Payment Card Industry (PCI)

Datensicherheitsstandard

Anforderungen und Sicherheitsbeurteilungsverfahren

Version 3.0

November 2013

Dokumentänderungen

Datum	Version	Beschreibung	Seiten
Oktober 2008	1.2	*Zur Einführung von PCI-DSS v1.2 als „PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren“ und zur Abschaffung von Redundanzen zwischen verschiedenen Dokumenten und zur Implementierung sowohl allgemeiner als auch spezifischer Änderungen seit dem PCI-DSS-Sicherheitsprüfverfahren v1.1. Ausführliche Informationen finden Sie in der Änderungsübersicht von PCI-DSS-Version 1.1 auf 1.2.*	
Juli 2009	1.2.1	*Fügen Sie den Satz ein, der fälschlicherweise in PCI-DSS v1.1 und v1.2 gelöscht wurde.*	5
		Korrigieren Sie in der englischen Version der Prüfverfahren 6.3.7.a und 6.3.7.b „then“ in „than“.	32
		Entfernen Sie im Testverfahren 6.5.b die ausgegraute Markierung in den Spalten „Implementiert“ und „Nicht implementiert“.	33
		Für Arbeitsblätter zu Kompensationskontrollen – Muster, ändern Sie die Formulierung am Seitenanfang in der englischen Version um in „Use this worksheet to define compensating controls for any requirement noted as ‘in place’ via compensating controls.“	64
Oktober 2010	2.0	*Aktualisieren und Implementieren der Änderungen seit der Version 1.2.1. Siehe PCI-DSS – Änderungsübersicht von PCI-DSS-Version 1.2.1 auf 2.0.*	
November 2013	3.0	*Aktualisierung von v2.0. Siehe PCI-DSS – Änderungsübersicht von PCI-DSS-Version 2.0 auf 3.0.*	

Inhalt

Einführung und Überblick über den PCI-Datensicherheitsstandard

Der Payment Card Industry Data Security Standard (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 Karteninhaberdaten. Der PCI-DSS gilt für alle Einheiten, die an der Verarbeitung von Zahlungskarten beteiligt sind – einschließlich Händlern, Verarbeitungsunternehmen, abrechnenden Stellen, Kartenemittenten und Dienstleistern sowie anderen Stellen, die CHD (Cardholder Data, Karteninhaberdaten) und/oder SAD (Sensitive Authentication Data, Vertrauliche Authentifizierungsdaten) speichern, verarbeiten oder weitergeben. Im Folgenden finden Sie eine übergeordnete Übersicht über die zwölf PCI DSS-Anforderungen.

Überblick über den PCI-Datensicherheitsstandard

Erstellung und Wartung sicherer Netzwerke und Systeme	**1.** Installation und Aufrechterhaltung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten **2.** Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden
Schutz von Karteninhaberdaten	**3.** Schutz gespeicherter Karteninhaberdaten **4.** Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
Unterhaltung eines Anfälligkeits-Managementprogramms	**5.** Verwendung und regelmäßige Aktualisierung von Antivirensoftware **6.** Entwicklung und Wartung sicherer Systeme und Anwendungen
Implementierung starker Zugriffskontrollmaßnahmen	**7.** Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf **8.** Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten **9.** Physischen Zugriff auf Karteninhaberdaten beschränken
Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken	**10.** Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten **11.** Regelmäßiges Testen der Sicherheitssysteme und -prozesse
Befolgung einer Informationssicherheitsrichtlinie	**12.** Verwaltung einer Informationssicherheitsrichtlinie für das gesamte Personal

Das vorliegende Dokument, der *PCI-Datensicherheitsstandard - Anforderungen und Sicherheitsbeurteilungsverfahren*, kombiniert die 12 PCI-DSS-Anforderungen und die entsprechenden Prüfverfahren in ein Sicherheitsbeurteilungstool. Es wurde zur Verwendung während den PCI-DSS-Konformitätsbeurteilungen als Teil des Validierungsprozesses einer Stelle konzipiert. In den folgenden Abschnitten werden ausführliche Richtlinien und Best Practices dargelegt, um Stellen bei der Durchführung und Berichterstattung der Ergebnisse einer PCI-PSS-Beurteilung zu unterstützen. Die PCI-DSS-Anforderungen und Testverfahren beginnen auf Seite 15.

Der PCI-DSS setzt sich aus Mindestanforderungen zum Schutz von Karteninhaberdaten zusammen; er kann durch zusätzliche Kontrollen und Verfahren verbessert werden, um mögliche Risiken zu minimieren und den lokal, regional oder branchenweit geltenden Gesetzen und Regelungen zu entsprechen. Ferner können die gesetzlichen oder regulatorischen Anforderungen konkrete Schutzmaßnahmen personenbezogener Informationen oder anderer Datenelemente (z. B, der Name 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) finden Sie eine Vielzahl zusätzlicher Ressourcen rund um die PCI-DSS-Bewertungen und -Validierungen, wie z. B.:

- Dokumentbibliothek mit folgendem Inhalt:
  - *PCI-DSS – Änderungsübersicht von PCI-DSS-Version 2.0 auf 3.0*
  - *PCI-DSS-Kurzübersicht*
  - *Der PCI-DSS und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme*
  - *Ergänzungen und Richtlinien*
  - *Priorisierte Herangehensweise an den 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)
- PCI-Website 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 Ergänzungen vervollständigen den PCI-DSS und bestimmen zusätzliche Aspekte und Empfehlungen zur Einhaltung der PCI-DSS-Anforderungen – sie treten nicht an die Stelle des PCI-DSS oder von dessen Anforderungen und stellen auch keine Erweiterung des Standards dar.*

Informationen zu diesen und weiteren Ressourcen finden Sie unter *www.pcisecuritystandards.org*.

Informationen zur PCI DSS-Anwendbarkeit

Der PCI-DSS gilt für alle Einheiten, die an der Verarbeitung von Zahlungskarten beteiligt sind – einschließlich Händlern, Verarbeitungsunternehmen, Finanzinstitutionen und Dienstleistern sowie anderen Stellen, die Karteninhaberdaten und/oder vertrauliche Authentifizierungsdaten speichern, verarbeiten oder weitergeben.

Karteninhaberdaten und vertrauliche Authentifizierungsdaten sind wie folgt definiert:

Kontodaten	
Zu den Karteninhaberdaten zählen:	**Zu den vertraulichen Authentifizierungsdaten zählen:**
▪ Primary Account Number (PAN) ▪ Name des Karteninhabers ▪ Ablaufdatum ▪ Servicecode	▪ Vollständige Verfolgungsdaten (Magnetstreifendaten oder gleichwertige Daten auf einem Chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN-Blöcke

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 vorhanden sind, müssen diese Daten gemäß den PCI-DSS-Anforderungen geschützt werden.

Die PCI-DSS-Anforderungen gelten für Organisationen und Umgebungen, 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[1]. 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.

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

[1] Im Einklang mit den Konformitätsprogrammen der einzelnen Zahlungsmarken

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

[2] Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung (auch im verschlüsselten Zustand) nicht gespeichert werden.
[3] Vollständige Verfolgungsdaten vom Magnetstreifen, gleichwertige Daten auf dem Chip oder einem anderen Speicherort
[4] Die drei- bzw. vierstellige Zahl auf der Vorder- bzw. Rückseite der Zahlungskarte
[5] 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.

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

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, Rechengeräte 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 Hypervisors.
- 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 Anwendungen (z. B. Internet).
- 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 und sicherstellen, dass diese in dem PCI-DSS-Umfang enthalten sind. Um die Richtigkeit und Angemessenheit des PCI-DSS-Umfangs zu bestätigen, gehen Sie wie folgt vor:

- Die betreffende Einheit identifiziert und dokumentiert sämtliche vorhandenen Karteninhaberdaten in ihrer Umgebung, damit keine Karteninhaberdaten außerhalb der aktuell definierten CDE existieren.
- Sobald alle Speicherorte von Karteninhaberdaten identifiziert und dokumentiert sind, setzt die betreffende Stelle die entsprechenden Ergebnisse ein, um zu überprüfen, ob der PCI-DSS-Umfang angemessen ist (die Ergebnisse können z. B. in Form eines Diagramms oder eines Bestands der Speicherorte von Karteninhaberdaten dargestellt werden).
- Die Einheit berücksichtigt sämtliche Karteninhaberdaten, die sich im Umfang der PCI-DSS-Bewertung befinden und Teile der CDE sind. Falls die Einheit Daten ermittelt, die sich zurzeit nicht in der CDE befinden, müssen diese Daten sicher gelöscht, migriert und 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 genau 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-Beurteilung
- Die Kosten der PCI-DSS-Beurteilung
- Die Kosten und Schwierigkeiten der Implementierung und Verwaltung von PCI-DSS-Kontrollen
- Das Risiko für ein Unternehmen (wird durch die Konsolidierung von Karteninhaberdaten in weniger, stärker kontrollierte Speicherorte verringert)

Ohne eine adäquate Netzwerksegmentierung (die manchmal als „flaches Netzwerk“ bezeichnet wird), befindet sich das gesamte Netzwerk im Umfang der PCI-DSS-Beurteilung. Die Netzwerksegmentierung kann mithilfe einer Vielzahl von physischen oder logischen Mitteln erreicht werden, beispielsweise durch angemessen konfigurierte interne Netzwerk-Firewalls, Router mit umfassenden Zugriffssteuerungslisten oder andere Technologien, die den Zugriff auf ein bestimmtes Segment eines Netzwerks einschränken. 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 Einschränkung von Karteninhaberdaten auf möglichst wenig Speicherorte durch die Beseitigung nicht erforderlicher Daten und die Konsolidierung erforderlicher Daten erfordert unter Umständen die Überarbeitung bewährter Unternehmensverfahren.

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

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

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

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 eine Stelle den Technologiebedarf sorgfältig gegen die Risiken abwägen. Sie sollten den Einsatz drahtloser Technologie nur für die Übertragung nicht vertraulicher Daten in Erwägung ziehen.

Ausgliederung an Drittanbieter

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

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

Die Parteien müssen unmissverständlich angeben, welche Services und Systemkomponenten zum Umfang der PCI-DSS-Bewertung des Dienstanbieters gehören. Außerdem muss geklärt werden, welche konkreten PCI-DSS-Anforderungen vom Dienstanbieter erfüllt werden und welche Anforderungen im Verantwortungsbereich der Kunden des Dienstanbieters liegen und von diesen in eigenen PCI-DSS-Prüfungen zu berücksichtigen sind. So muss ein Anbieter von Aufnehmen 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.

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

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

Falls der Drittanbieter eine eigene PCI-DSS-Bewertung vornimmt, muss er den Kunden gegenüber in ausreichendem Umfang belegen, dass der Umfang der PCI-DSS-Bewertung 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 eine Einheit die Effektivität der Sicherheitskontrollen fortwährend überwachen und dafür sorgen, dass die Umgebung auch zwischen zwei PCI-DSS-Bewertungen PCI-DSS-konform ist. Unter anderem kann der PCI-DSS wie folgt 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 wie beabsichtigt funktionieren.
2. Schnelle Erkennung und Behebung aller Ausfälle bei den Sicherheitskontrollen. Die Reaktion auf Ausfälle bei den Sicherheitskontrollen muss die folgenden Prozesse umfassen:
    - 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 angemessenen Sicherheitskontrollen.
4. Änderungen an der Organisationsstruktur (z. B. Unternehmensfusion oder -übernahme) müssen zu einer formellen Prüfung der Auswirkungen auf den Geltungsbereich und die Anforderungen des PCI-DSS führen.
5. Es muss regelmäßig geprüft und kommuniziert werden, 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 Sie die 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 einzelne Technologien vom Anbieter nicht mehr unterstützt werden oder die Sicherheitsanforderungen der Einheit nicht erfüllen, muss die Einheit einen Plan zur Abhilfe erarbeiten, 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 sein, dass niemand die vollständige 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: *Diese bewährten Verfahren für die Umsetzung des PCI-DSS in BAU-Prozessen werden ausschließlich als Empfehlungen und Leitlinien zur Verfügung gestellt. Sie stellen keinen Ersatz bzw. keine Erweiterung von PCI-DSS-Anforderungen dar.*

Für Bewerter: 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 einer Einheit auf PCI-DSS-Konformität Stichproben der Unternehmenseinrichtungen/Systemkomponenten untersuchen, aber eine Einheit kann nicht die PCI-DSS-Anforderungen nur auf Stichproben der Umgebung anwenden (beispielsweise gelten die Anforderungen für die vierteljährlichen Schwachstellenprüfungen für sämtliche Systemkomponenten). Gleichzeitig 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 Konformität der Einheit mit den PCI-DSS-Anforderungen zu bewerten. 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 zumindest verschiedene Anwendungen (z. B. Datenbankserver, Webserver, Datenübertragungsserver) enthalten.

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

- Wenn standardisierte, zentralisierte PCI-DSS-Sicherheits- und Betriebsprozesse und -kontrollen zur Konsistenzsicherung implementiert sind, welche von den einzelnen Unternehmenseinrichtungen und Systemkomponenten eingehalten werden müssen, können die Stichproben begrenzter ausfallen, als wenn keine standardisierten Prozesse/Kontrollen vorhanden sind. Die Stichprobe muss groß genug sein, um dem Prüfer die Sicherheit zu geben, dass alle Unternehmenseinrichtungen und Systemkomponenten gemäß den Standardprozessen aufgebaut sind. 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, um Unternehmenseinrichtungen/Systemkomponenten aller einzelnen Prozesstypen aufzunehmen.

- Wenn keine standardisierten PCI-DSS-Prozesse/Kontrollen implementiert sind und alle Unternehmenseinrichtungen/Systemkomponenten über einen nicht standardisierten Prozess verwaltet werden, muss die Stichprobe größer sein, damit der Prüfer die Gewissheit hat, dass alle Unternehmenseinrichtungen/Systemkomponenten die PCI-DSS-Anforderungen korrekt umgesetzt haben.
- 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 Sie, warum die jeweilige Stichprobentechnik und -größe ausgewählt wurde,
- Dokumentieren und validieren Sie die zur Ermittlung der Stichprobengröße usw. verwendeten standardisierten PCI-PSS-Prozesse und Kontrollen und
- Erläutern Sie, inwieweit die Stichprobe angemessen und repräsentativ für den gesamten Bestand ist.

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

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

Kompensationskontrollen

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

Das Arbeitsblatt zu Kompensationskontrollen *(Anhang C)* **muss** für jede Kompensationskontrolle ausgefüllt werden. Darüber hinaus sollten Kompensationskontrollergebnisse 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) werden jetzt in der *ROC-Berichtsvorlage für den PCI-DSS* bereitgestellt.

Die *ROC-Berichtsvorlage für den PCI-DSS* muss als Vorlage zum Erstellen des *Konformitätsberichts* verwendet werden. Die beurteilte Einhaltung sollte die entsprechenden Reporting-Anforderungen jeder Zahlungsmarke befolgen, um zu gewährleisten, dass jede Zahlungsmarke den Konformitätsstatus der Einheit anerkennt. Setzen Sie sich mit jeder Zahlungsmarke bzw. dem Acquirer in Verbindung, um Reporting-Anforderungen und Anweisungen zu ermitteln.

Prozess zur PCI-DSS-Bewertung

1. Bestätigen Sie den Umfang der PCI-DSS-Bewertung.
2. Führen Sie die PCI-DSS-Bewertung der Umgebung aus, und befolgen Sie die Testverfahren für die einzelnen Anforderungen.
3. Führen Sie bei Bedarf Abhilfemaßnahmen für alle nicht vorhandenen Elemente durch.
4. 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.
5. Füllen Sie die Konformitätsbescheinigung je nachdem für Dienstanbieter oder Händler vollständig aus. Konformitätsbescheinigungen finden Sie auf der PCI-SSC-Website.
6. 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 bei der Zahlungsmarke oder einer anderen Anforderungsstelle (für Dienstanbieter) ein.

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.
- **Leitfaden** – 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 PA-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-Bewertung stehen Ihnen auf der PCI-SSC-Website die folgenden Ressourcen zur Verfügung:

- *Anweisungen zur Fertigstellung 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 vertraulicheren Bereichen innerhalb dem internen vertrauenswürdigen Netzwerk 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	LEITFADEN
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 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. Dank der Konfigurationsstandards und Verfahren wird die erste Verteidigungslinie eines Unternehmens in Sachen Datenschutz aufrechterhalten.
1.1.1 Ein offizieller 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: • Sämtliche Netzwerkverbindungen • Sämtliche Änderungen an den Firewall- und Router-Konfigurationen	Ein dokumentierter und umgesetzter 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. Ohne formale Genehmigung und ohne Test der Änderungen werden die Datensätze zu den
	1.1.1.b Eine Stichprobe der Netzwerkverbindungen erhalten	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
	Sie, wenn Sie mit dem verantwortlichen Personal sprechen und anhand von Datensätzen prüfen, ob die Netzwerkverbindungen genehmigt und getestet wurden.	Änderungen unter Umständen nicht aktualisiert. Dies könnte zu Widersprüchen zwischen der Netzwerkdokumentation und der tatsächlichen Konfiguration führen.
	1.1.1.c Legen Sie eine Stichprobe mit tatsächlich an den Firewall- und Router-Konfigurationen vorgenommenen Änderungen fest, vergleichen Sie die Daten mit den Änderungsdatensätzen, und fragen Sie das zuständige Personal, ob die Änderungen genehmigt waren und getestet wurden.	
1.1.2 Ein aktuelles Netzwerkdiagramm mit allen Verbindungen zwischen der CDE und anderen Netzwerken, einschließlich aller drahtlosen Netzwerke	**1.1.2.a** Überprüfen Sie die Diagramme und Netzwerkkonfigurationen daraufhin, ob ein aktuelles Netzwerkdiagramm vorhanden ist und alle Verbindungen mit Karteninhaberdaten dokumentiert, einschließlich aller drahtlosen Netzwerke.	Aus Netzwerkdiagrammen sind die Konfiguration von Netzwerken und die Standorte der einzelnen Netzwerkgeräte ersichtlich. 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.
	1.1.2.b Klären Sie durch Befragung des zuständigen Personals, ob das Diagramm auf dem neuesten Stand gehalten wird.	
1.1.3 Aktuelles Diagramm mit den system- und netzwerkübergreifenden Flüssen von Karteninhaberdaten	**1.1.3** Untersuchen Sie das Datenflussdiagramm, und prüfen Sie das Diagramm im Gespräch mit den Mitarbeitern: • Umfasst die system- und netzwerkübergreifenden Flüsse von Karteninhaberdaten. • Wird auf dem neuesten Stand gehalten und bei Änderungen in der Umgebung entsprechend aktualisiert.	Anhand von Flussdiagrammen für Karteninhaberdaten lässt sich der Speicherort von allen gespeicherten, verarbeiteten oder im Netzwerk weitergegebenen Karteninhaberdaten ermitteln. 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.
1.1.4 Anforderungen für eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone	**1.1.4.a** Überprüfen Sie, ob alle Standards für die Firewall-Konfiguration Anforderungen für eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone enthalten.	Durch den Einsatz einer Firewall für alle eingehenden (sowie ausgehenden) Netzwerkverbindungen sowie zwischen DMZ und internem Netzwerk können Organisationen den Zugriff überwachen und kontrollieren und damit weitestgehend verhindern, dass sich eine böswillige Person Zugriff auf das interne Netzwerk verschafft.
	1.1.4.b Überprüfen Sie, ob das aktuelle Netzwerkdiagramm den Standards für die Firewall-Konfiguration entspricht.	
	1.1.4.c Überprüfen Sie die Netzwerkkonfigurationen darauf,	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
	ob sich gemäß den dokumentierten Konfigurationsstandards und Netzwerkdiagrammen eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone befindet.	
1.1.5 Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die Verwaltung der Netzwerkkomponenten	**1.1.5.a** Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration eine Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die Verwaltung der Netzwerkkomponenten enthalten.	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.
	1.1.5.b Prüfen Sie durch eine Befragung des für das Management der Netzwerkkomponenten verantwortlichen Personals, ob die Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen sind.	
1.1.6 Dokumentation und Begründung für den Einsatz aller zulässigen Services, Protokolle und Ports, einschließlich der Dokumentation von Sicherheitsfunktionen für die Protokolle, die als unsicher gelten. Zu unsicheren Diensten, Protokollen und Ports gehören unter anderem FTP, Telnet, POP3, IMAP und SNMP v1 und v2.	**1.1.6.a**Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration eine dokumentierte Liste aller Services, Protokolle und Ports mit betrieblicher Begründung enthalten, z. B. Hypertext Transfer Protocol (HTTP) und Secure Sockets Layer (SSL), Secure Shell (SSH) und Virtual Private Network (VPN).	Sicherheitsverletzungen treten häufig durch unbenutzte oder unsichere Dienste und Ports auf, zumal diese nicht selten bekannte Sicherheitsrisiken aufweisen. Viele Unternehmen sorgen nicht mithilfe von Patches für eine Behebung derartiger Sicherheitsrisiken in ungenutzten Diensten, Protokollen und Ports. 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. 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 Unternehmen nicht wesentlich sind, sollten sie deaktiviert oder gelöscht werden.
	1.1.6.b Identifizieren Sie zulässige unsichere Services, Protokolle und Ports, und überprüfen Sie, ob Sicherheitsfunktionen für jeden Dienst dokumentiert wurden.	
	1.1.6.c 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.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
1.1.7 Prüfung der Firewall- und Router-Regelsätze mindestens alle sechs Monate	**1.1.7.a** Überprüfen Sie, ob Standards für die Firewall- und Router-Konfiguration mindestens alle sechs Monate eine Prüfung von Firewall- und Router-Regelsätzen erfordern. **1.1.7.b** Prüfen Sie die Regelsatz-Dokumentation, und fragen Sie das zuständige Personal, ob die Regelsätze mindestens alle sechs Monate überprüft werden.	Diese Überprüfung bietet dem Unternehmen die Gelegenheit, mindestens alle sechs Monate sämtliche unnötigen, veralteten oder fehlerhaften Regeln zu entfernen und dafür zu sorgen, dass alle Regelsätze nur autorisierte Dienste und Ports zulassen, die den dokumentierten betrieblichen Begründungen entsprechen. 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.
1.2 Aufbau von Firewall- und Router-Konfigurationen, die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der CDE einschränken. ***Hinweis:*** *Ein „nicht vertrauenswürdiges Netzwerk“ ist jedes Netzwerk, das außerhalb der Netzwerke liegt, die zu der geprüften Einheit gehören und/oder das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Einheit liegt.*	**1.2** Prüfen Sie bei Firewall- und Router-Konfigurationen wie folgt, ob Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der CDE eingeschränkt werden:	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. 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.
1.2.1 Beschränken des ein- und ausgehenden Datenverkehrs auf das für die CDE absolut notwendige Maß und Ablehnung des gesamten sonstigen Datenverkehrs.	**1.2.1** Untersuchen Sie die Standards für die Firewall- und Router-Konfiguration daraufhin, ob der für die CDE absolut notwendige ein- und ausgehende Datenverkehr identifiziert wird. **1.2.1.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. **1.2.1.c** Überprüfen Sie in den Firewall- und Router-Konfigurationen, ob jeder andere ein- und ausgehende	Diese Anforderung soll verhindern, 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 Ihr Netzwerk gelangt sind, an einen nicht vertrauenswürdigen Server senden). Mit einer Regel zur Unterbindung des gesamten nicht unbedingt erforderlichen eingehenden sowie ausgehenden Datenverkehrs werden

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
	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.	unbeabsichtigte Sicherheitslücken vermieden, die sämtlichen unerwünschten und möglicherweise schädlichen Datenverkehr zuließen.
1.2.2 Sichern und Synchronisieren von Router-Konfigurationsdateien.	**1.2.2.a** Überprüfen Sie, ob die Dateien zur Router-Konfiguration vor unbefugtem Zugriff geschützt sind. **1.2.2.b** Überprüfen Sie, ob Router-Konfigurationsdateien synchronisiert sind. So sollte beispielsweise die aktive Konfiguration der Startkonfiguration (für den Geräteneustart) entsprechen.	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. 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.
1.2.3 Installieren von Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der CDE und Konfigurieren dieser Firewalls, sodass der gesamte Verkehr zwischen der drahtlosen Umgebung und der CDE abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten und für die Geschäftszwecke notwendigen Datenverkehr handelt.	**1.2.3.a** Prüfen Sie bei Firewall- und Router-Konfigurationen, ob Umkreis-Firewalls zwischen allen Drahtlos-Netzwerken und der CDE installiert sind. **1.2.3.b** Prüfen Sie, ob der gesamte Verkehr zwischen der drahtlosen Umgebung und der CDE von den Firewalls abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten und für die Geschäftszwecke notwendigen Datenverkehr handelt.	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 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. Firewalls müssen zwischen allen drahtlosen

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
		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.
1.3 Verbieten des direkten öffentlichen Zugriffs zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung.	**1.3** 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:	Der Zweck einer Firewall besteht darin, alle Verbindungen zwischen öffentlichen und internen Systemen zu verwalten und zu kontrollieren. Dies gilt insbesondere für jene 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 und Systemkomponenten mit Karteninhaberdaten sind unter Umständen gefährdet.
1.3.1 Implementieren einer DMZ, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene, öffentlich zugängliche Dienste, Protokolle und Ports anbieten.	**1.3.1** 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.	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.
1.3.2 Beschränken des eingehenden Internetverkehrs auf IP-Adressen innerhalb der DMZ.	**1.3.2** Überprüfen Sie in der Konfiguration der Firewall und des Routers, ob der eingehende Internetverkehr auf IP-Adressen innerhalb der DMZ beschränkt wird.	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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
1.3.3 Keine direkten eingehenden oder ausgehenden Verbindungen für Datenverkehr zwischen dem Internet und der Karteninhaberdaten-Umgebung zulassen.	**1.3.3** Überprüfen Sie in der Konfiguration der Firewall und des Routers, dass keine direkten eingehenden oder ausgehenden Verbindungen für Datenverkehr zwischen dem Internet und der CDE zugelassen wird.	Die Untersuchung aller eingehenden und ausgehenden Verbindungen bietet Gelegenheit zur Prüfung und Einschränkung von Datenverkehr auf der Basis der Quell- bzw. Zieladresse sowie zur Prüfung bzw. Blockierung von unerwünschten Inhalten, damit es nicht zu ungefilterten Zugriffen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Umgebungen kommt. Hierdurch wird beispielsweise vermieden, dass böswillige Personen Daten, an die sie über Ihr Netzwerk gelangt sind, an einen externen nicht vertrauenswürdigen Server in einer unbekannten Umgebung senden.
1.3.4 Implementierung von Anti-Spoofing-Maßnahmen zur Erkennung und Blockierung gefälschter Quell-IP-Adressen, über die auf das Netzwerk zugegriffen wird. (So kann beispielsweise der Datenverkehr blockiert werden, der trotz einer internen Quelladresse über das Internet zuzugreifen versucht.)	**1.3.4** 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**.**	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 mittels Spoofing, die IP-Adresse des Absenders so zu fälschen, dass das Zielsystem davon ausgeht, das Paket stamme aus einer vertrauenswürdigen Quelle. Indem Sie die Pakete filtern, die in Ihr Netzwerk gelangen, können Sie unter anderem dafür sorgen, dass die Pakete nicht gefälscht sind, d. h . den Anschein erwecken, sie kämen aus Ihrem eigenen internen Netzwerk.
1.3.5 Unterbindung von nicht autorisiertem ausgehenden Datenverkehr von der CDE zum Internet.	**1.3.5** Überprüfen Sie in der Konfiguration der Firewall und des Routers, ob ausgehender Datenverkehr von der CDE zum Internet ausdrücklich zugelassen ist.	Der gesamte von der CDE ausgehende Datenverkehr muss daraufhin untersucht werden, ob er den implementierten, zugelassenen Regeln entspricht. Die Verbindungen sollten überprüft werden, um den Datenverkehr ausschließlich auf zugelassene Kommunikationen zu beschränken (z. B. indem Quell-/Ziel-Adressen bzw. Ports eingeschränkt und/oder Inhalte blockiert werden).
1.3.6 Implementieren der statusgesteuerten Inspektion, die auch als dynamische Paketfilterung bekannt ist. (Das bedeutet, dass nur „etablierte“	**1.3.6** Überprüfen Sie in der Konfiguration der Firewall und des Routers, ob die Firewall eine statusgesteuerte Inspektion (dynamische Paketfilterung) durchführt. (Es sollten nur etablierte Verbindungen zugelassen werden und auch nur	Eine Firewall, die statusgesteuerte Paketinspektionen ausführt, hält den Status der einzelnen Verbindungen durch die Firewall aufrecht. Durch die Aufrechterhaltung des Status

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Verbindungen in das Netzwerk zulässig sind.)	dann, wenn sie Bestandteil einer zuvor festgelegten Sitzung sind.)	weiß die Firewall, ob es sich bei den Antworten auf eine vorige Verbindung tatsächlich um gültige und autorisierte Antworten (weil der Status jeder einzelnen Verbindung aufrechterhalten wird) oder um schädlichen Datenverkehr handelt, der versucht, die Firewall zu täuschen, damit sie die Verbindung zulässt.
1.3.7 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.	**1.3.7** 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.	Wenn sich Karteninhaberdaten innerhalb einer DMZ befinden, ist es aufgrund 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, trägt dazu bei, das nicht autorisierter Netzwerkverkehr die Systemkomponente nicht erreicht. ***Hinweis:*** *Diese Anforderung gilt nicht für die temporäre Speicherung von Karteninhaberdaten in einem flüchtigen Speicher.*
1.3.8 Vermeidung der Weitergabe privater IP-Adressen und Routing-Informationen an unbefugte Dritte. ***Hinweis:*** *Zu den Methoden zum Verbergen von IP-Adressen zählen unter anderem:*	**1.3.8.a** 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.	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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
• *Network Address Translation (NAT);* • *Das Platzieren von Servern mit Karteninhaberdaten hinter Proxy-Servern/Firewalls;* • *Löschen oder Filtern von Route-Advertisements für private Netzwerke, die registrierte Adressen verwenden;* • *Interne Nutzung eines RFC1918-Adressraums anstatt registrierter Adressen.*	**1.3.8.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.	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.
1.4 Installieren von persönlicher Firewall-Software 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 Netzwerk eingesetzt werden. Die Firewall-Konfigurationen umfassen Folgendes: • Für persönliche Firewall-Software werden spezielle Konfigurationseinstellungen festgelegt. • Die persönliche Firewall-Software wird aktiv ausgeführt. • Die persönliche Firewall-Software ist nicht durch Benutzer mobiler Geräte und/oder Geräte von Mitarbeitern veränderbar.	**1.4.a** Überprüfen Sie die Richtlinien und Konfigurationsstandards auf Folgendes: • Persönliche Firewall-Software ist 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 Netzwerk eingesetzt werden. • Für persönliche Firewall-Software werden spezielle Konfigurationseinstellungen festgelegt. • Die persönliche Firewall-Software ist so konfiguriert, dass sie aktiv ausgeführt wird. • Die persönliche Firewall-Software ist nicht durch Benutzer mobiler Geräte und/oder Geräte von Mitarbeitern veränderbar. **1.4.b** Untersuchen Sie stichprobenartig die mobilen oder im Besitz von Mitarbeitern befindlichen Geräte auf folgende Punkte: • Die persönliche Firewall-Software wird gemäß den konkreten Konfigurationseinstellungen der Organisation installiert und konfiguriert. • Die persönliche Firewall-Software wird aktiv ausgeführt. • Die persönliche Firewall-Software ist nicht durch Benutzer mobiler Geräte und/oder Geräte von Mitarbeitern veränderbar.	Tragbare Computer und Geräte, die außerhalb der Unternehmens-Firewall eine Verbindung zum Internet herstellen dürfen, sind Bedrohungen aus dem Internet stärker ausgesetzt. Durch eine persönliche Firewall 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. Wie die Firewall im konkreten Fall konfiguriert werden muss, wird von der Organisation festgelegt. ***Hinweis:*** *Diese Anforderung bezieht sich auf Computer, die sich im Besitz eines Mitarbeiters oder des Unternehmens befinden. Systeme, die nicht mittels Unternehmensrichtlinien verwaltet werden können, schwächen den Netzwerkrand und bieten böswilligen Personen Angriffsmöglichkeiten. Wenn nicht vertrauenswürdige Systeme eine Verbindung zum Netzwerk der Organisation herstellen dürfen, könnten sich Angreifer und andere böswillige Benutzer Zugriff auf das Netzwerk verschaffen.*
1.5 Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung der Firewalls müssen dokumentiert sein,	**1.5** Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung der Firewalls Folgendes	Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit Firewalls und Router

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
verwendet werden und allen Beteiligten bekannt sein.	gilt: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	dauerhaft einen nicht autorisierten Zugriff auf das Netzwerk verhindern.

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 bekannt und können durch öffentliche Informationen mühelos ausfindig gemacht werden.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
2.1 Änderung der Standardeinstellungen des Anbieters und Entfernung bzw. Deaktivierung unnötiger Standardkonten stets **vor** der Installation eines Systems im Netzwerk. 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.	**2.1.a**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.)	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 bekannt sind, müssen diese Einstellungen geändert werden, damit Ihr System weniger anfällig gegenüber Angriffen wird. 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.
	2.1.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.	
	2.1.c Klären Sie durch Befragungen des Personals und durch Prüfung der Dokumentation Folgendes: • 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. • 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.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
2.1.1 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.	**2.1.1.a** Klären Sie durch Befragungen des Personals und durch Prüfung der Dokumentation Folgendes: • Die Standardwerte der Verschlüsselungsschlüssel wurden zum Zeitpunkt der Installation geändert. • Die Verschlüsselungsschlüssel werden jedes Mal geändert, wenn ein Mitarbeiter, der die Schlüssel kennt, das Unternehmen verlässt oder die Position wechselt.	Wenn Drahtlosnetzwerke nicht mit ausreichenden Sicherheitskonfigurationen (einschließlich die Änderung von Standardeinstellungen) implementiert werden, können Wireless-Sniffer den Datenverkehr belauschen, im Handumdrehen Daten und Kennwörter erfassen und sich Zugriff auf Ihr Netzwerk verschaffen und es schädigen. 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.
	2.1.1.b Klären Sie durch eine Überprüfung der Dokumentation und Verfahren sowie durch eine Befragung des Personals Folgendes ab: • Müssen Standard-SNMP-Community-Zeichenfolgen bei der Installation geändert werden? • Müssen Standardkennwörter/-sätze an Zugriffspunkten bei der Installation geändert werden?	
	2.1.1.c Prüfen Sie durch eine Untersuchung der Anbieterdokumentation sowie durch eine Anmeldung an Wireless-Geräten (mit Unterstützung de Systemadministrators) Folgendes: • Werden Standard-SNMP-Community-Zeichenfolgen nicht verwendet? • Werden Standardkennwörter/-sätze an Zugriffspunkten nicht verändert?	
	2.1.1.d 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: • Authentifizierung über Drahtlosnetzwerke • Übertragung über Drahtlosnetzwerke	
	2.1.1.e Prüfen Sie in der Anbieterdokumentation und in der Drahtlos-Konfiguration, ob gegebenenfalls andere sicherheitsbezogene Standardeinstellungen des Anbieters des Drahtlossystems geändert wurden.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
2.2 Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit akzeptierter Standards zur Systemstabilisierung zählen unter anderem: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institut • National Institute of Standards and Technology (NIST)	**2.2.a**Überprüfen Sie die Systemkonfigurationsstandards des Unternehmens für alle Arten von Systemkomponenten, und prüfen Sie, ob die Systemkonfigurationsstandards branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. **2.2.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. **2.2.c** 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. **2.2.d** Überprüfen Sie, ob die Systemkonfigurationsstandards die folgenden Verfahren für alle Arten von Systemkomponenten enthalten: • Ändern sämtlicher Standards der Anbieter und Löschen unnötiger Standardkonten • Implementieren von nur einer primären Funktion pro Server, um zu vermeiden, dass auf einem Server Funktionen mit verschiedenen Sicherheitsniveauanforderungen vorhanden sind • Aktivieren der Dienste, Protokolle, Daemons usw., die für die Systemfunktion unbedingt erforderlich sind • Implementieren zusätzlicher Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden • Konfigurieren von Systemsicherheitsparametern zur Missbrauchsvermeidung • Entfernen aller unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver	In vielen Betriebssystemen, Datenbanken und Firmenanwendungen gibt es bekannte Schwachstellen, welche mithilfe bestimmter Konfigurationen behoben werden können. Um jenen unter die Arme zu greifen, die keine Sicherheitsexperten sind, haben eine Reihe von Sicherheitsunternehmen Empfehlungen zur Korrektur dieser Schwächen erarbeitet. Beispiele für Empfehlungen zu Konfigurationsstandards finden Sie unter anderem auf den folgenden Websites: www.nist.gov, www.sans.org, www.cisecurity.org und www.iso.org sowie bei den Anbietern entsprechender Produkte. Systemkonfigurationsstandards müssen auf dem neuesten Stand gehalten werden, damit neu entdeckte Sicherheitslücken geschlossen werden, bevor ein System im Netzwerk installiert wird.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
2.2.1 Implementieren Sie nur eine primäre Funktion pro Server, um zu vermeiden, dass auf einem Server gleichzeitig mehrere Funktionen mit verschiedenen Sicherheitsniveauanforderungen existieren. (Webserver, Datenbankserver und DNS sollten beispielsweise auf separaten Servern implementiert sein.) ***Hinweis:*** *Wenn Virtualisierungstechnologien eingesetzt werden, implementieren Sie pro virtuelle Systemkomponente nur eine primäre Funktion.*	**2.2.1.a**Überprüfen Sie in den Systemkonfigurationen für eine Stichprobe von Systemkomponenten, ob nur eine primäre Funktion pro Server implementiert ist. **2.2.1.b** Wenn Virtualisierungstechnologien eingesetzt werden, überprüfen Sie in der Systemkonfiguration, ob pro virtuelle Systemkomponente oder Gerät nur eine primäre Funktion implementiert ist.	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.
2.2.2 Ausschließliches Aktivieren notwendiger Dienste, Protokolle, Daemons usw. entsprechend dem Bedarf der Systemfunktion.	**2.2.2.a** Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob nur notwendige Systemdienste, Daemons und Protokolle aktiviert sind. **2.2.2.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.	Wie bereits in der Anforderung 1.1.6 erwähnt, gibt es zahlreiche Protokolle, die ein Unternehmen unter Umständen benötigt (oder standardmäßig aktiviert hat) und die wiederholt 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.
2.2.3 Implementieren zusätzlicher Sicherheitsfunktionen für alle erforderlichen Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden – Verwenden Sie z. B. gesicherte Technologien wie SSH, S-FTP, SSL oder IPSec VPN, um unsichere Dienste wie beispielsweise NetBIOS, File-Sharing, Telnet, FTP etc. zu schützen.	**2.2.3** Überprüfen Sie in den Konfigurationseinstellungen, ob Sicherheitsfunktionen für jeden unsicheren Dienst, jeden unsicheren Deamon und jedes unsichere Protokoll dokumentiert und implementiert wurden.	Wenn Sicherheitsfunktionen schon vor der Bereitstellung von neuen Servern aktiviert werden, können Server mit unsicheren Konfigurationen nicht in der Umgebung installiert werden. Wenn sämtliche unsicheren Dienste, Protokolle und Daemons durch angemessene Funktionen sicher gemacht werden, wird böswilligen Benutzern die Ausnutzung bekannter Schwachpunkte in einem Netzwerk erschwert.
2.2.4 Konfigurieren von Systemsicherheitsparametern zur	**2.2.4.a** Prüfen Sie in Gesprächen mit Systemadministratoren und/oder Sicherheitsbeauftragten, ob diese die gängigen	Systemkonfigurationsstandards und zugehörige Prozesse sollten insbesondere jene

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Missbrauchsvermeidung.	Sicherheitsparametereinstellungen für Systemkomponenten kennen.	Sicherheitseinstellungen und Parameter ansprechen, die sich bekanntermaßen auf die Sicherheit aller verwendeten Systeme auswirken.
	2.2.4.b Überprüfen Sie, ob gängige Sicherheitsparametereinstellungen in den Systemkonfigurationsstandards enthalten sind.	
	2.2.4.c Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob gängige Sicherheitsparameter angemessen und in Übereinstimmung mit den Konfigurationsstandards festgelegt sind.	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.
2.2.5 Entfernen aller unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver.	**2.2.5.a** Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob alle unnötigen Funktionen (z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme usw.) aus der Konfiguration entfernt wurden	Unnötige Funktionen bieten böswilligen Personen zusätzliche Möglichkeiten für einen Zugriff auf ein System. Durch die Entfernung unnötiger Funktionen können sich Organisationen darauf konzentrieren, die wirklich notwendigen Funktionen sicher zu machen und das Risiko eines Missbrauchs unbekannter Funktionen zu senken. Die Einbindung dieser Überlegungen in Standards zur Absicherung von Servern und Prozessen geht auf konkrete Sicherheitsauswirkungen im Zusammenhang mit unnötigen Funktionen ein (z. B. indem der FTP- oder der Webserver gelöscht/deaktiviert wird, wenn der Server diese Funktionen nicht nutzt).
	2.2.5.b Überprüfen Sie in der Dokumentation und den Sicherheitsparametern, ob aktivierte Funktionen dokumentiert sind und eine sichere Konfiguration unterstützen.	
	2.2.5.c Überprüfen Sie in der Dokumentation und in den Sicherheitsparametern, ob auf den Systemkomponenten der Stichprobe ausschließlich dokumentierte Funktionen vorhanden sind.	
2.3 Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs mithilfe einer starken Kryptographie. Verwenden von Technologien wie SSH, VPN oder SSL/TLS für die webbasierte Verwaltung und sonstigen Nichtkonsolen-Verwaltungszugriff	**2.3** Überprüfen Sie für eine Stichprobe von Systemkomponenten, ob der nicht über die Konsole erfolgte Verwaltungszugriff durch folgende Maßnahmen verschlüsselt ist:	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
	2.3.a Befolgen Sie den Anmeldevorgang eines Administrators an jedem System, und überprüfen Sie in den Systemkonfigurationen, ob eine starke Verschlüsselungsmethode aufgerufen wird, bevor das Administratorkennwort angefordert wird.	
	2.3.b Vergewissern Sie sich bei den Diensten und	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
	Parameterdateien auf Systemen, dass Telnet und andere unsichere Remote-Anmeldebefehle nicht für den Zugriff ohne Konsole verfügbar sind.	und Daten zu entwenden. Bei Klartextprotokollen (wie HTTP, Telnet usw.) werden weder der Datenverkehr noch die Anmeldedaten verschlüsselt. Dies erleichtert das Abfangen dieser Informationen. Eine „starke Kryptographie“ kann nur erreicht werden, wenn branchenweit anerkannte Protokolle mit angemessen sicherer Verschlüsselung und Schlüsselverwaltung nach Bedarf für die verwendete Technologie verwendet werden. (Die Definition des Begriffs „starke Kryptographie“ finden Sie im *Glossar für Begriffe, Abkürzungen und Akronyme* für PCI-DSS und PA-DSS.)
	2.3.c Überprüfen Sie bei den Administratoranmeldungen an den einzelnen Systemen, ob der Administratorzugriff auf die webbasierten Managementschnittstellen mit einer starken Kryptographie verschlüsselt ist.	
	2.3.d Überprüfen Sie unter Zuhilfenahme der Anbieterdokumentation und durch Befragung des Personals, ob für die verwendete Technologie eine starke Kryptographie gemäß den bewährten Branchenverfahren und/oder Anbieterempfehlungen implementiert wird.	
2.4 Führen eines Bestands an Systemkomponenten für den PCI-DSS.	**2.4.a** Überprüfen Sie im Systembestand, ob eine Liste der Hardware- und Softwarekomponenten mit einer Beschreibung der einzelnen Funktionen/Einsatzgebiete geführt wird.	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.
	2.4.b Klären Sie durch Befragung des zuständigen Personals, ob die Bestandsdokumentation auf dem neuesten Stand gehalten wird.	
2.5 Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung von Anbieterstandards und sonstigen Sicherheitsparametern müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**2.5** Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung von Anbieterstandards Folgendes gilt: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit Anbieterstandards und andere Sicherheitsparameter dauerhaft verwaltet und unsichere Konfigurationen verhindert werden.
2.6 Anbieter von gemeinsam genutzten Hosting-Services müssen die gehostete Umgebung und Karteninhaberdaten aller Einheiten schützen. Diese Anbieter müssen bestimmte Anforderungen erfüllen, wie in *Anhang A: Zusätzliche PCI DSS-Anforderungen für gemeinsam*	**2.6** Überprüfen Sie für PCI-DSS-Bewertungen gemeinsam verwendeter Hosting-Anbieter mit den Testverfahren **A.1.1** bis **A.1.4**, die in *Anhang A: Zusätzliche PCI-DSS-Anforderungen für Anbieter von gemeinsam genutzten Hosting-Services* erläutert werden, ob gemeinsam verwendete Hosting-Anbieter die gehostete Umgebung und die Daten ihrer Einheiten (Händler und Dienstanbieter) schützen.	Sie gelten 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 vielmals nicht von einem

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
verwendete Hosting-Provider dargestellt.		einzigen Client verwalten. Den Clients wird die Möglichkeit eingeräumt, 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 *Anhang A*.

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 leserlich und für diese Person unbrauchbar. Andere effektive Methoden zum Schutz gespeicherter Daten sollten als Möglichkeit zur Risikoabschwächung angesehen werden. Zu den Methoden zur Risikominimierung gehört es beispielsweise, Karteninhaberdaten nur zu speichern, wenn dies unbedingt erforderlich ist, Karteninhaberdaten abzukürzen, wenn die vollständige PAN nicht benötigt wird, und die 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	LEITFADEN
3.1 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: • Begrenzen der Speichermenge und der Aufbewahrungszeit auf die für rechtliche, gesetzliche oder geschäftliche Zwecke festgelegten Vorgaben. • Prozesse zum Löschen von Daten, sobald diese nicht mehr benötigt werden. • Spezifische Aufbewahrungsanforderungen für	**3.1.a** Prüfen Sie, ob die Richtlinien und Verfahren zur Datenaufbewahrung und -löschung mindestens folgende Elemente enthalten: • Rechtliche, behördliche und betriebliche Anforderungen an die Datenaufbewahrung wie z. B.: • Spezielle Anforderungen an die Aufbewahrung von Karteninhaberdaten (Karteninhaberdaten müssen z. B. für den Zeitraum X aus den Geschäftsgründen Y aufbewahrt werden) • Sicheres Löschen von Karteninhaberdaten, wenn sie nicht länger zu juristischen, gesetzlichen oder geschäftlichen Zwecken benötigt werden • Abdeckung der gesamten Speicherung von Karteninhaberdaten • Ein vierteljährlicher Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten, die den festgelegten Aufbewahrungszeitraum überschritten haben	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. 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. 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 eine Stelle zunächst über ihre eigenen Betriebsbedürfnisse sowie jegliche

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Karteninhaberdaten • Ein vierteljährlicher Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten, die den festgelegten Aufbewahrungszeitraum überschritten haben.	**3.1.b** Klären Sie durch Befragung des zuständigen Personals Folgendes ab: • Die Speicherorte der Karteninhaberdaten sind in den Prozessen zur Datenaufbewahrung und -löschung enthalten. • Es gibt einen vierteljährlichen automatischen oder manuellen Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten. • Dieser vierteljährliche automatische bzw. manuelle Prozess wird an allen Speicherorten von Karteninhaberdaten ausgeführt.	Art von gesetzlichen oder behördlichen Pflichten im Klaren sein, die für ihre Branche und/oder den jeweiligen Datentyp gelten. *(Fortsetzung auf der nächsten Seite)*
	3.1.c Gehen Sie für eine Stichprobe von Systemkomponenten mit Karteninhaberdaten wie folgt vor: • Vergewissern Sie sich in den Dateien und Systemdatensätzen, dass die gespeicherten Daten nicht den in der Datenaufbewahrungsrichtlinie festgelegten Zeitraum überschreiten. • Überprüfen Sie die Löschmechanismen daraufhin, ob die Daten sicher gelöscht werden.	Durch die Ermittlung und Löschung von Daten, deren Aufbewahrungsfrist überschritten wurde, wird verhindert, dass nicht mehr benötigte Daten unnötig aufbewahrt werden. Der Prozess kann automatisch ablaufen und/oder manuell gesteuert werden. Es könnte beispielsweise eine (automatisch oder manuell ausgelöste) Programmprozedur zur Suche und Entfernung von Daten und/oder eine manuelle Prüfung der Datenspeicherbereiche durchgeführt werden. Der Einsatz sicherer Verfahren zum Löschen von Daten gewährleistet, dass diese nicht mehr wiederhergestellt werden können, wenn hierfür kein Bedarf mehr besteht. ***Denken Sie daran – wenn nicht benötigt, nicht speichern!***

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
3.2 Speichern Sie keine vertraulichen Authentifizierungsdaten nach der Autorisierung (auch wenn diese verschlüsselt sind). Falls vertrauliche Authentifizierungsdaten empfangen werden, müssen sämtliche Daten nach Abschluss des Autorisierungsprozesses so gelöscht werden, dass sie nicht wiederhergestellt werden können. *Kartenemittenten und Unternehmen, die Ausstellungsdienste unterstützen, dürfen in den folgenden Fällen vertrauliche Authentifizierungsdaten speichern:* • wenn es eine geschäftliche Begründung gibt • wenn die Daten sicher gespeichert werden Vertrauliche Authentifizierungsdaten umfassen die Daten, die in den folgenden Anforderungen 3.2.1 bis 3.2.3 aufgeführt sind:	**3.2.a** Prüfen Sie bei Kartenemittenten und/oder Unternehmen, die Ausstellungsdienste unterstützen und vertrauliche Authentifizierungsdaten speichern, durch Betrachtung der Richtlinien und Befragung des Personals, ob für die Speicherung von vertraulichen Authentifizierungsdaten eine dokumentierte Begründung vorliegt.	Vertrauliche Authentifizierungsdaten umfassen vollständige Verfolgungsdaten, Kartenvalidierungscodes 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, zumal sie ihnen ermöglichen, gefälschte Zahlungskarten zu generieren und betrügerische Transaktionen zu erstellen.
	3.2.b Prüfen Sie bei Kartenemittenten und/oder Unternehmen, die Ausstellungsdienste unterstützen und vertrauliche Authentifizierungsdaten speichern, durch Untersuchung der Datenspeicher und Systemkonfigurationen, ob dies vertraulichen Authentifizierungsdaten sicher gespeichert werden.	Einheiten, die Zahlungskarten ausstellen bzw. Ausstellungsdienste erbringen oder unterstützen, erstellen und kontrollieren im Rahmen der Ausstellung häufig vertrauliche Authentifizierungsdaten. Unternehmen, die Ausstellungsdienste anbieten, fördern oder unterstützen, dürfen vertrauliche Authentifizierungsdaten NUR speichern, WENN für die Speicherung dieser Daten eine betriebliche Begründung vorliegt. Hierbei sei angemerkt, dass für Emittenten alle PCI-DSS-Anforderungen gelten und dass die einzige Ausnahme darin besteht, dass Emittenten und zugehörige Dienstleister vertrauliche Authentifizierungsdaten speichern dürfen, wenn hierfür berechtigte Gründe vorliegen. Ein berechtigter Grund dass der Emittent 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 Zahlungsmarken gespeichert werden.
	3.2.c Vergewissern Sie sich bei allen anderen Einheiten im Falle des Empfangs von vertraulichen Authentifizierungsdaten in den Richtlinien und Verfahren sowie in den Systemkonfigurationen, dass die Daten nach der Autorisierung nicht gespeichert werden.	
	3.2.d Vergewissern Sie sich bei allen anderen Einheiten im Falle des Empfangs von vertraulichen Authentifizierungsdaten in den Verfahren und Prozessen zum Löschen der Daten, dass die Daten nicht wiederhergestellt werden können.	Bei Einheiten, die keine Zahlungskarten ausstellen, ist das Speichern vertraulicher Authentifizierungsdaten nach der Autorisierung nicht zulässig.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
3.2.1 Speichern Sie nicht den gesamten Inhalt einer Spur (auf dem Magnetstreifen auf der Kartenrückseite, in einem Chip oder an anderer Stelle). Diese Daten werden auch als Full Track, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet. ***Hinweis:*** *Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:* • *Der Name des Karteninhabers* • *Primäre Kontonummer (Englisch: Primary Account Number, PAN)* • *Ablaufdatum* • *Servicecode* *Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.*	**3.2.1** Vergewissern Sie sich für einen 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: • Eingehende Transaktionsdaten • Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler) • Verlaufsdateien • Trace-Dateien • Mehrere Datenbankschemata • Datenbankinhalte	Wenn vollständige Verfolgungsdaten gespeichert werden, sind Angreifer, die auf diese Daten zugreifen können, in der Lage, Zahlungskarten zu reproduzieren und betrügerische Transaktionen durchzuführen.
3.2.2 Speichern Sie nicht den Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte), der zur Verifizierung bei Transaktionen verwendet wird, bei denen die Karte nicht physisch vorliegt.	**3.2.2** 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: • Eingehende Transaktionsdaten • Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler) • Verlaufsdateien • Trace-Dateien • Mehrere Datenbankschemata • Datenbankinhalte	Der Zweck des Kartenvalidierungscodes liegt im 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. Wenn diese Daten entwendet werden, sind Betrüger in der Lage, Transaktionen über das Internet und per Post/Telefon abzuwickeln.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
3.2.3 Speichern Sie keine persönlichen Identifizierungsnummern (PIN) oder den verschlüsselten PIN-Block.	**3.2.3** 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: • Eingehende Transaktionsdaten • Alle Protokolle (z. B. Transaktion, Verlauf, Fehlerbehebung, Fehler) • Verlaufsdateien • Trace-Dateien • Mehrere Datenbankschemata • Datenbankinhalte	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).
3.3 Maskieren Sie die PAN bei der Anzeige (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden), sodass nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund die vollständige PAN einsehen können. ***Hinweis:*** *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.*	**3.3.a** Untersuchen Sie die schriftlich fixierten Richtlinien und Verfahren zur Maskierung der PAN-Anzeige, und prüfen Sie Folgendes: • Eine Liste der Rollen, die auf die Anzeige der vollständigen PAN angewiesen sind, ist zusammen mit dem rechtmäßigen geschäftlichen Grund dieses Zugriffs dokumentiert. • Die PAN muss bei der Anzeige so maskiert sein, dass nur die Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund die vollständige PAN einsehen können. • Bei sämtlichen anderen nicht explizit für die Anzeige der PAN autorisierten Rollen werden ausschließlich maskierte PANs angezeigt.	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. Dadurch, dass die PAN nur bei Personen, die die vollständige PAN aus rechtmäßigen geschäftlichen Gründen einsehen müssen, in voller Länge angezeigt wird, verringert sich das Risiko eines unbefugten Zugriffs auf PAN-Daten. Diese Anforderung bezieht sich auf den Schutz von PANs, die auf Bildschirmen, Belegen usw. *abgebildet* sind und darf nicht mit der Anforderung 3.4 zum Schutz der in Dateien, Datenbanken usw. *gespeicherten* PANs verwechselt werden.
	3.3.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.	
	3.3 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 die vollständige PAN einsehen können.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
3.4 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: • Unidirektionale Hashes, die auf einer starken Kryptographie basieren (es muss von der vollständigen PAN ein Hash erstellt werden); • Abkürzung (die Hash-Funktion kann nicht verwendet werden, um das abgekürzte Segment der PAN zu ersetzen); • Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden); • Starke Kryptographie mit entsprechenden Schlüsselverwaltungsprozessen und -verfahren.	**3.4.a** 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: • Unidirektionale Hashes, die auf einer starken Kryptographie basieren • Abkürzung • Index-Token und -Pads (Pads müssen sicher aufbewahrt werden) • Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren	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 entsprechend geschützt werden. 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.
	3.4.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).	
	3.4.c Vergewissern Sie sich in einer Stichprobe von Wechseldatenträgern (z. B. Sicherungsbändern), dass die PAN nicht lesbar ist.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Hinweis: *Für eine Person mit böswilligen Absichten ist es eine relativ einfache Übung, die originalen PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die abgekürzte als auch auf die Hash-Version einer PAN hat. Wenn die gehashte und die abgekürzte Version derselben PAN in der Umgebung derselben Stelle nebeneinander bestehen, müssen zusätzliche Kontrollen eingesetzt werden, damit die originale PAN nicht durch den Vergleich von gehashten und abgekürzten Versionen rekonstruiert werden kann.*	**3.4.d** Vergewissern Sie sich in einer Stichprobe von Audit-Protokollen, dass die PAN nicht lesbar ist oder aus den Protokollen entfernt wurde.	Das Ziel der Abkürzung liegt darin, nur einen Teil (nicht mehr als die ersten sechs und die letzten vier Ziffern) der PAN zu speichern. Ein Index-Token ist ein kryptographisches Token, das die PAN anhand eines bestimmten Index für einen unvorhersehbaren Wert ersetzt. Ein One-Time-Pad ist ein System, bei dem ein per Zufallsgenerator erstellter privater Schlüssel nur einmal benutzt wird, um eine Nachricht zu verschlüsseln, welche anschließend mit einem entsprechenden One-Time-Pad und Schlüssel wieder entschlüsselt wird. Das Ziel der starken Kryptographie (gemäß der Definition im *PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme*) liegt darin, dass die Verschlüsselung auf der Grundlage branchenbewährter und akzeptierter Algorithmen (keine firmeneigenen oder selbst entwickelten Algorithmen) mit starken kryptographischen Schlüsseln erfolgt. Wenn ein Angreifer die gehashte und die abgekürzte Version einer bestimmten PAN miteinander vergleicht, kann er im Handumdrehen den ursprünglichen PAN-Wert ableiten. Damit die ursprüngliche PAN dauerhaft nicht gelesen werden kann, können Kontrollen hilfreich sein, die vermeiden, dass diese Daten einander zugeordnet werden.
3.4.1 Wenn Festplattenverschlüsselung verwendet wird (anstelle der Datenbankverschlüsselung auf Datei- oder Spaltenebene), muss der logische Zugriff unabhängig von nativen Authentifizierungs- und Zugriffskontrollmechanismen des	**3.4.1.a** 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.	Diese Anforderung geht auf 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

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Betriebssystems verwaltet werden (z. B. indem lokale Benutzerkontodatenbanken und allgemeine Netzwerkanmeldedaten nicht verwendet werden). Dechiffrierschlüssel dürfen nicht mit Benutzerkonten verbunden werden.	**3.4.1.b** Überprüfen Sie durch die Beobachtung von Prozessen und die Befragung von Personal, ob kryptographische Schlüssel sicher gespeichert sind (z. B. auf Wechseldatenträgern, die durch starke Zugriffskontrollen entsprechend geschützt sind).	Festplattenverschlüsselung fangen Lese- und Schreibvorgänge des Betriebssystems ab und führen die entsprechenden kryptographischen Umwandlungen ohne jegliches Zutun des Benutzers, außer der Eingabe eines Kennworts oder Kennsatzes beim Systemstart oder zu Beginn der Sitzung, aus. Basierend auf den Eigenschaften der Festplattenverschlüsselung darf Methode, um dieser Anforderung zu entsprechen, folgende Elemente nicht aufweisen: 1) Es darf nicht die gleiche Benutzerkonten-Authentifizierung wie für das Betriebssystem verwendet werden. 2) Es darf kein Dechiffrierschlüssel eingesetzt werden, der mit der lokalen Benutzerkonten-Datenbank des Systems bzw. allgemeinen Netzwerkanmeldedaten verknüpft ist oder daraus abgeleitet wird. Die vollständige Festplattenverschlüsselung trägt zum Schutz von Daten beim Verlust einer Festplatte bei und eignet sich daher zum Beispiel für tragbare Geräte mit Karteninhaberdaten.
	3.4.1.c Überprüfen Sie in den Konfigurationen und Prozessen, ob Karteninhaberdaten auf Wechseldatenträgern unabhängig vom Speicherort verschlüsselt sind. ***Hinweis:*** *Wenn keine Festplattenverschlüsselung zur Verschlüsselung von Wechseldatenträgern eingesetzt wird, müssen die auf diesen Datenträgern gespeicherten Daten mithilfe einer anderen Methode unlesbar gemacht werden.*	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
3.5 Dokumentieren und implementieren Sie Verfahren zum Schutz von Schlüsseln, die für die Sicherheit gespeicherter Karteninhaberdaten eingesetzt werden, vor Weitergabe und Missbrauch: ***Hinweis:*** *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.*	**3.5** 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: • Der Zugriff auf Schlüssel ist auf die unbedingt notwendige Anzahl von Personen beschränkt. • Die Schlüsselverschlüsselungsschlüssel sind mindestens so sicher wie die Datenverschlüsselungsschlüssel, zu deren Schutz sie eingesetzt werden. • Schlüsselverschlüsselungsschlüssel werden getrennt von Datenverschlüsselungsschlüsseln aufbewahrt. • Die Schlüssel werden sicher und an so wenigen Orten und in so wenigen Formen wie möglich aufbewahrt.	Kryptographische Schlüssel müssen dringend geschützt werden, da Personen, die in deren Besitz gelangen, in der Lage sind, Daten zu entschlüsseln. 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. 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.
3.5.1 Einschränken des Zugriff auf kryptographische Schlüssel auf die unbedingt notwendige Anzahl von Personen.	**3.5.1** Prüfen Sie in den Benutzerzugriffslisten, ob der Zugriff auf Schlüssel auf möglichst wenige Personen beschränkt ist.	Es sollten möglichst wenige Personen Zugriff auf die kryptographischen Schlüssel haben, und vorzugsweise 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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
3.5.2 Geheime und private Schlüssel zur Ver- und Entschlüsselung von Karteninhaberdaten müssen stets in einer (oder mehreren) der folgenden Formen gespeichert werden: • Verschlüsselung mit einem Schlüsselverschlüsselungsschlüssel, der mindestens so sicher wie der Datenverschlüsselungsschlüssel ist und separat von diesem gespeichert wird • 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)) • Speicherung gemäß branchenweit akzeptierter Methoden in mindestens zwei Schlüsselkomponenten voller Länge oder in Schlüssel-Shares ***Hinweis:*** *Öffentliche Schlüssel müssen nicht in dieser Form gespeichert werden.*	**3.5.2.a** Vergewissern Sie sich in dokumentierten Verfahren, dass Schlüssel zur Ver- und Entschlüsselung von Karteninhaberdaten stets nur in einer (oder mehreren) der folgenden Formen gespeichert werden: • Verschlüsselung mit einem Schlüsselverschlüsselungsschlüssel, der mindestens so sicher wie der Datenverschlüsselungsschlüssel ist und separat von diesem gespeichert wird • 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)) • Speicherung gemäß branchenweit akzeptierter Methoden in Schlüsselkomponenten oder Schlüssel-Shares	Kryptographische Schlüssel müssen sicher gespeichert werden, damit nicht autorisierter oder unnötiger Zugriff, der zur Preisgabe von Karteninhaberdaten führen könnte, verhindert wird. Zwar ist es 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.
	3.5.2.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: • Verschlüsselung mit einem Schlüsselverschlüsselungsschlüssel • 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)) • Speicherung gemäß branchenweit akzeptierter Methoden in Schlüsselkomponenten oder Schlüssel-Shares	
	3.5.2.c Überprüfen Sie bei Verwendung von Schlüsselverschlüsselungsschlüsseln Folgendes in den Systemkonfigurationen und an den Schlüsselspeicherorten: • Die Schlüsselverschlüsselungsschlüssel müssen mindestens so sicher wie die Datenverschlüsselungsschlüssel, zu deren Schutz sie eingesetzt werden, sein. • Schlüsselverschlüsselungsschlüssel werden getrennt von Datenverschlüsselungsschlüsseln aufbewahrt.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
3.5.3 Speichern kryptographischer Schlüssel an möglichst wenigen Speicherorten.	**3.5.3** Prüfen Sie an den Speicherorte von Schlüsseln und in Prozessen, ob die Schlüssel an so wenigen Orten wie möglich aufbewahrt werden.	Organisationen, die kryptographische Schlüssel an so wenigen Orten wie möglich speichern, haben weniger Probleme mit der Protokollierung und Überwachung aller Schlüsselspeicherorte und bieten eine geringere Angriffsfläche für den unbefugten Zugriff auf die Schlüssel.
3.6 Vollständige Dokumentation und Implementierung aller Schlüsselverwaltungsprozesse und -verfahren für kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, wie z. B.: ***Hinweis:*** *Zahlreiche Branchenstandards für die Schlüsselverwaltung sind über verschiedene Ressourcen verfügbar, unter anderem über NIST (unter http://csrc.nist.gov).*	**3.6.a** ***Zusätzliches Testverfahren für Dienstanbieter:*** Wenn der Dienstanbieter Schlüssel gemeinsam mit seinen Kunden für die Übertragung oder Speicherung von Karteninhaberdaten verwendet, überprüfen Sie, ob die vom Dienstanbieter 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. **3.6.b** Überprüfen Sie die Schlüsselverwaltungsverfahren und die Prozesse für Schlüssel zur Verschlüsselung von Karteninhaberdaten, und führen Sie Folgendes durch:	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 Schlüsselelemente ein. 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. Diese Anforderung gilt für Schlüssel, die zur Verschlüsselung gespeicherter Karteninhaberdaten dienen, sowie für sämtliche zugehörigen Schlüsselverschlüsselungsschlüssel.
3.6.1 Erstellung starker kryptographischer Schlüssel	**3.6.1.a** Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung festgelegt ist, wie starke Schlüssel erstellt werden. **3.6.1.b** Prüfen Sie, ob mit der Schlüsselerstellungsmethode starke Schlüssel generiert werden.	Die Verschlüsselungslösung muss in der Lage sein, starke Schlüssel entsprechend der Definition von „starke Kryptographie“ im PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme zu generieren. Durch den Einsatz starker kryptographischer Schlüssel wird die Sicherheit verschlüsselter Karteninhaberdaten deutlich erhöht.
3.6.2 Sichere Verteilung kryptographischer Schlüssel	**3.6.2.a** 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

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
	3.6.2.b Prüfen Sie, ob mit der Schlüsselverteilmethode die Schlüssel sicher verteilt werden.	Personen verteilt werden dürfen.
3.6.3 Sicheres Speichern kryptographischer Schlüssel	**3.6.3.a** Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung festgelegt ist, wie Schlüssel sicher gespeichert werden. **3.6.3.b** Prüfen Sie, ob mit der Schlüsselspeichermethode die 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.
3.6.4 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).	**3.6.4.a** Überprüfen Sie, ob Verfahren zur Schlüsselverwaltung implementiert sind, die Schlüsseländerungen nach Ablauf einer für die einzelnen Schlüsseltypen festgelegten Schlüssellebensdauer erfordern. **3.6.4.b** Befragen Sie das Personal, ob Schlüssel nach Ablauf der angegebenen Schlüssellebensdauer geändert werden.	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 von zentraler Bedeutung zur Minimierung des Risikos, dass sich Unbefugte Zugriff auf Verschlüsselungsschlüssel verschaffen und damit Daten entschlüsseln.
3.6.5 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. ***Hinweis:*** *Wenn entfernte oder ausgetauschte kryptographische*	**3.6.5.a** Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung Prozesse für die folgenden Punkte festgelegt sind: • Wenn die Integrität eines Schlüssels gefährdet ist, wird er entfernt oder ausgetauscht. • Schlüssel, bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden, werden ausgetauscht. • Nach der Entfernung bzw. dem Austausch aufbewahrte Schlüssel werden nicht mehr für Verschlüsselungsvorgänge eingesetzt.	Schlüssel, die nicht mehr genutzt oder gebraucht werden bzw. bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden, dass sie kompromittiert wurden, sollten zurückgerufen und/oder vernichtet werden, 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. Die Verschlüsselungslösung sollte einen Prozess

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
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.	**3.6.5.b** Befragen Sie die Mitarbeiter, ob die folgenden Prozesse implementiert sind: • 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. • Schlüssel, bei denen bekannt ist oder der Verdacht besteht, dass sie kompromittiert wurden, werden ausgetauscht. • Nach der Entfernung bzw. dem Austausch aufbewahrte Schlüssel werden nicht mehr für Verschlüsselungsvorgänge eingesetzt.	bereitstellen 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.
3.6.6 Bei einer manuellen Verwaltung kryptographischer Klartext-Schlüssel gilt das Prinzip der geteilten Kenntnis und doppelten Kontrollen. ***Hinweis:*** *Zu den manuellen Verfahren zur Schlüsselverwaltung zählen unter anderen das Generieren, Übertragen, Laden, Speichern und Vernichten von Schlüsseln.*	**3.6.6.a** Überprüfen Sie, ob in den Verfahren zur Schlüsselverwaltung Prozesse für die folgenden Punkte festgelegt sind: • Die Schlüsselkomponenten befinden sich in der Kontrolle von mindestens zwei Personen, die jeweils nur Kenntnisse zu ihrer Komponente haben, UND • 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. **3.6.6 b** Prüfen Sie durch Befragung des Personals und/oder Beobachtung von Prozessen, ob bei einer manuellen Verwaltung von Klartextschlüsseln folgende Prinzipien gelten: • Geteiltes Wissen UND • Doppelte Kontrolle	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. Geteiltes Wissen bedeutet, dass die Komponenten eines Schlüssels auf mindestens zwei Personen aufgeteilt werden. Jede Person kennt nur die eigene Komponente, und der ursprüngliche kryptographische Schlüssel kann nicht mithilfe der einzelnen Komponenten rekonstruiert werden. 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.
3.6.7 Verhindern der unbefugten Ersetzung kryptographischer Schlüssel.	**3.6.7.a** Überprüfen Sie, ob in Verfahren zur Schlüsselverwaltung Prozesse zur Vermeidung der unbefugten Schlüsselersetzung festgelegt sind.	Die Verschlüsselungslösung sollte keine Auswechselungen von Schlüsseln autorisieren, die aus nicht zugelassenen Quellen oder

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
	3.6.7 b Prüfen Sie durch Befragung des Personals und/oder Beobachtung von Prozessen, ob die nicht autorisierte Ersetzung von Schlüsseln verhindert wird.	unerwarteten Prozessen stammen.
3.6.8 Wächter kryptographischer Schlüssel müssen formal bestätigen, dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen.	**3.6.8.a** 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.	Dieser Prozess gewährleistet, dass sich Personen, die als Schlüsselwächter fungieren, an ihre Rolle als Schlüsselwächter halten und die damit verbundenen Verantwortlichkeiten verstehen.
	3.6.8.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.	
3.7 Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz gespeicherter Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**3.7** Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz gespeicherter Karteninhaberdaten Folgendes gilt: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	Das Personal muss die folgenden Sicherheitsrichtlinien und dokumentierten betrieblichen Verfahren kennen und befolgen, damit die Karteninhaberdaten dauerhaft sicher gespeichert werden.

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

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

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
4.1 Verwenden Sie starke Kryptographie- und Sicherheitsprotokolle (z. B. SSL/TLS, IPSEC, SSH usw.), damit vertrauliche Karteninhaberdaten während der Übertragung über offene und öffentliche Netzwerke gemäß den folgenden Kriterien geschützt sind:	**4.1.a** 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. Dadurch können Sie prüfen, ob an allen Standorten Sicherheitsprotokolle und eine starke Kryptographie eingesetzt werden.	Vertrauliche Informationen müssen während der Übertragung über öffentliche Netzwerke verschlüsselt werden, da böswillige Personen Daten während der Übertragung mühelos abfangen und/oder umleiten können. Eine sichere Übertragung von Karteninhaberdaten setzt die Verwendung vertrauenswürdiger

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
• Es werden ausschließlich vertrauenswürdige Schlüssel und Zertifikate akzeptiert. • Das verwendete Protokoll unterstützt ausschließlich sichere Versionen oder Konfigurationen. • Für die verwendete Verschlüsselungsmethode wird die richtige Verschlüsselungsstärke verwendet. *Zu den offenen, öffentlichen Netzwerken zählen unter anderem:* • *Das Internet* • *Wireless-Technologien wie 802.11 und Bluetooth* • *Mobilfunktechnologien wie GSM (Global System for Mobile Communications) und CDMA (Code Division Multiple Access)* • *General Packet Radio Service (GPRS).* • *Satellitenverbindungen*	**4.1.b** Prüfen Sie in den dokumentierten Richtlinien und Verfahren, ob Prozesse für Folgendes festgelegt wurden: • Werden ausschließlich vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert? • Unterstützt das verwendete Protokoll ausschließlich sichere Versionen und Konfigurationen? • Wird für die verwendete Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet?	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. Beachten Sie, dass einige Protokollimplementierungen (z. B. SSL v2.0, SSH v1.0 und TLS 1.0) bekannte Sicherheitsrisiken aufweisen, über die ein Angreifer die Kontrolle über das betroffene System erlangen könnte. Sorgen Sie unabhängig vom verwendeten Sicherheitsprotokoll dafür, dass ausschließlich sichere Konfigurationen und Versionen verwendet und unsichere Verbindungen vermieden werden. So können Sie beispielsweise in Erwägung ziehen, TLS ab Version 1.1 sowie starkt verschlüsselte Zertifikate von einer anerkannten öffentlichen Zertifikatsstelle zu verlangen. 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).
	4.1.c Wählen Sie eine Stichprobe aus ein- und ausgehenden Transaktionen aus, und prüfen Sie bei der Beobachtung der Stichproben, ob sämtliche Karteninhaberdaten während der Übertragung stark verschlüsselt werden.	
	4.1.d Überprüfen Sie, ob nur vertrauenswürdige Schlüssel und/oder Zertifikate akzeptiert werden.	
	4.1.e Überprüfen Sie in der Systemkonfiguration, ob das Protokoll so implementiert ist, dass ausschließlich sichere Konfigurationen verwendet und unsichere Versionen bzw. Konfigurationen nicht unterstützt werden.	
	4.1.f Überprüfen Sie in der Systemkonfiguration, ob für die verwendete Verschlüsselungsmethode die richtige Verschlüsselungsstärke verwendet wird. (Prüfen Sie Anbieterempfehlungen/bewährte Verfahren.)	
	4.1.g Prüfen Sie bei SSL/TLS-Implementierungen in den Systemkonfigurationen, ob SSL/TLS bei jeder Übertragung bzw. bei jedem Empfang von Karteninhaberdaten aktiviert wird. Bei browserbasierten Implementierungen ist beispielsweise Folgendes zu prüfen: • Wird „HTTPS“ als Bestandteil des Browser-URL-Protokolls angezeigt? • Werden Karteninhaberdaten nur angefordert, wenn die URL die Komponente „HTTPS“ enthält?	Im Allgemeinen beginnt die URL der Website mit „HTTPS“, und im Browser-Fenster wird ein Vorhängeschloss-Symbol angezeigt. Bei zahlreichen Anbieter von SSL-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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
4.1.1 Stellen Sie sicher, dass drahtlose Netzwerke, die Karteninhaberdaten übertragen oder mit der CDE verbunden sind, mittels bewährter Branchenverfahren (z. B. IEEE 802.11i) die starke Verschlüsselung für die Authentifizierung und Übertragung implementieren. ***Hinweis:*** *Die Nutzung von WEP als Sicherheitskontrolle ist verboten.*	**4.1.1** 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: • Es werden bewährte Branchenverfahren (z. B. IEEE 802.11i) eingesetzt, um eine starke Verschlüsselung bei der Authentifizierung und Übertragung zu implementieren. • Eine schwache Verschlüsselung (z. B. WEP, SSL bis Version 2.0) wird nicht als Sicherheitskontrolle für die Authentifizierung oder Übertragung eingesetzt.	Böswillige Personen verwenden kostenlose und allseits verfügbare Tools, um Drahtloskommunikationen zu belauschen. Durch eine starke Kryptographie kann die Weitergabe vertraulicher Informationen über Drahtlosnetzwerke eingeschränkt werden. Um zu vermeiden, dass sich böswillige Benutzer Zugriff auf das Drahtlosnetzwerk verschaffen oder über die Drahtlosnetzwerke andere interne Netzwerke oder Daten zu erreichen, muss eine starke Kryptographie zur Authentifizierung und Übertragung von Karteninhaberdaten eingesetzt werden.
4.2 Versenden Sie niemals ungeschützte PANs über Messaging-Technologien für Endbenutzer (z. B. E-Mail, Instant Messaging, Chat usw.).	**4.2.a** 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 nicht lesbar ist gemacht oder mittels einer starken Kryptographie gesichert wurde.	E-Mail, Instant Messaging 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 keine starke Verschlüsselung bieten.
	4.2.b Vergewissern Sie sich in den schriftlich fixierten Richtlinien, dass ungeschützte PANs nicht über Messaging-Technologien für Endbenutzer gesendet werden dürfen.	
4.3 Sicherheitsrichtlinien und betriebliche Verfahren zur Verschlüsselung der Übertragung von Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**4.3** 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: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit die Karteninhaberdaten dauerhaft sicher übertragen werden.

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	LEITFADEN
5.1 Implementieren von Antivirensoftware auf allen Systemen, die häufig von böswilliger Software befallen werden (insbesondere Personal Computer und Server).	**5.1** Überprüfen Sie für eine Stichprobe von Systemkomponenten, einschließlich aller Betriebssystemarten, die häufig von böswilliger Software befallen werden, ob eine Virenschutzsoftware implementiert ist, wenn eine anwendbare Virenschutztechnologie vorhanden ist.	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.
5.1.1 Sorgen Sie dafür, dass die Antivirenprogramme in der Lage sind, alle bekannten Malware-Typen zu erkennen, zu entfernen und davor zu schützen.	**5.1.1** Überprüfen Sie Folgendes in der Anbieterdokumentation und den Antiviren-Konfigurationen: • Werden alle bekannten Arten von Malware erkannt? • Werden alle bekannten Arten von Malware entfernt? • Werden die Systeme vor allen bekannten Arten von Malware geschützt? *Unter den Begriff „Malware“ fallen beispielsweise Viren, Würmer, Trojaner (Trojanische Pferde), Würmer, Spyware, Adware und Rootkits.*	Es ist wichtig, sich gegen **ALLE** Arten und Formen von Malware zu schützen.

PCI-DSS-Anforderungen	PRÜFVERFAHREN	LEITFADEN
5.1.2 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.	**5.1.2** Befragen Sie bei Systemen, die in der Regel nicht von Malware befallen sind, die Mitarbeiter, um herauszufinden, ob potenzielle Malware-Bedrohungen überwacht und analysiert werden, bevor festgelegt wird, dass weiterhin keine Antivirensoftware auf diesen Systemen installiert werden muss.	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 durch neue Malware frühzeitig erkannt werden. Die Malware-Trends müssen in der Identifizierung neuer Sicherheitsrisiken berücksichtigt werden, und auch Methoden zur Korrektur neuer Trends sollten je nach Bedarf in die Konfigurationsstandards und Schutzmechanismen eines Unternehmens aufgenommen werden.
5.2 Bei sämtlichen Antivirensysteme muss Folgendes beachtet werden: • Die Systeme müssen auf dem neuesten Stand gehalten werden. • Es müssen regelmäßige Suchläufe stattfinden. • Es sind Prüfprotokolle zu erstellen, die gemäß PCI-DSS-Anforderung 10.7 aufbewahrt werden müssen.	**5.2.a** Prüfen Sie in den Richtlinien und Verfahren, ob Antivirensoftware und Virendefinitionen immer auf dem neuesten Stand gehalten werden müssen.	Selbst die besten Antivirenlösungen funktionieren nur eingeschränkt, wenn sie nicht gewartet und mit Sicherheits-Updates, Signaturdateien und Malware-Schutz auf dem neuesten Stand gehalten werden. 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.
	5.2.b Untersuchen Sie die Antiviren-Konfigurationen einschließlich der Master-Installationen der Software auf folgende Punkte: • Werden die Antivirensysteme automatisch aktualisiert? • Finden regelmäßig Suchläufe statt?	
	5.2.c Überprüfen Sie für eine Stichprobe von Systemkomponenten, einschließlich aller Betriebssystemtypen, die häufig von Malware befallen werden, folgende Punkte: • Sind die Antivirensoftware und die Definitionen auf dem neuesten Stand? • Finden regelmäßig Suchläufe statt?	
	5.2.d Untersuchen Sie die Antiviren-Konfigurationen einschließlich der Master-Installationen der Software sowie eine Stichprobe der Systemkomponenten auf folgende Punkte: • Ist die Protokollerstellung in der Antivirensoftware aktiviert? • Werden die Protokolle gemäß PCI-DSS-Anforderung 10.7	

PCI-DSS-Anforderungen	PRÜFVERFAHREN	LEITFADEN
	aufbewahrt?	

PCI-DSS-Anforderungen	PRÜFVERFAHREN	LEITFADEN
5.3 Es muss sichergestellt sein, dass die Antivirensysteme aktiv ausgeführt werden und von den Benutzern weder deaktiviert noch verändert werden können. Ausnahmen hiervon sind nur fallweise und innerhalb eines beschränkten Zeitraums möglich. ***Hinweis:*** *Antivirenlösungen können nur dann vorübergehend deaktiviert werden, wenn es einen triftigen technischen Grund dafür gibt. Dieser muss vom Management fallweise autorisiert werden. Wenn der Virenschutz aus bestimmten Gründen deaktiviert werden muss, ist hierfür eine förmliche Autorisierung erforderlich. Zusätzliche Sicherheitsmaßnahmen müssen auch für den Zeitraum, in dem der Virenschutz nicht aktiv ist, getroffen werden.*	**5.3.a** Untersuchen Sie die Antiviren-Konfigurationen einschließlich der Master-Installationen der Software sowie eine Stichprobe der Systemkomponenten daraufhin, ob die Antivirensoftware aktiv ausgeführt wird. **5.3.b** Untersuchen Sie die Antiviren-Konfigurationen einschließlich der Master-Installationen der Software sowie eine Stichprobe der Systemkomponenten, und vergewissern Sie sich, dass die Antivirensoftware nicht von den Benutzern deaktiviert oder geändert werden kann. **5.3.c** Vergewissern Sie sich durch die Befragung der zuständigen Mitarbeiter und die Beobachtung von Prozessen, dass die Antivirensoftware von den Benutzern weder deaktiviert noch verändert werden kann, insofern die Änderungen nicht fallweise und innerhalb eines beschränkten Zeitraums vom Management autorisiert wurden.	Den besten Schutz vor Malware bietet Antivirensoftware, die ununterbrochen ausgeführt wird und nicht geändert werden kann. Die Verwendung richtlinienbasierter Kontrollen auf allen Systemen sorgt dafür, dass der Malware-Schutz nicht verändert oder deaktiviert werden kann. Dadurch wird verhindert, dass Systemschwachstellen von Malware ausgenutzt werden. Zusätzliche Sicherheitsmaßnahmen müssen auch für den Zeitraum, in dem der Virenschutz nicht aktiv ist, getroffen werden. Hierunter fallen beispielsweise das Trennen des ungeschützten Systems vom Internet, solange der Virenschutz deaktiviert ist, und die Durchführung einer vollständigen Systemprüfung, nachdem der Schutz wiederhergestellt wurde.
5.4 Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz von Systemen vor Malware müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**5.4** Klären Sie durch eine Überprüfung der Dokumentation und eine Befragung des Personals, ob für Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz der Systeme vor Malware Folgendes gilt: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren kennen und befolgen, damit die Systeme dauerhaft vor Malware geschützt sind.

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	LEITFADEN
6.1 Etablierung eines Prozesses zur Ermittlung von Sicherheitsrisiken auf der Grundlage verlässlicher Quellen und Einteilung neu ermittelter Sicherheitsrisiken in verschiedene Risikostufen (hoch/mittel/niedrig). ***Hinweis:*** *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.* *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*	**6.1.a** Prüfen Sie in den Richtlinien und Verfahren, ob Prozesse für Folgendes festgelegt wurden: • Ermittlung neuer Sicherheitsrisiken • Zuweisung von Risikostufen für Sicherheitsrisiken mit der Ermittlung sämtlicher „hohen" und „kritischen" Risiken • Nutzung verlässlicher externer Quellen von Informationen zu Sicherheitsrisiken **6.1.b** Klären Sie durch eine Befragung des Personals und die Beobachtung von Prozessen Folgendes ab: • Neue Sicherheitsrisiken werden ermittelt. • Die Sicherheitsrisiken werden verschiedenen Risikostufen zugeordnet, und alle „hohen" und „kritischen" Risiken werden ermittelt. • Bei den Prozessen zur Ermittlung neuer Sicherheitsrisiken werden verlässliche externe Quellen berücksichtigt.	Der Zweck dieser Anforderung besteht darin, dass ein Unternehmen stets auf dem neuesten Stand bezüglich Sicherheitsrisiken ist, die dessen Umgebung gefährden könnten. Die Quellen für Informationen zu Sicherheitsrisiken sollten vertrauenswürdig sein. Häufig zählen die Websites von Anbietern, Branchen-Newsgruppen, Mailinglisten und RSS-Feeds ebenso dazu. Sobald ein Unternehmen ein Sicherheitsrisiko entdeckt, das seine Umgebung beeinträchtigen könnte, muss das Risiko bewertet und entsprechend eingestuft werden. 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. Durch die Einstufung von Risiken (z. B. als „hoch", „mittel" oder „niedrig") sind Organisationen in der Lage, schneller die größten Risiken zu erkennen und zu beheben und somit die Wahrscheinlichkeit zu reduzieren, dass die größten Sicherheitsrisiken tatsächlich ausgenutzt werden.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
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.		
6.2 Alle Systemkomponenten und Softwareanwendungen müssen vor bekannten Sicherheitsrisiken mithilfe der neuesten Sicherheitspatches des jeweiligen Anbieter geschützt werden. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden. ***Hinweis:*** *Kritische Sicherheitspatches müssen gemäß dem in Anforderung 6.1 festgelegten Prozess zur Risikoeinstufung ermittelt werden.*	**6.2.a** Prüfen Sie in den Richtlinien und Verfahren im Zusammenhang mit Sicherheitspatches, ob Prozesse für Folgendes festgelegt wurden: • Kritische Sicherheitspatches der Anbieter müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden. • Alle sonstigen geltenden Sicherheitspatches der Anbieter müssen innerhalb eines angemessenen Zeitraums (z. B. innerhalb von drei Monaten) installiert werden. **6.2.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: • Werden kritische Sicherheitspatches der Anbieter innerhalb eines Monats nach ihrer Veröffentlichung installiert? • Werden alle sonstigen anwendbaren Sicherheitspatches der Anbieter innerhalb eines angemessenen Zeitraums (z. B. innerhalb von drei Monaten) installiert?	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. 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. Diese Anforderung gilt für sämtliche anwendbaren Patches zu allen installierten Softwareanwendungen.
6.3 Sichere Entwicklung von Softwareanwendungen (interne und externe, inklusive Web-Administrationszugriff auf die Anwendungen) unter Berücksichtigung der folgenden Punkte: • Werden Softwareanwendungen gemäß dem PCI-DSS entwickelt (z. B. sichere	**6.3.a** Überprüfen Sie, ob die schriftlich festgehaltenen Softwareentwicklungsprozesse auf Branchenstandards und/oder bewährten Praktiken basieren. **6.3.b** Untersuchen Sie in den schriftlichen Softwareentwicklungsprozessen, ob die Informationssicherheit während des gesamten Lebenszyklus enthalten ist.	Ohne die Einbindung von Informationssicherheitsmaßnahmen während der Definition der Anforderungen sowie der Design-, Analyse- und Testphasen in der Softwareentwicklung können Sicherheitslücken ungewollt oder in bösartiger Absicht in die Produktionsumgebung eingeschleust werden.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Authentifizierung und Protokollierung)? • Basieren die Entwicklungsprozesse auf Branchenstandards und/oder bewährten Verfahren? • Ist die Informationssicherheit während des gesamten Softwareentwicklungszyklus integriert? ***Hinweis**: Diese Anforderungen gelten für alle intern entwickelten Softwareanwendungen sowie individuell von Drittanbietern entwickelte Software.*	**6.3.c** Überprüfen Sie in den schriftlichen Softwareentwicklungsprozessen, ob die Softwareanwendungen gemäß den PCI-DSS-Anforderungen entwickelt werden. **6.3.d** Überprüfen Sie durch eine Befragung von Softwareentwicklern, ob die schriftlich festgehaltenen Softwareentwicklungsprozesse implementiert wurden.	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.
6.3.1 Löschen von Konten, Benutzer-IDs und Kennwörtern für Entwicklung, Tests und/oder individuelle Anwendungen, bevor die Anwendungen aktiv oder für Kunden freigegeben werden.	**6.3.1** Vergewissern Sie sich durch die Untersuchung von Softwareentwicklungsverfahren und durch die 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.	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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
6.3.2 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: • 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. • Mit Codeprüfungen wird dafür gesorgt, dass der Code gemäß sicheren Codierungsrichtlinien erstellt wird. • Vor der Freigabe werden entsprechende Korrekturen implementiert. • Ergebnisse der Codeprüfung werden vor der Freigabe vom Management geprüft und genehmigt.	**6.3.2.a** 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: • Codeänderungen werden von anderen Personen geprüft als dem ursprünglichen Ersteller des Codes sowie von Personen, die mit Verfahren zur Codeprüfung und sicheren Codierungsverfahren vertraut sind. • Codeprüfungen gewährleisten, dass der Code gemäß sicheren Codierungsrichtlinien erstellt wird (siehe PCI-DSS-Anforderung 6.5). • Vor der Freigabe werden entsprechende Korrekturen implementiert. • Ergebnisse der Codeprüfung werden vor der Freigabe vom Management geprüft und genehmigt.	Sicherheitslücken in benutzerspezifischen Codes werden von böswilligen Individuen häufig ausgenutzt, um sich Zugriff auf ein Netzwerk zu verschaffen und Karteninhaberdaten zu kompromittieren. In den Überprüfungsprozess muss eine kompetente und erfahrene Person eingebunden werden. 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 keine Codeprobleme erkennen lassen. Durch die Behebung von Codierungsfehlern vor der Bereitstellung in einer Produktionsumgebung bzw. vor der Freigabe für die Kunden wird verhindert, dass Umgebungen aufgrund von Codefehlern gefährdet werden. Nach der Bereitstellung bzw. Freigabe des Codes in Produktionsumgebungen ist es außerdem viel schwieriger und kostspieliger, Codefehler zu beheben. Eine offizielle Prüfung und die Abzeichnung durch das Management vor der Freigabe dienen zur Sicherstellung, dass der Code genehmigt und in Übereinstimmung mit den Richtlinien und Verfahren entwickelt wurde.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Hinweis: *Diese Anforderung für Code-Prüfungen gilt für den gesamten benutzerdefinierten (internen und öffentlichen) Code als Teil des Systementwicklungszyklus.* *Code-Prüfungen können durch qualifiziertes internes Personal oder durch Dritte ausgeführt werden. 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.*	**6.3.2.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.	
6.4 Befolgen von Änderungskontrollprozessen und -verfahren für alle Änderungen an Systemkomponenten. Die Prozesse müssen Folgendes umfassen:	**6.4** In den Richtlinien und Verfahren muss Folgendes definiert sein: • Die Entwicklungs-/Testumgebungen sind von den Produktionsumgebungen getrennt, und zur Durchsetzung dieser Trennung ist eine Zugriffskontrolle implementiert. • Es besteht eine Trennung der Aufgaben zwischen Mitarbeitern, die den Entwicklungs-/Testumgebungen zugewiesen sind, und Mitarbeitern, die der Produktionsumgebung zugeteilt sind. • Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet. • Testdaten und -konten werden gelöscht, bevor ein Produktionssystem aktiv wird. • Änderungskontrollverfahren im Hinblick auf die Implementierung von Sicherheitspatches und Softwareänderungen sind dokumentiert.	Ohne angemessen 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.
6.4.1 Trennung der Entwicklungs-/Testumgebungen von der Produktionsumgebung und Durchsetzung dieser Trennung mittels Zugriffskontrolle.	**6.4.1.a** Vergewissern Sie sich in der Netzwerkdokumentation und der Konfiguration der Netzwerkgeräte, dass die Entwicklungs-/Testumgebungen von den Produktionsumgebungen getrennt sind.	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

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
	6.4.1.b Vergewissern Sie sich in den Zugriffskontrolleinstellungen, dass die Trennung der Entwicklungs-/Testumgebungen von den Produktionsumgebungen erzwungen wird.	möglich, dass die Produktionsumgebung und die Karteninhaberdaten aufgrund von zu wenig stringenten Sicherheitskonfigurationen und von möglichen Sicherheitsrisiken in einer Test- oder Entwicklungsumgebung gefährdet sind.
6.4.2 Trennung der Aufgaben zwischen Entwicklungs-, Test- und Produktionsumgebungen	**6.4.2** 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.	Indem die Personenzahl, die Zugriff auf die Produktionsumgebung und die Karteninhaberdaten hat, eingeschränkt wird, kann das Risiko minimiert und sichergestellt werden, dass der Zugriff ausschließlich auf Personen mit einem geschäftlichen Informationsbedarf beschränkt ist. 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.
6.4.3 Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet	**6.4.3.a** Vergewissern Sie sich durch die Beobachtung der Testverfahren und die Befragung der Mitarbeiter, dass keine Produktionsdaten (Live-PANs) zum Testen oder zur Entwicklung verwendet werden.	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.
	6.4.3.b Vergewissern Sie sich in Stichproben von Testdaten, dass keine Produktionsdaten (Live-PANs) zum Testen oder zur Entwicklung verwendet werden.	
6.4.4 Löschung von Testdaten und -konten, bevor Produktionssysteme aktiv werden	**6.4.4** Vergewissern Sie sich durch die Beobachtung von Testverfahren und durch die Befragung von Mitarbeitern, dass Testdaten und -konten gelöscht werden, bevor ein Produktionssystem aktiv wird.	Testdaten und -konten müssen aus dem Produktionscode gelöscht werden, bevor die Anwendung aktiviert wird, 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.
	6.4.4.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.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
6.4.5 Änderungskontrollverfahren für die Implementierung von Sicherheitspatches und Softwareänderungen müssen folgende Punkte umfassen:	**6.4.5.a** Untersuchen Sie die dokumentierten Änderungskontrollverfahren im Hinblick auf die Implementierung von Sicherheitspatches und Softwareänderungen, und prüfen Sie, ob Verfahren für die folgenden Punkte definiert sind: • Dokumentation der Auswirkungen • Dokumentierte Genehmigung von Änderungen durch autorisierte Parteien • Testen der Funktionalität, damit die Änderung nicht die Sicherheit des Systems beeinträchtigt. • Back-Out-Verfahren	Wird die Verwaltung nicht ordnungsgemäß durchgeführt, sind die Auswirkungen von Softwareupdates und Sicherheitspatches möglicherweise nicht vollständig bekannt, und sie könnten unbeabsichtigte Folgen nach sich ziehen.
	6.4.5.b Befragen Sie zuständige Mitarbeiter, um aktuelle Änderungen/Sicherheitspatches 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:	
6.4.5.1 Dokumentation der Auswirkungen.	**6.4.5.1** Überprüfen Sie, ob die Dokumentation der Auswirkungen in der Änderungskontrolldokumentation für jede Änderung in der Stichprobe enthalten ist.	Die Auswirkungen der Änderung sollten dokumentiert werden, sodass alle betroffenen Parteien Prozessänderungen entsprechend vorausplanen können.
6.4.5.2 Dokumentierte Genehmigung von Änderungen durch autorisierte Parteien.	**6.4.5.2** Überprüfen Sie, ob für jede Änderung aus der Stichprobe eine dokumentierte Genehmigung durch autorisierte Parteien vorhanden ist.	Die Genehmigung durch eine autorisierte Partei deutet darauf hin, dass es sich um eine zulässige und von dem Unternehmen genehmigte Änderung handelt.
6.4.5.3 Testen der Funktionalität, damit die Änderung nicht die Sicherheit des Systems beeinträchtigt.	**6.4.5.3.a** Vergewissern Sie sich mit Funktionalitätstests für jede Änderung in der Stichprobe, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt.	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 jeglichen Änderungen in der Umgebung sogar intensiviert werden müssen.
	6.4.5.3.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.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
6.4.5.4 Back-Out-Verfahren.	**6.4.5.4** Überprüfen Sie, ob für jede Änderung in der Stichprobe Back-Out-Verfahren erstellt werden.	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.
6.5 Eingehen auf häufige Sicherheitsrisiken in Softwareentwicklungsprozessen, einschließlich der folgenden Punkte: • Schulung von Entwicklern in Techniken zur Erstellung sicherer Codes und zur Vermeidung häufiger Sicherheitsrisiken unter Berücksichtigung des Umgangs mit vertraulichen Daten im Speicher. • Entwicklung von Anwendungen auf der Grundlage sicherer Programmierungsrichtlinien. ***Hinweis:*** *Die unter 6.5.1 bis 6.5.10 aufgeführten Sicherheitsrisiken entsprachen*	**6.5.a** Vergewissern Sie sich durch Untersuchung von Richtlinien und Verfahren für die Softwareentwicklung, dass Schulungen im Hinblick auf sichere Programmierverfahren für Entwickler auf Basis der bewährten Verfahren der Branche sowie Leitfäden vorgeschrieben werden. **6.5.b** Überprüfen Sie in Gesprächen mit stichprobenartig ausgewählten Entwicklern, ob die Entwickler mit sicheren Codierungsverfahren vertraut sind. **6.5.c** Überprüfen Sie in Schulungsunterlagen, ob die Softwareentwickler in Techniken zur Erstellung sicherer Codes und zur Vermeidung häufiger Sicherheitsrisiken unter Berücksichtigung des Umgangs mit vertraulichen Daten im Speicher unterrichtet wurden.	Die Anwendungsschicht ist einem hohen Risiko ausgesetzt und ist sowohl durch interne als auch externe Bedrohungen gefährdet. Die Mindestkontrollen werden durch die Anforderungen 6.5.1 bis 6.5.10 festgelegt. Ein Unternehmen sollte basierend auf der jeweiligen Technologie in seiner Umgebung passende sichere Programmierverfahren implementieren. Anwendungsentwickler müssen ordnungsgemäß geschult sein, damit sie Probleme im Zusammenhang mit diesen (und anderen) gängigen Programmierrisiken erkennen und lösen können. Wenn die Mitarbeiter mit sicheren

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
zum Zeitpunkt der Veröffentlichung dieser Version des PA-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.), müssen für diese Anforderungen die aktuellen bewährten Verfahren verwendet werden.	**6.5.d.** Vergewissern Sie sich, dass Anwendungen durch entsprechende Prozesse mindestens vor den folgenden Sicherheitsrisiken geschützt sind:	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 bereitgestellt werden. Da sich die von der Branche akzeptierten Verfahrensweisen zur sicheren Programmierung im Laufe der Zeit ändern können, müssen die Programmierpraktiken in der Organisation und die Schulungen der Entwickler ebenfalls an neue Bedrohungen wie etwa Memory-Scraping-Angriffe angepasst werden. Die in den Punkten 6.5.1 bis 6.5.10 aufgeführten Sicherheitsrisiken stellen eine Mindestanforderung dar. Es ist die Aufgabe der Unternehmen, bei Sicherheitstrends auf dem neuesten Stand zu bleiben und angemessene Maßnahmen für eine sichere Programmierung zu ergreifen.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Hinweis: *Die Anforderungen 6.5.1 bis 6.5.6 gelten für alle Anwendungen (intern oder extern):*		
6.5.1 Injektionsfehler, insbesondere bei der SQL-Injektion. Injektion von Betriebssystembefehlen, LDAP- und Xpath-Injektionsfehler sowie andere Injektionsfehler sind ebenfalls zu berücksichtigen.	**6.5.1** 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: • Validierung der Eingabe, damit Benutzerdaten nicht die Bedeutung von Befehlen und Abfragen ändern können • Verwendung von parametrisierten Abfragen	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. Die Informationen müssen vor der Weiterleitung an die Anwendung validiert werden – beispielsweise werden sie auf das Vorhandensein von Buchstaben, alphanumerischen Zeichen usw. untersucht.
6.5.2 Pufferüberläufe	**6.5.2** 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: • Validierung von Puffergrenzen • Kürzung der eingegebenen Zeichenfolgen	Pufferüberläufe treten auf, wenn eine Anwendung auf ihrem Pufferspeicherplatz nicht über eine geeignete Bereichsüberprüfung 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, schädliche Codes 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 rechnerfernen Zugriff auf die Anwendung und/oder das betroffene System.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
6.5.3 Unsicherer kryptographischer Speicher	**6.5.3** 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 Programmiertechniken begegnet wird: • Verhindern Sie kryptographische Fehler. • Nutzung starker kryptographischer Algorithmen und Schlüssel	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, könnte er unter Umständen auch in der Lage sein, auf verschlüsselte Daten im Klartext zuzugreifen.
6.5.4 Unsichere Mitteilungen	**6.5.4** Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob unsicheren Mitteilungen mit Programmiertechniken 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, könnte er unter Umständen auch in der Lage sein, die Kontrolle über eine Anwendung zu erlangen oder verschlüsselte Daten in Klartext anzuzeigen.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
6.5.5 Inkorrekte Fehlerhandhabung	**6.5.5** Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob die 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.“
6.5.6 Alle „schwerwiegenden“ Sicherheitsrisiken werden entsprechend dem Identifikationsprozess ermittelt (wie in der PCI-DSS-Anforderung 6.1 definiert).	**6.5.6** 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 PA-DSS-Anforderung 6.1.	Alle Sicherheitsrisiken, die vom Unternehmensprozess zur Risikoeinstufung (in der PA-DSS-Anforderung 6.1 definiert) als „hohes Risiko“ eingestuft werden und die die Anwendung beeinträchtigen könnten, müssen während der Anwendungsentwicklung ermittelt und behoben werden.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Hinweis: *Die nachstehenden Anforderungen 6.5.7 bis 6.5.10 gelten für Webanwendungen und Anwendungsschnittstellen (intern oder extern):*		Webanwendungen sowohl intern als auch extern (öffentlich) sind aufgrund ihrer Architektur sowie der relativ einfachen Erstellung und der Häufigkeit von Angriffen besonderen Sicherheitsrisiken ausgesetzt.
6.5.7 Siteübergreifendes Scripting (XSS)	**6.5.7** 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 Programmiertechniken begegnet wird: • Validierung aller Parameter vor der Einbindung • Nutzung einer kontextabhängigen Außerkraftsetzungsfunktion	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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
6.5.8 Kontrolle unangemessener Zugriffe (z. B. unsichere direkte Objektverweise, fehlende Einschränkung des URL-Zugriffs, Directory Traversal und fehlende Einschränkung des Benutzerzugriffs auf bestimmte Funktionen).	**6.5.8** 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: • Ordnungsgemäße Benutzerauthentifizierung • Bereinigung der Eingaben • Keine Preisgabe interner Objektverweise an Benutzer • Benutzeroberflächen, die keinen Zugriff auf nicht autorisierte Funktionen zulassen	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. 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. 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. 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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
6.5.9 Cross-Site Request Forgery (CSRF)	**6.5.9** Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob auf CSRF (Cross-site Request Forgery, Websiteübergreifende Anfragenfälschung) mit Programmierverfahren eingegangen wird, damit Anwendungen sich nicht auf Autorisierungsinformationen und Token verlassen, 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).
6.5.10 Geknackte Authentifizierungs- und Sitzungsverwaltung ***Hinweis:*** *Die Anforderung 6.5.10 wird bis zum 30. Juni 2015 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*	**6.5.10** Überprüfen Sie durch die Untersuchung von Richtlinien und Verfahren zur Softwareentwicklung und die Befragung der zuständigen Mitarbeiter, ob einer geknackten Authentifizierungs- und Sitzungsverwaltung mit u. a. den folgenden Programmiertechniken begegnet wird: • Kennzeichnung von Sitzungstoken (zum Beispiel Cookies) als „sicher“ • Keine Anzeige von Sitzungs-IDs in der URL • Berücksichtigung angemessener Timeouts und Rotation der Sitzungs-IDs nach erfolgreicher Anmeldung	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	LEITFADEN
6.6 Kontinuierliche Betrachtung neuer Bedrohungen und Sicherheitsrisiken bei öffentliche Webanwendungen Schutz dieser Anwendungen vor bekannten Angriffen auf eine der folgenden Methoden: • Prüfen öffentlicher Webanwendungen durch manuelle oder automatisierte Tools oder Methoden zum Bewerten der Anwendungssicherheit mindestens jährlich sowie nach Änderungen ***Hinweis:*** *Diese Bewertung ist nicht mit den für Anforderung 11.2 durchgeführten Schwachstellenprüfungen identisch.* • Installation einer automatischen technischen Lösung zur Erkennung und Verhinderung webbasierter Angriffe (z. B. eine Webanwendungs-Firewall) bei öffentlichen Webanwendungen zur kontinuierlichen Prüfung des Datenverkehrs	**6.6** Achten Sie bei *öffentlichen* Webanwendungen darauf, dass *eine* der folgenden Methoden implementiert ist: • 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): - Mindestens jährlich - Nach jeder Änderung - Durch ein Unternehmen, das auf Anwendungssicherheit spezialisiert ist - In den Bewertungen sollten mindestens die in der Anforderung 6.5 aufgeführten Sicherheitsrisiken überprüft werden. - Dass alle Sicherheitslücken geschlossen werden - Dass die Anwendung nach den Korrekturen erneut bewertet wird • 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: - Die Lösung befindet sich vor öffentlichen Webanwendungen und dient dazu, webbasierte Angriffe zu erkennen und zu verhindern. - Die Lösung wird aktiv ausgeführt und auf dem neuesten Stand gehalten. - In der Lösung werden Prüfprotokolle erstellt. - Die Lösung ist so konfiguriert, dass webbasierte Angriffe abgeblockt werden oder ein Alarm ausgelöst wird.	Öffentliche Webanwendungen sind die primären 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 bezweckt, die Anzahl der Gefährdungen öffentlicher Webanwendungen zu reduzieren, durch die häufig Karteninhaberdaten gefährdet werden. • Manuelle oder automatisierte Tools oder Methoden zur Bewertung der Anwendungssicherheit dienen z ur Prüfung bzw. zum Test der Anwendung auf Sicherheitsrisiken. • 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. ***Hinweis:*** *„Ein Unternehmen, das auf Anwendungssicherheit spezialisiert ist“, kann ein Drittunternehmen oder eine interne Organisation sein, sofern sich die Prüfer auf Anwendungssicherheit spezialisieren und die Unabhängigkeit vom Entwicklungsteam nachweisen können.*

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
6.7 Die Sicherheitsrichtlinien und betriebliche Verfahren zum Aufbau und zur Wahrung sicherer Systeme und Anwendungen müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**6.7** 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: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	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.

Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

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

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

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
7.1 Beschränken des Zugriffs auf Systemkomponenten und Karteninhaberdaten auf die Personen, deren Tätigkeit diesen Zugriff erfordert.	**7.1** Überprüfen Sie, ob die schriftlich fixierte Richtlinie für die Zugriffskontrolle die Anforderungen 7.1.1 bis 7.1.4 wie folgt erfüllt: • Jeder Rolle werden Zugriffsanforderungen und -berechtigungen zugewiesen. • Der Zugriff für Benutzer-IDs ist auf Mindestberechtigungen, die zum Ausüben der tätigkeitsbezogenen Verpflichtungen erforderlich sind, beschränkt. • Die Zuweisung von Zugriffsberechtigungen basiert auf der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter. • Genehmigungen (in schriftlicher oder elektronischer Form) durch autorisierten Parteien müssen für alle Zugriffsberechtigungen, einschließlich einer Liste der genehmigten Berechtigungen, dokumentiert werden.	Je mehr Personen Zugriff auf die Karteninhaberdaten haben, desto höher ist das Risiko, dass das Konto eines Benutzers in böser Absicht ausgenutzt wird. Indem der Zugriff ausschließlich auf Personen beschränkt wird, die aus geschäftlichen Gründen Einsicht benötigen, kann ein falscher Umgang im Unternehmen mit den Karteninhaberdaten durch Unerfahrenheit oder Böswilligkeit vermieden werden.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
7.1.1 Definition der Zugriffsanforderungen für die einzelnen Rollen unter Berücksichtigung der folgenden Aspekte: • Systemkomponenten und Datenressourcen, die für die Ausführung der tätigkeitsbezogenen Funktionen benötigt werden • Erforderliche Berechtigungsstufe (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen	**7.1.1** Bestimmen Sie eine Stichprobe aus Rollen, und prüfen Sie, ob die Zugriffsanforderungen für die einzelnen Rollen definiert sind und die folgenden Punkte umfassen: • Systemkomponenten und Datenressourcen, die für die Ausführung der tätigkeitsbezogenen Funktionen benötigt werden • Ermittlung der für die Durchführung der tätigkeitsbezogenen Funktionen der Rolle erforderliche Berechtigungen	Damit der Zugriff auf Karteninhaberdaten auf diejenigen Personen beschränkt bleibt, die tatsächlich auf die Daten zugreifen müssen, müssen zuerst Zugriffsanforderungen für die einzelnen Rollen (Systemadministrator, Callcenter-Personal, Filialmitarbeiter usw.), die Systeme/Geräte/Daten, auf die die einzelnen Rollen zugreifen müssen, und die Berechtigungsstufe, die für eine effektive Ausführung der zugewiesenen Aufgaben erforderlich ist, definiert werden. Sobald die Rollen und die zugehörigen Zugriffsberechtigungen definiert sind, können die Berechtigungen den einzelnen Benutzern zugewiesen werden.
7.1.2 Beschränkung des Zugriffs für Benutzer-IDs auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind.	**7.1.2.a** Überprüfen Sie durch Gespräche mit den für die Zugriffszuweisung zuständigen Mitarbeitern, dass für den Zugriff auf die privilegierten Benutzer-IDs Folgendes gilt: • Die Zugriffsrechte werden nur Rollen zugewiesen, die diesen privilegierten Zugriff konkret benötigen. • Die Zugriffsrechte sind auf Mindestberechtigungen beschränkt, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind.	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. *(Fortsetzung auf der nächsten Seite)*
	7.1.2.b Überprüfen Sie an stichprobenartig zusammengestellten Benutzer-IDs mit privilegiertem Zugriff durch Gespräche mit den für die Verwaltung zuständigen Mitarbeitern, dass für die zugewiesenen Berechtigungen Folgendes gilt: • Die Berechtigungen sind für die tätigkeitsbezogenen Aufgaben der Person erforderlich. • Die Zugriffsrechte sind auf Mindestberechtigungen beschränkt, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind.	Das Zuweisen von Mindestberechtigungen trägt dazu bei zu verhindern, dass Benutzer ohne ausreichende Anwendungskenntnisse fälschlicherweise oder versehentlich die Anwendungskonfiguration oder ihre Sicherheitseinstellungen ändern. Durch die Durchsetzung der Mindestberechtigung wird auch das Ausmaß des Schadens minimiert, der entsteht, wenn eine nicht autorisierte Person Zugriff auf eine Benutzer-ID erhält.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
7.1.3 Zuweisung von Zugriffsberechtigungen basierend auf der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter.	**7.1.3** Überprüfen Sie an stichprobenartig zusammengestellten Benutzer-IDs durch Gespräche mit den für die Verwaltung zuständigen Mitarbeitern, dass die zugewiesenen Berechtigungen auf der Tätigkeitsklassifizierung und -funktion des jeweiligen Mitarbeiters basieren.	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.
7.1.4 Die Genehmigung durch autorisierte Parteien, in der die erforderlichen Berechtigungen angegeben sind, muss dokumentiert werden.	**7.1.4** Prüfen Sie für stichprobenartig ausgewählte Benutzer-IDs durch einen Vergleich mit dokumentierten Genehmigungen, dass Folgendes gilt: • Die Genehmigung der zugewiesenen Berechtigungen wurde dokumentiert. • Die Genehmigung wurde von autorisierten Parteien erteilt. • Die angegebenen Berechtigungen entsprechen den Rollen, die der Person zugewiesen sind.	Durch die (schriftliche oder elektronische) Dokumentation der Genehmigung wird erreicht, dass das Management die mit Zugriffsberechtigung und sonstigen Rechten ausgestatteten Personen kennt und dass der Zugriff für die Tätigkeitsfunktionen erforderlich ist.
7.2 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. Dieses Zugriffskontrollsystem muss Folgendes umfassen:	**7.2** Prüfen Sie anhand von Systemeinstellungen und der Anbieterdokumentation wie folgt, ob ein Zugriffskontrollsystem implementiert ist:	Ohne einen Mechanismus, um den Zugriff von Benutzern entsprechend ihres Informationsbedarfs einzuschränken, könnte einem Benutzer unter Umständen ungewollt Zugriff auf Dateninhaberdaten gewährt werden. In einem Zugriffskontrollsystem wird der Prozess z ur Beschränkung des Zugriffs und zur Zuweisung von Berechtigungen automatisiert. Darüber hinaus sorgt die Einstellung „Alle ablehnen“ dafür, dass niemandem Zugriff gewährt wird, solange keine Regel vorliegt, die einen Zugriff konkret gewährt. ***Hinweis:*** *Einige Zugriffskontrollsysteme sind standardmäßig auf „Alle zulassen“ gesetzt und lassen dadurch den Zugriff zu, bis eine Regel erstellt wird, die den Zugriff ausdrücklich ablehnt.*
7.2.1 Abdeckung aller Systemkomponenten	**7.2.1** Bestätigen Sie, dass in allen Systemkomponenten Zugriffskontrollsysteme implementiert sind.	
7.2.2 Zuweisung von Berechtigungen zu einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion.	**7.2.2** Bestätigen Sie, dass Zugriffskontrollsysteme konfiguriert sind, um Berechtigungen durchzusetzen, die einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion zugewiesen sind.	
7.2.3 Standardeinstellung „Alle ablehnen“	**7.2.3** Vergewissern Sie sich, dass die Zugriffskontrollsysteme die Standardeinstellung „Alle ablehnen“ aufweisen.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
7.3 Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des Zugriffs auf Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**7.3** 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: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	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.

Anforderung 8: Zugriff auf Systemkomponenten identifizieren und authentifizieren

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

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 nie auf mehrere Kartennummern gleichzeitig Zugriff haben. Auf diese Weise können einzelne Transaktionen vereinfacht werden (z. B. Kassierer-Konten).

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
8.1 Definition und Implementierung von Richtlinien und Verfahren zur geeigneten Benutzeridentifizierungsverwaltung für Nichtverbraucherbenutzer und Administratoren auf allen Systemkomponenten nach folgender Maßgabe:	**8.1.a** 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. Hierdurch können die Problembewältigung sowie der Einsatz von Vorbeugungsmaßnahmen im Falle von Missbrauch oder böswilligen Absichten beschleunigt werden.
	8.1.b Überprüfen Sie auf folgende Weise, ob die Verfahren zur Benutzeridentifizierungsverwaltung implementiert wurden:	
8.1.1 Zuweisen einer eindeutigen ID für alle Benutzer, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird.	**8.1.1** Vergewissern Sie sich durch Befragung des administrativen Personals, dass allen Benutzern eine eindeutige ID für den Zugriff auf Systemkomponenten oder Karteninhaberdaten zugewiesen wird.	
8.1.2 Kontrollieren der Vorgänge zum Hinzufügen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsobjekten.	**8.1.2** 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	LEITFADEN
8.1.3 Sofortige Deaktivierung des Zugriffs ehemaliger Benutzer.	**8.1.3.a** 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. **8.1.3.b** Überprüfen Sie, ob sämtliche Methoden zur physischen Authentifizierung – Smartcards, Tokens usw. zurückgegeben bzw. deaktiviert wurden.	Wenn ein Mitarbeiter, der das Unternehmen verlassen hat, weiterhin Zugriff auf das Netzwerk über dessen Benutzerkonto besitzt, können unnötige Zugriffe oder Zugriffe in böswilliger Absicht auf Karteninhaberdaten eintreten – sowohl durch den früheren Mitarbeiter als auch durch nicht autorisierte Dritte, die das alte und/oder nicht verwendete Benutzerkonto missbrauchen. Um einen nicht autorisierten Zugriff zu vermeiden, müssen Anmeldedaten und sonstige Authentifizierungsmethoden sofort (schnellstmöglich) nach Ausscheiden des Mitarbeiters deaktiviert werden.
8.1.4 Entfernen bzw. Deaktivieren inaktiver Benutzerkonten mindestens alle 90 Tage.	**8.1.4** Überprüfen Sie, ob seit mehr als 90 Tagen inaktive Konten entfernt oder deaktiviert werden.	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.
8.1.5 Beim Management von IDs, die von Anbietern für den Zugriff, den Support oder die Wartung von Systemkomponenten per Remote-Zugriff verwendet werden, müssen folgende Aspekte berücksichtigt werden: • Sie werden nur in dem Zeitraum aktiviert, in dem sie benötigt werden, und anschließend wieder deaktiviert. • Verwendete IDs werden überwacht.	**8.1.5.a** Vergewissern Sie sich durch Gespräche mit den Mitarbeitern und die Beobachtung von Prozessen der Anbieter für den Zugriff, den Support und die Wartung von Systemkomponenten, dass für die von den Anbietern für den Remote-Zugriff verwendeten Konten Folgendes gilt: • Nicht verwendete Konten werden deaktiviert. • Vom Anbieter benötigte Konten werden nur in dem Zeitraum aktiviert, in dem sie benötigt werden, und anschließend wieder deaktiviert. **8.1.5.b** Überprüfen Sie durch Befragung der Mitarbeiter und die Beobachtung von Prozessen, ob der Remote-Zugriff auf Konten durch den Anbieter überwacht wird.	Wenn Sie Anbietern ermöglichen, an 7 Tagen in der Wochen durchgehend auf Ihr Netzwerk zuzugreifen, um bei Bedarf Arbeiten an Ihrem System vorzunehmen, erhöht sich das Risiko für unbefugte 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. Durch eine Überwachung des Anbieterzugriffs sorgen Sie dafür, dass die Anbieter nur auf notwendige Systeme und nur innerhalb der genehmigten Zeiträume zugreifen.
8.1.6 Begrenzen der wiederholten Zugriffsversuche durch Sperren der Benutzer-ID nach spätestens sechs	**8.1.6.a** Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Authentifizierungsparameter so eingestellt	Ohne implementierte Mechanismen für Kontosperrungen kann ein Angreifer fortwährend versuchen, ein Kennwort über manuelle oder

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Versuchen.	sind, dass ein Benutzerkonto nach spätestens sechs ungültigen Anmeldeversuchen gesperrt wird. **8.1.6.b *Zusätzliches Testverfahren für Dienstanbieter*:** 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.	automatisierte Tools zu erraten (z. B. Kennwort-Cracking-Tools), bis er letztendlich Erfolg hatte und sich Zugriff auf das Konto eines Benutzers verschafft hat.
8.1.7 Festlegen einer Aussperrdauer von mindestens 30 Minuten, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann.	**8.1.7** 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.	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.
8.1.8 Nach mehr als 15-minütiger Inaktivität müssen sich die Benutzer erneut authentifizieren und das Terminal oder die Sitzung reaktivieren.	**8.1.8** Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Systemkonfigurationseinstellungen daraufhin, ob die Sperre des Systems bzw. der Sitzung nach einer höchstens 15-minütigen Inaktivitätszeit eintritt.	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. Die erneute Authentifizierung kann entweder auf Systemebene (damit alle auf diesem Rechner ausgeführten Sitzungen geschützt sind) oder auf Anwendungsebene erfolgen.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
8.2 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: • Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz; • Etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard; • Etwas, das Sie sind, wie zum Beispiel biometrische Daten.	**8.2** Gehen Sie wie folgt vor, um zu überprüfen, ob sich die Benutzer mittels einer eindeutigen ID und eines zusätzlichen Authentifizierungsmerkmals (z. B. Kennwort oder -satz) für den Zugriff auf die CDE authentifiziert haben: • Untersuchen Sie Dokumente, aus denen hervorgeht, welche Authentifizierungsmethode(n) verwendet wurde(n). • Schauen Sie sich bei jeder Authentifizierungsmethode und jeder Systemkomponente eine Authentifizierung genauer daraufhin an, ob diese in Übereinstimmung mit den dokumentierten Authentifizierungsmethoden erfolgt.	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“. 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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
8.2.1 Nicht entschlüsselbare Übertragung und Speicherung von Kennwörtern und -sätzen auf sämtlichen Systemkomponenten unter Verwendung einer sicheren Verschlüsselung.	**8.2.1.a** 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.	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.
	8.2.1.b Testen Sie stichprobenartig die Kennwortdateien von Systemkomponenten auf die Verschlüsselung von Kennwörtern bei der Speicherung.	
	8.2.1.c Testen Sie stichprobenartig die Datenübertragungen bei Systemkomponenten auf die Verschlüsselung von Kennwörtern.	
	8.2.1.d ***Zusätzliches Testverfahren für Dienstanbieter*****:** Vergewissern Sie sich in den Kennwortdateien, dass die gespeicherten Kundenkennwörter nicht lesbar sind.	
	8.2.1.e ***Zusätzliches Testverfahren für Dienstanbieter:*** Vergewissern Sie sich bei Datenübertragungen, dass die Kundenkennwörter während der Übertragung nicht lesbar sind.	
8.2.2 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.	**8.2.2** 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.	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 dessen Kennwort zurücksetzen oder ändern.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
8.2.3 Kennwörter/-sätze müssen die folgenden Anforderungen erfüllen: • Die Mindestlänge beträgt sieben Zeichen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden. Alternativ müssen die Komplexität und Stärke eines Kennworts/Kennsatzes mindestens den oben angegebenen Parametern entsprechen.	**8.2.3a** Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass mindestens die folgende Kennwortstärke/-komplexität erforderlich ist: • Die Mindestlänge beträgt sieben Zeichen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden.	Starke Kennwörter/-sätze 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. Diese Anforderung legt fest, dass die Mindestlänge für Kennwörter sieben Zeichen ist, und dass sowohl Ziffern als auch Buchstaben verwendet werden sollten. Wenn diese Mindestanforderung aufgrund technischer Beschränkungen nicht erfüllt werden kann, können Einheiten zur Evaluierung der Alternative auf „gleichwertige Stärke“ setzen. In NIST SP 800-63-1 ist „Entropie“ als „ein Maß der Schwierigkeit, ein Kennwort oder einen Schlüssel zu erraten oder zu bestimmen“ definiert. Dieses Dokument und andere, in denen die „Entropie von Kennwörtern“ behandelt wird, bieten zusätzliche Informationen zum Entropiewert und zu identischer Stärke von Kennwörtern/-sätzen mit unterschiedlichen Formaten.
	8.2.3.b *Zusätzliches Testverfahren für Dienstanbieter*: Überprüfen Sie in internen Prozessen und in der Kunden-/Benutzerdokumentation, ob die folgenden Mindestanforderungen an die Stärke/Komplexität von Kennwörtern für Nichtverbraucherbenutzer gelten: • Die Mindestlänge beträgt sieben Zeichen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden.	
8.2.4 Änderung der Benutzerkennwörter/-sätze mindestens alle 90 Tage.	**8.2.4.a** Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass die Benutzer mindestens alle 90 Tage ihr Kennwort ändern müssen.	Wenn Kennwörter/Kennsätze über einen langen Zeitraum hinweg unverändert gültig sind, haben Angreifer länger Zeit, das Kennwort bzw. den Kennsatz herauszufinden.
	8.2.4.b *Zusätzliches Testverfahren für Dienstanbieter*: *Überprüfen Sie interne* Prozesse und die Kunden-/Benutzerdokumentation auf folgende Punkte: • Kennwörter von Nichtverbraucherbenutzern müssen regelmäßig geändert werden. • Nichtverbraucherbenutzer erhalten Hinweise dazu, wann und unter welchen Umständen Kennwörter geändert werden müssen.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
8.2.5 Neue Kennwörter/-sätze müssen sich von den letzten vier Kennwörtern/-sätzen unterscheiden.	**8.2.5.a** Überprüfen Sie stichprobenartig bei bestimmten Systemkomponenten die Konfigurationseinstellungen daraufhin, ob die Kennwortparameter so eingestellt sind, dass sich ein neues Kennwort von den letzten vier Kennwörtern unterscheiden muss. **8.2.5.b** ***Zusätzliches Testverfahren für Dienstanbieter:*** Vergewissern Sie sich in internen Prozessen und der Kunden-/Benutzerdokumentation, dass sich neue Kennwörter von Nichtverbraucherbenutzern von den letzten vier Kennwörtern unterscheiden müssen.	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.
8.2.6 Festlegen von Kennwörtern 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.	**8.2.6** Vergewissern Sie sich bei einer Untersuchung des Kennwortverfahrens und durch die Beobachtung des Sicherheitspersonals, dass Kennwörter neuer Benutzer für die erste Verwendung und zurückgesetzte Kennwörter für vorhandene Benutzer auf einen eindeutigen Wert gesetzt und nach der ersten Nutzung geändert werden.	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.
8.3 Authentifizierung anhand zweier Faktoren beim Remote-Zugriff auf das Netzwerk durch interne Mitarbeiter (Benutzer und Administratoren) und Dritte (einschließlich Anbieterzugriff zu Support- oder Wartungszwecken). ***Hinweis:*** *Bei der Zwei-Faktor-Authentifizierung müssen zwei der drei Authentifizierungsmethoden (siehe Anforderung 8.2 für eine Beschreibung der Authentifizierungsmethoden) bei der Authentifizierung eingesetzt werden. Wenn ein Faktor zweimalig verwendet wird (z. B. wenn zwei separate Kennwörter eingesetzt werden) handelt es sich nicht um eine Zwei-Faktor-Authentifizierung.* *Beispiele für Technologien mit zwei Faktoren sind der Remote-Authentifizierungs- und Einwähldienst (RADIUS) mit Tokens; Terminal Access*	**8.3.a** Vergewissern Sie sich bei einer Untersuchung der Konfigurationen von Servern und Systemen für den Remote-Zugriff, dass die Zwei-Faktor-Authentifizierung für folgende Fälle erforderlich ist: • Den gesamten Remote-Zugriff durch das Personal • Sämtlichen Remote-Zugriff von Dritten/Anbietern (einschließlich des Zugriffs auf Anwendungen und Systemkomponenten zu Support- und Wartungszwecken). **8.3.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.	Die Zwei-Faktor-Authentifizierung erfordert zwei Authentifizierungsarten für Zugriffe mit einem höheren Risiko, wie etwa solche, die von außerhalb des Netzwerks getätigt werden. 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 Zwei-Faktor-Authentifizierung erforderlich. Nichtsdestotrotz ist eine Zwei-Faktor-Authentifizierung für alle Remote-Zugriffe auf Netzwerke mit Zugang auf die Karteninhaberdaten-Umgebung erforderlich und empfehlenswert für alle Remote-Zugriffe auf die Netzwerke der Einheit.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Controller Access Control System (TACACS) mit Tokens und andere Technologien, die eine Zwei-Faktor-Authentifizierung ermöglichen.		
8.4 Dokumentation und Weitergabe der Authentifizierungsverfahren und -richtlinien an alle Benutzer unter Einschluss der folgenden Informationen: • Hinweise zur Auswahl starker Authentifizierungsinformationen • Hinweise zum Schutz der Authentifizierungsinformationen durch die Benutzer • Anweisungen zur Vermeidung wiederverwendeter Kennwörter • Anweisungen zur Änderung von Kennwörtern beim Verdacht einer Gefährdung	**8.4.a** Vergewissern Sie sich durch eine Überprüfung der Verfahren sowie durch eine Befragung des Personals, dass Authentifizierungsverfahren und -richtlinien an alle Benutzer verteilt werden.	Durch die Mitteilung von Kennwort-/Authentifizierungsverfahren an alle Benutzer sind diese in der Lage, die Richtlinien besser zu verstehen und sich an diese zu halten. 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 aufzuschreien 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). 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.
	8.4.b Vergewissern Sie sich, dass die an die Benutzer weitergegebenen Authentifizierungsverfahren und -richtlinien folgende Punkte enthalten: • Hinweise zur Auswahl starker Authentifizierungsinformationen • Hinweise zum Schutz der Authentifizierungsinformationen durch die Benutzer • Anweisungen zur Vermeidung wiederverwendeter Kennwörter • Anweisungen zur Änderung von Kennwörtern beim Verdacht einer Gefährdung	
	8.4.c Befragen Sie stichprobenartig einige Benutzer nach ihren Kenntnissen der Authentifizierungsverfahren und -richtlinien.	
8.5 Keine Verwendung von IDs und Kennwörtern für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder von anderen Authentifizierungsmethoden und Beachtung der folgenden Punkte: • Allgemeine Benutzer-IDs werden deaktiviert oder entfernt. • Es gibt keine gemeinsamen	**8.5.a** Vergewissern Sie sich bei einer Stichprobe von Systemkomponenten, dass für die Benutzer-ID-Listen Folgendes gilt: • Allgemeine Benutzer-IDs werden deaktiviert oder entfernt. • Es gibt keine gemeinsamen Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen. • Es werden keine gemeinsamen und allgemeinen Benutzer-IDs zur Administration von Systemkomponenten verwendet.	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

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen. • Es werden keine gemeinsamen und allgemeinen Benutzer-IDs zur Administration von Systemkomponenten verwendet.	**8.5.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. **8.5.c** Vergewissern Sie sich durch Gespräche mit Systemadministratoren, dass selbst auf Anfrage keine Gruppen- bzw. gemeinsamen Kennwörter vergeben oder andere Authentifizierungsmethoden genutzt werden.	Gruppe, der die Authentifizierungsinformationen kennt, hätte durchgeführt werden können.
8.5.1 ***Zusätzliche Anforderung für Dienstanbieter:*** 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). ***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.* ***Hinweis:*** *Die Anforderung 8.5.1 wird bis zum 30. Juni 2015 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*	**8.5.1** ***Zusätzliches Testverfahren für Dienstanbieter:*** Vergewissern Sie sich durch die Untersuchung von Authentifizierungsrichtlinien und die Befragung von Mitarbeitern, dass für jeden Kundenzugriff andere Authentifizierungsinformationen verwendet werden.	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. 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 Zwei-Faktor-Authentifizierung.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
8.6 Bei Verwendung anderer Authentifizierungsmethoden (z. B. Tokens für die physische/logische Sicherheit, Smartcards, Zertifikate usw.) muss die folgende Zuweisung beachtet werden: • Authentifizierungsinformationen müssen einem einzelnen Konto zugewiesen sein und dürfen nicht von mehreren Konten gemeinsam genutzt werden. • Mit physischen und/oder logischen Kontrollen muss gewährleistet werden, dass der Zugriff nur über das Konto erfolgen kann, für das die Authentifizierungsinformationen gedacht sind.	**8.6.a** 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: • Authentifizierungsinformationen sind einem einzelnen Konto zugewiesen und werden nicht von mehreren Konten gemeinsam genutzt. • Mit physischen und/oder logischen Kontrollen muss gewährleistet werden, dass der Zugriff nur über das Konto erfolgen kann, für das die Authentifizierungsinformationen gedacht sind.	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.
	8.6.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.	
	8.6.c 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.	
8.7 Der gesamte Zugriff auf die Datenbank mit den Karteninhaberdaten (einschließlich des Zugriffs durch Anwendungen, Administratoren und alle anderen Benutzer) wird wie folgt beschränkt: • Sämtliche Zugriffe, Anfragen und Aktionen der Benutzer im Bezug auf die Datenbank erfolgen mittels	**8.7.a** Überprüfen Sie in den Konfigurationseinstellungen für Datenbank und Anwendungen, ob alle Benutzer vor dem Zugriff authentifiziert werden.	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
	8.7.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.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
programmierter Verfahren. • Nur Datenbankadministratoren können direkt auf die Datenbanken zugreifen und Abfragen durchführen. • Die Anwendungs-IDs für Datenbankanwendungen können nur von den Anwendungen (und nicht von Einzelbenutzern oder nicht zu den Anwendungen gehörenden Prozessen) verwendet werden.	**8.7.c** 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.	die Datenbank durch Endbenutzer (mit Ausnahme von DBAs, die direkten Zugriff auf die Datenbank zur Erfüllung ihrer administrativen Aufgaben benötigen).
	8.7.d 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.	
8.8 Sicherheitsrichtlinien und betriebliche Verfahren zur Identifizierung und Authentifizierung müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**8.8** 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: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren für ein dauerhaftes Management von Identifizierung und Authentifizierung kennen und befolgen.

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 Ausdrucke 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	LEITFADEN
9.1 Verwenden angemessener Zugangskontrollen, um den physischen Zugriff auf Systeme in der CDE zu überwachen und zu beschränken.	**9.1** Überprüfen Sie, ob für die einzelnen Computerräume, Rechenzentren und sonstigen Bereiche mit Systemen in der CDE physische Sicherheitskontrollen existieren. • Überprüfen Sie, ob der Zugang über eine elektronische Ausweiskontrolle oder per Schlüssel erfolgt. • Schauen Sie sich an, wie der Anmeldeversuch eines Systemadministrators an den Konsolen willkürlich ausgewählter Systeme mit Karteninhaberdaten abläuft, und überprüfen Sie, ob die Sperre zur Verhinderung der unbefugten Nutzung funktioniert.	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. 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.
9.1.1 Überwachen des Zugangs zu zugangsbeschränkten Bereichen mithilfe von Videokameras und/oder	**9.1.1.a** Überprüfen Sie, ob der Zugang zu zugangsbeschränkten Bereichen mithilfe von Videokameras und/oder Kontrollsystemen überwacht wird.	Wenn Verletzungen der physischen Integrität untersucht werden, können diese Kontrollen dabei helfen, jene Personen ausfindig zu machen, die

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Kontrollsystemen. Überprüfen der gesammelten Daten und Korrelation mit anderen Daten. Speichern der Daten mindestens drei Monate lang, wenn dies gesetzlich zulässig ist. ***Hinweis:*** *„Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Nicht hierzu zählen die öffentlichen Bereiche, in denen lediglich POS-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).*	**9.1.1.b** Überprüfen Sie, ob Videokameras und/oder Kontrollsysteme vor Manipulation oder Deaktivierung geschützt sind.	direkt auf diese zugangsbeschränkten Bereiche zugreifen, und festzustellen, wann sie auf die Bereiche zugegriffen und sie wieder verlassen haben. 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. *(Fortsetzung auf der nächsten Seite)*
	9.1.1.c Überprüfen Sie, ob Videokameras und/oder Kontrollsysteme überwacht werden und ob die von diesen Kameras oder anderen Systemen aufgezeichneten Daten mindestens drei Monate lang gespeichert werden.	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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
9.1.2 Implementierung physischer und/oder logischer Kontrollen zur Beschränkung des Zugriffs auf öffentlich zugängliche Netzwerkbuchsen. *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.*	**9.1.2** 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.	Durch Einschränkung des Zugriffs auf Netzwerkbuchsen wird verhindert, dass Angreifer über leicht zugängliche Netzwerkbuchsen auf interne Netzwerkressourcen zugreifen. Logische und/oder physische Kontrollen müssen so ausgelegt sein, dass Personen oder Geräte ohne ausdrückliche Autorisierung keine Verbindung zum Netzwerk herstellen können.
9.1.3 Beschränkung des physischen Zugriffs auf WLAN-Zugriffspunkte, Gateways, Handgeräte, Netzwerk- und Kommunikations-hardware und Telekommunikationsleitungen.	**9.1.3** Überprüfen Sie, ob der physische Zugriff auf WLAN-Zugriffspunkte, Gateways, Handgeräte, Netzwerk- und Kommunikations-hardware und Telekommunikationsleitungen entsprechend eingeschränkt ist.	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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
9.2 Entwicklung von Verfahren mit den folgenden Elementen zur leichteren Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern: • Identifizierung von Besuchern und neuen Mitarbeitern vor Ort (z. B. durch Vergabe von Ausweisen) • Änderungen bei den Zugangs- bzw. Zugriffsanforderungen • Rücknahme bzw. Beendigung der Identifizierung von Vor-Ort-Mitarbeitern und Besuchern (z. B. mittels Ausweis) bei Ablauf des Status	**9.2.a** Prüfen Sie in den dokumentierten Prozessen, ob Verfahren zur Identifizierung und zur Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern definiert sind. Die Verfahren müssen folgende Anforderungen erfüllen: • Identifizierung von Besuchern und neuen Mitarbeitern vor Ort (z. B. durch Vergabe von Ausweisen) • Zugangs- bzw. Zugriffsanforderungen und • Rücknahme der Identifizierung (z. B. mittels Ausweis) von ehemaligen Vor-Ort-Mitarbeitern und Besuchern, deren Besuchsstatus abgelaufen ist	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.
	9.2.b Prüfen Sie in den Verfahren zur Identifizierung und zur Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern, ob folgende Punkte erfüllt sind: • Die Besucher werden eindeutig identifiziert. • Die Besucher lassen sich leicht von den Mitarbeitern vor Ort unterscheiden.	
	9.2.c Überprüfen Sie, ob der Zugriff auf den Identifizierungsprozess (z. B. ein Ausweissystem) befugtem Personal vorbehalten ist.	
	9.2.d Überprüfen Sie, ob sich die Besucher mit den derzeit verwendeten Identifizierungsmethoden (z. B. Ausweise)klar identifizieren lassen und ob leicht zwischen Mitarbeitern vor Ort und Besuchern unterschieden werden kann.	
9.3 Kontrolle des Zugangs von Vor-Ort-Personal zu den zugangsbeschränkten Bereichen gemäß den folgenden Anforderungen: • Der Zugang muss autorisiert sein und auf der jeweiligen tätigkeitsbezogenen Aufgabe basieren. • Die Zugangsberechtigung wird sofort nach dem Ende der Beschäftigung	**9.3.a** Vergewissern Sie sich für eine Stichprobe der Vor-Ort-Mitarbeiter mit Zugriff auf die CDE durch die Befragung des zuständigen Personals und die Prüfung von Zugriffskontrolllisten, dass Folgendes gilt: • Der Zugriff auf die CDE ist autorisiert. • Der Zugriff ist für die jeweiligen tätigkeitsbezogenen Aufgaben erforderlich.	Eine Kontrolle des physischen Zugriffs auf die CDE sorgt dafür, dass nur autorisiertem Personal mit legitimen geschäftlichen Anforderungen Zugriff gewährt wird. 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 CDE zugreifen können.
	9.3.b Überprüfen Sie beim Zugriff des Personals auf die CDE, ob alle Mitarbeiter autorisiert werden, bevor ihnen der Zugriff gewährt wird.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
zurückgenommen, und sämtliche physischen Zugangssysteme wie Schlüssel, Karten usw. werden zurückgegeben oder deaktiviert.	**9.3.c** Vergewissern Sie sich stichprobenartig in den Zugriffskontrolllisten bei Mitarbeitern, deren Beschäftigung kürzlich endete, dass die Mitarbeiter nicht mehr physisch auf die CDE zugreifen können.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
9.4 Implementierung von Verfahren zur Identifizierung und Autorisierung von Besuchern. Die Verfahren müssen Folgendes umfassen:	**9.4** Überprüfen Sie, ob die Autorisierungs- und Zugriffskontrollen für Benutzer wie folgt umgesetzt werden:	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. 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. 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. 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.
9.4.1 Besucher müssen vor dem Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder gepflegt werden, autorisiert und innerhalb dieser Bereiche jederzeit begleitet werden.	**9.4.1.a** 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.	
	9.4.1.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.	
9.4.2 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.	**9.4.2.a** Überprüfen Sie, ob Personen innerhalb der Einrichtung, Besucherausweise oder andere Identifizierungsmöglichkeiten nutzen und sich leicht vom Personal vor Ort unterscheiden lassen.	
	9.4.2.b Überprüfen Sie, ob die Besucherausweise eine begrenzte Gültigkeit haben.	
9.4.3 Die Besucher werden um Rückgabe des Ausweises bzw. der Identifizierung gebeten, wenn die Besucher die Einrichtung verlassen oder die Erlaubnis ausläuft.	**9.4.3** Beobachten Sie, ob Besucher den Ausweis bzw. die sonstige Identifizierung beim Verlassen der Einrichtung bzw. beim Auslaufen der Erlaubnis zurückgeben müssen.	
9.4.4 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. Dokumentieren Sie den Namen des Besuchers, den Firmennamen und den Namen des Mitarbeiters vor Ort, der	**9.4.4.a** Überprüfen Sie, ob es ein Besucherprotokoll gibt, in dem der Zugang zur Einrichtung sowie zu den Computerräumen und Rechenzentren, in denen Karteninhaberdaten gespeichert oder übertragen werden, protokolliert wird.	
	9.4.4.b Vergewissern Sie sich, dass das Protokoll folgende Informationen enthält: • Name des Besuchers • Unternehmen, das der Besucher vertritt • Mitarbeiter vor Ort, der dem Besucher Zugang gewährt hat	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
dem Besucher Zugang gewährt. Aufbewahren des Besucherprotokolls für die Dauer von mindestens drei Monaten, wenn dies gesetzlich zulässig ist.	**9.4.4.c** Überprüfen Sie, ob das Protokoll mindestens drei Monate lang aufbewahrt wird.	
9.5 Stellen Sie die physische Sicherheit aller Medien sicher.	**9.5** 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.	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.
9.5.1 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.	**9.5.1.a** Vergewissern Sie sich durch Überprüfung der physischen Sicherheit am Speicherstandort, dass der Backup-Speicher sicher ist.	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.
	9.5.1.b Kontrollieren Sie, ob die Sicherheit am Speicherort mindestens einmal jährlich überprüft wird.	Durch eine regelmäßige Prüfung des Speicherorts können ermittelte Sicherheitsrisiken frühzeitig angegangen und die potenziellen Risiken so gering wie möglich gehalten werden.
9.6 Durchführung strikter Kontrollen der internen bzw. externen Verteilung jeglicher Art von Medien, einschließlich der folgenden:	**9.6** 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).	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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
9.6.1 Klassifizieren Sie die Medien, sodass das Gefährdungspotenzial der Daten bestimmt werden kann.	**9.6.1** Überprüfen Sie, ob alle Medien klassifiziert sind, sodass das Gefährdungspotenzial der Daten bestimmt werden kann.	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. ***Hinweis:*** *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.*
9.6.2 Versenden Sie die Medien über einen sicheren Kurier oder eine andere Liefermethode, die präzise nachverfolgt werden kann.	**9.6.2.a** 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.	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.
	9.6.2.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.	
9.6.3 Das Management muss den Transfer sämtlicher Medien aus einem geschützten Bereich genehmigen (insbesondere, wenn die Medien an einzelne Personen weitergegeben werden).	**9.6.3** 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).	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.
9.7 Strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien.	**9.7** 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.	Ohne sorgfältige Inventurmethoden und Speicherkontrollen können entwendete oder abhanden gekommene Daten auf unbestimmte Zeit unbemerkt bleiben.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
9.7.1 Ordnungsgemäße Verwaltung von Medieninventurlisten und Durchführung von mindestens einer Medieninventur im Jahr.	**9.7.1** Überprüfen Sie im Medien-Inventurprotokoll, ob mindestens einmal pro Jahr eine Inventur der vorhandenen Medien stattfindet.	Wenn keine Bestandsaufnahme der Datenträger durchgeführt wird, können entwendete oder abhanden gekommene Daten auf unbestimmte Zeit oder womöglich für immer unentdeckt bleiben.
9.8 Vernichtung von Medien, die nicht mehr zu geschäftlichen oder juristischen Zwecken benötigt werden, nach folgenden Maßgaben:	**9.8** 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: • Ausdrucke müssen der Aktenvernichtung zugeführt werden, damit nach allgemeinem Ermessen ausgeschlossen werden kann, dass die Einzelteile wieder zusammengefügt werden. • Container zur Aufbewahrung von zu vernichtendem Material müssen geschützt werden. • Karteninhaberdaten auf elektronischen Medien müssen nach Branchenstandards für Secure Wipes (sichere Löschverfahren) in einen Zustand versetzt werden, in dem sie nicht wiederherstellbar sind. Ansonsten können auch die Medien physisch unbrauchbar gemacht werden.	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. 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. 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).
9.8.1 Papierausdrucke müssen in einer Form vernichtet werden, dass keine Karteninhaberdaten wiederhergestellt werden können. Container zur Aufbewahrung von zu vernichtendem Material müssen geschützt werden.	**9.8.1.a** Überprüfen Sie durch die Befragung der Mitarbeiter oder die Untersuchung von Verfahrensweisen, ob Papierausdrucke vernichtet werden und nach allgemeinem Ermessen ausgeschlossen werden kann, dass diese Dokumente wiederhergestellt werden können.	
	9.8.1.b Überprüfen Sie, ob Container zur Aufbewahrung von Informationen, die vernichtet werden sollen, geschützt sind.	
9.8.2 Löschen von Karteninhaberdaten auf elektronischen Medien in einer Art und Weise, die eine Wiederherstellung der Daten unmöglich macht.	**9.8.2** Überprüfen Sie, ob die Karteninhaberdaten auf elektronischen Medien nach Branchenstandards für Secure Wipes (sichere Löschverfahren) unbrauchbar und nicht wiederherstellbar gemacht werden bzw. dass die Medien ansonsten physisch unbrauchbar gemacht werden.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
9.9 Manipulations- und Austauschschutz von Geräten zur Erfassung von Zahlungskartendaten über eine direkte physische Interaktion mit der Karte. ***Hinweis:*** *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.* ***Hinweis:*** *Die Anforderung 9.9 wird bis zum 30. Juni 2015 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*	**9.9** Überprüfen Sie, ob in den dokumentierten Richtlinien und Verfahren folgende Punkte enthalten sind: • Führen einer Geräteliste • Regelmäßige Prüfung der Geräte auf Manipulations- oder Austauschversuche • Förderung des Bewusstseins der Mitarbeiter für verdächtiges Verhalten und Melden der Manipulation bzw. des Austauschs von Geräten	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. Diese Anforderung wird für Komponenten zur manuellen Eingabe wie Computertastaturen und POS-Ziffernblöcke empfohlen, ist jedoch nicht zwingend vorgeschrieben. Zusätzliche bewährte Verfahren zur Vermeidung von Skimming-Angriffen finden Sie auf der PCI-SSC-Website.
9.9.1 Führen einer aktuellen Geräteliste. Die Liste muss folgende Punkte enthalten: • Fabrikat und Modell des Geräts • Standort des Geräts (zum Beispiel die Adresse des Standorts oder der Einrichtung, an der sich das Gerät befindet)	**9.9.1.a** Prüfen Sie, ob die Liste der Geräte folgende Informationen enthält: • Fabrikat und Modell des Geräts • Standort des Geräts (zum Beispiel die Adresse des Standorts oder der Einrichtung, an der sich das Gerät befindet) • Seriennummer des Geräts oder andere Informationen zur eindeutigen Identifizierung.	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. Die Methode zum Führen einer Geräteliste kann automatisiert werden (z. B. in einem Gerätemanagementsystem) oder manuell

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
• Seriennummer des Geräts oder andere Informationen zur eindeutigen Identifizierung.	**9.9.1.b** Wählen Sie stichprobenartig einige Geräte aus der Liste aus, und überprüfen Sie, ob die Standortangaben in der Liste korrekt und aktuell sind.	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.
	9.9.1.c Fragen Sie die Mitarbeiter, ob die Geräteliste aktualisiert wird, sobald Geräte hinzugefügt, an einen anderen Standort gebracht oder außer Betrieb genommen werden usw.	
9.9.2 Regelmäßige Untersuchung der Geräte auf Spuren von Manipulation (z. B. Anbringen von Skimming-Technik) oder Austausch (stimmen	**9.9.2.a** Prüfen Sie in den dokumentierten Verfahren, ob Prozesse für folgende Punkte festgelegt wurden: • Verfahren zur Untersuchung von Geräten • Häufigkeit der Untersuchungen	Regelmäßige Untersuchungen von Geräten helfen Unternehmen dabei, schneller Manipulationen oder den Austausch eines Geräts zu erkennen und damit die potenziellen Auswirkungen des Einsatzes

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
beispielsweise die Seriennummer oder andere Gerätemerkmale, oder wurde das Gerät durch ein anderes ausgetauscht?). ***Hinweis:*** *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.*	**9.9.2.b** Klären Sie durch eine Befragung des zuständigen Personals und die Beobachtung der Untersuchungsprozesse Folgendes ab: • Kennen die Mitarbeiter die Verfahren zur Untersuchung von Geräten? • Werden sämtliche Geräte regelmäßig auf Manipulations- oder Austauschversuche geprüft?	falscher Geräte so gering wie möglich zu halten. 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. Geräteanbieter verfügen unter Umständen über eigene Sicherheitshinweise und Leitlinien zur Frage, wie sich Manipulationen am Gerät erkennen lassen. 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.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
9.9.3 Personalschulungen zur Förderung des Bewusstseins im Hinblick auf Manipulations- oder Austauschversuche. Die Schulungen sollten Folgendes umfassen: • 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). • Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe. • Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen). • Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter).	**9.9.3.a** Überprüfen Sie, ob das Schulungsmaterial für die Mitarbeiter an POS-Standorten die folgenden Punkte umfasst: • 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) • Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe • Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen) • Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter) **9.9.3.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: • 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) • Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe • Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen) • Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter)	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. 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 Schreiben 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.
9.10 Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des physischen Zugangs zu Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**9.10** 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: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren zur Beschränkung des physischen Zugangs zu Karteninhaberdaten und CDE-Systemen kennen und dauerhaft befolgen.

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	LEITFADEN
10.1 Implementierung von Audit-Trails zur Verknüpfung des gesamten Zugriffs auf Systemkomponenten mit den einzelnen Benutzern.	**10.1** Prüfen Sie durch Beobachtungen und durch Befragung des Systemadministrators folgende Punkte: • Sind Audit-Trails für die Systemkomponenten vorhanden und aktiv? • Ist der Zugriff auf Systemkomponenten mit den einzelnen Benutzern verknüpft?	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.
10.2 Implementierung automatisierter Audit-Trails für alle Systemkomponenten zur Rekonstruktion der folgenden Ereignisse:	**10.2** Führen Sie durch Gespräche, die Untersuchung von Audit-Protokollen und die Prüfung der 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.
10.2.1 Alle individuellen Zugriffe auf Karteninhaberdaten	**10.2.1** 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	LEITFADEN
10.2.2 Alle von einer Einzelperson mit Root- oder Administratorrechten vorgenommene Aktionen	**10.2.2** Prüfen Sie, ob alle von einer Einzelperson mit Root- oder Administratorrechten vorgenommenen Aktionen protokolliert werden.	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.
10.2.3 Zugriff auf alle Audit-Trails	**10.2.3** Prüfen Sie, ob der Zugriff auf alle Audit-Trails protokolliert wird.	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.
10.2.4 Ungültige logische Zugriffsversuche	**10.2.4** Prüfen Sie, ob ungültige logische Zugriffsversuche protokolliert werden.	Angreifer 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.
10.2.5 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	**10.2.5** Prüfen Sie, ob die Verwendung von Identifizierungs- und Authentifizierungssystemen protokolliert wird.	Wenn nicht bekannt ist, wer zu dem Zeitpunkt eines Vorfalls 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.
	10.2.5.b Überprüfen Sie, ob sämtliche Heraufstufungen von Rechten protokolliert werden.	
	10.2.5.c Prüfen Sie, ob alle Änderungen, Ergänzungen oder Löschungen an einem Konto mit Root- oder Administratorrechten protokolliert werden.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
10.2.6 Initialisieren, Beenden oder Anhalten der Prüfprotokolle	**10.2.6** Überprüfen Sie, ob Folgendes protokolliert wird: • Initialisierung der Prüfprotokolle • Beenden bzw. Anhalten der Prüfprotokolle	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.
10.2.7 Erstellen und Löschen von Objekten auf Systemebene	**10.2.7** Prüfen Sie, ob das Erstellen und Löschen von Objekten auf Systemebene protokolliert wird.	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.
10.3 Aufzeichnung von mindestens den folgenden Audit-Trail-Einträgen für alle Systemkomponenten zu jedem Ereignis:	**10.3** 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.
10.3.1 Benutzeridentifizierung	**10.3.1** Prüfen Sie, ob die Benutzer-ID in den Protokolleinträgen enthalten ist.	
10.3.2 Ereignistyp	**10.3.2** Prüfen Sie, ob die Art des Ereignisses in den Protokolleinträgen enthalten ist.	
10.3.3 Datum und Uhrzeit	**10.3.3** Prüfen Sie, ob die Datums- und Zeitangabe in den Protokolleinträgen enthalten ist.	
10.3.4 Angabe von Erfolgen oder Fehlschlägen	**10.3.4** Prüfen Sie, ob der Hinweis auf die erfolgreiche oder fehlgeschlagene Ausführung in den Protokolleinträgen enthalten ist.	
10.3.5 Ereignisursprung	**10.3.5** Prüfen Sie, ob der Ursprung des Ereignisses in den Protokolleinträgen enthalten ist.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
10.3.6 Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen.	**10.3.6** Überprüfen Sie, ob die Identität oder der Name der betroffenen Daten, Systemkomponenten oder Ressourcen in den Protokolleinträgen enthalten ist.	
10.4 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: ***Hinweis:*** *Eine Zeitsynchronisierungstechnologie ist beispielsweise das Network Time Protocol (NTP).*	**10.4** 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.	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.
10.4.1 Auf wichtigen Systeme ist die Uhrzeit korrekt und einheitlich.	**10.4.1.a** Untersuchen Sie den Prozess zur Erfassung, Verteilung und Speicherung der richtigen Uhrzeit im Unternehmen, und überprüfen Sie dabei folgende Punkte: • Ausschließlich die festgelegten zentralen Zeitserver empfangen Zeitsignale von externen Quellen, und diese Zeitsignale basieren auf der Internationalen Atomzeit bzw. der Koordinierten Weltzeit (UTC). • Wenn es mehrere festgelegte Zeitserver gibt, bestimmen diese Server untereinander die richtige Uhrzeit. • Die Zeitinformationen auf den Systemen stammen ausschließlich von den festgelegten zentralen Zeitservern.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
	10.4.1.b Untersuchen Sie für eine Stichprobe der Systemkomponenten die zeitbezogenen Systemparametereinstellungen, und überprüfen Sie Folgendes: • Ausschließlich die festgelegten zentralen Zeitserver empfangen Zeitsignale von externen Quellen, und diese Zeitsignale basieren auf der Internationalen Atomzeit bzw. der Koordinierten Weltzeit (UTC). • Wenn es mehrere festgelegte Zeitserver gibt, bestimmen die festgelegten zentralen Zeitserver untereinander die richtige Uhrzeit. • Die Zeitinformationen auf den Systemen stammen ausschließlich von den festgelegten zentralen Zeitservern.	
10.4.2 Zeitinformationen sind geschützt.	**10.4.2.a** 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.	
	10.4.2.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.	
10.4.3 Zeiteinstellungen werden von branchenüblichen Zeitquellen empfangen.	**10.4.3** 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.)	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
10.5 Schutz der Audit-Trails vor Veränderungen.	**10.5** 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:	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.
10.5.1 Beschränkung der Anzeige der Audit-Trails auf Personen, die aus geschäftlichen Gründen darauf zugreifen müssen.	**10.5.1** Auf Audit-Trail-Dateien haben nur einzelne Personen Zugriff, die aus geschäftlichen Gründen darauf zugreifen müssen.	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). 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.
10.5.2 Schutz von Audit-Trail-Dateien vor nicht autorisierten Änderungen.	**10.5.2** Die Dateien des aktuellen Audit-Trails werden mit Zugriffskontrollsystemen, räumlicher Trennung und/oder Netzwerktrennung vor unbefugten Änderungen geschützt.	
10.5.3 Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.	**10.5.3** Die Dateien des aktuellen Audit-Trails werden sofort auf einem zentralen Protokollserver oder auf Medien gesichert, die sich nur schwer ändern lassen.	
10.5.4 Erstellung von Protokollen für nach außen gerichtete Technologien auf sicheren zentralen und internen Protokollservern oder Medien.	**10.5.4** Protokolle für nach außen gerichtete Technologien (z. B. Wireless-Systeme, Firewalls, DNS, E-Mail) werden auf sicheren, zentralen und internen Protokollservern oder Medien abgelegt.	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. Protokolle können direkt in den sicheren internen Systemen bzw. Medien geschrieben oder von externen Systemen dorthin verschoben bzw. kopiert werden.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
10.5.5 Mithilfe von Software zur Dateiintegritätsüberwachung und zur Erfassung von Änderungen in Protokollen muss dafür gesorgt werden, dass bei der Änderung von bestehenden Protokolldaten ein Alarm ausgelöst wird (nicht jedoch bei der Eingabe neuer Daten).	**10.5.5** 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.	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.
10.6 Überprüfung von Protokollen und Systemereignissen für alle Systemkomponenten auf Unregelmäßigkeiten oder verdächtige Aktivitäten. ***Hinweis:*** *Zur Einhaltung dieser Anforderung können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.*	**10.6** Führen Sie Folgendes durch:	Viele Verstöße erstrecken sich über Tage oder Monate, bevor sie entdeckt werden. Durch das tägliche Kontrollieren der Protokolle können die Gefährdung und der Zeitraum, über den möglicherweise eine Sicherheitsverletzung stattfindet, reduziert werden. Regelmäßige Protokollprüfungen durch Mitarbeiter oder automatisierte Systeme ermöglichen die Ermittlung und frühzeitige Bekämpfung von nicht autorisiertem Zugriff auf die CDE. Der Protokollüberprüfungsprozess muss nicht manuell durchgeführt werden. Der Einsatz von Protokoll-Harvesting-, -Analyse- und Alarmtools kann die Ermittlung von genauer zu prüfenden Protokollereignissen erleichtern.

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
10.6.1 Prüfen Sie mindestens einmal täglich die folgenden Punkte: • Sämtliche Sicherheitsereignisse • Die Protokolle aller Systemkomponenten, auf denen CHD und/oder SAD gespeichert, verarbeitet oder übertragen werden oder die Auswirkungen auf die Sicherheit von CHD und/oder SAD haben könnten • Die Protokolle aller wichtigen Systemkomponenten • 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.)	**10.6.1.a** Prüfen Sie in den Sicherheitsrichtlinien und Verfahren, ob Verfahren für eine mindestens tägliche Prüfung der folgenden Elemente (manuell oder mittels Protokolltools) festgelegt sind: • Sämtliche Sicherheitsereignisse • Die Protokolle aller Systemkomponenten, auf denen CHD und/oder SAD gespeichert, verarbeitet oder übertragen werden oder die Auswirkungen auf die Sicherheit von CHD und/oder SAD haben könnten • Die Protokolle aller wichtigen Systemkomponenten • 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.)	Viele Verstöße erstrecken sich über Tage oder Monate, bevor sie entdeckt werden. Durch das tägliche Kontrollieren der Protokolle können die Gefährdung und der Zeitraum, über den möglicherweise eine Sicherheitsverletzung stattfindet, reduziert werden. 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 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.
	10.6.1.b Vergewissern Sie sich durch die Beobachtung von Prozessen und die Befragung von Mitarbeitern, dass folgende Elemente mindestens einmal täglich geprüft werden: • Sämtliche Sicherheitsereignisse • Die Protokolle aller Systemkomponenten, auf denen CHD und/oder SAD gespeichert, verarbeitet oder übertragen werden oder die Auswirkungen auf die Sicherheit von CHD und/oder SAD haben könnten • Die Protokolle aller wichtigen Systemkomponenten • 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.)	
10.6.2 Regelmäßige Prüfung der Protokolle aller anderen Systemkomponenten auf der Grundlage der Richtlinien und der Risikomanagementstrategie des	**10.6.2.a** 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:	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

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Unternehmens und gemäß der jährlichen Risikobewertung des Unternehmens.	**10.6.2.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.	gesicherte Systeme gibt. Wie häufig diese Prüfungen durchgeführt werden sollen, wird in der jährlichen Risikobewertung der Einheit festgelegt.
10.6.3 Nachverfolgung von bei der Prüfung ermittelten Ausnahmen und Unregelmäßigkeiten.	**10.6.3.a** Prüfen Sie in den Sicherheitsrichtlinien und Verfahren, ob Prozesse für eine Nachverfolgung von bei der Prüfung ermittelten Ausnahmen und Unregelmäßigkeiten festgelegt wurden:	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.
	10.6.3.b Klären Sie durch eine Befragung des Personals und die Beobachtung von Prozessen ab, ob bei Ausnahmen und Unregelmäßigkeiten eine Nachverfolgung stattfindet.	
10.7 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).	**10.7.a** Prüfen Sie, ob in den Sicherheitsrichtlinien und Verfahren Prozesse für Folgendes festgelegt wurden: • Richtlinien zur Aufbewahrung von Prüfprotokollen • Verfahren zur Aufbewahrung von Prüfprotokollen für die Dauer von mindestens einem Jahr, wobei mindestens drei Monate online verfügbar sind.	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.
	10.7.b Vergewissern Sie sich durch die Befragung von Mitarbeitern und die Untersuchung von Prüfprotokollen, dass die Prüfprotokolle mindestens ein Jahr lang zur Verfügung stehen.	
	10.7.c Vergewissern Sie sich durch die Befragung von Mitarbeitern und die Beobachtung von Prozessen, dass zumindest die Protokolle aus den letzten drei Monaten zu Analysezwecken sofort wiederhergestellt werden können.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
10.8 Sicherheitsrichtlinien und betriebliche Verfahren zur Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**10.8** 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: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren zur Überwachung des Zugriffs auf alle Netzwerkressourcen und Karteninhaberdaten kennen und dauerhaft befolgen.

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	LEITFADEN
11.1 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. ***Hinweis:*** *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.* *Sie können sich für eine beliebige Methode entscheiden, solange damit autorisierte und nicht autorisierte Geräte erkannt und identifiziert werden können.*	**11.1a** 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. **11.1.b** Überprüfen Sie, ob mit der angewandten Methodik nicht autorisierte WLAN-Zugriffspunkte erkannt und identifiziert werden können. Dazu zählen mindestens die folgenden Elemente: • In Systemkomponenten eingefügte WLAN-Karten • An Systemkomponenten angeschlossene tragbare Geräte (z. B. durch USB), mit denen ein WLAN-Zugriffspunkt eingerichtet wird • An einen Netzwerkport oder ein Netzwerkgerät angeschlossene Drahtlosgeräte **11.1.c** Prüfen Sie, ob für die zuletzt durchgeführten Scan-Vorgänge für die Suche nach Drahtlossystemen Folgendes gilt: • Es werden autorisierte und nicht autorisierte WLAN-Zugriffspunkte gefunden. • Der Scan findet mindestens einmal vierteljährlich auf allen Systemkomponenten und in allen Einrichtungen statt. **11.1.d** Überprüfen Sie bei automatischer Überwachung (z. B. Wireless IDS/IPS-System oder NAC), ob in der Konfiguration Alarmmeldungen für das Personal vorgesehen sind.	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. 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. 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. Die Größe und Komplexität einer bestimmten Umgebung geben Hinweise auf die erforderlichen

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
		Tools und Prozesse, die eingesetzt werden müssen, um ausreichend Sicherheit dahingehend zu bieten, dass in der Umgebung kein unbefugter drahtloser Zugriffspunkt installiert wurde. *(Fortsetzung auf der nächsten Seite)*
11.1.1 Inventarisierung von autorisierten WLAN-Zugriffspunkten mit dokumentierter geschäftlicher Begründung.	**11.1.1** Überprüfen Sie durch eine Untersuchung der Dokumentation, ob die autorisierten WLAN-Zugriffspunkten inventarisiert werden und ob zu jedem Zugriffspunkt eine geschäftliche Begründung dokumentiert ist.	***Beispiel:*** *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.*
11.1.2 Implementierung von Vorfallreaktionsverfahren für den Fall, dass nicht autorisierte WLAN-Zugriffspunkte entdeckt werden.	**11.1.2.a** Überprüfen Sie, ob im Vorfallreaktionsplan (Anforderung 12.10) eine Reaktion für den Fall definiert ist, dass ein nicht autorisierter WLAN-Zugriffspunkt entdeckt wird.	
	11.1.2.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.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
11.2 Ausführen interner und externer Netzwerkanfälligkeits-Scans mindestens einmal pro Quartal und nach jeder wesentlichen Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Änderung der Firewall-Regeln, Produkt-Upgrades). ***Hinweis:*** *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.* *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.*	**11.2** Überprüfen Sie in den Scan-Berichten und der zugehörigen Dokumentation, ob die internen und externen Scans auf Sicherheitsrisiken wie folgt durchgeführt werden:	Ein Scan auf Sicherheitsrisiken ist ein automatisiertes Tool, das auf externen und internen Netzwerkgeräten und -servern ausgeführt wird und dazu dient, potentielle Sicherheitsrisiken in Netzwerken aufzudecken, die von böswilligen Personen erkannt und ausgenutzt werden könnten. Für den PCI-DSS sind drei Arten von Scans auf Sicherheitsrisiken erforderlich: • 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) • Externe vierteljährliche Scans, die von einem ASV durchgeführt werden müssen • Bedarfsweise nach wesentlichen Änderungen vorgenommene interne und externe Scans Sobald diese Sicherheitsrisiken erkannt wurden, werden von der Einheit Korrekturmaßnahmen ergriffen. Anschließend wird bei einem erneuten Scan geprüft, ob die Sicherheitsrisiken tatsächlich behoben wurden. Die rechtzeitige Erkennung und Korrektur von Schwachstellen reduziert die Wahrscheinlichkeit, dass eine solche Sicherheitslücke ausgenutzt wird und eine Systemkomponente oder Karteninhaberdaten gefährdet werden.
11.2.1 Durchführung von internen vierteljährlichen Scans auf Sicherheitsrisiken und bei Bedarf von	**11.2.1.a** Vergewissern Sie sich durch die Überprüfung der Scan-Berichte, dass in den letzten zwölf Monaten vier vierteljährliche interne Scans stattgefunden haben.	Ein etablierter Prozess zur Erkennung von Sicherheitsrisiken in internen Systemen setzt voraus, dass vierteljährliche Scans durchgeführt

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
weiteren Scans, bis alle hohen Sicherheitsrisiken (gemäß Anforderung 6.1) behoben sind. Scans müssen von qualifizierten Mitarbeitern durchgeführt werden.	**11.2.1.b** Vergewissern Sie sich durch die Prüfung der Scan-Berichte, dass der Prozess erneute Scans vorsieht, bis alle „hohen“ Sicherheitsrisiken gemäß PCI-DSS-Anforderung 6.1 beseitigt wurden.	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. 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, dass auf Sicherheitsrisiko-Scans spezialisiert ist, durchführen zu lassen.
	11.2.1.c 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).	
11.2.2 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. ***Hinweis:*** *Vierteljährliche externe Schwachstellenprüfungen müssen von einem Scanninganbieter (ASV) durchgeführt werden, der vom Payment Card Industry Security Standards Council (PCI-SSC) zugelassen wurde.* *Informationen zu den Scan-Kunden-Zuständigkeiten, der Scan-Vorbereitung usw. finden Sie im ASV-Programmführer auf der PCI-SSC-Website.*	**11.2.2.a** 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.	Da externe Netzwerke eher durch Angriffe gefährdet sind, muss vierteljährlich ein externer Anfälligkeits-Scan von einem vom PCI-SSC zugelassenen Scanninganbieter (ASV) durchgeführt werden.
	11.2.2.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).	
	11.2.2.c Überprüfen Sie in den Scan-Berichten, ob die Tests von einem vom PCI SSC zugelassenen ASV durchgeführt wurden.	
11.2.3 Führen Sie nach jeder wesentlichen Änderung interne und externe Scans und nach Bedarf erneute Scans durch. Scans müssen von	**11.2.3.a** Vergewissern Sie sich in der Änderungskontrolldokumentation und den Scan-Berichten, dass Systemkomponenten, an denen wesentliche Änderungen vorgenommen wurden, gescannt wurden.	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

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
qualifizierten Mitarbeitern durchgeführt werden.	**11.2.3.b** Überprüfen Sie die Prüfungsberichte und stellen Sie sicher, dass der Scan-Vorgang so lange durchgeführt wird, bis: • … bei externen Scans keine Sicherheitsrisiken mehr vorhanden sind, die vom CVSS mit einer Klassifizierung höher als 4.0 bewertet wurden. • … bei internen Scans alle „hohen“ Sicherheitsrisiken gemäß PCI-DSS-Anforderung 6.1 beseitigt wurden.	Karteninhaberdaten ermöglicht oder sich auf die Sicherheit der CDE auswirkt, kann sie als wesentlich betrachtet werden. 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.
	11.2.3.c Überprüfen Sie, ob die Prüfung 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).	
11.3 Implementierung einer Methodik für Penetrationstests, die die folgenden Elemente umfasst: • Die Methodik basiert auf branchenweit akzeptierten Verfahren für Penetrationstests (z. B. NIST SP800-115). • Die Methodik umfasst die gesamte Umgebung der CDE und wichtige Systeme • Es werden Tests innerhalb und außerhalb des Netzwerks durchgeführt. • Bei den Tests werden auch Kontrollen zur Segmentierung und zur Reduktion des Umfangs validiert. • Bei der Definition von Penetrationstests auf Anwendungsebene müssen mindestens die in Anforderung 6.5 aufgeführten Sicherheitsrisiken berücksichtigt werden.	**11.3** 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: • Die Methodik basiert auf branchenweit akzeptierten Verfahren für Penetrationstests (z. B. NIST SP800-115). • Die Methodik umfasst die gesamte Umgebung der CDE und wichtige Systeme • Es werden Tests innerhalb und außerhalb des Netzwerks durchgeführt. • Bei den Tests werden auch Kontrollen zur Segmentierung und zur Reduktion des Umfangs validiert. • Bei der Definition von Penetrationstests auf Anwendungsebene müssen mindestens die in Anforderung 6.5 aufgeführten Sicherheitsrisiken berücksichtigt werden. • Es müssen Penetrationstests auf Netzwerkebene definiert werden, die sämtliche Komponenten zur Unterstützung von Netzwerkfunktionen und Betriebssysteme enthalten. • Bei der Methodik müssen die in den letzten 12 Monaten	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. 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 hinreichend Informationen über das System, um mögliche Sicherheitslücken zu erkennen. Penetrationstests sind überwiegend manuelle

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
• Es müssen Penetrationstests auf Netzwerkebene definiert werden, die sämtliche Komponenten zur Unterstützung von Netzwerkfunktionen und Betriebssysteme enthalten. • Bei der Methodik müssen die in den letzten 12 Monaten aufgetretenen Bedrohungen und Sicherheitsrisiken berücksichtigt werden. • Es muss festgelegt sein, wo die Ergebnisse von Penetrationstests und Abhilfemaßnahmen gespeichert werden sollen. ***Hinweis:*** *Diese Änderung von Anforderung 11.3 wird bis zum 30. Juni 2015 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung. Die Anforderungen zu Penetrationstests aus Version 2.0 des PCI-DSS müssen befolgt werden, bis Version 3.0 in Kraft ist.*	aufgetretenen Bedrohungen und Sicherheitsrisiken berücksichtigt werden. • Es muss festgelegt sein, wo die Ergebnisse von Penetrationstests und Abhilfemaßnahmen gespeichert werden sollen.	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. *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.*
11.3.1 Durchführen *externer* 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).	**11.3.1.a** Untersuchen Sie den Arbeitsaufwand und die Ergebnisse des aktuellsten Penetrationstests, und prüfen Sie, ob die Penetrationstests wie folgt durchgeführt werden: • Gemäß der definierten Methodik • Mindestens jährlich • Nach wesentlichen Änderungen an der Umgebung	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. 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
	11.3.1.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).	
11.3.2 Durchführen *interner* Penetrationstests mindestens einmal im Jahr und nach jeder wesentlichen	**11.3.2.a** Untersuchen Sie den Arbeitsaufwand und die Ergebnisse des aktuellsten Penetrationstests, und prüfen Sie, ob der Penetrationstest mindestens einmal im Jahr und	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
Infrastruktur- oder Anwendungsaktualisierung oder -änderung (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver in der Umgebung).	nach jeder wesentlichen Änderung der Umgebung durchgeführt wird. • Gemäß der definierten Methodik • Mindestens jährlich • Nach wesentlichen Änderungen an der Umgebung	nach der Aktualisierung/Änderung noch wirksam sind.
	11.3.2.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).	
11.3.3 Beim Penetrationstest ermittelte ausnutzbare Sicherheitsrisiken müssen behoben werden, und anschließend muss ein erneuter Test durchgeführt werden.	**11.3.3** 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.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
11.3.4 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 Bereichs isoliert werden.	**11.3.4.a** 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 Bereichs isoliert werden. **11.3.4.b** Untersuchen Sie die Ergebnisse des aktuellsten Penetrationstests, und prüfen Sie, ob für Penetrationstests zur Prüfung von Segmentierungskontrollen Folgendes gilt: • Die Tests werden mindestens einmal jährlich und nach Änderungen an den Segmentierungskontrollen/-methoden durchgeführt. • Bei den Tests werden alle verwendeten Segmentierungskontrollen/-methoden geprüft. • Es wird geprüft, ob die Segmentierungsmethoden funktionieren und effektiv sind, und alle Systeme außerhalb des Bereichs müssen von den Systemen innerhalb des Bereichs isoliert werden.	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 Netzwerktest und/oder einer Suche nach offenen Ports geprüft werden, dass keine Verbindung zwischen innerhalb und außerhalb des Bereichs befindlichen Netzwerken besteht.
11.4 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. Ständige Aktualisierung der Systeme zur Erkennung und Verhinderung von Eindringversuchen, der Basis und der Signaturen.	**11.4.a** 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: • In der Umgebung der CDE • An kritischen Punkten in der CDE **11.4.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.	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 unentdeckt Angriffe auf (oder Missbrauch von) Computerressourcen ereignen. Die von diesen Systemen ausgegebenen

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
	11.4.c 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.	Sicherheitsalarmmeldungen müssen überwacht werden, damit Eindringlinge abgewehrt werden können.
11.5 Bereitstellung von Systemen zur Erkennung von Änderungen (z. B. Tools zur Überwachung der Dateiintegrität), die das Personal über nicht autorisierte Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien alarmieren, und Konfiguration der Software für einen mindestens wöchentlich durchgeführten Vergleich wichtiger Dateien. ***Hinweis:*** *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 Dateiintegritätsüberwachung, 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 Dienstanbieter) beurteilt und definiert werden.*	**11.5.a** Überprüfen Sie die Nutzung von Tools zur Änderungserkennung innerhalb der CDE, indem Sie die Systemeinstellungen und die überwachten Dateien sowie Ergebnisse aus der Aktivitätsüberwachung untersuchen. Beispiele für Dateien, die überwacht werden sollten: ▪ Ausführbare Systemdateien, ▪ Ausführbare Anwendungsdateien, ▪ Konfigurations- und Parameterdateien, ▪ Zentral gespeicherte Protokoll- und Audit-Dateien (alt oder archiviert). ▪ Zusätzliche von der Einheit als wichtig betrachtete Dateien (z. B. aufgrund einer Risikobewertung o. ä.)	Lösungen zur Änderungserkennung wie etwa FIM-Tools (File-Integrity Monitoring, Überwachung der Dateiintegrität) suchen nach Änderungen 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 die Inhalte der Konfigurationsdateien, Betriebssystemprogramme oder ausführbare Anwendungsdateien 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.
	11.5.b Überprüfen Sie, ob die Methoden zur Alarmierung des Personals über nicht zulässige Änderungen an wichtigen Dateien und zur mindestens einmal wöchentlichen Durchführung von Vergleichen wichtiger Dateien konfiguriert sind.	
11.5.1 Implementierung eines Prozesses z ur Reaktion auf Alarme der Lösung zur Änderungserkennung.	**11.5.1** Klären Sie durch eine Befragung des Personals, ob alle Alarmmeldungen untersucht und die Ursachen behoben wurden.	

PCI-DSS-ANFORDERUNGEN	PRÜFVERFAHREN	LEITFADEN
11.6 Die Sicherheitsrichtlinien und betrieblichen Verfahren zur Sicherheitsüberwachung und für Tests müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.	**11.6** 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: • Die Richtlinien und Verfahren sind dokumentiert, • werden verwendet und • sind allen Beteiligten bekannt.	Das Personal muss die folgenden Sicherheitsrichtlinien und betrieblichen Verfahren zur Sicherheitsüberwachung und für Tests kennen und dauerhaft befolgen.

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	Leitfaden
12.1 Festlegen, Veröffentlichen, Verwalten und Verbreiten einer Sicherheitsrichtlinie.	**12.1** 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.
12.1.1 Überarbeitung der Richtlinie mindestens einmal pro Jahr und Aktualisierung bei Umgebungsänderungen.	**12.1.1** 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.
12.2 Implementierung eines Risikobewertungsprozesses, für den Folgendes gilt: • Der Prozess wird mindestens einmal	**12.2.a** Überprüfen Sie, ob ein Prozess zur jährlichen Risikobewertung dokumentiert ist, in dem Ressourcen, Bedrohungen und Sicherheitsrisiken ermittelt werden und an dessen Ende eine formale Risikobewertung steht.	Eine Risikobewertung ermöglicht es einem Unternehmen, Bedrohungen und entsprechende Sicherheitsrisiken mit potenziell negativen geschäftlichen Auswirkungen zu erkennen.

PCI-DSS-Anforderungen	Prüfverfahren	Leitfaden
im Jahr und nach wesentlichen Änderungen an der Umgebung (z. B. Übernahmen, Fusionen, Umzüge usw.) durchgeführt. • Beim Prozess werden wichtige Ressourcen, Bedrohungen und Sicherheitsrisiken ermittelt. • Am Ende des Prozesses steht eine formale Risikobewertung. *Beispiele von Risikobewertungsmethoden sind unter anderen OCTAVE, ISO 27005 und NIST SP 800-30.*	**12.2.b** Vergewissern Sie sich durch Prüfung der Risikobewertungsdokumentation, dass der Risikobewertungsprozess mindestens einmal jährlich und nach wesentlichen Änderungen an der Umgebung durchgeführt wird.	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. 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.
12.3 Entwicklung von Verwendungsrichtlinien für wichtige Technologien und Definition der korrekten Verwendung dieser Technologien. ***Hinweis:*** *Beispiele für wichtige Technologien sind unter anderem Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, elektronische Wechselmedien, E-Mail-Programme und Internet-Anwendungen.* Die Verwendungsrichtlinien umfassen folgende Punkte:	**12.3** 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:	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.
12.3.1 Ausdrückliche Genehmigung durch autorisierte Parteien	**12.3.1** Überprüfen Sie, ob in den Verwendungsrichtlinien Prozesse für eine ausdrückliche Genehmigung von Befugten für die Verwendung dieser Technologien festgelegt sind.	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.

PCI-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.3.2 Authentifizierung zur Verwendung der Technologie	**12.3.2** 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.	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.
12.3.3 Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff	**12.3.3** Überprüfen Sie, ob laut Verwendungsrichtlinien eine Liste sämtlicher Geräte und der zur Verwendung der Geräte befugten Mitarbeiter angelegt werden muss.	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.
12.3.4 Methode zur genauen und schnellen Bestimmung von Eigentümern, Kontaktinformationen und Zweck (z. B. Etikettierung und Codierung von Geräten sowie Einbuchung in den Bestand)	**12.3.4** 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.	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.
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

PCI-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.3.6 Akzeptable Netzwerkorte für die Technologien	**12.3.6** Überprüfen Sie, ob in den Verwendungsrichtlinien angemessene Netzwerkorte für die Technologie festgelegt werden.	Unternehmen besser vorbereitet, um Lücken in Konfigurationen und Betriebskontrollen zu bewältigen und zu kontrollieren und um sicherzustellen, dass Angreifern keine Hintertürchen geöffnet werden, um sich Zugriff auf wichtige Systeme und Karteninhaberdaten zu verschaffen.
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 Hintertürchen 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	Leitfaden
12.3.10 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. Wenn ein bekanntes geschäftliches Bedürfnis besteht, muss in den Nutzungsrichtlinien festgelegt sein, dass die Daten entsprechend den geltenden PCI-DSS-Anforderungen geschützt werden.	**12.3.10.a** 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.	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.
	12.3.10.b Überprüfen Sie, ob die Verwendungsrichtlinien für Mitarbeiter mit entsprechenden Befugnissen den Schutz der Karteninhaberdaten gemäß den PCI-DSS-Anforderungen voraussetzen.	
12.4 Klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter in den Sicherheitsrichtlinien und Verfahren.	**12.4.a** Überprüfen Sie, ob die Sicherheitsrichtlinien eine klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter enthalten.	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.
	12.4.b Überprüfen Sie durch eine stichprobenartige Befragung , ob die zuständigen Mitarbeiter die Sicherheitsrichtlinien verstehen.	
12.5 Zuweisung der folgenden Managementverantwortungsbereiche in puncto Informationssicherheit zu einer Einzelperson oder einem Team:	**12.5** Überprüfen Sie, ob in den Richtlinien und Verfahren zur Informationssicherheit folgende Punkte enthalten sind: • Die Übertragung der formalen Verantwortung für die Informationssicherheit an einen Sicherheitsbeauftragten ein anderes für die Sicherheit zuständiges Mitglied des Managements • Die folgenden Verantwortlichkeiten im Zusammenhang mit der Informationssicherheit werden konkret und formal geregelt:	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.
12.5.1 Festlegen, Dokumentieren und Verteilen von Sicherheitsrichtlinien und -verfahren.	**12.5.1** Überprüfen Sie, ob die Verantwortlichkeit zur Erstellung, Dokumentation und Verteilung von Sicherheitsrichtlinien und -verfahren formal festgelegt wurde.	

PCI-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.5.2 Überwachung und Analyse von Sicherheitsalarmen und -informationen und Verteilung an das entsprechende Personal.	**12.5.2** 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.	
12.5.3 Festlegen, Dokumentieren und Verteilen von Reaktions- und Eskalationsverfahren für Sicherheitsvorfälle, damit eine rechtzeitige und effektive Vorgehensweise in allen Situationen gewährleistet ist.	**12.5.3** Überprüfen Sie, ob die Verantwortlichkeit für die Festlegung, Dokumentation und Verteilung von Reaktions- und Eskalationsverfahren für Sicherheitsvorfälle formal geregelt wurde.	
12.5.4 Administration von Benutzerkonten, einschließlich Ergänzungen, Löschungen und Änderungen.	**12.5.4** Überprüfen Sie, ob die Verantwortlichkeit für die Administration von Benutzerkonten (Hinzufügen/Löschen/Ändern) und für das Authentifizierungsmanagement formal geregelt wurde.	
12.5.5 Überwachung und Kontrolle des gesamten Datenzugriffs.	**12.5.5** Überprüfen Sie, ob die Verantwortlichkeiten zur Überwachung und Kontrolle des gesamten Datenzugriffs formal zugewiesen wurden.	
12.6 Implementierung eines offiziellen Programms zur Förderung des Sicherheitsbewusstseins, durch das allen Mitarbeitern die Bedeutung der Sicherheit von Karteninhaberdaten vermittelt wird.	**12.6.a** Überprüfen Sie, ob das Programm zur Förderung des Sicherheitsbewusstseins allen Mitarbeitern die Bedeutung der Sicherheit von 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.
	12.6.b Untersuchen Sie die Verfahren und die Dokumentation des Programms zur Förderung des Sicherheitsbewusstseins, und führen Sie Folgendes durch:	
12.6.1 Durchführung von Mitarbeiterschulungen bei der Einstellung und danach mindestens einmal im Jahr. ***Hinweis:*** *Die Methoden sind abhängig von der Funktion der Mitarbeiter und deren Zugriffsrechten auf Karteninhaberdaten.*	**12.6.1.a** 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 Auffrischungskursen begleitet wird, geraten wichtige Sicherheitsprozesse und -verfahren in Vergessenheit oder werden umgangen, und zentrale Ressourcen und Karteninhaberdaten werden Gefahren ausgesetzt.
	12.6.1.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	Leitfaden
	12.6.1.c 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.	
12.6.2 Die Mitarbeiter müssen mindestens einmal pro Jahr schriftlich bestätigen, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens gelesen und verstanden haben.	**12.6.2** 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.	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.
12.7 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.) ***Hinweis:*** *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.*	**12.7** 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.	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.
12.8 Pflege und Implementierung von Richtlinien und Verfahren zur Verwaltung von Dienstanbietern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise:	**12.8** Prüfen Sie durch die Beobachtung und Untersuchung von Richtlinien und Verfahren sowie der zugehörigen Dokumentation, ob Prozesse zur Verwaltung von Dienstanbietern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten (z. B. Einrichtungen für die Aufbewahrung von Sicherungsbändern, Anbieter verwalteter Dienste wie Webhosting-Unternehmen und Sicherheitsdienstanbieter oder Unternehmen, die Daten zur Aufklärung eventueller Betrugsversuche benötigen), wie folgt implementiert sind:	Wenn ein Händler oder Dienstanbieter Karteninhaberdaten gemeinsam mit einem anderen Dienstanbieter verwendet, gelten bestimmte Anforderungen, um den dauerhaften Schutz dieser Daten durch diese Dienstanbieter zu gewährleisten.

PCI-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.8.1 Stellen Sie eine Liste der Dienstanbieter auf.	**12.8.1** Überprüfen Sie, ob eine Liste mit Dienstanbietern geführt wird.	Behalten Sie alle Dienstanbieter im Auge, bei denen ein potentielles Risiko nicht nur innerhalb des Unternehmens erkannt wurde.
12.8.2 Aufbewahrung einer schriftlichen Vereinbarung mit einer Bestätigung dazu, dass der Dienstanbieter 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. ***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.*	**12.8.2** Überprüfen Sie, ob schriftliche Vereinbarungen eine Bestätigung der Dienstanbieter enthalten, nach der die Dienstanbieter 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.	Die Bestätigung der Dienstanbieter ist Beleg für deren Verpflichtung, die Karteninhaberdaten, die sie von ihren Kunden anvertraut bekommen, entsprechend zu schützen. In Kombination mit Anforderung 12.9 geht es bei dieser Anforderung für schriftliche Vereinbarungen zwischen Unternehmen und Dienstanbietern 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.
12.8.3 Festlegung eines eindeutigen Prozesses für die Inanspruchnahme von Dienstanbietern, der die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht.	**12.8.3** Überprüfen Sie, ob Richtlinien und Verfahren für die Auswahl von Dienstanbietern dokumentiert und implementiert sind und ob vor der Wahl des Anbieters die erforderliche Sorgfalt beachtet wurde.	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. 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.

PCI-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.8.4 Einrichtung eines Programms zur mindestens einmal jährlichen Überwachung der Dienstanbieter-Konformität mit dem PCI-DSS.	**12.8.4** Überprüfen Sie, ob in der Einheit ein Programm zur mindestens einmal jährlichen Überwachung der Dienstanbieter-Konformität mit dem PCI-DSS vorliegt.	Wenn Sie den PCI-DSS-Konformitätstatus Ihres Serviceanbieters kennen, können Sie sich sicher sein, dass er denselben Anforderungen wie auch Ihr Unternehmen unterliegt. Sollte der Dienstanbieter 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-Bewertung des Kunden fallen. Welche Informationen eine Einheit konkret verwaltet, hängt von der Vereinbarung mit den Anbietern, dem Servicetyp usw. ab. Die Absicht besteht darin, dass die bewertete Einheit erkennt, welche PCI-DSS-Anforderungen ihre Dienstanbieter gemäß Vereinbarung erfüllen wollen.
12.8.5 Verwaltung von Informationen darüber, welche PCI-DSS-Anforderungen von den einzelnen Dienstanbietern und welche von der Einheit verwaltet werden.	**12.8.5** Prüfen Sie, ob die Einheit Informationen darüber verwaltet, welche PCI-DSS-Anforderungen von den einzelnen Dienstanbietern und welche von der Einheit verwaltet werden.	

PCI-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.9 ***Zusätzliche Anforderung für Dienstanbieter*****:** 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. ***Hinweis:*** *Diese Anforderung wird bis zum 30. Juni 2015 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.* ***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.*	**12.9** ***Zusätzliches Testverfahren für Dienstanbieter:*** 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 des Kunden oder vertrauliche Authentifizierungsdaten verarbeitet, speichert, verarbeitet oder überträgt bzw. darauf zugreifen kann, bzw. in dem er die CDE für den Kunden verwaltet.	Diese Anforderung muss beachtet werden, wenn es sich bei der zu bewertenden Einheit um einen Dienstanbieter handelt. 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. Auf welche Methode der Dienstanbieter die schriftliche Bestätigung gibt, muss zwischen dem Dienstanbieter und seinen Kunden vereinbart werden.
12.10 Implementierung eines Vorfallreaktionsplans, der eine sofortige Reaktion auf Sicherheitsverletzungen im System ermöglicht.	**12.10** Untersuchen Sie den Vorfallreaktionsplan sowie zugehörige Verfahren, und prüfen Sie, ob die Einheit in der Lage ist, sofort wie folgt auf eine Sicherheitsverletzung zu reagieren:	Ohne einen ausführlichen Vorfallreaktionsplan, 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.

PCI-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.10.1 Erstellung des Vorfallreaktionsplans, der im Falle einer Sicherheitsverletzung im System eingesetzt wird. Der Plan umfasst mindestens die folgenden Punkte: • Rollen, Verantwortungsbereiche und Kommunikations-- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken • Konkrete Verfahren für die Reaktion auf Vorfälle • Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs • Verfahren zur Datensicherung • Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen • Abdeckung sämtlicher wichtigen Systemkomponenten • Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle	**12.10.1.a** Überprüfen Sie, ob der Vorfallreaktionsplan Folgendes umfasst: • Rollen, Verantwortungsbereiche und Kommunikationsstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken • Konkrete Verfahren für die Reaktion auf Vorfälle • Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs • Verfahren zur Datensicherung • Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen (z. B. das California Bill 1386, in dem vorgeschrieben wird, dass Unternehmen bei einer tatsächlichen oder mutmaßlichen Sicherheitsverletzung die Betroffenen benachrichtigen müssen, falls sich in der Datenbank Daten von Bürgern des Staates Kalifornien befinden). • Abdeckung sämtlicher wichtigen Systemkomponenten • Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle	Der Vorfallreaktionsplan sollte gut durchdacht sein und alle Schlüsselelemente enthalten, die es Ihrem Unternehmen ermöglichen, effektiv potentiellen Verstößen zu begegnen, die die Karteninhaberdaten betreffen könnten.
	12.10.1.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 Vorfallreaktionsplan und die entsprechenden Verfahren befolgt wurden.	
12.10.2 Mindestens einmal jährlicher Test des Plans.	**12.10.2** Überprüfen Sie, ob der Plan mindestens einmal im Jahr getestet wird.	Ohne entsprechende Tests könnten wichtige Schritte vergessen werden, wodurch während eines Vorfalls hohe Risiken entstehen können.

PCI-DSS-Anforderungen	Prüfverfahren	Leitfaden
12.10.3 Zur Reaktion auf Alarmmeldungen muss rund um die Uhr spezielles Personal verfügbar sein.	**12.10.3** 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.	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 Vorfalls vereitelt werden.
12.10.4 Durchführung von Schulungen für Mitarbeiter, die für die Reaktion auf Sicherheitsverletzungen verantwortlich sind.	**12.10.4** 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.	
12.10.5 Berücksichtigung von Alarmmeldungen aus Sicherheitsüberwachungssystemen wie IDS/IPS, Firewalls und Systemen zur Überwachung der Dateiintegrität.	**12.10.5** Überprüfen Sie durch Beobachtung und Untersuchung der Prozesse, ob die Überwachung und die Reaktion auf Alarmmeldungen von Sicherheitssystemen, einschließlich der Erkennung unbefugter WLAN-Zugriffspunkte, im Vorfallreaktionsplan enthalten sind.	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.
12.10.6 Entwicklung eines Prozesses zur Änderung und Weiterentwicklung des Vorfallreaktionsplans unter Berücksichtigung von eigenen Erkenntnissen und Branchenentwicklungen.	**12.10.6** 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.	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.

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

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

Wie in den Anforderung 12.8 und 12.9 erläutert, müssen sämtliche Dienstanbieter, 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.

Anforderungen	Prüfverfahren	Leitfaden
A.1 Schutz der gehosteten Umgebung und der Daten jeder Einheit (d. h. Händler, Dienstanbieter oder andere Einheiten) gemäß A.1.1 bis A.1.4: Ein Hosting-Anbieter muss diese Anforderungen sowie die anderen relevanten Abschnitte des PCI-Datensicherheitsstandards erfüllen. ***Hinweis:*** *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.*	**A.1** Prüfen Sie insbesondere bei einer PCI-DSS-Bewertung eines Anbieters von gemeinsam genutzten Hosting-Services, ob die gehosteten Umgebungen und Daten der einzelnen Einheiten (Händler und Dienstanbieter) geschützt werden. Wählen Sie dazu stichprobenartig verschiedene Server (Microsoft Windows und Unix/Linux) aus einem repräsentativen Querschnitt aus Hosting-Händlern und -Dienstanbietern aus, und führen Sie die unter A.1.1 bis A.1.4 beschriebenen Tests durch:	*Anhang A* des PCI-DSS gilt für Anbieter von gemeinsam genutzten Hosting-Services, die den Kunden Ihrer Händler und/oder Dienstanbieter eine PCI-DSS konforme Hosting-Umgebung bieten möchten.

Anforderungen	Prüfverfahren	Leitfaden
A.1.1 In den einzelnen Einheiten dürfen nur Prozesse ausgeführt werden, die Zugriff auf die CDE dieser Einheit haben.	**A.1.1** Wenn ein gemeinsam genutzter Hosting-Anbieter Stellen (beispielsweise Händlern oder Dienstanbietern) die Möglichkeit gibt, eigene Anwendungen auszuführen, überprüfen Sie, ob diese Anwendungsprozesse mit der eindeutigen ID der Stelle ausgeführt werden. Beispiel: • Keine Stelle im System kann die Benutzer-ID eines gemeinsamen Webservers verwenden. • Sämtliche von einer Stelle verwendeten CGI-Skripte müssen als eindeutige Benutzer-ID der Stelle erstellt und ausgeführt werden.	Wenn ein Händler oder Dienstanbieter berechtigt ist, seine eigenen Anwendungen auf dem gemeinsam genutzten Server auszuführen, müssen diese mit der Benutzer-ID des Händlers oder Dienstanbieters anstatt als Benutzer mit besonderen Rechten ausgeführt werden.
A.1.2 Beschränkung des Zugriffs und der Berechtigungen aller Einheiten auf die jeweils eigene CDE.	**A.1.2.a** Vergewissern Sie sich, dass die Benutzer-ID eines Anwendungsprozesses nicht über besondere Rechte (root/admin) verfügt.	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: 1. Berechtigungen der Benutzer-ID für den Webserver des Händlers oder Dienstanbieters 2. Berechtigungen zum Lesen, Schreiben und Ausführen von Dateien 3. Berechtigungen zum Schreiben von Systemdateien 4. Berechtigungen für die Protokolldateien der Händler und Dienstanbieter 5. Kontrollen, mit denen verhindert wird, dass die Systemressourcen ausschließlich von einem Händler oder Dienstanbieter genutzt werden
	A.1.2.b Überprüfen Sie, ob die einzelnen Stellen (Händler, Dienstanbieter) Lese-, Schreib- und Ausführungsberechtigungen nur für eigene Dateien und Verzeichnisse oder für notwendige Systemdateien (eingeschränkt durch Dateisystemberechtigungen, Zugriffssteuerungslisten, chroot, jailshell usw.) besitzen. **Wichtig:** Die Dateien einer Stelle können nicht von einer Gruppe gemeinsam genutzt werden.	
	A.1.2.c Vergewissern Sie sich, dass die Benutzer einer Stelle keinen Schreibzugriff auf gemeinsam genutzte Systemdateien besitzen.	
	A.1.2.d Überprüfen Sie, ob die Anzeige von Protokolleinträgen auf die protokollbesitzende Einheit beschränkt ist.	
	A.1.2.e 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: • Festplattenkapazität • Bandbreite • Arbeitsspeicher • Prozessor.	

Anforderungen	Prüfverfahren	Leitfaden
A.1.3 Für die CDE jeder Einheit müssen eindeutige, mit der PCI-DSS-Anforderung 10 konforme Protokollierungs- und Audit-Trails aktiviert sein.	**A.1.3** Überprüfen Sie, ob der gemeinsame Hosting-Anbieter die Protokollierung für jede einzelne Händler- und Dienstanbieterumgebung wie folgt aktiviert hat: • Protokolle werden für gängige Anwendungen von Drittanbietern aktiviert. • Protokolle sind standardmäßig aktiviert. • Protokolle können von der Stelle, die sie besitzt, eingesehen werden. • Die Besitzer der Protokolle erhalten eine Mitteilung zum genauen Speicherort der Protokolle.	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.
A.1.4 Aktivierung von Prozessen für eine rechtzeitige Ursachenanalyse im Falle einer Sicherheitsverletzung bei einem gehosteten Händler oder Dienstanbieter.	**A.1.4** 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.	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.

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 zweier Faktoren erforderlich. Die Authentifizierung anhand zweier Faktoren *innerhalb des internen Netzwerks* kann für den nicht über die Konsole stattfindenden Administratorzugriff als Kompensationskontrolle betrachtet werden, wenn eine Übertragung verschlüsselter Kennwörter nicht möglich ist. Die Zwei-Faktoren-Authentifizierung ist eine akzeptable Kompensationskontrolle, wenn: (1) die Absicht der ursprünglichen Anforderung erfüllt wird (das Risiko des Abfangens unverschlüsselter Kennwörter wird verhindert) und (2) die Authentifizierung in einer sicheren Umgebung ordnungsgemäß konfiguriert wurde.

c) Die vorhandenen PCI-DSS-Anforderungen können mit neuen Kontrollen zusammen als Kompensationskontrolle fungieren. Zum Beispiel kann ein Unternehmen Karteninhaberdaten nicht nach Anforderung 3.4 unlesbar machen (z. B. durch Verschlüsselung). In diesem Fall könnte eine Kompensation darin bestehen, dass mit einem Gerät bzw. einer Kombination aus Geräten, Anwendungen und Kontrollen folgende Punkte sichergestellt sind: (1) interne

Netzwerksegmentierung; (2) Filtern von IP- oder MAC-Adressen und (3) Zwei-Faktor-Authentifizierung innerhalb des internen Netzwerks.

4. Sie müssen dem zusätzlichen Risiko, das durch die Nichteinhaltung der PCI-DSS-Anforderung entsteht, angemessen sein.

Der Prüfer führt im Rahmen der jährlichen PCI-DSS-Beurteilung eine eingehende Überprüfung der Kompensationskontrollen durch und stellt dabei unter Beachtung der vier oben genannten Kriterien fest, ob die jeweiligen Kompensationskontrollen einen angemessenen Schutz vor den Risiken bieten, wie 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
1. Einschränkungen	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	
2. Ziel	Definieren Sie das Ziel der ursprünglichen Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	
3. Ermitteltes Risiko	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	
4. Definition der Kompensationskontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	
5. Validierung der Kompensationskontrollen	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet werden.	
6. Verwaltung	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	

Arbeitsblatt – 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?*

	Erforderliche Informationen	Erklärung
1. Einschränkungen	Führen Sie Einschränkungen auf, die die Konformität mit der ursprünglichen Anforderung ausschließen.	*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.*
2. Ziel	Definieren Sie das Ziel der ursprünglichen Kontrolle, und ermitteln Sie das von der Kompensationskontrolle erfüllte Ziel.	*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.*
3. Ermitteltes Risiko	Ermitteln Sie jedes zusätzliche Risiko, das auf die fehlende ursprüngliche Kontrolle zurückzuführen ist.	*Für das Zugriffskontrollsystem entsteht ein zusätzliches Risiko, da nicht gewährleistet ist, dass alle Benutzer eine eindeutige ID haben und verfolgt werden können.*
4. Definition der Kompensationskontrollen	Definieren Sie die Kompensationskontrollen, und erklären Sie, wie sie die Ziele der ursprünglichen Kontrolle und ggf. das erhöhte Risiko ansprechen.	*Unternehmen XYZ erfordert von allen Benutzern die Anmeldung an den Servern über ihre Desktop-Computer unter Verwendung des Befehls SU (substitute user, Benutzer ersetzen). Der Befehl ermöglicht den Zugriff auf das Konto „root“ und die Durchführung von Aktionen unter dem Konto „root“, wobei der Vorgang im Verzeichnis „SU-log“ protokolliert werden kann. Auf diese Weise können die Aktionen der einzelnen Benutzer über das SU-Konto verfolgt werden, ohne dass das „root“-Kennwort an die Benutzer ausgegeben werden muss.*
5. Validierung der Kompensationskontrollen	Legen Sie fest, wie die Kompensationskontrollen validiert und getestet	*Unternehmen XYZ demonstriert dem Prüfer die Ausführung des Befehls SU und die Tatsache, dass sämtliche Aktivitäten der Personen, die den Befehl ausführen,*

	werden.	*protokolliert werden, woraus sich ableiten lässt, dass die Person mit „root“-Rechten arbeitet.*
6. Verwaltung	Legen Sie Prozesse und Kontrollen zur Verwaltung der Kompensationskontrollen fest.	*Unternehmen XYZ dokumentiert Prozesse und Verfahren, mit denen dafür gesorgt wird, dass SU-Konfigurationen nicht durch Änderung, Bearbeitung oder Löschen so bearbeitet werden können, dass eine Ausführung von „root“-Befehlen ohne individuelle Benutzerverfolgung bzw. Protokollierung möglich würde.*

Anhang D: Segmentierung und Stichprobenkontrolle von Unternehmenseinrichtungen/Systemkomponenten