ul style="list-style-type: none"> <li>• Die Methodik basiert auf branchenweit akzeptierten Verfahren für Penetrationstests (z. B. NIST SP800-115).</li> <li>• Die Methodik umfasst die gesamte Umgebung der CDE und wichtige Systeme.</li> <li>• Es werden Tests innerhalb und außerhalb des Netzwerks durchgeführt.</li> <li>• Bei den Tests werden auch Kontrollen zur Segmentierung und zur Reduktion des Umfangs validiert.</li> <li>• Bei der Definition von Penetrationstests auf Anwendungsebene müssen mindestens die in Anforderung 6.5 aufgeführten Sicherheitsrisiken berücksichtigt werden.</li> <li>• Es müssen Penetrationstests auf Netzwerkebene definiert werden, die sämtliche Komponenten zur Unterstützung von Netzwerkfunktionen und Betriebssysteme enthalten.</li> <li>• Bei der Methodik müssen die in den letzten 12 Monaten</li> </ul>	<p>Der Zweck eines Penetrationstests ist es, eine reale Angriffssituation zu simulieren, um zu ermitteln, wie weit ein Angreifer in der Lage wäre, in das System einzudringen. Hierdurch erhält die jeweilige Einheit ein tieferes Verständnis des potentiellen Risikos, dem sie ausgesetzt ist, und ist der Lage, eine entsprechende Strategie zu entwickeln, um sich vor Angriffen zu schützen.</p> <p>Ein Penetrationstest unterscheidet sich insofern von einem Scan auf Sicherheitsrisiken, als der Penetrationstest ein aktiver Prozess ist, bei dem unter anderem auch bekannte Sicherheitsrisiken ausgetestet werden. Oft ist die Durchführung eines Scans auf Sicherheitsrisiken der erste, jedoch nicht der einzige Schritt bei der Planung der Strategie für einen Penetrationstest. Selbst wenn bei einem Scan auf Sicherheitsrisiken bekannte Risiken nicht erkannt werden, erhält der Tester zumeist genügend Informationen über das System, um mögliche Sicherheitslücken zu erkennen.</p> <p>Penetrationstests sind überwiegend manuelle</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>aufgeführten Sicherheitsrisiken berücksichtigt werden.</p> <ul style="list-style-type: none"> <li>• Es müssen Penetrationstests auf Netzwerkebene definiert werden, die sämtliche Komponenten zur Unterstützung von Netzwerkfunktionen und Betriebssysteme enthalten.</li> <li>• Bei der Methodik müssen die in den letzten 12 Monaten aufgetretenen Bedrohungen und Sicherheitsrisiken berücksichtigt werden.</li> <li>• Es muss festgelegt sein, wo die Ergebnisse von Penetrationstests und Abhilfemaßnahmen gespeichert werden sollen.</li> </ul>	<p>aufgetretenen Bedrohungen und Sicherheitsrisiken berücksichtigt werden.</p> <ul style="list-style-type: none"> <li>• Es muss festgelegt sein, wo die Ergebnisse von Penetrationstests und Abhilfemaßnahmen gespeichert werden sollen.</li> </ul>	<p>Prozesse. Obwohl auch einige automatisierte Tools verwendet werden können, benötigt der Tester Systemkenntnisse, um in eine Umgebung einzudringen. Oft wird ein Prüfer mehrere Arten von Exploits miteinander verbinden, um verschiedene Sicherheitsschichten zu durchbrechen. Wenn ein Prüfer beispielsweise einen Weg findet, sich Zugriff auf einen Anwendungsserver zu verschaffen, wird er diesen gefährdeten Server als Ausgangspunkt für einen neuen Angriff abhängig von den Ressourcen, zu denen der Server Zugriff hat, nutzen. Mithilfe dieser Methode ist ein Prüfer in der Lage, die von einem Angreifer genutzten Methoden zu simulieren und somit in der Umgebung mögliche Schwachstellen zu identifizieren.</p> <p><i>Welche Techniken für die Penetrationstests eingesetzt werden, ist von Unternehmen zu Unternehmen unterschiedlich. Die Art, Intensität und Komplexität der Tests hängen von der jeweiligen Umgebung und der Risikobewertung des Unternehmens ab.</i></p>
<p><b>11.3.1</b> Durchführen <i>externer</i> Penetrationstests mindestens einmal im Jahr und nach jeder wesentlichen Infrastruktur- oder Anwendungsaktualisierung oder -änderung (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver in der Umgebung).</p>	<p><b>11.3.1.a</b> Untersuchen Sie den Arbeitsaufwand und die Ergebnisse des aktuellsten Penetrationstests, und prüfen Sie, ob die Penetrationstests wie folgt durchgeführt werden:</p> <ul style="list-style-type: none"> <li>• Gemäß der definierten Methodik</li> <li>• Mindestens jährlich</li> <li>• Nach wesentlichen Änderungen an der Umgebung</li> </ul> <p><b>11.3.1.b</b> Überprüfen Sie, ob der Test von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Dritten durchgeführt wurde und gegebenenfalls, ob der Tester organisatorisch unabhängig ist (muss kein QSA oder ASV sein).</p>	<p>Regelmäßig und nach wesentlichen Veränderungen der Umgebung durchgeführte Penetrationstests sind vorausschauende Sicherheitsmaßnahmen, mit denen sich der potenzielle Zugriff von Angreifern auf die CDE verkleinern lässt.</p> <p>Welche Aktualisierungen oder Änderungen als wesentlich zu betrachten sind, hängt im hohem Maße von der Konfiguration einer bestimmten Umgebung ab. Sofern eine Aktualisierung oder Änderung den Zugriff auf die Karteninhaberdaten ermöglicht oder sich auf die Sicherheit der CDE auswirkt, kann sie als wesentlich betrachtet werden. Mit einem Penetrationstest nach Netzwerkaktualisierungen und -änderungen wird geprüft, ob die in Kraft befindlichen Kontrollen auch nach der Aktualisierung/Änderung noch wirksam sind.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>11.3.2</b> Durchführen <i>interner</i> Penetrationstests mindestens einmal im Jahr und nach jeder wesentlichen Infrastruktur- oder Anwendungsaktualisierung oder -änderung (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver in der Umgebung).</p>	<p><b>11.3.2.a</b> Untersuchen Sie den Arbeitsaufwand und die Ergebnisse des aktuellsten internen Penetrationstests, und prüfen Sie, ob die Penetrationstests wie folgt durchgeführt werden:</p> <ul style="list-style-type: none"> <li>• Gemäß der definierten Methodik</li> <li>• Mindestens jährlich</li> <li>• Nach wesentlichen Änderungen an der Umgebung</li> </ul> <p><b>11.3.2.b</b> Überprüfen Sie, ob der Test von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Dritten durchgeführt wurde und gegebenenfalls, ob der Tester organisatorisch unabhängig ist (muss kein QSA oder ASV sein).</p>	
<p><b>11.3.3</b> Beim Penetrationstest ermittelte ausnutzbare Sicherheitsrisiken müssen behoben werden, und anschließend muss ein erneuter Test durchgeführt werden.</p>	<p><b>11.3.3</b> Prüfen Sie in den Testergebnissen, ob die beim Penetrationstest ermittelten ausnutzbaren Sicherheitsrisiken behoben wurden und ob anschließend bei einem erneuten Test die Beseitigung der Risiken überprüft wurde.</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>11.3.4</b> Falls die CDE durch Segmentierung von anderen Netzwerken isoliert wird, muss bei mindestens jährlich und nach Änderungen an den Segmentierungskontrollen/-methoden durchzuführenden Penetrationstests geprüft werden, ob die Segmentierungsmethode funktioniert und effektiv ist und alle Systeme außerhalb des Bereichs von den Systemen innerhalb des CDE isoliert werden.</p>	<p><b>11.3.4.a</b> Vergewissern Sie sich durch die Untersuchung von Segmentierungskontrollen und die Prüfung von Penetrationstestmethoden, dass die Penetrationstestverfahren wie folgt definiert sind: Es werden alle Segmentierungsmethoden daraufhin geprüft, ob sie funktionieren und effektiv sind, und alle Systeme außerhalb des Bereichs müssen von den Systemen innerhalb des CDE isoliert werden.</p>	<p>Mit Penetrationstests lässt sich gut ermitteln, ob die Segmentierung zur Isolierung der CDE von anderen Netzwerken funktioniert. Die Penetrationstests sollten sich auf die Segmentierungskontrollen außerhalb und innerhalb des Netzwerks der Einheit, aber außerhalb der CDE konzentrieren, damit überprüft werden kann, ob die Segmentierungskontrollen einen Zugriff auf die CDE verhindern. So kann zum Beispiel bei einem Netzwerkttest und/oder einer Suche nach offenen Ports geprüft werden, dass keine Verbindung zwischen innerhalb und außerhalb des Bereichs befindlichen Netzwerken besteht.</p>
	<p><b>11.3.4.b</b> Untersuchen Sie die Ergebnisse des aktuellsten Penetrationstests, und prüfen Sie, ob für Penetrationstests zur Prüfung von Segmentierungskontrollen Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Penetrationstests zur Überprüfung von Segmentierungskontrollen werden mindestens einmal jährlich und nach Änderungen an den Segmentierungskontrollen/-methoden durchgeführt.</li> <li>• Beim Penetrationstest werden alle verwendeten Segmentierungskontrollen/-methoden geprüft.</li> <li>• Die Penetrationstests bestätigen, dass die Segmentierungsmethoden funktionieren und effektiv sind, und alle Systeme außerhalb des Bereichs müssen von den Systemen innerhalb des CDE isoliert werden.</li> </ul>	
	<p><b>11.3.4.c</b> Überprüfen Sie, ob der Test von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Dritten durchgeführt wurde und gegebenenfalls, ob der Tester organisatorisch unabhängig ist (muss kein QSA oder ASV sein).</p>	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>11.3.4.1 Zusätzliche Anforderung nur für Dienstleister:</b> Falls Segmentierung verwendet wird, bestätigen Sie den PCI-DSS-Umfang durch Durchführung von Penetrationstest an Segmentierungskontrollen, mindestens alle sechs Monate nach Änderungen an den Segmentierungsmethoden.</p> <p><i>Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</i></p>	<p><b>11.3.4.1.a</b> Untersuchung der Ergebnisse des letzten Penetrationstests, um sicherzustellen, dass:</p> <ul style="list-style-type: none"> <li>• Penetrationstests zur Überprüfung von Segmentierungskontrollen mindestens alle sechs Monate und nach Änderungen an den Segmentierungskontrollen/-methoden durchgeführt werden.</li> <li>• Beim Penetrationstest alle verwendeten Segmentierungskontrollen/-methoden geprüft werden.</li> <li>• Die Penetrationstests bestätigen, dass die Segmentierungsmethoden funktionieren und effektiv sind, und alle Systeme außerhalb des Bereichs müssen von den Systemen innerhalb des CDE isoliert werden.</li> </ul>	<p><i>Hinweis: Diese Anforderung muss nur beachtet werden, wenn es sich bei der zu bewertenden Einheit um einen Dienstleister handelt.</i></p> <p>Für Dienstleister ist die Validierung des PCI-DSS-Umfangs so häufig wie möglich durchzuführen, um sicherzustellen, dass der PCI-DSS-Umfang aktuell und im Einklang mit den sich ändernden Geschäftszielen bleibt.</p>
	<p><b>11.3.4.1.b</b> Überprüfen Sie, ob der Test von einem dafür qualifizierten internen Mitarbeiter oder einem qualifizierten Dritten durchgeführt wurde und gegebenenfalls, ob der Tester organisatorisch unabhängig ist (muss kein QSA oder ASV sein).</p>	
<p><b>11.4</b> Nutzung von Techniken zur Erkennung und/oder Verhinderung von Eindringversuchen in das Netzwerk. Überwachung des gesamten Datenverkehrs in der Umgebung der CDE sowie an kritischen Punkten innerhalb der CDE und Alarmierung des Personals bei mutmaßlichen Sicherheitsverletzungen.</p> <p>Ständige Aktualisierung der Systeme zur Erkennung und Verhinderung von Eindringversuchen, der Basis und der Signaturen.</p>	<p><b>11.4.a</b> Überprüfen Sie durch Untersuchung der Systemkonfigurationen und Netzwerkdiagramme, ob Techniken wie etwa Systeme zur Erkennung und/oder Verhinderung von Eindringversuchen an den folgenden Stellen zur Datenverkehrsüberwachung eingesetzt sind:</p> <ul style="list-style-type: none"> <li>• In der Umgebung der CDE</li> <li>• an kritischen Punkten in der CDE</li> </ul> <p><b>11.4.b</b> Versichern Sie sich durch Untersuchung der Systemkonfigurationen und die Befragung der zuständigen Mitarbeiter, dass das Personal über Systeme zur Erkennung und/oder Verhinderung von Eindringversuchen vor mutmaßlichen Sicherheitsverletzungen gewarnt wird.</p>	<p>Systeme zur Erkennung und/oder Verhinderung von Eindringversuchen (IDS/IPS) vergleichen den aus dem Netzwerk stammenden Datenverkehr mit bekannten Signaturen und/oder Verhalten Tausender von Angriffstypen (Hacker-Tools, Trojaner und andere Malware), versenden Warnmeldungen und/oder unterbinden den Versuch sofort. Ohne einen vorausschauenden Ansatz zur Erkennung unbefugter Aktivitäten mithilfe dieser Tools können sich unentdeckte Angriffe auf (oder Missbrauch von) Computerressourcen ereignen. Die von diesen Systemen ausgegebenen</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p><b>11.4.c</b> Untersuchen Sie die IDS/IPS-Konfigurationen und die Anbieterdokumentation, und prüfen Sie, ob Techniken zur Erkennung und/oder Verhinderung von Eindringversuchen im Sinne eines optimalen Schutzes entsprechend den Anbieteranweisungen konfiguriert, gewartet und aktualisiert werden.</p>	<p>Sicherheitsalarmmeldungen müssen überwacht werden, damit Eindringlinge abgewehrt werden können.</p>
<p><b>11.5</b> Bereitstellung von Systemen zur Erkennung von Änderungen (z. B. Tools zur Überwachung der Dateintegrität), die das Personal über nicht autorisierte Änderungen (einschließlich Änderungen, Hinzufügungen und Löschungen) an wichtigen System-, Konfigurations- oder Inhaltsdateien alarmieren, und Konfiguration der Software für einen mindestens wöchentlich durchgeführten Vergleich wichtiger Dateien.</p> <p><i>(Fortsetzung auf der nächsten Seite)</i></p> <p><b>Hinweis:</b> Zum Zwecke der Erkennung von Änderungen sind wichtige Dateien in der Regel Dateien, die sich nicht regelmäßig ändern, deren Änderung aber auf eine Sicherheitsverletzung im System oder auf das Risiko einer Verletzung hinweisen könnte. Systeme zur Änderungserkennung, wie beispielsweise Produkte zur Dateintegritätsüberwachung, sind in der Regel bereits vorab mit wichtigen Dateien für das jeweilige Betriebssystem konfiguriert. Andere wichtige Dateien wie solche für benutzerdefinierte Anwendungen müssen von der jeweiligen Stelle (Händler oder Dienstleister) beurteilt und definiert werden.</p>	<p><b>11.5.a</b> Überprüfen Sie die Nutzung von Tools zur Änderungserkennung, 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> <li>• Zusätzliche von der Einheit als wichtig betrachtete Dateien (z. B. aufgrund einer Risikobewertung o. ä.)</li> </ul> <p><b>11.5.b</b> Überprüfen Sie, ob die Methoden zur Alarmierung des Personals über nicht zulässige Änderungen (einschließlich Änderungen, Hinzufügungen und Löschungen) an wichtigen Dateien und zur mindestens einmal wöchentlichen Durchführung von Vergleichen wichtiger Dateien konfiguriert sind.</p>	<p>Lösungen zur Änderungserkennung wie etwa FIM-Tools (File-Integrity Monitoring, Überwachung der Dateintegrität) suchen nach Änderungen, Hinzufügungen und Löschungen an wichtigen Dateien und melden, wenn Änderungen entdeckt werden. Falls diese nicht ordnungsgemäß implementiert sind und die Ergebnisse der Änderungserkennung nicht überwacht werden, könnte ein Angreifer Inhalte der Konfigurationsdateien, Betriebssystemprogramme oder ausführbare Anwendungsdateien hinzufügen, löschen oder ändern. Derartige unbefugte Änderungen könnten, falls sie unentdeckt bleiben, vorhandene Sicherheitskontrollen unwirksam machen und/oder dazu führen, dass Karteninhaberdaten ohne merkliche Auswirkungen auf die normale Verarbeitung gestohlen werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>11.5.1</b> Implementierung eines Prozesses zur Reaktion auf Alarme der Lösung zur Änderungserkennung.</p>	<p><b>11.5.1</b> Klären Sie durch eine Befragung des Personals, ob alle Alarmmeldungen untersucht und die Ursachen behoben wurden.</p>	
<p><b>11.6</b> Die Sicherheitsrichtlinien und betrieblichen Verfahren zur Sicherheitsüberwachung und für Tests müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.</p>	<p><b>11.6</b> Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zur Sicherheitsüberwachung und für Tests Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Die Richtlinien und Verfahren sind dokumentiert,</li> <li>• werden verwendet und</li> <li>• sind allen Beteiligten bekannt.</li> </ul>	<p>Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren zur Sicherheitsüberwachung und für Tests kennen und dauerhaft befolgen.</p>

## Befolgung einer Informationssicherheitsrichtlinie

### **Anforderung 12: Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal**

Eine strenge Sicherheitsrichtlinie gibt den Takt für die gesamte Einheit 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“ bzw. „Personal“ hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter, Subunternehmer und Berater, die am Standort der jeweiligen Einheit „ansässig“ sind oder anderweitig Zugriff auf die CDE haben.

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<b>12.1</b> Festlegen, Veröffentlichen, Verwalten und Verbreiten einer Sicherheitsrichtlinie.	<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.	Die Informationssicherheitsrichtlinie eines Unternehmens stellt die Grundlage zur Implementierung von Sicherheitsmaßnahmen zum Schutz wertvoller Unternehmensressourcen dar. Alle Mitarbeiter sollten sich darüber im Klaren sein, dass Daten Gefahren ausgesetzt sind und dass sie für deren Schutz verantwortlich sind.
<b>12.1.1</b> Überarbeitung der Richtlinie mindestens einmal pro Jahr und Aktualisierung bei Umgebungsänderungen.	<b>12.1.1</b> Überprüfen Sie, ob die Richtlinie zur Informationssicherheit mindestens einmal im Jahr überarbeitet und an die geänderten Geschäftsziele bzw. Risiken angepasst wird.	Neue Sicherheitsrisiken und Schutzmaßnahmen entwickeln sich innerhalb kürzester Zeit. Ohne eine regelmäßige Anpassung der Sicherheitsrichtlinie an neue wichtige Änderungen können neue Schutzmaßnahmen zur Bekämpfung dieser Bedrohungen nicht berücksichtigt werden.
<b>12.2</b> Implementierung eines Risikobewertungsprozesses, für den Folgendes gilt: <ul style="list-style-type: none"> <li>• Der Prozess wird mindestens einmal im Jahr und nach wesentlichen Änderungen an der Umgebung (z. B. Übernahmen,</li> </ul>	<b>12.2.a</b> Überprüfen Sie, ob ein jährlicher Prozess zur Risikobewertung dokumentiert ist, der Folgendes beinhaltet: <ul style="list-style-type: none"> <li>• Wichtige Ressourcen, Bedrohungen und Schwachstellen werden ermittelt</li> <li>• Der Prozess führt zu einer offiziellen, dokumentierten Risikoanalyse</li> </ul>	Eine Risikobewertung ermöglicht es einem Unternehmen, Bedrohungen und entsprechende Sicherheitsrisiken mit potenziell negativen geschäftlichen Auswirkungen zu erkennen. Beispiele für verschiedene Risikoüberlegungen sind unter anderem

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>Fusionen, Umzüge usw.) durchgeführt.</p> <ul style="list-style-type: none"> <li>• Beim Prozess werden wichtige Ressourcen, Bedrohungen und Sicherheitsrisiken ermittelt.</li> <li>• Der Prozess führt zu einer offiziellen, dokumentierten Risikoanalyse.</li> </ul> <p><i>Beispiele von Risikobewertungsmethoden sind unter anderen OCTAVE, ISO 27005 und NIST SP 800-30.</i></p>	<p><b>12.2.b</b> Vergewissern Sie sich durch Prüfung der Risikobewertungsdokumentation, dass der Risikobewertungsprozess mindestens einmal jährlich und nach wesentlichen Änderungen an der Umgebung durchgeführt wird.</p>	<p>Cyber-Kriminalität, Web-Angriffe und Schadsoftware auf POS. Anschließend können effektiv entsprechende Ressourcen zur Implementierung von Kontrollen eingesetzt werden, mit denen sich die Wahrscheinlichkeit und/oder die möglichen Auswirkungen eines Angriffs minimieren lassen.</p> <p>Mit Risikobewertungen, die mindestens einmal pro Jahr und bei wesentlichen Änderungen vorgenommen werden, kann das Unternehmen stets auf dem neuesten Stand bezüglich organisatorischen Veränderungen sowie neuen Bedrohungen, Trends und Technologien bleiben.</p>
<p><b>12.3</b> Entwicklung von Verwendungsrichtlinien für wichtige Technologien und Definition der korrekten Verwendung dieser Technologien.</p> <p><i>Hinweis: Beispiele für wichtige Technologien sind unter anderem Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, elektronische Wechselmedien, E-Mail-Programme und Internet-Anwendungen.</i></p> <p>Die Verwendungsrichtlinien umfassen folgende Punkte:</p>	<p><b>12.3</b> Vergewissern Sie sich durch die Untersuchung der Verwendungsrichtlinien für wichtige Technologien und die Befragung der zuständigen Mitarbeiter, ob die folgenden Richtlinien implementiert sind und befolgt werden:</p>	<p>Verwendungsrichtlinien für das Personal können entweder die Nutzung bestimmter Geräte oder Technologien untersagen, sollte dies von der Unternehmensrichtlinie vorgeschrieben sein, oder das Personal über die korrekte Nutzung und Implementierung informieren. Sind keine Verwendungsrichtlinien implementiert, könnte das Personal die Technologien entgegen der Unternehmensrichtlinie nutzen und Angreifern den Weg zu wichtigen Systemen und Karteninhaberdaten freimachen.</p>
<p><b>12.3.1</b> Ausdrückliche Genehmigung durch autorisierte Parteien</p>	<p><b>12.3.1</b> Überprüfen Sie, ob in den Verwendungsrichtlinien Prozesse für eine ausdrückliche Genehmigung von Befugten für die Verwendung dieser Technologien festgelegt sind.</p>	<p>Wird keine entsprechende Genehmigung für Implementierungen vorausgesetzt, können einzelne Personen in gutem Glauben eine Lösung für einen vermuteten Unternehmensbedarf installieren, jedoch gleichzeitig eine nicht unerhebliche Sicherheitslücke öffnen, die wichtige Systeme und Daten böswilligen Personen aussetzt.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>12.3.2</b> Authentifizierung zur Verwendung der Technologie</p>	<p><b>12.3.2</b> Überprüfen Sie, ob die Verwendungsrichtlinien Prozesse enthalten, nach denen sämtliche Technologie nur nach Authentifizierung mittels Benutzer-ID und Kennwort oder mit einem anderen Element (z. B. einem Token) genutzt werden kann.</p>	<p>Wenn Technologien ohne eine entsprechende Authentifizierung implementiert werden (Benutzernamen und Kennwörter, Tokens, VPNs, usw.), können Angreifer diese ungeschützte Technologie mühelos ausnutzen, um auf wichtige Systeme und Karteninhaberdaten zuzugreifen.</p>
<p><b>12.3.3</b> Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff</p>	<p><b>12.3.3</b> Überprüfen Sie, ob die Nutzungsrichtlinien Folgendes definiert:</p> <ul style="list-style-type: none"> <li>• Eine Liste aller wichtigen Geräte, und</li> <li>• Eine Liste aller Mitarbeiter, die zur Verwendung der Geräte autorisiert sind.</li> </ul>	<p>Angreifer können physische Sicherheitsvorrichtungen durchbrechen und ihre eigenen Geräte an das Netzwerk anschließen und somit ein „Hintertürchen“ einzurichten. Es kann auch vorkommen, dass die Mitarbeiter sich nicht an die Verfahren halten. Doch mithilfe einer punktgenauen Bestandsaufnahme und Kennzeichnung der Geräte können nicht zugelassene Installationen schnell entdeckt werden.</p>
<p><b>12.3.4</b> Methode zur genauen und schnellen Bestimmung von Eigentümern, Kontaktinformationen und Zweck (z. B. Etikettierung und Codierung von Geräten sowie Einbuchung in den Bestand)</p>	<p><b>12.3.4</b> Überprüfen Sie, ob in den Nutzungsrichtlinien eine Methode zur genauen und schnellen Bestimmung von Eigentümern, Kontaktinformationen und Zweck (z. B. Etikettierung und Codierung von Geräten sowie Einbuchung in den Bestand) definiert ist.</p>	<p>Angreifer können physische Sicherheitsvorrichtungen durchbrechen und ihre eigenen Geräte an das Netzwerk anschließen und somit ein „Hintertürchen“ einzurichten. Es kann auch vorkommen, dass die Mitarbeiter sich nicht an die Verfahren halten. Doch mithilfe einer punktgenauen Bestandsaufnahme und Kennzeichnung der Geräte können nicht zugelassene Installationen schnell entdeckt werden. Ziehen Sie die Festlegung einer offiziellen Namenskonvention für Geräte in Betracht, und protokollieren Sie alle Geräte gemäß den eingeführten Bestandskontrollen. Eine logische Kennzeichnung mit Informationen, wie etwa Codes, die Aufschluss auf den Besitzer, dessen Kontaktinformationen und den Zweck des Geräts geben, könnten in Erwägung gezogen werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
12.3.5 Akzeptable Verwendung der Technologie	12.3.5 Überprüfen Sie, ob in den Verwendungsrichtlinien eine angemessene Verwendung der Technologie festgelegt ist.	Indem die zulässige betriebliche Nutzung und der Standort der vom Unternehmen genehmigten Geräte und Technologien definiert werden, ist das Unternehmen besser vorbereitet, um Lücken in Konfigurationen und Betriebskontrollen zu bewältigen und zu kontrollieren und um sicherzustellen, dass Angreifern keine Hintertüren geöffnet werden, um sich Zugriff auf wichtige Systeme und Karteninhaberdaten zu verschaffen.
12.3.6 Akzeptable Netzwerkorte für die Technologien	12.3.6 Überprüfen Sie, ob in den Verwendungsrichtlinien angemessene Netzwerkorte für die Technologie festgelegt werden.	
12.3.7 Liste der vom Unternehmen zugelassenen Produkte	12.3.7 Überprüfen Sie, ob in den Verwendungsrichtlinien eine Liste mit vom Unternehmen zugelassenen Produkten enthalten ist.	
12.3.8 Automatisches Trennen von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität	12.3.8.a Überprüfen Sie, ob in den Verwendungsrichtlinien eine automatische Trennung von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität festgelegt ist.	Remotezugriff-Technologien stellen nicht selten Hintertüren zu wichtigen Ressourcen und Karteninhaberdaten dar. Wenn Remotezugriff-Technologien jedoch ausgeschaltet werden, wenn sie nicht in Verwendung sind (z. B. jene, die Ihr POS-Anbieter, andere Anbieter oder Geschäftspartner für den System-Support verwenden), können der Zugriff auf die Netzwerke und die entsprechenden Risiken minimiert werden.
	12.3.8.b Untersuchen Sie Konfigurationen für Remotezugriff-Technologien darauf, ob Remotezugriff-Sitzungen automatisch nach einer bestimmten Zeit der Inaktivität getrennt werden.	
12.3.9 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	12.3.9 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.	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>12.3.10</b> Untersagen Sie Mitarbeitern, die auf Karteninhaberdaten per Remotezugriff zugreifen, die Daten auf lokale Festplatten und elektronische Wechselmedien zu kopieren, zu verschieben oder darauf zu speichern, sofern nicht ausdrücklich aufgrund bekannter geschäftlicher Bedürfnisse gestattet.</p> <p>Wenn ein bekanntes geschäftliches Bedürfnis besteht, muss in den Nutzungsrichtlinien festgelegt sein, dass die Daten entsprechend den geltenden PCI-DSS-Anforderungen geschützt werden.</p>	<p><b>12.3.10.a</b> Überprüfen Sie, ob in den Verwendungsrichtlinien festgelegt ist, dass Karteninhaberdaten, auf die über Remotezugriff-Technologien zugegriffen wird, nicht auf lokale Festplatten und elektronische Wechselmedien kopiert, verschoben oder darauf 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>Damit sich alle Mitarbeiter ihrer Pflicht dahingehend, keine Karteninhaberdaten auf ihren lokalen PCs oder andere Datenträgern zu speichern oder zu kopieren, bewusst sind, muss die Richtlinie ein derartiges Vorgehen strikt untersagen, ausgenommen für Personal, das hierfür eine ausdrückliche Genehmigung besitzt. Das Speichern bzw. Kopieren von Karteninhaberdaten auf eine lokale Festplatte oder andere Medien muss in Übereinstimmung mit den geltenden PCI-DSS-Anforderungen erfolgen.</p>
<p><b>12.4</b> Klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter in den Sicherheitsrichtlinien und Verfahren.</p>	<p><b>12.4.a</b> Überprüfen Sie, ob die Sicherheitsrichtlinien eine klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter enthalten.</p> <p><b>12.4.b</b> Überprüfen Sie durch eine stichprobenartige Befragung, ob die zuständigen Mitarbeiter die Sicherheitsrichtlinien verstehen.</p>	<p>Wenn keine klar definierten Sicherheitsrollen und -verantwortlichkeiten zugewiesen werden, könnte die Folge ein widersprüchliches Zusammenwirken mit der IT-Sicherheitsabteilung sein und daraus anschließend unsichere Implementierungen von Technologien oder die Nutzung veralteter oder nicht gesicherter Technologien entstehen.</p>
<p><b>12.4.1 Zusätzliche Anforderung nur für Dienstanbieter:</b> Die Geschäftsleitung hat die Verantwortung für den Schutz der Karteninhaberdaten und ein PCI-DSS-</p>	<p><b>12.4.1.a</b> Klären Sie durch eine Überprüfung der Dokumentation, ob die Geschäftsleitung die Gesamtverantwortung zur Pflege der PCI-DSS-Konformität der Einrichtung abgetreten hat.</p>	<p><b>Hinweis:</b> Diese Anforderung muss nur beachtet werden, wenn es sich bei der zu bewertenden Einheit um einen Dienstanbieter</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p>Konformitätsprogramm übernommen, das Folgendes beinhaltet:</p> <ul style="list-style-type: none"> <li>• Gesamtverantwortung für die Aufrechterhaltung der PCI-PSS-Konformität</li> <li>• Definition einer Charta für das PCI-DSS-Konformitätsprogramm und die Kommunikation mit der Geschäftsleitung</li> </ul> <p><b>Hinweis:</b> Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</p>	<p><b>12.4.1.b</b> Vergewissern Sie sich durch Überprüfen der PCI-DSS-Charta des Unternehmens, dass sie die Bedingungen darlegt, gemäß denen das PCI-DSS-Konformitätsprogramm organisiert und mit der Geschäftsleitung kommuniziert wird.</p>	<p><i>handelt.</i></p> <p>Die Zuweisung der Verantwortlichkeit für die PCI-DSS-Konformität an die Geschäftsleitung gewährleistet eine Sichtbarkeit des PCI-DSS-Konformitätsprogramm auf Führungsebene und bietet die Gelegenheit, geeignete Fragen zu stellen, um die Effizienz des Programms zu bestimmen und strategische Prioritäten zu beeinflussen. Die Gesamtverantwortung für das PCI-DSS-Konformitätsprogramm kann einzelnen Rollen und/oder Geschäftseinheiten innerhalb der Organisation zugewiesen werden.</p> <p>Zur Geschäftsleitung können C-Level-Positionen, Verwaltungsrat oder gleichwertige Funktionen gezählt werden. Die genauen Titel hängen von der Organisationsstruktur ab. Die Ausführlichkeit der Informationen, die an die Geschäftsleitung geliefert werden, sollte der jeweiligen Organisation und der angesprochenen Zielgruppe entsprechen.</p>
<p><b>12.5</b> Zuweisung der folgenden Managementverantwortungsbereiche in puncto Informationssicherheit zu einer Einzelperson oder einem Team:</p>	<p><b>12.5</b> Überprüfen Sie, ob in den Richtlinien und Verfahren zur Informationssicherheit folgende Punkte enthalten sind:</p> <ul style="list-style-type: none"> <li>• Die Übertragung der formalen Verantwortung für die Informationssicherheit an einen Sicherheitsbeauftragten ein anderes für die Sicherheit zuständiges Mitglied des Managements</li> <li>• Die folgenden Verantwortlichkeiten im Zusammenhang mit der Informationssicherheit werden konkret und formal geregelt:</li> </ul>	<p>Jede Person oder jedes Team, das für das Management der Informationssicherheit zuständig ist, sollte seine Verantwortlichkeiten und Aufgaben durch das Hinzuziehen einer spezifischen Richtlinie kennen. Ohne eine derartige Verpflichtung können Verfahrenslücken den Zugriff auf wichtige Ressourcen oder Karteninhaberdaten ermöglichen.</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, Dokumentation und Verteilung von Sicherheitsrichtlinien und -verfahren formal festgelegt wurde.</p>	<p>Einrichtungen sollten außerdem die Übergangs- und/oder Nachfolgeplanung für Schlüsselpersonal berücksichtigen, um Lücken bei Sicherheitsaufgaben zu vermeiden, welche dazu führen könnten, dass Verantwortlichkeiten nicht zugewiesen sind und diese deshalb nicht durchgeführt werden.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<b>12.5.2</b> Überwachung und Analyse von Sicherheitsalarmen und -informationen und Verteilung an das entsprechende Personal.	<b>12.5.2</b> Überprüfen Sie, ob die Verantwortlichkeit für die Überwachung und Analyse von Sicherheitsalarmen sowie für die Weitergabe von Informationen an das für die Informationssicherheit und die Geschäftseinheit zuständige Managementpersonal formal zugewiesen wurde.	
<b>12.5.3</b> Festlegen, Dokumentieren und Verteilen von Reaktions- und Eskalationsverfahren für Sicherheitsvorfälle, damit eine rechtzeitige und effektive Vorgehensweise in allen Situationen gewährleistet ist.	<b>12.5.3</b> Überprüfen Sie, ob die Verantwortlichkeit für die Festlegung, Dokumentation und Verteilung von Reaktions- und Eskalationsverfahren für Sicherheitsvorfälle formal geregelt wurde.	
<b>12.5.4</b> Administration von Benutzerkonten, einschließlich Ergänzungen, Löschungen und Änderungen.	<b>12.5.4</b> Überprüfen Sie, ob die Verantwortlichkeit für die Administration von Benutzerkonten (Hinzufügen/Löschen/Ändern) und für das Authentifizierungsmanagement formal geregelt wurde.	
<b>12.5.5</b> Überwachung und Kontrolle des gesamten Datenzugriffs.	<b>12.5.5</b> Überprüfen Sie, ob die Verantwortlichkeiten zur Überwachung und Kontrolle des gesamten Datenzugriffs formal zugewiesen wurden.	
<b>12.6</b> Implementierung eines offiziellen Programms zur Förderung des Sicherheitsbewusstseins, das allen Mitarbeitern die Bedeutung der Sicherheitsrichtlinien und Verfahren für Karteninhaberdaten vermittelt.	<b>12.6.a</b> Überprüfen Sie, ob das Programm zur Förderung des Sicherheitsbewusstseins allen Mitarbeitern die Bedeutung der Sicherheitsrichtlinien und Verfahren für Karteninhaberdaten vermittelt.	Wenn das Personal nicht bezüglich seiner Verantwortlichkeiten in punkto Sicherheit und implementierte Sicherheitsvorkehrungen und -verfahren geschult wird, kann es dem Unternehmen durch unterlaufene Fehler oder vorsätzliche Handlungen schaden.
	<b>12.6.b</b> Untersuchen Sie die Verfahren und die Dokumentation des Programms zur Förderung des Sicherheitsbewusstseins, und führen Sie Folgendes durch:	
<b>12.6.1</b> Durchführung von Mitarbeiterschulungen bei der Einstellung und danach mindestens einmal im Jahr.  <i>Hinweis: Die Methoden sind abhängig von der Funktion der Mitarbeiter und deren Zugriffsrechten auf Karteninhaberdaten.</i>	<b>12.6.1.a</b> Überprüfen Sie, ob im Programm zur Förderung des Sicherheitsbewusstseins mehrere Methoden zur Vermittlung des Bewusstseins und zur Schulung des Personals genutzt werden (beispielsweise Poster, Briefe, Memos, webbasierte Schulungen, Meetings und Sonderaktionen).	Wenn das Sicherheitsbewusstseinsprogramm nicht von regelmäßigen Auffrischkursen begleitet wird, geraten wichtige Sicherheitsprozesse und -verfahren in Vergessenheit oder werden umgangen, und zentrale Ressourcen und Karteninhaberdaten werden Gefahren ausgesetzt.
	<b>12.6.1.b</b> Überprüfen Sie, ob die Mitarbeiter zur Einstellung und danach mindestens einmal im Jahr an Schulungen zur Förderung des Sicherheitsbewusstseins teilnehmen.	

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
	<p><b>12.6.1.c</b> Prüfen Sie durch Gespräche mit Mitarbeitern, ob Schulungen zur Förderung des Bewusstseins durchgeführt werden und ob sich die Mitarbeiter der Bedeutung der Sicherheit von Karteninhaberdaten bewusst sind.</p>	
<p><b>12.6.2</b> Die Mitarbeiter müssen mindestens einmal pro Jahr schriftlich bestätigen, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens gelesen und verstanden haben.</p>	<p><b>12.6.2</b> Überprüfen Sie, ob im Programm zur Förderung des Sicherheitsbewusstseins festgelegt ist, dass die Mitarbeiter mindestens einmal im Jahr schriftlich oder elektronisch bestätigen müssen, dass sie die Datensicherheitsrichtlinie gelesen und verstanden haben.</p>	<p>Auch die Aufforderung an das Personal, eine schriftliche oder elektronische Bestätigung abzugeben, hilft dabei, sicherzustellen, dass die Sicherheitsrichtlinien und -verfahren gelesen und verstanden wurden und dass in der Vergangenheit sowie in Zukunft alles daran gesetzt wurde bzw. wird, diese Richtlinien einzuhalten.</p>
<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><b>Hinweis:</b> Für potentielle neue Mitarbeiter wie z. B. Kassierer, die nie Zugriff auf mehrere Kartennummern gleichzeitig haben, wenn eine Transaktion durchgeführt wird, ist diese Anforderung lediglich eine Empfehlung.</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), bevor sie den Zuschlag für eine Stelle erhalten, auf der sie Zugriff auf Karteninhaberdaten haben oder in der Umgebung mit Karteninhaberdaten arbeiten.</p>	<p>Indem gründliche Hintergrundrecherchen über potenzielle neue Mitarbeiter mit potenziellem Zugriff auf Karteninhaberdaten durchgeführt werden, wird das Risiko der unerlaubten Nutzung von PANs und anderen Karteninhaberdaten durch Personen mit fragwürdigem oder gar kriminellem Hintergrund minimiert.</p>
<p><b>12.8</b> Pflege und Implementierung von Richtlinien und Verfahren zur Verwaltung von Dienstleistern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise:</p>	<p><b>12.8</b> Vergewissern Sie sich durch Beobachten und Überprüfen der Richtlinien und Verfahren sowie der unterstützenden Dokumentation, dass alle Prozesse zur Verwaltung von Dienstleistern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise implementiert wurden:</p>	<p>Wenn ein Händler oder Dienstleister Karteninhaberdaten gemeinsam mit einem anderen Dienstleister verwendet, gelten bestimmte Anforderungen, um den dauerhaften Schutz dieser Daten durch diese Dienstleister zu gewährleisten.</p> <p>Einige Beispiele für verschiedene Arten von Dienstleistern sind unter anderem Lagereinrichtungen für Sicherungsbänder, verwaltete Dienstleister wie Webhosting-Anbieter oder Sicherheitsdienstleister, Einrichtungen, die Daten zu Zwecken der Betrugs-Modellierung erhalten, etc.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>12.8.1</b> Pflegen Sie eine Liste von Dienst Anbietern mit Angabe der geleisteten Dienstleistungen.</p>	<p><b>12.8.1</b> Überprüfen Sie, ob eine Liste von Dienst Anbietern gepflegt wird, und ob diese eine Beschreibung der geleisteten Dienstleistungen enthält.</p>	<p>Behalten Sie alle Dienst Anbieter im Auge, bei denen ein potentielles Risiko nicht nur innerhalb des Unternehmens erkannt wurde.</p>
<p><b>12.8.2</b> Aufbewahrung einer schriftlichen Vereinbarung mit einer Bestätigung dazu, dass der Dienst Anbieter für die Sicherheit der Karteninhaberdaten haftet, die sich in seinem Besitz befinden bzw. die er für den Kunden speichert, verarbeitet oder überträgt, bzw. dahingehend, dass die Sicherheit der CDE betroffen sein könnte.</p> <p><b>Hinweis:</b> Der genaue Wortlaut einer Bestätigung hängt davon ab, was die beiden Parteien miteinander vereinbart haben, welche Dienste bereitgestellt wurden und welche Zuständigkeiten den Parteien zugewiesen wurden. Die Bestätigung muss nicht den exakten Wortlaut aus dieser Anforderung enthalten.</p>	<p><b>12.8.2</b> Überprüfen Sie, ob schriftliche Vereinbarungen eine Bestätigung der Dienst Anbieter enthalten, nach der die Dienst Anbieter für die Sicherheit der Karteninhaberdaten haften, die sich in ihrem Besitz befinden bzw. die sie für den Kunden speichern, verarbeiten oder übertragen, bzw. dahingehend, dass die Sicherheit der CDE betroffen sein könnte.</p>	<p>Die Bestätigung der Dienst Anbieter ist Beleg für deren Verpflichtung, die Karteninhaberdaten, die sie von ihren Kunden anvertraut bekommen, entsprechend zu schützen. Das Ausmaß der Verantwortlichkeit des Dienst Anbieters für die Sicherheit von Karteninhaberdaten hängt vom jeweiligen Dienst und der Vereinbarung zwischen dem Anbieter und der beurteilten Einheit ab.</p> <p>In Kombination mit Anforderung 12.9 geht es bei dieser Anforderung darum, ein Grundverständnis über die jeweiligen Verantwortlichkeiten im Rahmen des PCI-DSS herzustellen. So kann die Vereinbarung beispielsweise die anwendbaren PCI-DSS-Anforderungen enthalten, die im Rahmen des bereitgestellten Diensts erfüllt werden sollen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>12.8.3</b> Festlegung eines eindeutigen Prozesses für die Inanspruchnahme von Dienstleistern, der 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 Dienstleistern dokumentiert und implementiert sind und ob vor der Wahl des Anbieters die erforderliche Sorgfalt beachtet wurde.</p>	<p>Das Verfahren gewährleistet, dass jegliche Einbindungen von Serviceanbietern intern vom Unternehmen geprüft werden, dazu zählt auch eine Risikoanalyse vor der Vereinbarung einer formalen Beziehung zu dem Serviceanbieter.</p> <p>Konkrete Prozesse und Ziele zur Wahrung der Sorgfalt sind von Unternehmen zu Unternehmen unterschiedlich. So können beispielsweise die Berichtspraxis des Anbieters sowie Verfahren zur Benachrichtigung bei Verstößen und zur Reaktion auf Vorfälle berücksichtigt werden, aber auch Details zur Aufteilung der PCI-DSS-Verantwortlichkeiten auf die einzelnen Parteien oder zur Validierung der PCI-DSS-Konformität durch den Anbieter bzw. zur Frage, welche Belege bereitgestellt werden.</p>
<p><b>12.8.4</b> Einrichtung eines Programms zur mindestens einmal jährlichen Überwachung der Dienstleister-Konformität mit dem PCI-DSS.</p>	<p><b>12.8.4</b> Überprüfen Sie, ob in der Einheit ein Programm zur mindestens einmal jährlichen Überwachung der Dienstleister-Konformität mit dem PCI-DSS vorliegt.</p>	<p>Wenn Sie den PCI-DSS-Konformitätsstatus Ihres Serviceanbieters kennen, können Sie sich sicher sein, dass er denselben Anforderungen wie auch Ihr Unternehmen unterliegt. Sollte der Dienstleister verschiedene Dienstleistungen anbieten, gilt diese Anforderung nur für jene Dienste, die der Kunde tatsächlich in Anspruch genommen hat und die in den Umfang der PCI-DSS-Untersuchung des Kunden fallen.</p>
<p><b>12.8.5</b> Verwaltung von Informationen darüber, welche PCI-DSS-Anforderungen von den einzelnen Dienstleistern und welche von der Einheit verwaltet werden.</p>	<p><b>12.8.5</b> Prüfen Sie, ob die Einheit Informationen darüber verwaltet, welche PCI-DSS-Anforderungen von den einzelnen Dienstleistern und welche von der Einheit verwaltet werden.</p>	<p>Welche Informationen eine Einheit konkret verwaltet, hängt von der Vereinbarung mit den Anbietern, dem Servicetyp usw. ab. Die Absicht ist, dass die bewertete Einheit erkennt, welche PCI-DSS-Anforderungen ihre Dienstleister gemäß Vereinbarung erfüllen wollen.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>12.9 Zusätzliche Anforderung nur für Dienstanbieter:</b> Dienstanbieter bestätigen den Kunden gegenüber schriftlich, dass sie für die Sicherheit der Karteninhaberdaten haften, die sich in ihrem Besitz befinden bzw. die sie für den Kunden speichern, verarbeiten oder übertragen, bzw. dahingehend, dass die Sicherheit der CDE betroffen sein könnte.</p> <p><i>Hinweis: Der genaue Wortlaut einer Bestätigung hängt davon ab, was die beiden Parteien miteinander vereinbart haben, welche Dienste bereitgestellt wurden und welche Zuständigkeiten den Parteien zugewiesen wurden. Die Bestätigung muss nicht den exakten Wortlaut aus dieser Anforderung enthalten.</i></p>	<p><b>12.9 Zusätzliches Testverfahren nur für die Beurteilung von Dienstanbietern:</b> Vergewissern Sie sich durch Prüfung der Richtlinien und Verfahren des Dienstanbieters und der Vorlagen für schriftliche Vereinbarungen, dass der Dienstanbieter den Kunden schriftlich bestätigt, sämtliche anwendbaren PCI-DSS-Anforderungen in dem Maße zu beachten, in dem der Dienstanbieter die Karteninhaberdaten im Auftrag des Kunden, oder auf eine Weise, die die sich auf die Sicherheit des CDE des Kunden auswirken könnte speichert, verarbeitet oder überträgt.</p>	<p><i>Hinweis: Diese Anforderung ist nur zu beachten, wenn es sich bei der zu bewertenden Einheit um einen Dienstanbieter handelt.</i></p> <p>In Kombination mit Anforderung 12.8.2 geht es bei dieser Anforderung darum, ein Grundverständnis über die Verantwortlichkeiten der Dienstanbieter und ihrer Kunden im Rahmen des PCI-DSS herzustellen. Die Bestätigung der Dienstanbieter ist Beleg für deren Verpflichtung, die Karteninhaberdaten, die sie von ihren Kunden anvertraut bekommen, entsprechend zu schützen.</p> <p>Die internen Richtlinien und Verfahren des Dienstanbieters in Verbindung mit ihrem Kundenbindungsprozess sowie sämtliche Vorlagen für schriftliche Vereinbarungen müssen eine Bestimmung einer geltenden PCI-DSS-Bestätigung an ihre Kunden enthalten. Auf welche Methode der Dienstanbieter die schriftliche Bestätigung gibt, muss zwischen dem Dienstanbieter und seinen Kunden vereinbart werden.</p>
<p><b>12.10</b> Implementierung eines Vorfalldaktionsplans, der eine sofortige Reaktion auf Sicherheitsverletzungen im System ermöglicht.</p>	<p><b>12.10</b> Untersuchen Sie den Vorfalldaktionsplan sowie zugehörige Verfahren, und prüfen Sie, ob die Einheit in der Lage ist, sofort wie folgt auf eine Sicherheitsverletzung zu reagieren:</p>	<p>Ohne einen ausführlichen Vorfalldaktionsplan, der an die verantwortlichen Parteien weitergeleitet, gelesen und verstanden wurde, können Verwirrung und eine fehlende einheitliche Reaktion dem Unternehmen zusätzliche Ausfallszeiten, unnötige Medienpräsenz sowie neue rechtliche Haftungen bescheren.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>12.10.1</b> Erstellung des Vorfalldaktionsplans, der im Falle einer Sicherheitsverletzung im System eingesetzt wird. Der Plan umfasst mindestens die folgenden Punkte:</p> <ul style="list-style-type: none"> <li>• Rollen, Verantwortungsbereiche und Kommunikations-- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Kartenunternehmen</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 Kartenunternehmen zur Reaktion auf Vorfälle</li> </ul>	<p><b>12.10.1.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 Kartenunternehmen</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 Daten von Bürgern des Staates Kalifornien befinden).</li> <li>• Abdeckung sämtlicher wichtigen Systemkomponenten</li> <li>• Verweis auf oder Einbeziehung von Verfahren der Kartenunternehmen zur Reaktion auf Vorfälle</li> </ul> <p><b>12.10.1.b</b> Vergewissern Sie sich durch die Befragung der Mitarbeiter und die stichprobenartige Prüfung der Dokumentation von in der Vergangenheit gemeldeten Sicherheitsverletzungen oder Warnmeldungen, dass der dokumentierte Vorfalldaktionsplan und die entsprechenden Verfahren befolgt wurden.</p>	<p>Der Vorfalldaktionsplan sollte gut durchdacht sein und alle Schlüsselemente enthalten, die es Ihrem Unternehmen ermöglichen, effektiv potentiellen Verstößen zu begegnen, die die Karteninhaberdaten betreffen könnten.</p>
<p><b>12.10.2</b> Überprüfen und testen Sie den Plan mindestens jährlich, einschließlich aller in Anforderung 12.10.1 genannter Elemente.</p>	<p><b>12.10.2</b> Vergewissern Sie sich durch Befragung der Mitarbeiter und Überprüfung der Dokumentation des Testverfahrens, dass der Plan mindestens jährlich getestet wird, und dass das Testverfahren alle in Anforderung 12.10.1 genannten Elemente enthält.</p>	<p>Ohne entsprechende Tests könnten wichtige Schritte vergessen werden, wodurch während eines Vorfalles hohe Risiken entstehen können.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>12.10.3</b> Zur Reaktion auf Alarmmeldungen muss rund um die Uhr spezielles Personal verfügbar sein.</p>	<p><b>12.10.3</b> Überprüfen Sie durch Beobachtung und Untersuchung der Richtlinien sowie Befragung der zuständigen Mitarbeiter, ob Personal bestimmt wurde, das rund um die Uhr sofort auf Vorfälle reagiert sowie sämtlichen Verdachtsmomenten hinsichtlich nicht autorisierter Aktivität, unbefugter WLAN-Zugriffspunkte, wichtiger IDS-Alarme und/oder nicht autorisierter Änderungen an wichtigen Systemen oder Inhaltsdateien nachgeht.</p>	<p>Ohne ein entsprechend ausgebildetes und stets verfügbares Team zur Durchsetzung der Vorfallreaktionspläne könnten größere Schäden am Netzwerk verursacht und wichtige Daten und Systeme durch die unsachgemäße Handhabung der anvisierten Systeme „befallen“ werden. Hierdurch kann auch der Erfolg einer nachträglichen Ursachenanalyse eines Vorfalles vereitelt werden.</p>
<p><b>12.10.4</b> Durchführung von Schulungen für Mitarbeiter, die für die Reaktion auf Sicherheitsverletzungen verantwortlich sind.</p>	<p><b>12.10.4</b> Überprüfen Sie durch Beobachtung und Untersuchung von Richtlinien sowie Befragung des zuständigen Personals, ob die Mitarbeiter, die für die Reaktion auf Sicherheitsverletzungen verantwortlich sind, regelmäßig geschult werden.</p>	
<p><b>12.10.5</b> Berücksichtigung von Alarmmeldungen aus Sicherheitsüberwachungssystemen wie IDS/IPS, Firewalls und Systemen zur Überwachung der Dateiintegrität.</p>	<p><b>12.10.5</b> Überprüfen Sie durch Beobachtung und Untersuchung der Prozesse, ob die Überwachung und die Reaktion auf Alarmmeldungen von Sicherheitssystemen im Vorfallreaktionsplan enthalten sind.</p>	<p>Diese Überwachungssysteme wurden konzipiert, um sich vorrangig auf potentielle Risiken für Daten zu konzentrieren, sie sind von zentraler Bedeutung, wenn es darum geht, eine Sicherheitsverletzung zu verhindern und müssen folglich in die Vorfallreaktionsprozesse aufgenommen werden.</p>
<p><b>12.10.6</b> Entwicklung eines Prozesses zur Änderung und Weiterentwicklung des Vorfallreaktionsplans unter Berücksichtigung von eigenen Erkenntnissen und Branchenentwicklungen.</p>	<p><b>12.10.6</b> Überprüfen Sie durch Beobachtung und Untersuchung von Richtlinien sowie Befragung des zuständigen Personals, ob ein Prozess zur Änderung und Weiterentwicklung des Vorfallreaktionsplans unter Berücksichtigung von eigenen Erkenntnissen und Branchenentwicklungen vorhanden ist.</p>	<p>Durch die Eingliederung der eigenen Erfahrungen in den Vorfallreaktionsplan nach einem Vorfall wird der Plan aktualisiert und in die Lage versetzt, auch auf aufkommende Bedrohungen und Sicherheitstrends zu reagieren.</p>

PCI-DSS-Anforderungen	Prüfverfahren	Anweisung
<p><b>12.11 Zusätzliche Anforderung nur für Dienstanbieter:</b> Führen Sie mindestens einmal vierteljährlich Überprüfungen durch, um zu bestätigen, dass die Mitarbeiter den Sicherheitsrichtlinien und betrieblichen Verfahren folgen. Die Überprüfungen müssen die folgenden Prozesse abdecken:</p> <ul style="list-style-type: none"> <li>• Tägliche Überprüfung der Protokolle</li> <li>• Überprüfung der Firewall-Regelsätze</li> <li>• Anwendung von Konfigurationsstandards auf neue Systeme</li> <li>• Reaktion auf Sicherheitsalarme</li> <li>• Change-Management-Prozesse</li> </ul> <p><i>Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</i></p>	<p><b>12.11.a</b> Prüfen Sie in den Richtlinien und Verfahren, ob Prozesse zur Überprüfung und Bestätigung, dass die Mitarbeiter den Sicherheitsrichtlinien und betrieblichen Verfahren folgen, definiert sind, und dass die Überprüfungen Folgendes abdecken:</p> <ul style="list-style-type: none"> <li>• Tägliche Überprüfung der Protokolle</li> <li>• Überprüfung der Firewall-Regelsätze</li> <li>• Anwendung von Konfigurationsstandards auf neue Systeme</li> <li>• Reaktion auf Sicherheitsalarme</li> <li>• Change-Management-Prozesse</li> </ul> <p><b>12.11.b</b> Vergewissern Sie sich durch Befragung der verantwortlichen Mitarbeiter und Prüfen der Aufzeichnungen der Überprüfungen, dass die Überprüfungen mindestens vierteljährlich durchgeführt werden.</p>	<p><b>Hinweis:</b> Diese Anforderung muss nur beachtet werden, wenn es sich bei der zu bewertenden Einheit um einen Dienstanbieter handelt.</p> <p>Die regelmäßige Bestätigung darüber, dass Sicherheitsrichtlinien und -verfahren befolgt werden, bietet Gewissheit darüber, dass die vorausgesetzten Kontrollen aktiv sind und wie vorgesehen arbeiten. Ziel dieser Überprüfungen ist nicht das erneute Durchführen anderer PCI-DSS-Anforderungen, sondern die Bestätigung darüber, dass Verfahren wie erwartet befolgt werden.</p>
<p><b>12.11.1 Zusätzliche Anforderung nur für Dienstanbieter:</b> Pflegen Sie die Dokumentation des vierteljährlichen Überprüfungsprozesses, sodass diese Folgendes enthält:</p> <ul style="list-style-type: none"> <li>• Dokumentierung der Überprüfungsergebnisse</li> <li>• Überprüfung und Unterzeichnung der Ergebnisse durch Mitarbeiter, welchen die Verantwortung für das PCI-DSS-Konformitätsprogramm übertragen wurde</li> </ul> <p><i>Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.</i></p>	<p><b>12.11.1</b> Klären Sie durch eine Überprüfung der Dokumentation der vierteljährlichen Überprüfung, ob diese Folgendes beinhaltet:</p> <ul style="list-style-type: none"> <li>• Dokumentierung der Überprüfungsergebnisse</li> <li>• Überprüfung und Unterzeichnung der Ergebnisse durch Mitarbeiter, welchen die Verantwortung für das PCI-DSS-Konformitätsprogramm übertragen wurde</li> </ul>	<p><b>Hinweis:</b> Diese Anforderung muss nur beachtet werden, wenn es sich bei der zu bewertenden Einheit um einen Dienstanbieter handelt.</p> <p>Der Zweck dieser unabhängigen Prüfungen ist zu bestätigen, dass Sicherheitsmaßnahmen regelmäßig durchgeführt werden. Anhand dieser Prüfungen kann auch festgestellt werden, ob die entsprechenden Belege gespeichert werden – etwa Audit-Protokolle, Berichte von Schwachstellenprüfungen, Firewall-Prüfungen usw. Diese Informationen sind bei der Vorbereitung der nächsten PCI-DSS-Untersuchung hilfreich.</p>

## Anhang A: Zusätzliche PCI DSS Anforderungen

Dieser Anhang enthält zusätzliche PCI-DSS-Anforderungen für verschiedene Arten von Einrichtungen. Die Abschnitte in diesem Anhang enthalten:

- Anhang A1: Zusätzliche PCI-DSS-Anforderungen für Anbieter von gemeinsamem Hosting
- Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Einheiten, welche SSL/eine frühe Version von TLS verwenden
- Anhang A3: Ergänzende Überprüfung bestimmter Einheiten (Designated Entities Supplemental Validation)

Anleitungen und Informationen zum Geltungsbereich sind in den jeweiligen Abschnitten enthalten.

## Anhang A1: Zusätzliche PCI-DSS-Anforderungen für von mehreren Benutzern gemeinsam genutzte Hosting-Anbieter

Wie in den Anforderung 12.8 und 12.9 erläutert, müssen sämtliche Dienstleister, die auf Karteninhaberdaten zugreifen können (auch Anbieter von gemeinsam genutzten Hosting-Services), den PCI-DSS erfüllen. Außerdem geht aus Anforderung 2.6 hervor, dass Anbieter von gemeinsam genutzten Hosting-Services die gehostete Umgebung und die Daten jeder Einheit schützen müssen. Aus diesem Grund müssen die Hosting-Anbieter auch die Anforderungen in diesem Anhang erfüllen.

A1 Anforderungen	Prüfverfahren	Anweisung
<p><b>A1</b> Schutz der gehosteten Umgebung und der Daten jeder Einheit (d. h. Händler, Dienstleister oder andere Einheiten) gemäß A1 bis A1.4:</p> <p>Ein Hosting-Anbieter muss diese Anforderungen sowie die anderen relevanten Abschnitte des PCI-Datensicherheitsstandards erfüllen.</p> <p><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 Einheit muss PCI-DSS-konform arbeiten und die Konformität von Fall zu Fall beurteilen.</p>	<p><b>A1</b> Prüfen Sie insbesondere bei einer PCI-DSS-Untersuchung eines Anbieters von gemeinsam genutzten Hosting-Services, ob die gehosteten Umgebungen und Daten der einzelnen Einheiten (Händler und Dienstleister) geschützt werden. Wählen Sie dazu stichprobenartig verschiedene Server (Microsoft Windows und Unix/Linux) aus einem repräsentativen Querschnitt aus Hosting-Händlern und -Dienstleistern aus, und führen Sie die unter A1.1 bis A1.4 beschriebenen Tests durch:</p>	<p><i>Anhang A</i> des PCI-DSS gilt für Anbieter von gemeinsam genutzten Hosting-Services, die den Kunden Ihrer Händler und/oder Dienstleister eine PCI-DSS konforme Hosting-Umgebung bieten möchten.</p>
<p><b>A1.1</b> In den einzelnen Einheiten dürfen nur Prozesse ausgeführt werden, die Zugriff auf die CDE dieser Einheit haben.</p>	<p><b>A1.1</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:</p> <ul style="list-style-type: none"> <li>Keine Stelle im System kann die Benutzer-ID eines gemeinsamen Webservers verwenden.</li> <li>Sämtliche von einer Stelle verwendeten CGI-Skripte müssen als eindeutige Benutzer-ID der Stelle erstellt und ausgeführt werden.</li> </ul>	<p>Wenn ein Händler oder Dienstleister berechtigt ist, seine eigenen Anwendungen auf dem gemeinsam genutzten Server auszuführen, müssen diese mit der Benutzer-ID des Händlers oder Dienstleisters anstatt als Benutzer mit besonderen Rechten ausgeführt werden.</p>

A1 Anforderungen	Prüfverfahren	Anweisung
<p><b>A1.2</b> Beschränkung des Zugriffs und der Berechtigungen aller Einheiten auf die jeweils eigene CDE.</p>	<p><b>A1.2.a</b> Vergewissern Sie sich, dass die Benutzer-ID eines Anwendungsprozesses nicht über besondere Rechte (root/admin) verfügt.</p>	<p>Damit die Zugriffsberechtigungen und Rechte so eingeschränkt sind, dass alle Händler bzw. Dienstanbieter nur Zugang zu ihrer eigenen Umgebung haben, müssen folgende Punkte beachtet werden:</p> <ol style="list-style-type: none"> <li>1. Berechtigungen der Benutzer-ID für den Webserver des Händlers oder Dienstanbieters</li> <li>2. Berechtigungen zum Lesen, Schreiben und Ausführen von Dateien</li> <li>3. Berechtigungen zum Schreiben von Systemdateien</li> <li>4. Berechtigungen für die Protokolldateien der Händler und Dienstanbieter</li> <li>5. Kontrollen, mit denen verhindert wird, dass die Systemressourcen ausschließlich von einem Händler oder Dienstanbieter genutzt werden</li> </ol>
	<p><b>A1.2.b</b> Überprüfen Sie, ob die einzelnen Stellen (Händler, Dienstanbieter) Lese-, Schreib- und Ausführungsberechtigungen nur für eigene Dateien und Verzeichnisse oder für notwendige Systemdateien (eingeschränkt durch Dateisystemberechtigungen, Zugriffssteuerungslisten, chroot, jailshell usw.) besitzen.</p> <p><b>Wichtig:</b> Die Dateien einer Stelle können nicht von einer Gruppe gemeinsam genutzt werden.</p>	
	<p><b>A1.2.c</b> Vergewissern Sie sich, dass die Benutzer einer Stelle keinen Schreibzugriff auf gemeinsam genutzte Systemdateien besitzen.</p>	
	<p><b>A1.2.d</b> Überprüfen Sie, ob die Anzeige von Protokolleinträgen auf die protokollbesitzende Einheit beschränkt ist.</p>	
	<p><b>A1.2.e</b> Damit die einzelnen Einheiten die Serverressourcen nicht komplett für sich in Anspruch nehmen und Sicherheitsrisiken (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>	

A1 Anforderungen	Prüfverfahren	Anweisung
<p><b>A1.3</b> Für die CDE jeder Einheit müssen eindeutige, mit der PCI-DSS-Anforderung 10 konforme Protokollierungs- und Audit-Trails aktiviert sein.</p>	<p><b>A1.3</b> Überprüfen Sie, ob der gemeinsame Hosting-Anbieter die Protokollierung für jede einzelne Händler- und Dienstanbieterumgebung wie folgt aktiviert hat:</p> <ul style="list-style-type: none"> <li>• Protokolle werden für gängige Anwendungen von Drittanbietern aktiviert.</li> <li>• Protokolle sind standardmäßig aktiviert.</li> <li>• Protokolle können von der Stelle, die sie besitzt, eingesehen werden.</li> <li>• Die Besitzer der Protokolle erhalten eine Mitteilung zum genauen Speicherort der Protokolle.</li> </ul>	<p>Protokolle sollten in gemeinsam genutzten Hosting-Umgebungen verfügbar sein, damit die Händler und Serviceanbieter auf zu ihrer CDE zugehörige Protokolle zugreifen und diese überprüfen können.</p>
<p><b>A1.4</b> Aktivierung von Prozessen für eine rechtzeitige Ursachenanalyse im Falle einer Sicherheitsverletzung bei einem gehosteten Händler oder Dienstanbieter.</p>	<p><b>A1.4</b> Überprüfen Sie, ob der Anbieter von gemeinsam genutzten Hosting-Services über schriftlich festgehaltene Richtlinien verfügt, die eine rechtzeitige Untersuchung von betroffenen Servern im Falle einer Sicherheitsverletzung ermöglichen.</p>	<p>Von mehreren Benutzern genutzte Hosting-Anbieter müssen über Prozesse mit einer entsprechenden Informationstiefe verfügen, um einerseits schnell und unkompliziert zu antworten, sollte eine Ursachenanalyse bezüglich eines Angriffs notwendig werden, und andererseits damit die Informationen zu den einzelnen Händler oder Serviceanbietern ersichtlich werden.</p>

### **Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Einheiten, die SSL/eine frühe Version von TLS verwenden**

Einheiten, die SSL und frühe Versionen von TLS verwenden, müssen so schnell wie möglich auf Protokolle mit starker Kryptographie hin aktualisieren. Darüberhinaus dürfen SSL und/oder frühe Versionen von TLS nicht in Umgebungen eingeführt werden, in denen diese Protokolle nicht bereits vorhanden sind. Zum Zeitpunkt der Veröffentlichung können die bekannten Schwachstellen nur schwer in POS-POS-Zahlungsumgebungen ausgenutzt werden. Neue Schwachstellen könnten jedoch jederzeit auftauchen, und es ist Aufgabe der Organisation, über die Trends bei Schwachstellen auf dem Laufenden zu bleiben und zu ermitteln, ob sie anfällig für bekannte Schwachstellen ist oder nicht.

Die direkt betroffenen PCI-DSS-Anforderungen sind:

- Anforderung 2.2.3** Implementieren zusätzlicher Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden.

**Anforderung 2.3** Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs mithilfe einer starken Kryptographie.

**Anforderung 4.1** Verwenden von starker Kryptographie und Sicherheitsprotokollen, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen.

SSL und frühe Versionen von TLS dürfen nicht als Sicherheitskontrolle verwendet werden, um diese Anforderungen zu erfüllen. Zur Unterstützung von Einheiten bei der Migration weg von SSL/frühen Versionen von TLS sind die folgenden Bestimmungen enthalten:

- Neue Implementierungen dürfen SSL oder frühe Versionen von TLS nicht als Sicherheitskontrolle verwenden.
- Alle Dienstanbieter müssen ab 30. Juni **2016 ein sicheres Serviceangebot bieten.**
- Nach dem 30. Juni **2018** müssen alle Einheiten die Verwendung von SSL/frühen Versionen von TLS als Sicherheitskontrolle eingestellt haben und ausschließlich sichere Versionen des Protokolls (eine Ausnahmeregelung für bestimmte POS-POI-Terminals wird weiter unten im letzten Aufzählungspunkt beschrieben) verwenden.
- Vor dem 30. Juni 2018 müssen alle vorhandenen Implementierungen, die SSL und/oder frühe Versionen von TLS verwenden, über einen offiziellen Plan zur Risikoabschwächung und Migration verfügen.
- POS-POI-Terminals (und die SSL/TLS Abschlusspunkte, mit welchen sich diese Verbinden), bei welchen nachgewiesen werden kann, dass diese nicht anfällig für bekannte Sicherheitsrisiken von SSL und frühen Versionen von TLS sind, dürfen diese nach dem 30. Juni 2018 weiterhin als Sicherheitskontrolle verwenden.

Dieser Anhang gilt für Einheiten, die SSL/frühe Versionen von TLS als Sicherheitskontrolle zum Schutz des CDE und/oder CHD (z. B. SSL/frühe Versionen von TLS, die zur Erfüllung der PCI-DSS-Anforderungen 2.2.3, 2.3 oder 4.1 verwendet wurden) verwenden. Weitere Informationen zur Verwendung von SSL/frühen Versionen von TLS finden Sie in den aktuellen *PCI SSC ergänzende Informationen zur Migration von SSL und frühen Versionen von TLS*.

A2 Anforderungen	Prüfverfahren	Anweisung
<p><b>A2.1</b> Für POS-POI-Terminals (und die SSL/TLS Abschlusspunkte, mit welchen sich diese Verbinden), die SSL und/oder eine frühe Version von TLS verwenden muss die Einheit entweder:</p> <ul style="list-style-type: none"> <li>Bestätigen, dass die Geräte nicht anfällig für bekannte Sicherheitsrisiken dieser Protokolle sind.</li> </ul> <p><b>Oder:</b></p> <ul style="list-style-type: none"> <li>Über einen offiziellen Plan zur Risikoabschwächung und Migration verfügen.</li> </ul>	<p><b>A2.1</b> Für POS-POI-Terminals (und die SSL/TLS Abschlusspunkte, mit welchen sich diese Verbinden), die SSL und/oder eine frühe Version von TLS verwenden:</p> <ul style="list-style-type: none"> <li>Bestätigen Sie, dass die Einheit über Dokumentation (zum Beispiel Herstellerdokumente, Details der System-/Netzwerkkonfiguration, usw.) verfügt, die bestätigt, dass die Geräte nicht anfällig für bekannte Schwachstellen von SSL/einer frühen Version von TLS sind.</li> </ul> <p>Oder:</p> <ul style="list-style-type: none"> <li>Schließen Sie untenstehenden A2.2 ab.</li> </ul>	<p>POI können weiterhin SSL/eine frühe Version von TLS verwenden, wenn nachgewiesen werden kann, dass der POI nicht anfällig für aktuell bekannte Schwachstellen ist. Bei SSL handelt es sich jedoch um veraltete Technologie und kann daher in Zukunft von weiteren Sicherheitsrisiken betroffen sein; es wird daher dringend empfohlen, dass POI-Umgebungen so schnell wie möglich auf sichere Protokolle aktualisiert werden. Wenn SSL/eine frühe Version von TLS in der Umgebung nicht benötigt werden, sollte die Verwendung dieser Versionen und ein Fallback deaktiviert werden.</p> <p>Sollte die POS-POI-Umgebung anfällig für bekannte Sicherheitsrisiken sein, ist sofort mit der Planung zur Migration auf eine sichere Alternative zu beginnen.</p> <p><b>Hinweis:</b> Die Ausnahmeregelung für POS-POI-Umgebungen, die derzeit nicht anfällig für bekannte Sicherheitsrisiken sind, basiert auf aktuellen, bekannten Risiken. Sollten sich neue Schwachstellen ergeben, für die POI-Umgebungen anfällig sind, müssen diese aktualisiert werden.</p>

A2 Anforderungen	Prüfverfahren	Anweisung
<p><b>A2.2</b> Einrichtungen mit vorhandenen Implementierungen (andere, als die in A2.1 erlaubten), die SSL und/oder frühe Versionen von TLS verwenden, müssen über einen offiziellen Plan zur Risikoabschwächung und Migration verfügen.</p>	<p><b>A2.2</b> Überprüfen Sie den dokumentierten Plan zur Risikoabschwächung und Migration, um sicherzustellen, dass dieser folgende Elemente enthält:</p> <ul style="list-style-type: none"> <li>• Beschreibung der Verwendung einschließlich der Art der verarbeiteten Daten, Arten und Anzahl der Systeme, die SSL/eine frühe Version von TLS verwenden/unterstützen, Art der Umgebung;</li> <li>• Ergebnisse der Risikobewertung und vorhandene Kontrollen zur Risikominderung;</li> <li>• Beschreibung der Prozesse zur Überwachung neuer Schwachstellen in Zusammenhang mit SSL/einer frühen Version von TLS;</li> <li>• Beschreibung der Verfahren zur Änderungskontrolle, die implementiert wurden, um zu gewährleisten, dass SSL/eine frühe Version von TLS nicht in neuen Umgebungen implementiert wird;</li> <li>• Einen Überblick über den Migrationsprojektplan, einschließlich einem Termin für den Abschluss der Migration bis spätestens 30. Juni 2018.</li> </ul>	<p>Der Plan zur Risikoabschwächung und Migration ist ein von der Einheit vorbereitetes Dokument, das die Pläne zur Migration auf ein sicheres Protokoll aufführt und außerdem die Kontrollen der Einheit beschreibt, die diese zur Minderung der Risiken in Verbindung mit SSL/einer frühen Version von TLS verwendet, bis die Migration abgeschlossen ist.</p> <p>Weitere Informationen zu den Plänen zur Risikoabschwächung und Migration finden Sie in den "ergänzende PCI-SSC-Informationen zur Migration von SSL und frühen Versionen von TLS".</p>
<p><b>A2.3 Zusätzliche Anforderung nur für Dienstanbieter:</b> Alle Dienstanbieter müssen ab 30. Juni 2016 ein sicheres Serviceangebot vorhalten.</p> <p><b>Hinweis:</b> Vor dem 30. Juni 2016 muss der Dienstanbieter entweder die Option auf ein sicheres Protokoll in seinem Angebot einschließen, <b>oder</b> über einen dokumentierten Plan zur Risikoabschwächung und Migration (gemäß A2.2) verfügen, der einen Termin bis spätestens 30. Juni 2016 für die Einrichtung eines sicheren Protokolls vorsieht. Nach diesem Datum müssen alle Dienstanbieter die Option auf ein sicheres Protokoll für ihren Service vorhalten.</p>	<p><b>A2.3</b> Vergewissern Sie durch eine Überprüfung der Systemkonfigurationen und der unterstützenden Dokumentation, dass der Dienstanbieter für seinen Dienst die Option auf ein sicheres Protokoll bietet.</p>	<p>Weitere Informationen finden Sie unter "Dienstanbieter" im <i>PCI DSS und PCI-DSS Glossar der Begriffe, Abkürzungen und Akronyme</i>.</p>

### **Anhang A3: Ergänzende Überprüfung bestimmter Einheiten (Designated Entities Supplemental Validation, DESV)**

Dieser Anhang gilt ausschließlich für Einheiten, die von einem Kartenunternehmen oder Acquirer zu einer zusätzlichen Überprüfung der vorhandenen PCI-DSS-Anforderungen aufgefordert wurden. Beispiele für Einrichtungen, für die dieser Anhang gelten **könnte**, sind unter anderem:

- Einrichtungen, die große Mengen an Karteninhaberdaten speichern, verarbeiten und/oder übertragen,
- Einrichtungen, die Aggregationspunkte für Karteninhaberdaten bieten, oder
- Einrichtungen, die schwere oder wiederholte Verletzungen von Karteninhaberdaten erlitten haben.

Diese ergänzenden Validierungsschritte sollen eine größere Sicherheit darüber bieten, dass PCI-DSS-Kontrollen effizient und kontinuierlich durch Validierung der BAU-Prozesse (business-as-usual, Standardbetrieb) und erhöhter Berücksichtigung der Validierung und Umfangsbestimmung erhalten werden.

Die zusätzlichen Validierungsschritte in diesem Dokument sind in folgende Kontrollbereiche organisiert:

**A3.1** Implementierung eines PCI-DSS-Konformitätsprogramms.

**A3.2** Dokumentation und Validierung des PCI-DSS-Umfangs.

**A3.3** Bestätigung darüber, dass PCI DSS in BAU-Aktivitäten (business-as-usual, Standardbetrieb) integriert ist.

**A3.4** Kontrolle und Verwaltung des logischen Zugriffs auf die Karteninhaberdaten-Umgebung.

**A3.5** Ermittlung von und Reaktion auf verdächtige Ereignisse.

**Hinweis:** Einige Anforderungen besitzen definierte Zeiträume (z. B. mindestens vierteljährlich oder alle sechs Monate), in welchen bestimmte Aktivitäten durchgeführt werden. Für die Erstbewertung nach diesem Dokument ist es nicht erforderlich, dass eine Aktivität im jeweiligen Zeitraum des Vorjahres durchgeführt wurde, sofern der Prüfer bestätigt, dass:

- 1) Die Aktivität gemäß der zutreffenden Anforderung innerhalb des letzten Zeitrahmens (das vergangene Quartal oder der vergangene Sechs-Monats-Zeitraum) durchgeführt wurde, und
- 2) Die Einheit über dokumentierte Richtlinien und Verfahren zur weiteren Durchführung der Aktivität innerhalb des definierten Zeitrahmens verfügt.

In den folgenden Jahren nach der Erstbewertung muss eine Aktivität in jedem dafür erforderlichen Zeitraum durchgeführt werden (beispielsweise muss eine vierteljährliche Aktivität in jedem Quartal des Vorjahres durchgeführt worden sein).

**Hinweis:** Eine Einheit muss sich einer Bewertung gemäß diesem Anhang **NUR unterziehen, wenn sie dazu** von einem Acquirer oder einem Kartenunternehmen aufgefordert wird.

A3 Anforderungen	Prüfverfahren	Anweisung
<b>A3.1 Implementierung eines PCI-DSS-Konformitätsprogramms</b>		
<p><b>A3.1.1</b> Die Geschäftsleitung hat die Verantwortung für den Schutz der Karteninhaberdaten und ein PCI-DSS-Konformitätsprogramm übernommen, das Folgendes beinhaltet:</p> <ul style="list-style-type: none"> <li>• Gesamtverantwortung für die Beibehaltung der PCI-PSS-Konformität</li> <li>• Definition einer Charta für das PCI-DSS-Konformitätsprogramm</li> <li>• Melden von Fortschritten über PCI-DSS-Initiativen und -Probleme, einschließlich der Maßnahmen zur Behebung, an die Geschäftsleitung und den Verwaltungsrat, mindestens einmal jährlich</li> </ul> <p><b>PCI-DSS-Referenz:</b> Anforderung 12</p>	<p><b>A3.1.1.a</b> Klären Sie durch eine Überprüfung der Dokumentation, ob die Geschäftsleitung die Gesamtverantwortung zur Pflege der PCI-DSS-Konformität der Einrichtung abgetreten hat.</p> <p><b>A3.1.1.b</b> Vergewissern Sie sich durch Überprüfen der PCI-DSS-Charta des Unternehmens, dass diese die Bedingungen darlegt, unter welchen das PCI-DSS-Konformitätsprogramm organisiert wird.</p> <p><b>A3.1.1.c</b> Stellen Sie durch Überprüfung der Sitzungsprotokolle und/oder Präsentationen der Geschäftsleitung und des Verwaltungsrates sicher, dass die Initiativen und Abhilfemaßnahmen zur PCI-DSS-Konformität mindestens einmal jährlich kommuniziert werden.</p>	<p>Die Zuweisung der Verantwortlichkeit für die PCI-DSS-Konformität an die Geschäftsleitung gewährleistet eine Sichtbarkeit des PCI-DSS-Konformitätsprogramms auf Führungsebene und ermöglicht die Gelegenheit, geeignete Fragen zu stellen, um die Effizienz des Programms zu bestimmen und strategische Prioritäten zu beeinflussen. Die Gesamtverantwortung für das PCI-DSS-Konformitätsprogramm kann einzelnen Rollen und/oder Geschäftseinheiten innerhalb der Organisation zugewiesen werden.</p>
<p><b>A3.1.2</b> Es muss ein offizielles PCI-DSS-Konformitätsprogramm vorhanden sein und folgende Elemente beinhalten:</p> <ul style="list-style-type: none"> <li>• Definition der Aktivitäten zur Erhaltung und Überwachung der PCI-DSS-Konformität insgesamt, einschließlich der BAU-Aktivitäten (business-as-usual, Standardbetrieb)</li> <li>• Jährliche Prozesse zur PCI-DSS-Untersuchung</li> <li>• Prozesse zur kontinuierlichen Validierung der PCI-DSS-Anforderungen (z. B. täglich, wöchentlich, vierteljährlich, etc., gemäß der jeweiligen Anforderung)</li> <li>• Ein Prozess zur Durchführung von Business-Impact-Analysen, um potentielle PCI-DSS-Auswirkungen für strategische Geschäftsentscheidungen</li> </ul>	<p><b>A3.1.2.a</b> Prüfen Sie in den Richtlinien und Verfahren zur Informationssicherheit, ob Prozesse für Folgendes festgelegt wurden:</p> <ul style="list-style-type: none"> <li>• Erhaltung und Überwachung der PCI-DSS-Konformität insgesamt, einschließlich der BAU-Aktivitäten (business-as-usual, Standardbetrieb)</li> <li>• Jährliche PCI-DSS-Untersuchung(en)</li> <li>• Kontinuierliche Validierung von PCI-DSS-Anforderungen</li> <li>• Business-Impact-Analysen zur Bestimmung potentieller PCI-DSS-Auswirkungen für strategische Geschäftsentscheidungen</li> </ul>	<p>Ein offizielles Konformitätsprogramm ermöglicht einer Organisation die Überwachung des Zustandes seiner Sicherheitskontrollen, proaktiv zu sein, wenn eine Kontrolle ausfällt, und eine effiziente Kommunikation der Aktivitäten und des Konformitätsstatus innerhalb der Organisation.</p> <p>Das PCI-DSS-Konformitätsprogramm kann ein eigenständiges Programm, oder Teil eines übergreifenden Konformitäts- und/oder Governance-Programms sein und sollte eine klar definierte Methodik beinhalten, die eine konsistente und effektive Bewertung demonstriert. Beispiele für Methodiken sind unter anderem: Deming-Regelkreis Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC, und Six Sigma.</p> <p style="text-align: right;"><i>(Fortsetzung auf der nächsten Seite)</i></p>

A3 Anforderungen	Prüfverfahren	Anweisung
zu bestimmen <b>PCI-DSS-Referenz:</b> Anforderungen 1 bis 12		
	<p><b>A3.1.2.b</b> Vergewissern Sie sich durch Befragung der Mitarbeiter und Beobachtung der Konformitäts-Aktivitäten, dass die definierten Prozesse für Folgendes implementiert sind:</p> <ul style="list-style-type: none"> <li>• Erhaltung und Überwachung der PCI-DSS-Konformität insgesamt, einschließlich der BAU-Aktivitäten (business-as-usual, Standardbetrieb)</li> <li>• Jährliche PCI-DSS-Untersuchung(en)</li> <li>• Kontinuierliche Validierung von PCI-DSS-Anforderungen</li> <li>• Business-Impact-Analysen zur Bestimmung potentieller PCI-DSS-Auswirkungen für strategische Geschäftsentscheidungen</li> </ul>	<p>Die Erhaltung und Überwachung der gesamten PCI-PSS-Konformität einer Organisation umfasst Aktivitäten, die täglich, wöchentlich, monatlich, vierteljährlich oder jährlich durchgeführt werden müssen und das Sicherstellen, dass diese Aktivitäten entsprechend durchgeführt werden (z. B. Verwenden einer Sicherheits-Selbstbewertung oder PDCA-Methode).</p> <p>Beispiele für strategische Geschäftsentscheidungen, die auf potentielle PCI-DSS-Auswirkungen hin analysiert werden sollten, sind unter anderem Fusionen und Übernahmen, Anschaffungen neuer Technologien, oder neuer Kanäle für die Hereinnahme von Zahlungen.</p>
<p><b>A3.1.3</b> Die Rollen und Verantwortlichkeiten für die PCI-DSS-Konformität müssen spezifisch definiert, einem oder mehreren Mitarbeitern förmlich zugewiesen werden und mindestens folgende Elemente umfassen:</p> <ul style="list-style-type: none"> <li>• Verwaltung von PCI-DSS-Bau (business as usual, Standardgeschäft)-Aktivitäten</li> <li>• Verwaltung jährlicher PCI-DSS-Untersuchungen</li> <li>• Verwaltung der kontinuierlichen Validierung der PCI-DSS-Anforderungen (z. B. täglich, wöchentlich, vierteljährlich, etc., gemäß der jeweiligen Anforderung)</li> <li>• Verwaltung von Business-Impact-</li> </ul>	<p><b>A3.1.3.a</b> Vergewissern Sie sich durch Überprüfung der Richtlinien und Verfahren für Informationssicherheit und durch Befragung von Mitarbeitern, dass Rollen klar definiert und Pflichten zugewiesen sind, und mindestens folgende Elemente enthalten:</p> <ul style="list-style-type: none"> <li>• Verwaltung von PCI-DSS-Bau (business as usual, Standardgeschäft)-Aktivitäten</li> <li>• Verwaltung jährlicher PCI-DSS-Untersuchungen</li> <li>• Verwaltung der kontinuierlichen Validierung der PCI-DSS-Anforderungen (z. B. täglich, wöchentlich, vierteljährlich, etc., gemäß der jeweiligen Anforderung)</li> <li>• Verwaltung von Business-Impact-Analysen zur Bestimmung potentieller PCI-DSS-Auswirkungen für strategische Geschäftsentscheidungen</li> </ul>	<p>Die offizielle Definition der spezifischen Rollen und Verantwortlichkeiten für die PCI-DSS-Konformität hilft dabei, die Verantwortung sicherzustellen und die fortlaufenden Anstrengungen zur PCI-DSS-Konformität zu überwachen. Diese Rollen können einem einzigen oder mehreren Besitzern für die unterschiedlichen Aspekte zugewiesen werden. Diese sollten Personen zugewiesen werden, die berechtigt sind, risikobasierte Entscheidungen zu treffen und die Verantwortung für die spezifische Funktion tragen. Pflichten sollten offiziell definiert sein und die betreffenden Personen in der Lage sein, Verständnis ihrer Aufgaben und Verantwortlichkeiten zu</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p>Analysen zur Bestimmung potentieller PCI-DSS-Auswirkungen für strategische Geschäftsentscheidungen</p> <p><b>PCI-DSS-Referenz:</b> Anforderung 12</p>	<p><b>A3.1.3.b</b> Vergewissern Sie sich durch Befragen der verantwortlichen Mitarbeiter, dass sie mit den ihnen zugewiesenen Aufgaben zur PCI-DSS-Konformität vertraut sind und diese durchführen.</p>	<p>demonstrieren.</p>
<p><b>A3.1.4</b> Bieten Sie Mitarbeitern mit Verantwortung für die PCI-DSS-Konformität mindestens einmal jährlich aktuelle Schulungen zu PCI DSS und/oder Informationssicherheit an (wie in A3.1.3 angegeben).</p> <p><b>PCI-DSS-Referenz:</b> Anforderung 12</p>	<p><b>A3.1.4.a</b> Vergewissern Sie sich durch Überprüfung der Richtlinien und Verfahren für Informationssicherheit, dass Schulungen zu PCI DSS und/oder Informationssicherheit für jede Rolle mit Verantwortung für PCI-DSS-Konformität mindestens jährlich gefordert werden.</p> <p><b>A3.1.4.b</b> Vergewissern Sie sich durch Befragung von Mitarbeitern und Überprüfen der Teilnahmebescheinigungen oder anderer Aufzeichnungen, dass Mitarbeiter mit Verantwortung für die PCI-DSS-Konformität mindestens jährlich aktuelle PCI-DSS-Schulungen beziehungsweise ähnliche Schulungen zur Informationssicherheit erhalten.</p>	<p>Mitarbeiter, die für die PCI-DSS-Konformität verantwortlich sind, haben einen bestimmten Ausbildungsbedarf, der üblicherweise über eine Schulung zum allgemeinen Sicherheitsbewusstsein gedeckt wird. Personen mit Verantwortung für die PCI-DSS-Konformität müssen zusätzlich zur Schulung zur allgemeinen Vertrautheit mit Informationssicherheit außerdem eine spezialisierte Schulung mit Augenmerk auf spezifische Sicherheitsthemen, Fähigkeiten, Prozessen oder Methoden erhalten, die zur effektiven Durchführung ihrer Compliance-Aufgaben erforderlich sind.</p> <p>Die Schulung kann von Drittparteien wie SANS oder PCI SSC (PCI Awareness, PCIP und ISA), Kartenunternehmen und Acquirern oder intern durchgeführt werden. Die Schulungsinhalte müssen für den jeweiligen Tätigkeitsbereich anwendbar sein, aktuell sein und die neuesten Sicherheitsbedrohungen beziehungsweise Versionen des PCI DSS umfassen.</p> <p>Weitere Informationen zur Entwicklung von geeigneten Schulungsinhalten für spezialisierte Rollen finden Sie in den ergänzenden Informationen von PCI SSC unter <i>Bewährte Verfahren zur Umsetzung eines Sicherheitsbewusstseinsprogramms</i>.</p>
<p><b>A3.2 Dokumentation und Validierung des PCI-DSS-Umfangs.</b></p>		
<p><b>A3.2.1</b> Dokumentieren und bestätigen Sie die Genauigkeit des PCI-DSS-Umfangs</p>	<p><b>A3.2.1.a</b> Vergewissern Sie sich durch Überprüfung der Ergebnisse von Umfangsprüfungen und durch</p>	<p>Die Validierung des PCI-DSS-Umfangs ist so häufig wie möglich durchzuführen, um</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p>mindestens vierteljährlich sowie bei signifikanten Änderungen am Anwendungsbereich. Die vierteljährliche Validierung des Umfangs muss mindestens folgende Tätigkeiten umfassen:</p> <ul style="list-style-type: none"> <li>• Identifikation aller Netzwerk und Systemkomponenten innerhalb des Anwendungsbereiches</li> <li>• Identifikation aller Netzwerke außerhalb des Anwendungsbereiches und Begründung für die Außerbetrachtlassung dieser Netzwerke einschließlich einer Beschreibung aller implementierten Segmentierungskontrollen</li> <li>• Identifikation aller verbundener Einheiten—z. B. Drittparteien mit Zugriff auf die Karteninhaberdaten-Umgebung (CDE)</li> </ul> <p><b>PCI-DSS-Referenz:</b> Geltungsbereich der PCI-DSS-Anforderungen</p>	<p>Befragung von Mitarbeitern, dass die Überprüfungen folgendermaßen durchgeführt werden:</p> <ul style="list-style-type: none"> <li>• Mindestens vierteljährlich</li> <li>• Nach wesentlichen Änderungen an der Umgebung</li> </ul> <p><b>A3.2.1.b</b> Überprüfen Sie die Ergebnisse der vierteljährlichen Umfangsprüfungen, um sicherzustellen, dass folgende Tätigkeiten durchgeführt werden:</p> <ul style="list-style-type: none"> <li>• Identifikation aller Netzwerke und Systemkomponenten im Anwendungsbereich</li> <li>• Identifikation aller Netzwerke außerhalb des Anwendungsbereiches und Begründung für die Außerbetrachtlassung dieser Netzwerke einschließlich einer Beschreibung aller implementierten Segmentierungskontrollen</li> <li>• Identifikation aller verbundener Einheiten—z. B. Drittparteien mit Zugang auf das CDE</li> </ul>	<p>sicherzustellen, dass er aktuell ist und den sich ändernden Geschäftszielen entspricht.</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p><b>A3.2.2</b> Bestimmen Sie die Auswirkungen auf den PCI-DSS-Umfang aller Änderungen an Systemen oder Netzwerken, einschließlich Hinzufügungen neuer Systeme und neuer Netzwerkverbindungen. Die Prozesse müssen Folgendes beinhalten:</p> <ul style="list-style-type: none"> <li>• Durchführung einer offiziellen PCI-DSS-Auswirkungsanalyse</li> <li>• Identifikation der auf das System oder Netzwerk anwendbaren PCI-DSS-Anforderungen</li> <li>• Gegebenenfalls Aktualisierung des PCI-DSS-Umfangs</li> <li>• Dokumentierte Unterzeichnung der Ergebnisse der Auswirkungsanalyse durch den verantwortlichen Mitarbeiter (wie in A3.1.3 definiert)</li> </ul> <p><b>PCI-DSS-Referenz:</b> Umfang der PCI-DSS-Anforderungen; Anforderungen 1 bis 12</p>	<p><b>A3.2.2</b> Vergewissern Sie sich durch Überprüfen der Änderungsdokumentation und Befragen von Mitarbeitern, dass für jede Änderung an Systemen oder Netzwerken Folgendes gilt:</p> <ul style="list-style-type: none"> <li>• Eine offizielle PCI-DSS-Auswirkungsanalyse wurde durchgeführt.</li> <li>• Auf System- oder Netzwerkänderungen anwendbare PCI-DSS-Anforderungen wurden ermittelt.</li> <li>• Der PCI-DSS-Umfang wurde entsprechend der Änderung aktualisiert.</li> <li>• Eine Unterzeichnung durch den verantwortlichen Mitarbeiter (wie in A3.1.3 definiert) wurde eingeholt und dokumentiert.</li> </ul>	<p>Änderungen an Systemen oder Netzwerken können signifikante Auswirkungen auf den PCI-DSS-Umfang haben. Zum Beispiel kann das Ändern einer Regel der Firewall ganze Abschnitte des Netzwerks in den Anwendungsbereich verlagern, oder es werden neue Systeme zum CDE hinzugefügt, die angemessen geschützt werden müssen.</p> <p>Prozesse zur Bestimmung der potenziellen Auswirkungen von Änderungen an Systemen und Netzwerken auf den PCI-DSS-Umfang einer Einheit, können als Teil eines PCI-DSS-Konformitätsprogrammes durchgeführt werden, oder unter ein übergreifendes Konformitäts-beziehungsweise Governance-Programms der Einheit fallen.</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p><b>A3.2.2.1</b> Nach Abschluss einer Änderung müssen alle relevanten PCI-DSS-Anforderungen auf allen neuen oder veränderten Systemen und Netzwerken überprüft, und die Dokumentation entsprechend aktualisiert werden. Beispiele für PCI-DSS-Anforderungen, die überprüft werden müssen, sind unter anderem:</p> <ul style="list-style-type: none"> <li>▪ Das Netzwerkdiagramm wird zur Wiedergabe der Änderungen aktualisiert.</li> <li>▪ Die Systeme sind gemäß Konfigurationsstandard konfiguriert, alle Standardkennwörter wurden geändert und nicht benötigte Dienste deaktiviert.</li> <li>▪ Die Systeme sind durch die erforderlichen Kontrollen geschützt— z. B. Tools zur Überwachung der Dateintegrität (FIM), Antivirus, Patches, Audit-Protokollierung.</li> <li>▪ Vergewissern Sie sich, dass vertrauliche Authentifizierungsdaten (SAD) nicht gespeichert werden und alle Speicher von Karteninhaberdaten (CHD) dokumentiert und fester Bestandteil der Richtlinien und Verfahren zur Datenspeicherung sind</li> <li>▪ Neue Systeme werden in die vierteljährlichen Schwachstellenprüfungen mit einbezogen.</li> </ul> <p><b>PCI-DSS-Referenz:</b> Umfang der PCI-DSS-Anforderungen; Anforderungen 1 bis 12</p>	<p><b>A3.2.2.1</b> Untersuchen Sie für eine Stichprobe der System- und Netzwerkänderungen die Änderungsdokumentation, befragen Sie Mitarbeiter und beobachten Sie die betroffenen Systeme/Netzwerke, um sicherzustellen, dass alle anwendbaren PCI-DSS-Anforderungen implementiert wurden und die Dokumentation als Teil der Änderung aktualisiert wurde.</p>	<p>Es ist wichtig, Prozesse zur Analyse aller Änderungen vorzuhalten, um sicherzustellen, dass auf allen Systemen oder Netzwerken, die aufgrund einer Änderung innerhalb der Umgebung hinzugefügt wurden, alle entsprechenden PCI-DSS-Kontrollen angewendet werden.</p> <p>Die Integration dieser Validierung in die Change-Management-Prozesse hilft dabei sicherzustellen, dass die Standards für Gerätebestände und -konfiguration aktuell gehalten und Sicherheitskontrollen wo nötig angewendet werden.</p> <p>Ein Change-Management-Prozess sollte unterstützende Belege dafür enthalten, dass PCI-DSS-Anforderungen implementiert oder über das iterative Verfahren aufrechterhalten wurden.</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p><b>A3.2.3</b> Änderungen an der organisatorischen Struktur—zum Beispiel ein Unternehmenszusammenschluss oder eine Übernahme, oder Änderungen am für Sicherheitskontrollen zuständigen Personal—führen zu einer förmlichen (internen) Überprüfung der Auswirkungen auf den PCI-DSS-Umfang und der Veranlassung von Kontrollen.</p> <p><b>PCI-DSS-Referenz:</b> Anforderung 12</p>	<p><b>A3.2.3</b> Vergewissern Sie sich durch Überprüfung der Richtlinien und Verfahren, dass eine Änderung an der organisatorischen Struktur zu einer offiziellen Überprüfung der Auswirkungen auf den PCI-DSS-Umfang und der Veranlassung von Kontrollen führt.</p>	<p>Die Struktur und das Management einer Organisation definieren die Anforderungen und das Protokoll für effektiven und sicheren Geschäftsbetrieb. Änderungen an dieser Struktur können sich negativ auf vorhandene Kontrollen und Rahmenwerke auswirken, wenn Ressourcen entfernt oder neu verteilt werden, die ehemals PCI-DSS-Kontrollen unterstützt haben, oder neue Verantwortlichkeiten vergeben werden, für die noch keine Kontrollen vorhanden sind. Deshalb ist es wichtig, den PCI-DSS-Umfang und die Kontrollen bei Änderungen zu überprüfen, um sicherzustellen, dass Kontrollen vorhanden und aktiv sind.</p>
<p><b>A3.2.4</b> Falls Segmentierung verwendet wird, bestätigen Sie den PCI-DSS-Umfang durch Durchführung von Penetrationstest an Segmentierungskontrollen, mindestens alle sechs Monate nach Änderungen an den Segmentierungsmethoden.</p> <p><b>PCI-DSS-Referenz:</b> Anforderung 11</p>	<p><b>A3.2.4</b> Untersuchung der Ergebnisse des letzten Penetrationstests, um sicherzustellen, dass:</p> <ul style="list-style-type: none"> <li>• Penetrationstests zur Überprüfung von Segmentierungskontrollen mindestens alle sechs Monate und nach Änderungen an den Segmentierungskontrollen/-methoden durchgeführt werden.</li> <li>• Beim Penetrationstest alle verwendeten Segmentierungskontrollen/-methoden geprüft werden.</li> <li>• Die Penetrationstests bestätigen, dass die Segmentierungsmethoden funktionieren und effektiv sind, und alle Systeme außerhalb des Bereichs müssen von den Systemen innerhalb des CDE isoliert werden.</li> </ul>	<p>Falls Netzwerke innerhalb des Anwendungsbereiches durch Segmentierung von Netzwerken außerhalb des Anwendungsbereiches isoliert werden, müssen diese Segmentierungskontrollen mittels Penetrationstests überprüft werden, um zu bestätigen, dass diese effektiv und wie beabsichtigt arbeiten. Techniken für Penetrationstest müssen der vorhandenen Methodik für Penetrationstest wie in PCI-DSS-Anforderung 11 angegeben folgen.</p> <p>Weitere Informationen zu wirksamen Penetrationstests finden Sie in den ergänzenden Informationen von PCI SSC unter <i>Anleitung für Penetrationstests</i>.</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p><b>A3.2.5</b> Implementieren Sie Methoden zur Datenermittlung zur Bestätigung des PCI-DSS-Umfanges und zur Lokalisierung aller Quellen und Standorte von Klartext-PANs mindestens vierteljährlich und bei signifikanten Änderungen an der Karteninhaber-Umgebung oder -Prozesse.</p> <p>Die Methoden zur Datenermittlung müssen berücksichtigen, dass sich Klartext-PANs eventuell auf Systemen und Netzwerken außerhalb des gegenwärtig definierten CDE befinden.</p> <p><b>PCI-DSS-Referenz:</b> Geltungsbereich der PCI-DSS-Anforderungen</p>	<p><b>A3.2.5.a</b> Vergewissern Sie sich durch Überprüfen der dokumentierten Methoden zur Datenermittlung, dass:</p> <ul style="list-style-type: none"> <li>• Die Methoden zur Datenermittlung Prozesse zur Identifizierung aller Quellen und Standorte von Klartext-PANs enthalten.</li> <li>• Die Methoden berücksichtigen, dass sich Klartext-PANs eventuell auf Systemen und Netzwerken außerhalb des gegenwärtig definierten CDE befinden.</li> </ul> <p><b>A3.2.5.b</b> Überprüfen Sie die Ergebnisse der letzten Anstrengungen zur Datenermittlung und befragen Sie verantwortliche Mitarbeiter, um sicherzustellen, dass die Datenermittlung mindestens vierteljährlich und nach signifikanten Änderungen an der Karteninhaber-Umgebung oder -Prozessen durchgeführt wird.</p>	<p>Der PCI DSS erfordert, dass die bewerteten Einheiten als Teil der Umfangsbestimmung die Existenz aller Klartext-PANs in ihren Umgebungen identifizieren und dokumentieren. Die Implementierung einer Methode zur Datenermittlung, die alle Quellen und Standorte von Klartext-PANs identifiziert und berücksichtigt, dass sich Klartext-PANs eventuell auf Systemen und Netzwerken außerhalb des gegenwärtig definierten CDE oder an unerwarteten Orten innerhalb des definierten CDE befinden—zum Beispiel in einem Fehlerprotokoll oder einem Speicherauszug—hilft dabei sicherzustellen, dass zuvor unbekannte Standorte von Klartext-PANs ermittelt und ordnungsgemäß gesichert werden.</p> <p>Ein Prozess zur Datenermittlung kann mithilfe verschiedener Methoden durchgeführt werden, darunter folgende: (1) kommerziell verfügbare Software für Datenermittlung, (2) ein intern entwickeltes Programm zur Datenermittlung oder (3) eine manuelle Suche. Ungeachtet der verwendeten Methode ist das Ziel der Bemühungen, alle Quellen und Standorte von Klartext-PANs (nicht nur im definierten CDE) zu finden.</p>
<p><b>A3.2.5.1</b> Gewährleisten Sie die Wirksamkeit der Methoden zur Datenermittlung—beispielsweise müssen diese dazu in der Lage sein, Klartext-PANs auf allen Arten von Systemkomponenten (z. B. auf jedem Betriebssystem oder jeder Plattform) und verwendeten Dateivormaten zu entdecken.</p> <p>Die Wirksamkeit von Methoden zur</p>	<p><b>A3.2.5.1.a</b> Vergewissern Sie durch Befragung von Mitarbeitern, dass:</p> <ul style="list-style-type: none"> <li>▪ Die Einheit über einen Prozess zum Testen der Wirksamkeit der Methoden zur Datenidentifikation verfügt.</li> <li>▪ Der Prozess die Bestätigung umfasst, dass die Methoden Klartext-PANs auf allen Arten von Systemkomponenten und verwendeten Dateiformaten ermitteln können.</li> </ul>	<p>Ein Prozess zum Testen der Wirksamkeit der für die Datenermittlung verwendeten Methoden stellt die Vollständigkeit und Präzision der Erkennung von Karteninhaberdaten sicher. Zur Vollständigkeit muss mindesten eine Stichprobenkontrolle von Systemkomponenten sowohl von Netzwerken innerhalb, als auch außerhalb des Anwendungsbereiches im Prozess zur Datenermittlung enthalten sein. Die</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p>Datenermittlung muss mindestens jährlich überprüft werden.</p> <p><b>PCI-DSS-Referenz:</b> <i>Geltungsbereich der PCI-DSS-Anforderungen</i></p>	<p><b>A3.2.5.1.b</b> Vergewissern Sie sich durch Überprüfen von Ergebnissen der Wirksamkeitsprüfungen, dass die Wirksamkeit der Methoden zur Datenerkennung mindestens jährlich überprüft wird.</p>	<p>Genauigkeit kann getestet werden, indem Test-PANs auf eine Probe von Systemkomponenten und verwendeten Dateiformaten abgelegt werden und dabei geprüft wird, ob die Methode zur Datenerkennung diese Test-PANs erkennt.</p>
<p><b>A3.2.5.2</b> Implementieren Sie Reaktionsverfahren, die ausgelöst werden, sobald Klartext-PANs außerhalb des CDE ermittelt werden, und die folgende Elemente enthalten:</p> <ul style="list-style-type: none"> <li>▪ Verfahren zur Bestimmung der Vorgehensweise bei entdeckten Klartext-PANs außerhalb des CDE, einschließlich ihrer Wiederherstellung, sicheren Löschung beziehungsweise Migration in das gegenwärtig definierte CDE, sofern zutreffend</li> <li>▪ Verfahren zur Ermittlung, wie Daten außerhalb des CDE gelangen konnten</li> <li>▪ Verfahren zur Behebung von Datenlecks oder Prozesslücken, die dazu geführt haben, dass Daten außerhalb des CDE gelangt sind</li> <li>▪ Verfahren zur Identifikation der Datenquelle</li> <li>▪ Verfahren zur Ermittlung, ob Spurdaten zusammen mit den PANs gespeichert werden</li> </ul>	<p><b>A3.2.5.2.a</b> Vergewissern Sie sich in dokumentierten Reaktionsverfahren, dass die Verfahren zur Reaktion auf die Erkennung von Klartext-PANs außerhalb des CDE definiert sind und die folgenden Elemente enthalten:</p> <ul style="list-style-type: none"> <li>▪ Verfahren zur Bestimmung des Vorgehens bei entdeckten Klartext-PANs außerhalb des CDE gegebenenfalls einschließlich ihrer Wiederherstellung, sicheren Löschung beziehungsweise Migration in das gegenwärtig definierte CDE</li> <li>▪ Verfahren zur Ermittlung, wie Daten nach außerhalb des CDE gelangen konnten</li> <li>▪ Verfahren zur Behebung von Datenlecks oder Prozesslücken, die dazu geführt haben, dass Daten nach außerhalb des CDE gelangt sind</li> <li>▪ Verfahren zur Identifikation der Datenquelle</li> <li>▪ Verfahren zur Ermittlung, ob Spurdaten zusammen mit den PANs gespeichert werden</li> </ul> <p><b>A3.2.5.2.b</b> Vergewissern Sie sich durch Befragen von Mitarbeitern und Überprüfen der Reaktionsmaßnahmen, dass Abhilfemaßnahmen durchgeführt werden, wenn Klartext-PANs außerhalb des CDE ermittelt werden.</p>	<p>Dokumentierte Reaktionsverfahren für den Fall, dass Klartext-PANs außerhalb des CDE gefunden werden, helfen dabei, die notwendigen Abhilfemaßnahmen zu ermitteln und zukünftige Datenlecks zu verhindern. Wenn beispielsweise eine PAN außerhalb des CDE gefunden wird, muss eine Analyse durchgeführt werden, um (1) zu bestimmen, ob diese unabhängig von anderen Daten gespeichert war (oder Teil einer gesamten Spur war), (2) um die Datenquelle zu ermitteln und (3) um die Lücken in den Kontrollen zu identifizieren, die dazu geführt haben, dass die Daten nach außerhalb des CDE gelangen konnten.</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p><b>A3.2.6</b> Implementieren Sie Mechanismen zur Ermittlung und Verhinderung von Ereignissen, bei welchen Klartext-PANs das CDE über einen nicht autorisierten Kanal, Methode oder Prozess verlassen, einschließlich der Erzeugung von Prüfprotokollen und Alarmen.</p> <p><i>PCI-DSS-Referenz: Geltungsbereich der PCI-DSS-Anforderungen</i></p>	<p><b>A3.2.6.a</b> Klären Sie durch Überprüfung der Dokumentation und Beobachtung der implementierten Mechanismen, dass diese folgende Eigenschaften aufweisen:</p> <ul style="list-style-type: none"> <li>• Sie sind implementiert und werden aktiv ausgeführt</li> <li>• Sie sind so konfiguriert, dass sie feststellen, wenn Klartext-PANs das CDE über einen nicht autorisierten Kanal, Methode oder Prozess verlassen, und dies ggf. verhindern</li> <li>• Sie generieren Protokolle und lösen Alarme aus, wenn festgestellt wird, dass Klartext-PANs das CDE über nicht autorisierte Kanäle, Methoden oder Prozesse verlassen</li> </ul> <p><b>A3.2.6.b</b> Vergewissern Sie sich durch Befragung der verantwortlichen Mitarbeiter und Überprüfung von Prüfprotokollen und Alarmen, dass Alarme untersucht werden.</p>	<p>Mechanismen zur Ermittlung und Vermeidung eines nicht autorisierten Verlusts von Klartext-PANs können geeignete Tools wie Data Loss Prevention (DLP)-Lösungen beziehungsweise manuelle Prozesse und Verfahren sein. Diese Mechanismen müssen unter anderem E-Mails, Downloads auf Wechselmedien und Ausgabe auf Drucker abdecken. Die Verwendung dieser Mechanismen ermöglicht einer Organisation, Situationen zu ermitteln und zu verhindern, die zu Datenverlusten führen könnten.</p>
<p><b>A3.2.6.1</b> Implementieren Sie Reaktionsverfahren, die ausgelöst werden, sobald ein Versuch erkannt wird, Klartext-PANs aus dem CDE über nicht autorisierte Kanäle, Methoden oder Prozess zu entfernen. Reaktionsverfahren müssen folgende Elemente beinhalten:</p> <ul style="list-style-type: none"> <li>▪ Verfahren für die zügige Untersuchung von Alarmen durch verantwortliche Mitarbeiter</li> <li>▪ Verfahren für die Beseitigung von allfälligen Datenlecks oder Prozesslücken zur Verhinderung von Datenverlust</li> </ul>	<p><b>A3.2.6.1.a</b> Vergewissern Sie sich durch Überprüfen der dokumentierten Reaktionsverfahren, dass die Verfahren für die Reaktion auf versuchte Entnahme von Klartext-PANs aus dem CDE über nicht autorisierte Kanäle, Methoden oder Prozesse, die folgenden Elemente enthalten:</p> <ul style="list-style-type: none"> <li>▪ Verfahren für die zügige Untersuchung von Alarmen durch verantwortliche Mitarbeiter</li> <li>▪ Verfahren für die Beseitigung von allfälligen Datenlecks oder Prozesslücken zur Verhinderung von Datenverlust</li> </ul> <p><b>A3.2.6.1.b</b> Befragen Sie Mitarbeiter und überprüfen Sie Aufzeichnungen über Maßnahmen, die ergriffen wurden, wenn Klartext-PANs das CDE über nicht autorisierte Kanäle, Methoden oder Prozesse verlassen haben, und vergewissern Sie sich, dass entsprechende Abhilfemaßnahmen durchgeführt wurden.</p>	<p>Der Versuch, eine Klartext-PAN über nicht autorisierte Kanäle, Methoden oder Prozesse zu entfernen, kann ein Anzeichen für die böswillige Absicht zum Stehlen von Daten sei, oder die Handlung eines autorisierten Mitarbeiters, der sich der ordnungsgemäßen Methoden nicht bewusst ist oder sie einfach nicht befolgt. Durch eine zügige Untersuchung dieser Vorgänge kann bestimmt werden, wo Maßnahmen zur Behebung angewendet werden müssen, und bietet wertvolle Informationen darüber, woher die Bedrohungen stammen.</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<b>A3.3 Bestätigung darüber, dass PCI DSS in BAU-Aktivitäten (business-as-usual, Standardbetrieb) integriert ist</b>		
<p><b>A3.3.1</b> Implementierung eines Prozesses zur sofortigen Ermittlung und Alarmierung von Ausfällen wichtiger Sicherheitskontrollen. Beispiele wichtiger Sicherheitskontrollen sind unter anderem Folgende:</p> <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• IDS/IPS</li> <li>• FIM</li> <li>• Antivirus</li> <li>• Physische Zugangskontrollen</li> <li>• Logische Zugriffskontrollen</li> <li>• Mechanismen zur Audit-Protokollierung</li> <li>• Segmentierungskontrollen (falls verwendet)</li> </ul> <p><b>PCI-DSS-Referenz:</b> Anforderungen 1 bis 12</p>	<p><b>A3.3.1.a</b> Vergewissern Sie sich durch Überprüfen der dokumentierten Richtlinien und Verfahren, dass Prozesse zur sofortigen Erkennung und Alarmierung von Ausfällen wichtiger Sicherheitskontrollen definiert sind.</p> <p><b>A3.3.1.b</b> Klären Sie durch eine Überprüfung der Prozesse zur Ermittlung und Alarmierung und eine Befragung des Personals, ob alle Prozesse für alle wichtigen Sicherheitskontrollen implementiert wurden, und ob ein Ausfall dieser zu einem Alarm führen.</p>	<p>Ohne offizielle Prozesse für die zeitnahe (so schnell wie möglich) Ermittlung und Alarmierung von Ausfällen wichtiger Sicherheitskontrollen könnten Ausfälle längere Zeit unentdeckt bleiben und Angreifern genügend Zeit zur Kompromittierung der Systeme und dem Diebstahl sensibler Daten aus der Karteninhaberdaten-Umgebung bieten.</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p><b>A3.3.1.1</b> Reagieren Sie zeitnah auf Ausfälle wichtiger Sicherheitskontrollen. Die Reaktion auf Ausfälle bei den Sicherheitskontrollen muss die folgenden Prozesse umfassen:</p> <ul style="list-style-type: none"> <li>▪ Wiederherstellung der Sicherheitsfunktionen</li> <li>▪ Ermittlung und Dokumentierung der Dauer (Datum und Zeit von Anfang bis Ende) des Sicherheitsausfalls</li> <li>▪ Ermittlung und Dokumentierung der Ursache(n) des Ausfalls, einschließlich der Fehlerursache, und Dokumentierung der erforderlichen Maßnahmen zur Behebung der Fehlerursache</li> <li>▪ Ermittlung und Lösung von Sicherheitsproblemen, die während des Ausfalls aufgetreten sind</li> <li>▪ Durchführung einer Risikobeurteilung zur Feststellung, ob weitere Maßnahmen als Folge des Sicherheitsausfalls erforderlich sind</li> <li>▪ Implementierung von Kontrollen zur Verhinderung eines Wiederauftretens der Fehlerursache</li> <li>▪ Wiederaufnahme der Überwachung von Sicherheitskontrollen</li> </ul> <p><b>PCI-DSS-Referenz:</b> Anforderungen 1 bis 12</p>	<p><b>A3.3.1.1.a</b> Vergewissern Sie sich in dokumentierten Richtlinien und Verfahren, dass Prozesse zur Reaktion auf den Ausfall von Sicherheitskontrollen festgelegt und implementiert wurden und die folgenden Elemente umfassen:</p> <ul style="list-style-type: none"> <li>▪ Wiederherstellung der Sicherheitsfunktionen</li> <li>▪ Ermittlung und Dokumentierung der Dauer (Datum und Zeit von Anfang bis Ende) des Sicherheitsausfalls</li> <li>▪ Ermittlung und Dokumentierung der Ursache(n) des Ausfalls, einschließlich der Fehlerursache, und Dokumentierung der erforderlichen Maßnahmen zur Behebung der Fehlerursache</li> <li>▪ Ermittlung und Behebung von Sicherheitsproblemen, die während des Ausfalls aufgetreten sind</li> <li>▪ Durchführung einer Risikobeurteilung zur Feststellung, ob weitere Maßnahmen als Folge des Sicherheitsausfalls erforderlich sind</li> <li>▪ Implementierung von Kontrollen zur Verhinderung eines Wiederauftretens der Fehlerursache</li> <li>▪ Wiederaufnahme der Überwachung von Sicherheitskontrollen</li> </ul> <hr/> <p><b>A3.3.1.1.b</b> Vergewissern Sie sich durch eine Überprüfung der Aufzeichnungen, dass Ausfälle von Sicherheitskontrollen dokumentiert sind und die folgenden Elemente enthalten:</p> <ul style="list-style-type: none"> <li>▪ Ermittlung der Ursache(n) des Ausfalls, einschließlich der Fehlerursache</li> <li>▪ Dauer (Datum und Zeit von Anfang bis Ende) des Sicherheitsausfalls</li> <li>▪ Details zu den erforderlichen Maßnahmen zur Behebung der Fehlerursache</li> </ul>	<p>Dokumentierte Belege (z. B. Aufzeichnungen in einem Problemmanagement-System) müssen die vorhandenen Prozesse und Verfahren zur Reaktion auf Sicherheitsausfälle unterstützen. Des weiteren müssen die Mitarbeiter ihre Verantwortung im Falle eines Ausfalles kennen. Maßnahmen und Reaktionen auf den Ausfall müssen in den dokumentierten Belegen erfasst werden.</p>

A3 Anforderungen	Prüfverfahren	Anweisung
<p><b>A3.3.2</b> Bestätigen Sie durch Überprüfung von Hard- und Softwaretechnologien mindestens jährlich, dass diese weiterhin die PCI-DSS-Anforderungen der Organisation erfüllen. (Beispielsweise eine Überprüfung von Technologien, die nicht mehr vom Hersteller unterstützt werden beziehungsweise nicht mehr die Sicherheitsanforderungen der Organisation erfüllen.)</p> <p>Der Prozess umfasst einen Plan zur Bereinigung von Technologien, die nicht mehr den PCI-DSS-Anforderungen der Organisation entsprechen gegebenenfalls einschließlich des Ersatzes dieser Technologien.</p> <p><b>PCI-DSS-Referenz:</b> Anforderungen 2, 6</p>	<p><b>A3.3.2.a</b> Vergewissern Sie sich in dokumentierten Richtlinien und Verfahren und durch Befragen von Mitarbeitern, dass Prozesse zur Überprüfung von Hard- und Softwaretechnologien festgelegt und implementiert sind, die bestätigen, dass diese weiterhin den PCI-DSS-Anforderungen der Organisation entsprechen,.</p> <p><b>A3.3.2.b</b> Vergewissern Sie sich durch Überprüfung der Ergebnisse der letzten Prüfungen, dass Überprüfungen mindestens jährlich stattfinden.</p> <p><b>A3.3.2.c</b> Vergewissern Sie sich, dass für alle Technologien, die nicht mehr den PCI-DSS-Anforderungen der Organisation entsprechen, ein Plan zum Ersatz dieser Technologie vorhanden ist.</p> <p><b>A3.3.3.b</b> Vergewissern Sie sich durch Befragung der verantwortlichen Mitarbeiter und Prüfen der Aufzeichnungen der Überprüfungen, dass:</p> <ul style="list-style-type: none"> <li>• Überprüfungen werden von Mitarbeitern durchgeführt, die dem PCI-DSS-Konformitätsprogramm zugewiesen wurden</li> <li>• Überprüfungen werden mindestens vierteljährlich durchgeführt</li> </ul>	<p>Da Hard- und Softwaretechnologien ständig weiterentwickelt werden müssen sich Organisationen Kenntnis über Änderungen an den Technologien verschaffen, die sie verwenden, ebenso der Entwicklung der Bedrohungen dieser Technologien. Außerdem müssen Organisationen Kenntnis der Änderungen haben, die Technologieanbieter an ihren Produkten oder Support-Prozessen vornehmen, um einschätzen zu können, wie diese Änderungen sich auf die Verwendung dieser Technologien in der Organisation auswirken könnte.</p> <p>Regelmäßige Überprüfungen von Technologien, die die PCI-DSS-Kontrollen beeinflussen, können bei Entscheidungen über Kauf, Verwendung und Einsatz helfen und gewährleisten, dass auf diese Technologien angewiesene Kontrollen effizient bleiben.</p>
<p><b>A3.4 Kontrolle und Verwaltung des logischen Zugriffs auf die Karteninhaberdaten-Umgebung.</b></p>		
<p><b>A3.4.1</b> Stellen Sie durch Überprüfen von Benutzerkonten und Zugangsberechtigungen zu Systemkomponenten im Anwendungsbereich mindestens alle sechs Monate sicher, dass diese Benutzerkonten und Zugänge entsprechend der Tätigkeit weiterhin angemessen und autorisiert sind.</p> <p><b>PCI-DSS-Referenz:</b> Anforderung 7</p>	<p><b>A3.4.1</b> Klären Sie durch Befragungen des Personals und durch Prüfung der Dokumentation Folgendes:</p> <ul style="list-style-type: none"> <li>• Benutzerkonten und Zugangsberechtigungen werden mindestens alle sechs Monate überprüft.</li> <li>• Die Überprüfungen bestätigen, dass der Zugang der dienstlichen Tätigkeit entspricht und dass jeglicher Zugang autorisiert ist.</li> </ul>	<p>Zugangsanforderungen wandeln sich im Laufe der Zeit in dem Maße, in dem sich die Rollen von Personen ändern oder diese das Unternehmen verlassen und sich Funktionen ändern. Die Geschäftsführung muss den Nutzerzugriff bei Bedarf regelmäßig überprüfen, erneut bestätigen und aktualisieren, um ihn an Personaländerungen einschließlich Dritter und an Änderungen der Funktionen anzupassen.</p>
<p><b>A3.5 Ermittlung von und Reaktion auf verdächtige Ereignisse.</b></p>		

A3 Anforderungen	Prüfverfahren	Anweisung
<p><b>A3.5.1</b> Implementieren Sie eine Methode zur zeitnahen und systemweiten Erkennung von Angriffsmustern und unerwünschtem Verhalten—z. B. unter Verwendung koordinierter manueller Überprüfungen beziehungsweise zentral verwalteter oder automatisierter Tools zur Korrelation von Protokollen—die mindestens die folgenden Aktivitäten umfasst:</p> <ul style="list-style-type: none"> <li>• Identifikation von Anomalien oder verdächtigen Aktivitäten, sobald diese auftreten</li> <li>• Zeitnahe Alarmierung von verantwortlichen Mitarbeitern bei Ermittlung verdächtiger Aktivitäten oder Anomalien</li> <li>• Reaktion auf Alarme gemäß den dokumentierten Reaktionsverfahren</li> </ul> <p><b>PCI-DSS-Referenz:</b> Anforderungen 10, 12</p>	<p><b>A3.5.1.a</b> Vergewissern Sie sich durch Befragung der verantwortlichen Mitarbeiter und Überprüfung der Dokumentation, dass eine Methode zur zeitnahen und systemübergreifenden Identifizierung von Angriffsmustern und unerwünschtem Verhalten definiert und implementiert ist und die folgenden Elemente enthält:</p> <ul style="list-style-type: none"> <li>• Identifikation von Anomalien oder verdächtigen Aktivitäten, sobald diese auftreten</li> <li>• Zeitnahe Alarmierung von verantwortlichen Mitarbeitern</li> <li>• Reaktion auf Alarme gemäß den dokumentierten Reaktionsverfahren</li> </ul> <p><b>A3.5.1.b</b> Vergewissern Sie durch Überprüfung der Reaktionsverfahren und Befragung verantwortlicher Mitarbeiter, dass:</p> <ul style="list-style-type: none"> <li>• Bereitschaftspersonal zügig alarmiert wird.</li> <li>• Auf Alarme entsprechend den dokumentierten Reaktionsverfahren reagiert wird.</li> </ul>	<p>Die Fähigkeit, Angriffsmuster und unerwünschte Verhaltensweisen systemübergreifend zu identifizieren, ist entscheidend für das Verhindern, Ermitteln oder Minimieren von Auswirkungen einer Datenkompromittierung. Mithilfe von Protokollen in allen Umgebungen kann die Ursache von Problemen schnell gefunden werden. Außerdem können Warnmeldungen ausgegeben und Analysen erstellt werden. Die Ursache einer Kompromittierung ohne einen Prozess zur Erfassung von Daten wichtiger Systemkomponenten und Systemen festzustellen, die Sicherheitsfunktionen ausführen—wie Firewalls, IDS/IPS und Systemen zur Überwachung der Datenintegrität (FIM), ist wenn überhaupt nur schwer möglich. Daher müssen Protokolle für alle wichtigen Systemkomponenten und Systeme, die Sicherheitsfunktionen ausführen, gesammelt, korreliert und gepflegt werden. Dies könnte auch die Verwendung von Softwareprodukten und Dienstleistungen umfassen, die Echtzeitanalysen, Alarmierung und Meldung bieten—wie Security-Information und Event-Management Lösungen (SIEM), Tools zur Überwachung der Datenintegrität (FIM), oder Systemen zur Änderungserkennung.</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 aufwiegt. (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. Den 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, da 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 Remote-Zugriff ist gemäß PCI-DSS eine Authentifizierung anhand mehrerer Faktoren erforderlich. Die Authentifizierung anhand mehrerer 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 Multi-Faktor-Authentifizierung kann eine akzeptable Kompensationskontrolle darstellen, sofern: (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. Kann beispielsweise ein Unternehmen Karteninhaberdaten nicht nach Anforderung 3.4 unlesbar machen (z. B. durch Verschlüsselung), so 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) Multi-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 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 – Kompensationskontrollen

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

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

### Anforderungsnummer und -definition:

	Erforderliche Informationen	Erklärung
<b>1. Einschränkungen</b>	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung verhindern.	
<b>2. Ziel</b>	Definieren Sie das Ziel der ursprünglichen Kontrolle und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	
<b>3. Ermitteltes Risiko</b>	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	
<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.	
<b>5. Validierung der Kompensationskontrollen</b>	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	
<b>6. Verwaltung</b>	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	

## Arbeitsblatt – Kompensationskontrollen – Beispiel

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

**Anforderungsnummer:** 8.1.1 – Werden alle Benutzer anhand einer eindeutigen Benutzer-ID 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	<i>Unternehmen XYZ verlangt von allen Anwendern, sich an den Servern mit ihren regulären Benutzerkonten anzumelden und anschließend den Befehl</i>

	Risiko ansprechen.	<p>„sudo“ zu verwenden, um administrative Befehle auszuführen. Dies ermöglicht die Verwendung von Berechtigungen des Kontos „root“ zum Ausführen vordefinierter Befehle, die von sudo im Sicherheitsprotokoll aufgezeichnet werden. Auf diese Weise können die Aktionen jedes Benutzers auf ein individuelles Nutzerkonto verfolgt werden, ohne dass das „root“-Kennwort an die Benutzer ausgegeben werden muss.</p>
<b>5. Validierung der Kompensationskontrollen</b>	Festlegen, wie die Kompensationskontrollen validiert und getestet werden.	<p>Das Unternehmen XYZ demonstriert dem Prüfer, dass der sudo Befehl ordnungsgemäß mithilfe einer „sdoers“-Datei konfiguriert ist, wodurch ausschließlich vordefinierte Befehle von bestimmten Anwendern ausgeführt werden können, und dass alle von Personen mittels sudo durchgeführten Aktivitäten protokolliert werden, um so die Person identifizieren zu können, welche die Aktivität mit „root“-Berechtigung durchführt.</p>
<b>6. Pflege</b>	Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen festlegen.	<p>Unternehmen XYZ dokumentiert Prozesse und Verfahren, mit denen dafür gesorgt wird, dass sudo-Konfigurationen nicht durch Änderung, Bearbeitung oder Löschen so bearbeitet werden können, dass eine Ausführung von „root“-Befehlen ohne individuelle Benutzerverfolgung bzw. Protokollierung möglich würde.</p>

## Anhang D: Segmentierung und Stichprobenkontrolle von Unternehmenseinrichtungen/Systemkomponenten

