Payment Card Industry
Datensicherheitsstandard

Anforderungen und Testprozeduren

Version 4.0

März 2022

Dokumentänderungen

Datum	Version	Beschreibung
Oktober 2008	1.2	Einführung von PCI DSS v1.2 als „PCI DSS Requirements and Security Assessment Procedures", wobei Redundanzen zwischen den Dokumenten beseitigt und sowohl allgemeine als auch spezifische Änderungen gegenüber PCI DSS Security Audit Procedures v1.1 vorgenommen werden sollen. Vollständige Informationen finden Sie unter PCI Datensicherheitsstandard Zusammenfassung der Änderungen von PCI DSS Version 1.1 bis 1.2.
Juli 2009	1.2.1	Fügen Sie einen Satz hinzu, der zwischen PCI DSS v1.1 und v1.2 fälschlicherweise gelöscht wurde.
		Berichtigen Sie „dann" in „als" in den Prüfverfahren 6.3.7.a und 6.3.7.b.
		Entfernen Sie die ausgegraute Markierung für die Spalten „vorhanden" und „nicht vorhanden" in der Testprozedur 6.5.b.
		Für das Arbeitsblatt Kompensationskontrollen - Ausgefülltes Beispiel, korrigieren Sie den Wortlaut oben auf der Seite, um zu sagen: „Verwenden Sie dieses Arbeitsblatt, um Kompensationskontrollen für jede Anforderung zu definieren, die über Kompensationskontrollen als „vorhanden" vermerkt ist."
Oktober 2010	2.0	Aktualisierung und umgesetzte Änderungen von v1.2.1. Siehe PCI DSS – Zusammenfassung der Änderungen von PCI DSS Version 1.2.1 zu 2.0.
November 2013	3.0	Aktualisierung von v2.0. Siehe PCI DSS – Zusammenfassung der Änderungen von PCI DSS Version 2.0 zu 3.0.
April 2015	3.1	Aktualisierung von PCI DSS v3.0. Siehe PCI DSS – Zusammenfassung der Änderungen von PCI DSS Version 3.0 zu 3.1 für Details zu Änderungen.
April 2016	3.2	Aktualisierung von PCI DSS v3.1. Siehe PCI DSS – Zusammenfassung der Änderungen von PCI DSS Version 3.1 zu 3.2 für Details zu Änderungen.
Mai 2018	3.2.1	Aktualisierung von PCI DSS v3.2. Siehe PCI DSS – Zusammenfassung der Änderungen von PCI DSS Version 3.2 zu 3.2.1 für Details zu Änderungen.
März 2022	4.0	Umbenennung des Dokumententitels zu „Payment Card Industry Datensicherheitsstandard: Anforderungen und Testprozeduren." Akktualisierung von PCI DSS v3.2.1. Siehe PCI DSS – Zusammenfassung der Änderungen von PCI DSS Version 3.2.1 zu 4.0 für Details zu Änderungen.

ANMERKUNG: Die englische Textversion dieses Dokuments wie auf der PCI SSC-Website angezeigt gilt für alle Zwecke als offizielle Version dieses Dokuments. Für den Fall von Mehrdeutigkeit oder Unstimmigkeit zwischen diesem und dem englischen Text hat die englische Version Vorrang.

Inhaltsverzeichnis

1 Einführung und Übersicht über den PCI-Datensicherheitsstandard

Der Payment Card Industry Datensicherheitsstandard (PCI DSS) wurde entwickelt, um Zahlungskarten-Kontendaten-Sicherheit zu fördern und die breite Annahme von konsistenten Datensicherheitsmaßnahmen weltweit zu erleichtern. PCI DSS bietet einen Grundstock an technischen und betrieblichen Anforderungen zum Schutz von Kontodaten. PCI DSS wurde zwar speziell für Umgebungen mit Zahlungskartenkontodaten entwickelt, kann aber auch zum Schutz vor Bedrohungen und zur Sicherung anderer Elemente im Zahlungssystem eingesetzt werden.

Tabelle 1 zeigt die 12 wichtigsten Anforderungen des PCI DSS.

Tabelle 1. Hauptsächlich PCI DSS-Anforderungen

PCI Datensicherheitsstandard – Übersicht auf hoher Ebene	
Aufbau und Wartung eines sicheren Netzwerks und sicherer Systeme	**1.** Installation und Wartung von Netzsicherheitskontrollen. **2.** Anwendung von sicheren Konfigurationen auf alle Systemkomponenten.
Schutz von Kontodaten	**3.** Schutz von gespeicherten Kontodaten. **4.** Schutz von Karteninhaberdaten mit starker Kryptographie während der Übertragung über offene, öffentliche Netzwerke
Wartung eines Programms zur Verwaltung von Schwachstellen	**5.** Schutz aller Systeme und Netzwerke vor bösartiger Software. **6.** Entwicklung und Wartung sicherer Systeme und Software.
Implementierung starker Zugriffskontrollmaßnahmen	**7.** Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten nach geschäftlichem Bedarf. **8.** Identifizierung von Benutzern und Authentisierung von Zugriff auf Systemkomponenten. **9.** Beschränkung des physischen Zugriffs auf Karteninhaberdaten.
Regelmäßige Überwachung und Prüfung der Netzwerke	**10.** Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten. **11.** Regelmäßige Prüfung der Sicherheit von Systemen und Netzwerken.
Beibehaltung einer Informationssicherheitspolitik	**12.** Unterstützung der Informationssicherheit durch organisatorische Richtlinien und Programme.

Dieses Dokument, Payment Card Industry Datensicherheitsstandard Anforderungen und Sicherheitsbewertungsprozeduren, besteht aus den 12 Hauptanforderungen des PCI DSS, den detaillierten Sicherheitsanforderungen, den entsprechenden Testprozeduren und anderen Informationen, die für jede Anforderung relevant sind. Die folgenden Abschnitte stellen detaillierte Richtlinien und bewährte Praktiken bereit, um Entitäten bei der Vorbereitung, Durchführung und Berichterstattung der Ergebnisse einer PCI DSS-Bewertung zu unterstützen. Die PCI DSS-Anforderungen und Testprozeduren beginnen ab Seite 40.

PCI DSS umfasst ein Mindestmaß an Anforderungen zum Schutz von Kontodaten und kann durch zusätzliche Kontrollen und Praktiken erweitert werden, um die Risiken weiter zu mindern und lokale, regionale und sektorale Gesetze und Vorschriften zu berücksichtigen. Darüber hinaus können Gesetze oder behördliche Vorschriften einen besonderen Schutz personenbezogener Informationen oder anderer Datenelemente (z. B. den Namen des Karteninhabers) vorschreiben.

Einschränkungen

Sollte eine der in dieser Norm enthaltenen Anforderungen im Widerspruch zu den Gesetzen des Landes, des Bundesstaates oder der Gemeinde stehen, gelten die Gesetze des Landes, des Bundesstaates oder der Gemeinde.

PCI DSS-Ressourcen

Die Webseite von PCI Security Standards Council (PCI SSC) (www.pcisecuritystandards.org) bietet die folgenden zusätzlichen Ressourcen, um Organisationen bei ihren PCI DSS-Bewertungen und -Validierungen zu unterstützen:

- Dokumentenbibliothek, beinhaltend:
  - *PCI DSS* Zusammenfassung der Änderungen:
  - PCI DSS Kurzreferenz Leitfaden
  - Ergänzende Informationen und Richtlinien
  - Prioritärer Ansatz für PCI DSS
  - Bericht über die Konformität der Vorschriften (ROC) Berichtsvorlage und Anweisungen zur Berichterstattung
  - Selbstbeurteilungsfragebögen (SAQs) und SAQ-Anweisungen und -Richtlinien
  - Konformitätsbescheinigungen *(AOCs)*
- Häufig gestellte Fragen (FAQs)
- PCI für Webseiten von kleinen Händlern
- PCI-Schulungen und informative Webinare
- Liste der qualifizierten Sicherheitsgutachter (QSAs) und zugelassenen Scanning-Anbieter (ASVs)

- Listen von PCI-zugelassenen Geräten, Anwendungen, und Lösungen

Auf der Webseite des PCI SSC sind mehr als 60 Anleitungsdokumente und Ergänzungsinformationen verfügbar, die spezifische Anleitungen und Überlegungen zum PCI DSS enthalten. Beispiele beinhalten:

- Anleitungen für PCI DSS-Scoping und Netzwerksegmentierung
- PCI SSC Cloud-Berechnungs-Richtlinien
- Anleitungen zur Multi-Faktor-Authentifizierung
- Sicherheitsgarantie von Drittanbietern
- Wirksame tägliche Protokollüberwachung
- Anleitungen für Penetrationstests
- Bewährte Praktiken für die Implementierung eines Sicherheitsbewusstsein-Programms
- Bewährte Praktiken zur Aufrechterhaltung der PCI-DSS-Konformität
- PCI DSS für große Organisationen
- Verwendung von SSL/Vorzeitigen TLS und Auswirkungen auf ASV-Scans
- Verwendung von SSL/Vorzeitigen TLS für POS-POI-Terminalverbindungen
- Sicherheitsrichtlinien für Tokenisierungsprodukte
- Schutz von telefonbasierten Zahlungskartendaten

Hinweis: *Informationsergänzungen ergänzen den PCI-DSS und identifizieren zusätzliche Überlegungen und Empfehlungen zur Erfüllung der PCI-DSS-Anforderungen. Die Informationsergänzungen ersetzen oder erweitern weder den PCI DSS noch irgendwelche seiner Anforderungen.*

Informationen über diese und andere Ressourcen finden Sie in der Dokumentenbibliothek unter www.pcisecuritystandards.org.

Darüber hinaus finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

2 PCI DSS Informationen zur Anwendbarkeit

PCI DSS richtet sich an alle Entitäten, die Karteninhaberdaten (CHD) und/oder sensible Authentifizierungsdaten (SAD) speichern, verarbeiten oder übertragen oder die Sicherheit der Karteninhaberdatenumgebung (CDE) beeinflussen könnten. Dazu gehören alle Entitäten, die an der Bearbeitung von Zahlungskartenkonten beteiligt sind - einschließlich Händler, Verarbeiter, Erwerber, Herausgeben und andere Dienstleistungsanbieter.

Ob eine Entität verpflichtet ist, den PCI DSS einzuhalten oder seine Konformität zu bestätigen, liegt im Ermessen der Organisationen, die die Konformitätsprogramme verwalten (z. B. Zahlungsanbieter und Erwerber). Erkundigen Sie sich bei den Organisationen, die Sie interessieren, nach zusätzlichen Kriterien.

Definition von Kontodaten, Karteninhaberdaten und sensiblen Authentifizierungsdaten

Karteninhaberdaten und sensible Authentifizierungsdaten werden als Kontendaten angesehen und sind wie folgt definiert:

Tabelle 2. Kontodaten

Kontodaten	
Karteninhaberdaten beinhalten:	**Sensible Authentifizierungsdaten beinhalten:**
• Primäre Kontonummer (PAN) • Name des Karteninhabers • Ablaufdatum • Dienstleistungskodex	• Vollständige Nachverfolgungsdaten (Magnetstreifendaten oder gleichwertige Daten auf einem Chip) • Kartenverifizierungscode • PINs/PIN-Sperren

Die Anforderungen des PCI DSS gelten für Entitäten mit Umgebungen, in denen Kontodaten (Karteninhaberdaten und/oder sensible Authentifizierungsdaten) gespeichert, verarbeitet oder übertragen werden, sowie für Entitäten mit Umgebungen, die die Sicherheit des CDE beeinflussen können. Einige PCI DSS-Anforderungen können auch für Entitäten mit Umgebungen gelten, die keine Kontodaten speichern, verarbeiten oder übertragen, z. B. Entitäten, die den Zahlungsverkehr oder die Verwaltung ihres CDE auslagern.[1]. Entitäten, die ihre Zahlungsumgebungen oder Zahlungsvorgänge an Dritte auslagern, bleiben dafür verantwortlich, dass die Kontodaten durch den Dritten gemäß den geltenden PCI DSS-Anforderungen geschützt werden.

[1] In Übereinstimmung mit den Organisationen, die Konformitätsprogramme verwalten (z. B. Zahlungsmarken und Erwerber); sollten Entitäten sich für weitere Einzelheiten an die betreffenden Organisationen wenden.

Die primäre Kontonummer (PAN) ist der bestimmende Faktor für Karteninhaberdaten. Der Begriff Kontodaten umfasst daher Folgendes: die vollständige PAN, alle anderen Elemente der Karteninhaberdaten, die zusammen mit der PAN vorhanden sind, und alle Elemente der sensiblen Authentifizierungsdaten.

Wenn der Name des Karteninhabers, der Dienstleistungskodex und/oder das Ablaufdatum mit der PAN gespeichert, verarbeitet oder übertragen werden oder anderweitig im CDE vorhanden sind, müssen sie gemäß den für Karteninhaberdaten geltenden PCI DSS-Anforderungen geschützt werden

Wenn eine Entität PAN speichert, verarbeitet oder überträgt, liegt ein CDE vor, für das die PCI DSS-Anforderungen gelten. Einige Anforderungen sind möglicherweise nicht anwendbar, z. B. wenn die Entität keine PAN speichert, dann sind die Anforderungen zum Schutz der gespeicherten PAN in Anforderung 3 nicht auf die Entität anwendbar.

Auch wenn eine Entität PAN nicht speichert, verarbeitet oder überträgt, können einige PCI DSS-Anforderungen dennoch gelten. Überlegen Sie sich Folgendes:

- Wenn die Entität SAD speichert, gelten die speziellen Anforderungen für die Speicherung des SAD in Anforderung 3.
- Beauftragt die Entität Drittanbieter von Dienstleistungen mit der Speicherung, Verarbeitung oder Übermittlung von PAN in ihrem Namen, gelten die Anforderungen für die Verwaltung von Dienstleistungsanbietern gemäß Anforderung 12.
- Wenn die Entität die Sicherheit eines CDE beeinflussen kann, weil die Sicherheit der Infrastruktur einer Entität die Verarbeitung von Karteninhaberdaten beeinflussen kann (z. B. über einen Webserver, der die Erstellung eines Zahlungsformulars oder einer Seite steuert), gelten bestimmte Anforderungen.
- Sind die Daten des Karteninhabers nur auf physischen Datenträgern (z. B. Papier) vorhanden, gelten die Anforderungen an die Sicherheit und Entsorgung physischer Datenträger gemäß Anforderung 9.
- Die Anforderungen an einen Notfallplan gelten für alle Entitäten, um sicherzustellen, dass Prozeduren vorhanden sind, die im Falle einer vermuteten oder tatsächlichen Verletzung der Vertraulichkeit von Karteninhaberdaten gefolgt werden sollen.

Verwendung von Kontodaten, sensiblen Authentifizierungsdaten, Karteninhaberdaten und primären Kontonummern im PCI DSS

PCI DSS beinhaltet Anforderungen, die sich speziell auf Kontodaten, Karteninhaberdaten und sensible Authentifizierungsdaten beziehen. Es ist wichtig zu beachten, dass jede dieser Arten von Daten unterschiedlich ist und die Begriffe nicht austauschbar sind. Spezifische Verweise in den Anforderungen auf Kontodaten, Karteninhaberdaten oder sensible Authentifizierungsdaten sind zweckmäßig, und die Anforderungen gelten speziell für die Art von Daten, auf die verwiesen wird.

Elemente der Kontodaten und Speicheranforderungen

Tabelle 3 identifiziert die Elemente der Karteninhaberdaten und der sensiblen Authentifizierungsdaten, ob die Speicherung jedes Datenelements erlaubt oder verboten ist, und ob jedes Datenelement bei der Speicherung unlesbar gemacht werden muss, z. B. durch starke Kryptografie. Diese Tabelle ist nicht vollständig und soll lediglich veranschaulichen, wie die genannten Anforderungen auf die verschiedenen Datenelemente anzuwenden sind.

Tabelle 3. Anforderungen an die Speicherung von Kontodatenelementen

		Datenelemente	Speicheranforderungen	Erforderlich, um gespeicherte Daten unlesbar zu machen
Kontodaten	Karteninhaberdaten	Primäre Kontonummer (PAN)	Die Speicherung wird auf ein Minimum beschränkt, wie in Anforderung 3.2 definiert.	Ja, wie in Anforderung 3.5 definiert
		Name des Karteninhabers	Die Speicherung wird auf ein Minimum beschränkt, wie in Anforderung 3.2 definiert[2]	Nein
		Dienstleistungskodex		
		Ablaufdatum		
	Sensible Authentifizierungsdaten	Vollständige Nachverfolgungsdaten	Kann nach der Autorisierung gemäß Anforderung 3.3.1 nicht gespeichert werden[3]	Ja, Daten, die bis zum Abschluss der Autorisierung gespeichert werden, müssen mit starker Kryptographie gemäß Anforderung 3.3.2 geschützt werden.
		Kartenverifizierungscode		
		PIN/PIN-Sperre		

Wenn die PAN zusammen mit anderen Elementen der Karteninhaberdaten gespeichert wird, muss nur die PAN gemäß der PCI DSS-Anforderung 3.5.1 unlesbar gemacht werden.

Sensible Authentifizierungsdaten dürfen nach der Autorisierung nicht gespeichert werden, auch wenn sie verschlüsselt sind. Dies gilt auch für Umgebungen, in denen kein PAN vorhanden ist.

[2] Wenn die Daten in der gleichen Umgebung wie PAN vorhanden sind.
[3] Außer als erlaubt für Herausgeber und Unternehmen, die herausgebende Dienstleistungen unterstützen. Anforderungen an Herausgeber und herausgebende Dienstleistungen sind in Anforderung 3.3.3 definiert.

3 Beziehung zwischen PCI-DSS- und PCI-SSC-Softwarestandards

PCI SSC unterstützt den Einsatz von sicherer Zahlungssoftware in Umgebungen mit Karteninhaberumgebungen (CDE) durch den Payment Application Datensicherheitsstandard (PA-DSS) und das Software Security Framework (SSF), das aus dem Secure Software Standard und dem Secure Software Lifecycle (Secure SLC) Standard besteht. Software, die vom PCI SSC validiert und gelistet ist, bietet die Gewissheit, dass die Software nach sicheren Verfahren entwickelt wurde und eine Reihe von Software-Sicherheitsanforderungen erfüllt.

Die PCI SSC-Programme für sichere Software enthalten Listen von Zahlungssoftware und Softwareanbietern, die als den geltenden PCI SSC-Software-Standards entsprechend validiert wurden.

- **Validierte Software**: Zahlungssoftware, die auf der Webseite des PCI SSC als validierte Zahlungsanwendung (PA-DSS) oder validierte Zahlungssoftware (der Secure Software Standard) aufgeführt ist, wurde von einem qualifizierten Bewerter bewertet, um zu bestätigen, dass die Software die Sicherheitsanforderungen dieses Standards erfüllt. Die Sicherheitsanforderungen in diesen Standards konzentrieren sich auf den Schutz der Integrität und Vertraulichkeit von Zahlungstransaktionen und Kontodaten.
- **Validierte Softwareanbieter**: Der Secure SLC Standard definiert Sicherheitsanforderungen für Softwareanbieter, um sichere Softwareentwicklungspraktiken in den gesamten Softwarelebenszyklus zu integrieren. Softwareanbieter, die den Secure SLC-Standard erfüllen, werden auf der PCI SSC-Webseite als „Sichere SLC-qualifizierte Anbieter" aufgeführt.

Hinweis: *PA-DSS und das zugehörige Programm werden im Oktober 2022 auslaufen. Die Ablaufdaten für PA-DSS-validierte Zahlungsanwendungen finden Sie in der PCI SSC Liste von validierten Zahlungsanwendungen. Nach Ablauf der Frist werden die Anträge als „Nur für bereits bestehende Einsätze akzeptabel" aufgeführt. Ob eine Entität eine PA-DSS-Anwendung mit einem abgelaufenen Eintrag weiterhin verwenden kann, liegt im Ermessen der Organisationen, die Konformitätsprogramme verwalten (z. B. Zahlungsmarken und Erwerber); Entitäten sollten sich für weitere Informationen an die interessierten Organisationen wenden.*

Weitere Informationen über den SSF oder PA-DSS finden Sie in den jeweiligen Programmleitfäden unter www.pcisecuritystandards.org.

Alle Software, die Kontodaten speichert, verarbeitet oder überträgt oder die sich auf die Sicherheit von Kontodaten oder eines CDE auswirken könnte, fällt in den Geltungsbereich der PCI DSS-Bewertung einer Entität. Die Verwendung von validierter Zahlungssoftware unterstützt zwar die Sicherheit des CDE einer Entität, aber die Verwendung einer solchen Software allein macht eine Entität noch nicht PCI DSS-konform. Die PCI DSS-Bewertung der Entität sollte die Verifizierung beinhalten, ob die Software ordnungsgemäß konfiguriert und sicher implementiert ist, um die geltenden PCI DSS-Anforderungen zu unterstützen. Zusätzlich, wenn eine PCI-gelistete Zahlungssoftware angepasst wurde, ist während der PCI DSS-Bewertung eine eingehendere Prüfung erforderlich, da die Software möglicherweise nicht mehr der ursprünglich validierten Version entspricht.

Da sich Sicherheitsbedrohungen ständig weiterentwickeln, bietet Software, die vom Anbieter nicht mehr unterstützt wird (z. B. wenn sie vom Anbieter als „Ende des Lebenszyklus" gekennzeichnet ist), möglicherweise nicht dasselbe Maß an Sicherheit wie unterstützte Versionen. Den Entitäten wird dringend empfohlen, ihre Software auf dem neuesten Stand zu halten und auf die neuesten verfügbaren Softwareversionen zu aktualisieren.

Entitäten, die ihre eigene Software entwickeln, werden ermutigt, sich auf die Software-Sicherheitsstandards des PCI SSC zu beziehen und die darin enthaltenen Anforderungen als bewährte Praktiken in ihren Entwicklungsumgebungen zu verwenden. Eine sichere Zahlungssoftware, die in einer PCI DSS-konformen Umgebung implementiert ist, trägt dazu bei, das Potenzial für Sicherheitsverletzungen zu minimieren, die zu einer Gefährdung von Kontodaten und Betrug führen können. Siehe Maßgeschneiderte und kundenspezifische Software.

Anwendbarkeit von PCI DSS auf Anbieter von Zahlungssoftware

PCI DSS kann auf einen Anbieter von Zahlungssoftware angewandt werden, wenn der Anbieter auch ein Dienstleistungsanbieter ist, der Kontodaten speichert, verarbeitet oder überträgt oder Zugang zu den Kontodaten seiner Kunden hat - beispielsweise in der Rolle eines Zahlungs-Dienstleistungsanbieters oder über Fernzugriff auf eine Kundenumgebung. Zu den Softwareanbietern, auf die PCI DSS anwendbar sein kann, gehören Anbieter von Zahlungsdiensten sowie Cloud-Dienstleistungs-Anbieter, die Zahlungsterminals in der Cloud, Software as a Service (SaaS), E-Commerce in der Cloud und andere Cloud-Zahlungsdienstleiste anbieten.

Maßgeschneiderte und kundenspezifische Software

Alle maßgeschneiderte und kundenspezifische Software, die Kontodaten speichert, verarbeitet oder überträgt oder die sich auf die Sicherheit von Kontodaten oder eines CDE auswirken könnte, fällt in den Geltungsbereich der PCI DSS-Bewertung einer Entität.

Maßgeschneiderte und kundenspezifische Software, die in Übereinstimmung mit einem der Standards des PCI SSC Software Security Framework entwickelt und gewartet wurde (der Secure Software Standard oder der Secure SLC Standard) unterstützt ein Entität bei der Erfüllung der PCI DSS-Anforderung 6.

Siehe Anhang F für weitere Einzelheiten.

Hinweis: *Die PCI DSS-Anforderung 6 gilt in vollem Geltungsbereich für maßgeschneiderte und kundenspezifische Software, die nicht in Übereinstimmung mit einem der Standards des PCI SSC Software Security Framework entwickelt und gewartet wurde. Entitäten, die Softwareanbieter mit der Entwicklung maßgeschneiderter oder kundenspezifischer Software verwenden, die sich auf die Sicherheit von Kontodaten oder ihres CDE auswirken könnte, sind dafür verantwortlich, dass diese Softwareanbieter die Software gemäß PCI DSS-Anforderung 6 entwickeln.*

4 Geltungsbereich der PCI-DSS-Anforderungen

PCI DSS-Anforderungen gelten für:

- Die Umgebung der Karteninhaberdaten (CDE), die folgende Komponenten umfasst:
  - Systemkomponenten, Personen und Prozessen, die Karteninhaberdaten und/oder sensible Authentifizierungsdaten speichern, verarbeiten und übertragen, und,
  - Systemkomponenten, die keine CHD/SAD speichern, verarbeiten oder übertragen dürfen, aber uneingeschränkt mit Systemkomponenten verbunden sind, die CHD/SAD speichern, verarbeiten oder übertragen.

UND

- Systemkomponenten, Personen und Prozesse, die die Sicherheit des CDE beeinträchtigen könnten.[4]

„Systemkomponenten" beinhalten Netzwerkgeräte, Server, Computergeräte, virtuelle Komponenten, Cloud-Komponenten und Software. Beispiele für Systemkomponenten sind unter anderem:

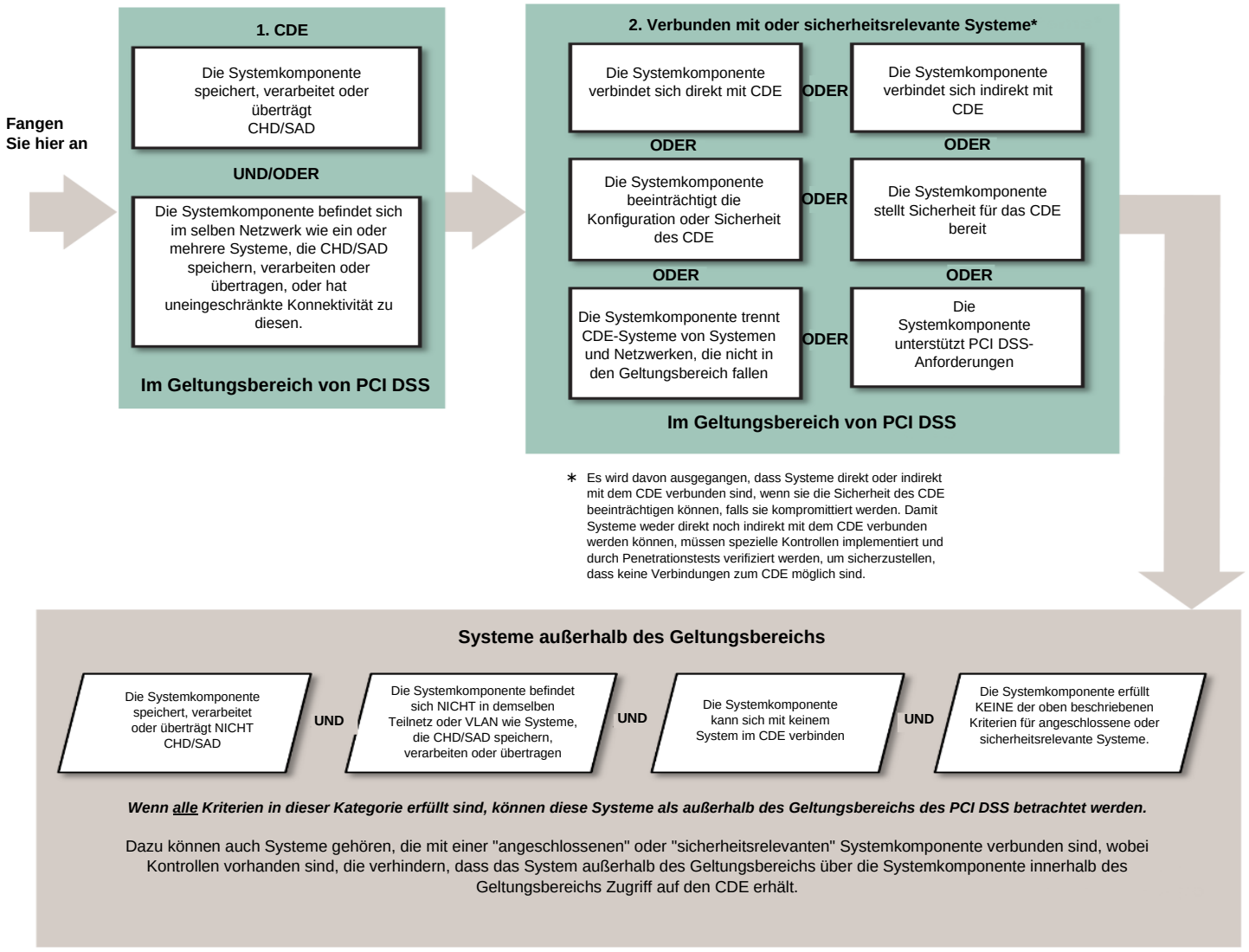
- Systeme, die Kontodaten (zum Beispiel Zahlungsterminals, Autorisierungssysteme, Clearing-Systeme, Middleware-Systeme für den Zahlungsverkehr, Back-Office-Systeme für den Zahlungsverkehr, Systeme für Einkaufswagen und Ladenfronten, Zahlungs-Gateways/Schalter-Systeme, Betrugsüberwachungssysteme) speichern, verarbeiten oder übertragen.
- Systeme, die Sicherheitsdienstleistungen bereitstellen (zum Beispiel Authentifizierungsserver, Zugriffskontrollserver, Sicherheitsinformationen- und Ereignisverwaltungssysteme (SIEM), physische Sicherheitssysteme (z. B. Badge Access oder CCTV), Multi-Faktor-Authentifizierungssysteme, Anti-Malware-Systeme).
- Systeme, die die Segmentierung erleichtern (z. B. interne Netzwerksicherheitskontrollen).
- Systeme, die die Sicherheit der Kontodaten oder des CDE beeinträchtigen könnten (zum Beispiel Server für die Namensauflösung oder die Umleitung des elektronischen Geschäftsverkehrs (Web)).
- Virtualisierungskomponenten wie virtuelle Maschinen, virtuelle Schalter/Router, virtuelle Geräte, virtuelle Anwendungen/Desktops und Hypervisoren.
- Cloud-Infrastruktur und -Komponenten, sowohl extern als auch vor Ort, einschließlich Instanziierungen von Containern oder Bildern, virtuelle private Clouds, Cloud-basierte Identitäts- und Zugriffsverwaltung, CDEs vor Ort oder in der Cloud, Service-Meshes mit containerisierten Anwendungen und Container-Orchestrierungstools.

[4] Für zusätzliche Anleitungen siehe *Informationsergänzung: Anleitungen für PCI DSS-Scoping und Netzwerksegmentierung* auf der PCI SSC-Webseite.

- Netzwerkkomponenten, beinhaltend, aber nicht beschränkt auf Netzwerksicherheitskontrollen, Schalter, Router, VoIP-Netzwerkgeräte, drahtlose Zugriffspunkte, Netzwerkgeräte und andere Sicherheitsgeräte.
- Servertypen, beinhaltend, aber nicht beschränkt auf Web-, Anwendungs-, Datenbank-, Authentifizierung-, Mail-, Proxy-, Network Time Protocol (NTP) und Domänennamensystem (DNS).
- Endbenutzergeräte wie Computer, Laptops, Arbeitsplätze, administrative Arbeitsplätze, Tablets und mobile Geräte.
- Drucker und Multifunktionsgeräte zum Scannen, Drucken und Faxen.
- Speicherung von Kontodaten in jedem Format (zum Beispiel Papier, Dateien, Audiodateien, Bilder und Videoaufzeichnungen).
- Anwendungen, Software und Softwarekomponenten, serverlose Anwendungen, einschließlich aller gekauften, abonnierten (z. B. Software-als Dienstleistung), maßgeschneiderte und kundenspezifische Software, einschließlich interne und externe (z. B. Internet-) Anwendungen.
- Werkzeuge, Code-Repositories und Systeme, die das Software-Konfigurationsmanagement oder die Bereitstellung von Objekten für CDE oder für Systeme, die Auswirkungen auf CDE haben können, implementieren.

Figur 1 zeigt Überlegungen zum Scoping von Systemkomponenten für PCI DSS.

Figur 1. Verständnis des PCI DSS-Scopings



Jährliche Bestätigung des PCI DSS-Geltungsbereichs

Der erste Schritt bei der Vorbereitung auf eine PCI DSS-Bewertung besteht für die Entität darin, den Geltungsbereich der Überprüfung genau zu bestimmen. Die bewertete Entität muss die Richtigkeit ihres PCI DSS-Geltungsbereichs gemäß PCI DSS-Anforderung 12.5.2 bestätigen, indem sie alle Standorte und Datenströme von Kontendaten identifiziert und alle Systeme identifiziert, die mit dem CDE verbunden sind, oder im Fall einer Kompromittierung Auswirkungen auf das CDE haben könnten (zum Beispiel Authentifizierungsserver, Server für den Fernzugriff, Protokollierungsserver), um sicherzustellen, dass sie im PCI DSS-Geltungsbereich enthalten sind. Während des Scoping-Prozesses sollten alle Arten von Systemen und Standorten in Betracht gezogen werden, einschließlich Backup-/Wiederherstellungsstandorte und Failover-Systeme.

Die Mindestschritte, die eine Entität unternehmen muss, um die Genauigkeit ihres PCI DSS-Geltungsbereichs zu bestätigen, sind in der PCI DSS-Anforderung 12.5.2 festgelegt. Es wird erwartet, dass die Entität Dokumentation aufbewahrt, aus denen hervorgeht, wie der PCI DSS-Geltungsbereich bestimmt wurde. Die Dokumentation wird zur Überprüfung durch den Bewerter und als Referenz bei der nächsten Bestätigung des PCI DSS-Geltungsbereichs von der Entität aufbewahrt. Bei jeder PCI DSS-Bewertung validiert der Bewerter, ob die Entität den Geltungsbereich der Bewertung korrekt definiert und dokumentiert hat.

***Hinweis**: Diese jährliche Bestätigung des PCI DSS-Geltungsbereichs ist in der PCI DSS-Anforderung 12.5.2 definiert und ist eine Aktivität, die von der Entität durchgeführt werden sollte. Diese Aktivität ist nicht mit der Scoping-Bestätigung identisch, die der Bewerter der Entität während der Bewertung durchgeführt hat, und soll auch nicht durch diese ersetzt werden.*

Segmentierung

Die Segmentierung (oder Isolierung) des CDE vom Rest des Netzwerks einer Entität ist keine des PCI DSS-Anforderung. Es wird jedoch nachdrücklich als ein Verfahren empfohlen, das das Risiko verringern kann:

- Geltungsbereich der PCI DSS-Bewertung
- Kosten der PCI DSS-Bewertung
- Kosten und Schwierigkeiten bei der Implementierung und Aufrechterhaltung von PCI DSS-Kontrollen
- Risiko für ein Entität in Bezug auf Zahlungskartenkontodaten (reduziert durch Konsolidierung dieser Daten an weniger, besser kontrollierten Standorten)

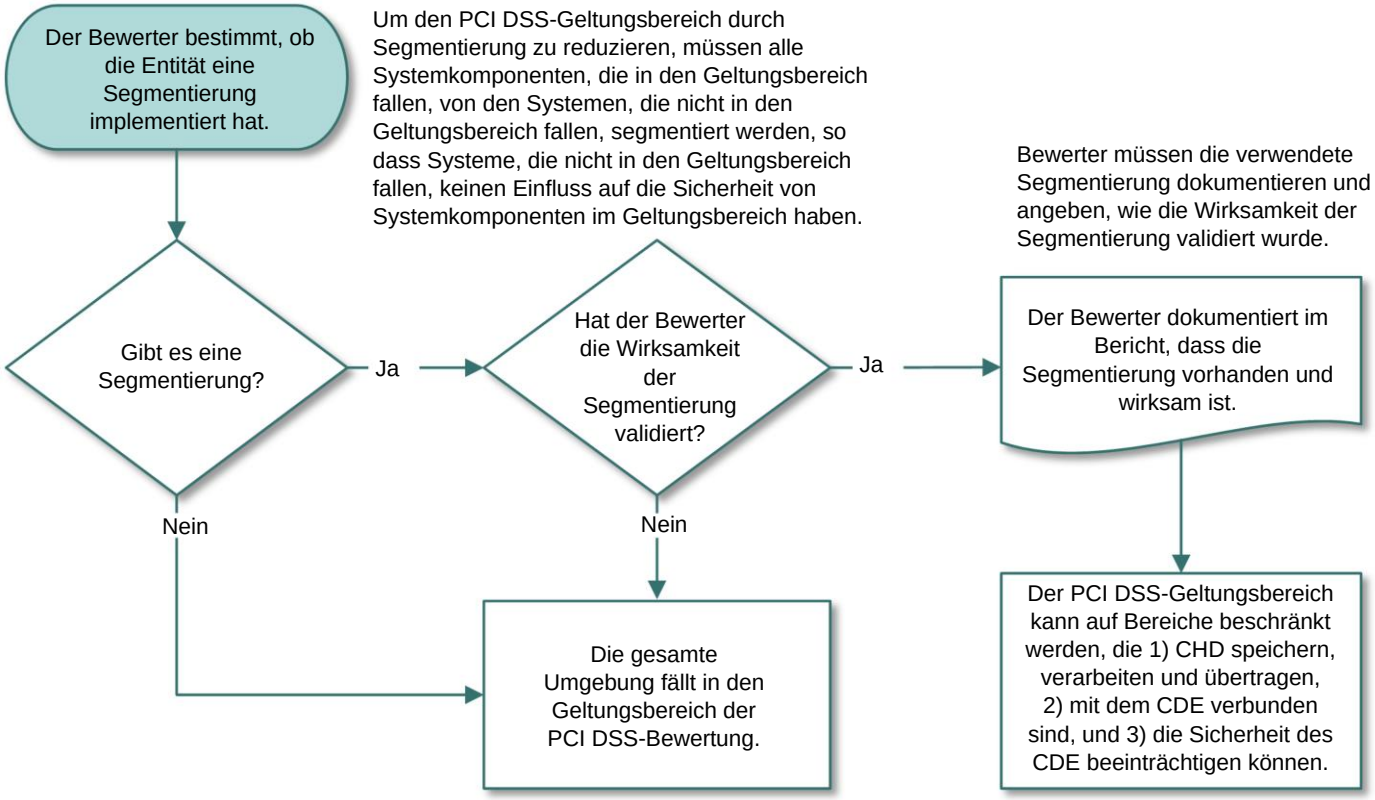
Ohne angemessene Segmentierung (manchmal als „flaches Netzwerk" bezeichnet) fällt das gesamte Netzwerk in den Geltungsbereich der PCI DSS-Bewertung. Die Segmentierung kann durch eine Reihe von physischen oder logischen Methoden erreicht werden, zum Beispiel durch ordnungsgemäß konfigurierte interne Netzsicherheitskontrollen, Router mit strengen Zugriffskontrolllisten oder andere Technologien, die den Zugriff auf ein bestimmtes Segment eines Netzwerks beschränken. Damit eine Systemkomponente als nicht in den Geltungsbereich des PCI DSS fallend betrachtet werden kann, muss sie ordnungsgemäß vom CDE segmentiert (isoliert) sein, so dass die nicht in den Geltungsbereich fallende Systemkomponente die Sicherheit des CDE nicht beeinträchtigen kann, selbst wenn diese Komponente kompromittiert wurde.

Eine wichtige Voraussetzung für die Verringerung des Geltungsbereichs des CDE ist ein klares Verständnis der geschäftlichen Anforderungen und Prozesse im Zusammenhang mit der Speicherung, Verarbeitung und Übertragung von Kontodaten. Die Beschränkung von Kontodaten auf möglichst wenige Standorte durch die Beseitigung unnötiger Daten und die Konsolidierung notwendiger Daten kann eine Umstellung langjähriger Geschäftspraktiken erfordern.

Die Dokumentation des Kontodatenflusses anhand eines Datenflussdiagramms hilft einer Entität, vollständig zu verstehen, wie die Kontodaten in eine Organisation gelangen, wo sie sich innerhalb des Organisation befinden und wie sie die verschiedenen Systeme innerhalb der Organisation durchlaufen. Datenflussdiagramme veranschaulichen auch alle Standorte, an denen Kontodaten gespeichert, verarbeitet und übertragen werden. Diese Informationen unterstützen eine Entität bei der Durchführung der Segmentierung und können auch dazu dienen, um zu bestätigen, dass die Segmentierung zur Isolierung des CDE von Netzwerken außerhalb des Geltungsbereichs verwendet wird.

Wenn eine Segmentierung zur Reduzierung des Geltungsbereiches der PCI DSS-Bewertung verwendet wird, muss der Bewerter verifizieren, ob die Segmentierung angemessen ist, um den Geltungsbereich der Bewertung zu reduzieren, wie in Figur 2 veranschaulicht. Auf einer hohen Ebene isoliert eine angemessene Segmentierung Systeme, die Kontodaten speichern, verarbeiten oder übertragen, von solchen, die dies nicht tun. Die Angemessenheit einer bestimmten Segmentierungsimplementierung ist jedoch sehr variabel und hängt von mehreren Faktoren ab, wie zum Beispiel der Konfiguration eines bestimmten Netzwerks, den eingesetzten Technologien und anderen Kontrollen, die implementiert werden können.

Figur 2. Segmentierung und Auswirkung auf den PCI DSS-Geltungsbereich



Drahtlos

Wenn drahtlose Technologien zur Speicherung, Verarbeitung oder Übertragung von Kontodaten verwendet werden (z. B. drahtlose POS-Geräte) oder wenn ein drahtloses lokales Netzwerk (WLAN) Teil des CDE ist oder mit diesem verbunden ist, gelten die PCI DSS-Anforderungen und Testprozeduren für die Sicherung drahtloser Umgebungen und müssen durchgeführt werden.

Erkennung von drahtlosen Betrügern muss gemäß PCI DSS-Anforderung 11.2.1 durchgeführt werden, selbst wenn drahtlos nicht im CDE verwendet wird und die Entität eine Richtlinie hat, die die Verwendung von drahtloser Technologie in seiner Umgebung verbietet. Der Grund dafür ist, dass ein drahtloser Zugriffspunkt leicht an ein Netzwerk angeschlossen werden kann, der Schwierigkeit, seine Anwesenheit zu erkennen, und das erhöhte Risiko, das durch nicht autorisierte drahtlose Geräte dargestellt wird.

Bevor eine drahtlose Technologie implementiert wird, sollte eine Entität den Bedarf an dieser Technologie sorgfältig gegen das Risiko abwägen. Erwägen Sie den Einsatz von drahtloser Technologie nur für nicht sensible Datenübertragung.

Verschlüsselte Karteninhaberdaten und Auswirkungen auf den PCI DSS-Geltungsbereich

Die Verschlüsselung von Karteninhaberdaten mit starker Kryptografie ist eine akzeptable Methode, um die Daten gemäß PCI DSS-Anforderung 3.5 unlesbar zu machen. Die Verschlüsselung allein reicht jedoch in der Regel nicht aus, um die Karteninhaberdaten aus dem Geltungsbereich des PCI DSS herauszunehmen, und macht den PCI DSS in dieser Umgebung nicht überflüssig. Die Umgebung der Einrichtung fällt aufgrund des Vorhandenseins von Karteninhaberdaten weiterhin in den Geltungsbereich des PCI DSS. In einer Umgebung, in der Händler mit Karten arbeiten, besteht zum Beispiel physischer Zugang zu den Zahlungskarten, um eine Transaktion abzuschließen, und es können auch Papierberichte oder Quittungen mit Karteninhaberdaten vorliegen. Ebenso in Umgebungen, in denen Händlerkarten nicht vorhanden sind, wie zum Beispiel im Versandhandel/Telefonbestellung und E-Commerce, werden Zahlungskartendaten über Kanäle bereitgestellt, die gemäß PCI DSS ausgewertet und geschützt werden müssen.

Die folgenden fallen alle in den Geltungsbereich von PCI DSS:

- Systeme zur Verschlüsselung und/oder Entschlüsselung von Karteninhaberdaten und Systeme zur Schlüsselverwaltung,
- Verschlüsselte Karteninhaberdaten, die nicht von den Verschlüsselungs- und Entschlüsselungs- und Schlüsselverwaltungsprozessen isoliert sind,
- Verschlüsselte Karteninhaberdaten, die sich auf einem System oder Medium befinden, das auch den Entschlüsselungsschlüssel enthält,
- Verschlüsselte Karteninhaberdaten, die sich in der gleichen Umgebung wie der Entschlüsselungsschlüssel befinden,
- Verschlüsselte Karteninhaberdaten, auf die eine Entität zugreifen kann, die auch Zugriff zum Entschlüsselungscode hat.

Hinweis: *Eine PCI-aufgelistete P2PE-Lösung kann die Anzahl der PCI DSS-Anforderungen für die Umgebung eines Händlers mit Karteninhaberdaten erheblich reduzieren. Die Anwendbarkeit des PCI DSS in der Händlerumgebung wird dadurch jedoch nicht vollständig aufgehoben.*

Verschlüsselte Karteninhaberdaten und Auswirkungen auf den PCI DSS-Geltungsbereich für dritte Dienstleistungsanbieter

Wenn ein dritter Dienstleistungsanbieter (TPSP) nur Daten empfängt und/oder speichert, die von einer anderen Entität verschlüsselt wurden, und wenn er nicht in der Lage ist, die Daten zu entschlüsseln, kann der TPSP die verschlüsselten Daten als nicht in den Anwendungsbereich fallend betrachten, wenn bestimmte Bedingungen erfüllt sind. Der Grund dafür ist, dass die Verantwortung für die Daten im Allgemeinen bei der Entität oder den Entitäten verbleibt, die in der Lage sind, die Daten zu entschlüsseln oder die Sicherheit der verschlüsselten Daten zu beeinflussen. Welche Partei für spezifische PCI DSS-Kontrollen verantwortlich ist, hängt von mehreren Faktoren ab, u. a. davon, wer Zugriff auf die Entschlüsselungsschlüssel hat, der Rolle, die jede Partei spielt, und der Vereinbarung zwischen den Parteien. Die Verantwortlichkeiten sollten klar definiert und dokumentiert werden, um sicherzustellen, dass sowohl der TPSP und die Entität, die die verschlüsselten Daten bereitstellt, wissen, welche Entität für welche Sicherheitskontrollen verantwortlich ist.

Beispielsweise empfängt und speichert ein TPSP, der Speicherdienstleistungen bereitstellt, verschlüsselte Karteninhaberdaten, die von Kunden zu Sicherungszwecken bereitgestellt werden. Dieser TPSP hat keinen Zugriff auf die Ver- und Entschlüsselungscodes und führt auch keine Schlüsselverwaltung für seine Kunden durch. Der TPSP kann solche verschlüsselten Daten bei der Bestimmung des PCI DSS-Geltungsbereichs ausschließen. Der TPSP ist jedoch im Rahmen seiner Dienstleistungsvereinbarungen mit seinen Kunden für die Kontrolle des Zugriffs auf den verschlüsselten Datenspeicher verantwortlich.

Die Verantwortung dafür, dass die verschlüsselten Daten und die kryptografischen Schlüssel gemäß den geltenden PCI DSS-Anforderungen geschützt sind, wird häufig zwischen Entitäten geteilt. Im obigen Beispiel bestimmt der Kunde, wer von seinem Personal autorisiert ist, auf die Speichermedien zuzugreifen, und der Speicher ist für die Verwaltung der physischen und/oder logischen Zugriffskontrollen verantwortlich, um sicherzustellen, dass nur vom Kunden autorisierte Personen Zugriff auf die Speichermedien erhalten. Die spezifischen PCI DSS-Anforderungen, die für einen TPSP gelten, hängen von den bereitgestellten Dienstleistungen und der Vereinbarung zwischen den beiden Parteien ab. Im Beispiel eines TPSP, der Speicherdienstleistungen anbietet, müssen die physischen und logischen Zugriffskontrollen, die der TPSP bereitstellt, mindestens jährlich überprüft werden. Diese Überprüfung könnte als Teil der PCI DSS-Bewertung des Händlers durchgeführt werden, oder alternativ dazu könnte der TPSP die Überprüfung durchführen und die Kontrollen validieren, wobei dem Händler entsprechende Nachweise bereitgestellt werden. Informationen zu „angemessenen Nachweisen“ siehe Optionen für TPSPs zur Validierung der PCI DSS-Konformität für TPSP-Dienstleistungen, die die PCI DSS-Anforderungen der Kunden erfüllen. Fehler! Referenzquelle nicht gefunden.

Als ein weiteres Beispiel, ein TPSP, der nur verschlüsselte Karteninhaberdaten zum Zwecke der Weiterleitung an andere Stellen erhält und keinen Zugriff auf die Daten oder kryptografischen Schlüssel hat, trägt möglicherweise keine PCI DSS-Verantwortung für diese

verschlüsselten Daten. In diesem Szenario, in dem der TPSP keine Sicherheitsdienstleistungen oder Zugriffskontrollen anbietet, kann er als öffentliches oder nicht vertrauenswürdiges Netzwerk betrachtet werden, und es liegt in der Verantwortung der Entität(en), die Kontodaten über das Netzwerk des TPSP zu senden/empfangen, um sicherzustellen, dass PCI DSS-Kontrollen zum Schutz der übertragenen Daten angewendet werden.

Verwendung von Drittanbietern von Dienstleistungen

Eine Entität (in diesem Abschnitt als "Kunde" bezeichnet) könnte sich dafür entscheiden, einen Drittanbieter von Dienstleistungen (TPSP) mit der Speicherung, Verarbeitung oder Übertragung von Kontodaten oder der Verwaltung von Systemkomponenten im Namen des Kunden zu verwenden. Die Verwendung eines TPSP kann Auswirkungen auf die Sicherheit des CDE eines Kunden haben.

Hinweis: *Die Verwendung eines PCI DSS-konformen TPSP macht einen Kunden nicht PCI DSS-konform und enthebt ihn auch nicht der Verantwortung für seine eigene PCI DSS-Konformität. Selbst wenn ein Kunde einen TPSP zur Erfüllung aller Kontodatenfunktionen einsetzt, bleibt er für die Bestätigung seiner eigenen Konformität verantwortlich, wie sie von Organisationen verlangt wird, die Konformitätsprogramme verwalten (zum Beispiel Zahlungsmarken und Erwerber). Kunden sollten sich bezüglich aller Anforderungen an die Organisationen wenden, die sie interessieren.*

Die Verwendung TPSPs und die Auswirkung auf Kunden, die die PCI DSS-Anforderung 12.8 erfüllen

Es gibt viele verschiedene Szenarien, in denen ein Kunde einen oder mehrere TPSPs für Funktionen innerhalb oder im Zusammenhang mit dem CDE des Kunden verwenden kann. In allen Szenarien, in denen ein TPSP verwendet wird, muss der Kunde den PCI DSS-Konformitätsstatus aller seiner TPSPs gemäß Anforderung 12.8 verwalten und überwachen, einschließlich TPSPs, die:

- Zugriff auf den CDE des Kunden haben,
- Systemkomponenten im Auftrag des Kunden verwalten, und/oder
- Die Sicherheit des CDE des Kunden beeinträchtigen können.

Die Verwaltung von TPSP gemäß Anforderung 12.8 beinhaltet die Durchführung einer gebührenden Sorgfalt, das Vorhandensein geeigneter Vereinbarungen, die Identifizierung, welche Anforderungen für den Kunden und welche für den TPSP gelten, und die mindestens jährliche Überwachung des Konformitätsstatus von TPSP.

Die Anforderung 12.8 schreibt nicht vor, dass die TPSP des Kunden PCI DSS-konform sein müssen, sondern nur, dass der Kunde ihren Konformitätsstatus wie in der Anforderung angegeben überwacht. Daher muss eine TPSPs nicht PCI DSS-konform sein,sodass ihr Kunde die Anforderung 12.8 erfüllen kann.

Auswirkungen der Verwendung von TPSPs für Dienstleistungen, die die PCI DSS-Anforderungen der Kunden erfüllen

Wenn der TPSP eine Dienstleistung bereitstellt, die eine oder mehrere PCI DSS-Anforderungen im Namen des Kunden erfüllt, oder wenn sich diese Dienstleistung auf die Sicherheit des CDE des Kunden auswirken kann, dann fallen diese Anforderungen in den Anwendungsbereich der Bewertung des Kunden, und die Konformität dieser Dienstleistung hat Auswirkungen auf die PCI DSS-Konformität des Kunden. Der TPSP muss nachweisen, dass er die geltenden PCI DSS-Anforderungen erfüllt, damit diese Anforderungen für seine Kunden gelten. Beauftragt eine Entität beispielsweise einen TPSP mit der Verwaltung ihrer Netzwerksicherheitskontrollen und der TPSP weist nicht nach, dass er die geltenden Anforderungen der PCI DSS-Anforderung 1 erfüllt, dann sind diese Anforderungen für die Bewertung durch den Kunden nicht erfüllt. Als weiteres Beispiel, TPSPs, die im Auftrag von Kunden Sicherungskopien von Karteninhaberdaten aufbewahren, müssten die geltenden Anforderungen in Bezug auf Zugriffskontrollen, physische Sicherheit usw. erfüllen, damit ihre Kunden diese Anforderungen bei ihren Bewertungen berücksichtigen können.

Wichtigkeit des Verständnisses der Verantwortlichkeiten zwischen TPSP-Kunden und TPSP

Kunden und TPSP sollten Folgendes klar erkennen und verstehen:

- Die Dienstleistungen und Systemkomponenten, die in den Anwendungsbereich der PCI DSS-Bewertung des TPSP fallen,
- Die spezifischen PCI DSS-Anforderungen und Unteranforderungen, die von der PCI DSS-Bewertung des TPSP abgedeckt werden,
- Alle Anforderungen, die die Kunden des TPSP in ihre eigenen PCI DSS-Bewertungen aufnehmen müssen, und
- Alle PCI DSS-Anforderungen, für die der TPSP und seine Kunden gemeinsam verantwortlich sind.

Ein Cloud-Anbieter sollte beispielsweise klar definieren, welche seiner IP-Adressen im Rahmen seines vierteljährlichen Schwachstellen-Scan-Prozesses gescannt werden und welche IP-Adressen von seinen Kunden gescannt werden müssen.

Gemäß Anforderung 12.9.2 sind TPSP verpflichtet, Anfragen ihrer Kunden nach Informationen über den Status der PCI DSS-Konformität des TPSP in Bezug auf die für die Kunden erbrachten Dienstleistungen zu unterstützen und darüber Auskunft zu geben, welche PCI DSS-Anforderungen in die Verantwortung des TPSP und welche in die Verantwortung des Kunden fallen und welche Verantwortungen zwischen dem Kunden und dem TPSP bestehen. Unter *Tipps und Tools zum Verständnis von PCI DSS v4.0* finden Sie eine Vorlage für eine Verantwortungsmatrix, die zur Dokumentation und Klärung der Aufteilung der Verantwortlichkeiten zwischen TPSP und Kunden verwendet werden kann.

Optionen für TPSPs zur Validierung der PCI DSS-Konformität für TPSP-Dienstleistungen, die die PCI DSS-Anforderungen der Kunden erfüllen

TPSPs sind dafür verantwortlich, ihre PCI DSS-Konformität nachzuweisen, wie es von Organisationen gefordert wird, die Konformitätsprogramme verwalten (z. B. Zahlungsmarken und Erwerber). TPSPs sollten sich bezüglich aller Anforderungen an die Organisationen wenden, die sie interessieren.

Wenn ein TPSP Dienstleistungen bereitstellt, die dazu dienen, die PCI DSS-Anforderungen eines Kunden zu erfüllen oder deren Erfüllung zu erleichtern, oder die sich auf die Sicherheit des CDE eines Kunden auswirken können, dann fallen diese Anforderungen in den Anwendungsbereich der PCI DSS-Bewertungen des Kunden. Es gibt zwei Optionen für TPSPs, um die Konformität in diesem Szenario zu validieren:

- **Jährliche Bewertung**: Der TPSP unterzieht sich einer/einer jährlichen PCI-DSS-Bewertung(en) und legt seinen Kunden Nachweise vor, um zu zeigen, dass der TPSP die geltenden PCI-DSS-Anforderungen erfüllt; oder
- **Mehrere Bewertungen auf Abruf**: Wenn ein TPSP keiner jährlichen PCI-DSS-Bewertung unterzogen wird, muss er sich auf Anfrage seiner Kunden einer Bewertung unterziehen und/oder an jeder PCI-DSS-Bewertung seiner Kunden teilnehmen, wobei die Ergebnisse jeder Überprüfung dem/den jeweiligen Kunden(n) bereitgestellt werden.

Wenn der TPSP sich einer eigenen PCI-DSS-Bewertung unterzieht, wird erwartet, dass er seinen Kunden ausreichende Nachweise vorlegt, um zu verifizieren, dass der Geltungsbereich der PCI-DSS-Bewertung des TPSP die für den Kunden geltenden Dienstleistungen umfasst und dass die relevanten PCI-DSS-Anforderungen untersucht wurden und festgestellt wurde, dass sie vorhanden sind. Wenn der Anbieter über eine PCI-DSS-Konformitätsbescheinigung (AOC) verfügt, dann wird erwartet, dass der TPSP den Kunden das AOC auf Anfrage zur Verfügung stellt. Der Kunde kann auch relevante Abschnitte des PCI DSS Berichts über die Konformität (ROC) des TPSP anfordern. Das ROC kann geschwärzt werden, um vertrauliche Informationen zu schützen.

Wenn der TPSP keiner eigenen PCI-DSS-Bewertung unterzogen wird und daher kein AOC hat, wird vom TPSP erwartet, dass er spezifische Nachweise in Bezug auf die geltenden PCI-DSS-Anforderungen vorlegt, damit der Kunde (oder sein Bewerter) den bestätigen kann, dass der TPSP diese PCI-DSS-Anforderungen erfüllt.

Präsenz von TPSPs auf einer Zahlungsmarkenliste(n) von PCI-DSS-einhaltenden Dienstleistungsanbietern

Für einen Kunden, der den Konformitätsstatus eines TPSP gemäß Anforderung 12.8 überwacht, kann die Präsenz des TPSP auf der Liste der PCI-DSS-konformen Dienstleistungsanbieter einer Zahlungsmarke ***ein ausreichender Beweis*** für den Compliance-Status des TPSP sein, wenn aus der Liste klar hervorgeht, dass die auf den Kunden anwendbaren Dienstleistungen durch die PCI-DSS-Bewertung des TPSP abgedeckt wurden. Wenn dies aus der Liste nicht ersichtlich ist, sollte der Kunde eine andere schriftliche Bestätigung einholen, die den PCI-DSS-Konformitätsstatus des TPSP adressiert.

Für einen Kunden, der nach einem Nachweis der PCI-DSS-Konformität für Anforderungen sucht, die ein TPSP im Auftrag eines Kunden erfüllt oder bei denen die bereitgestellte Dienstleistung die Sicherheit der CDE des Kunden beeinträchtigen kann, ist die Präsenz des TPSP auf der Liste der PCI-DSS-konformen Dienstleistungsanbieter einer Zahlungsmarke ***kein ausreichender Beweis***, dass die geltenden PCI-DSS-Anforderungen für diesen TPSP in die Bewertung beinhaltet wurden. Wenn der TPSP über ein PCI-DSS-AOC verfügt, wird es den Kunden auf Anfrage voraussichtlich bereitgestellt.

5 Bewährte Praktiken für die Implementierung von PCI DSS in Business-as-Usual-Prozessen

Eine Entität, die Business-as-Usual-Prozesse, auch bekannt alsBAU, als Teil ihrer Gesamtsicherheitsstrategie implementiert, ergreift Maßnahmen, um sicherzustellen, dass Sicherheitskontrollen, die zum Schutz von Daten und einer Umgebung implementiert wurden, weiterhin korrekt implementiert werden und ordnungsgemäß im normalen Geschäftsverlauf funktionieren.

Einige PCI-DSS-Anforderungen sollen als BAU-Prozesse fungieren, indem sie Sicherheitskontrollen überwachen, um ihre Wirksamkeit kontinuierlich sicherzustellen. Diese Aufsicht durch die Entität trägt dazu bei, eine angemessene Sicherheit dafür zu bieten, dass die Konformität seiner Umgebung zwischen den PCI-DSS-Bewertungen gewahrt wird. Obwohl derzeit einige BAU-Anforderungen im Standard definiert sind, sollte eine Entität nach Möglichkeit zusätzliche BAU-Prozesse anwenden, die für ihre Organisation und Umgebung spezifisch sind. BAU-Prozesse sind eine Möglichkeit zu verifizieren, ob automatisierte und manuelle Kontrollen wie erwartet funktionieren. Unabhängig davon, ob eine PCI-DSS-Anforderung automatisiert oder manuell ist, ist es für BAU-Prozesse wichtig, Anomalien zu erkennen und zu alarmieren und zu melden, damit die zuständigen Personen die Situation rechtzeitig angehen.

Beispiele dafür, wie PCI DSS in BAU-Aktivitäten integriert werden sollte, sind unter anderem:

- Zuweisung der Gesamtverantwortung und Rechenschaftspflicht für die PCI-DSS-Konformität an eine Einzelperson oder ein Team. Dies kann eine von der Geschäftsleitung festgelegte Charta für ein bestimmtes PCI-DSS-Konformitätsprogramm und eine Mitteilung an die Geschäftsleitung umfassen.
- Entwicklung von Leistungskennzahlen zur Messung der Wirksamkeit von Sicherheitsinitiativen und kontinuierliche Überwachung von Sicherheitskontrollen, einschließlich derer, auf die man sich stark verlässt, wie zum Beispiel Netzwerksicherheitskontrollen, Einbruchserkennungssysteme/Einbruchsverhinderungssysteme (IDS/IPS), Anti-Malware-Lösungen und Zugriffskontrollen, um sicherzustellen, dass sie effektiv und wie vorgesehen funktionieren.
- Häufigere Überprüfung protokollierter Daten, um Einblicke in Trends oder Verhaltensweisen zu gewinnen, die bei alleiniger Überwachung möglicherweise nicht offensichtlich sind.
- Sicherstellung, dass alle Fehler bei den Sicherheitskontrollen erkannt und umgehend beantwortet werden. Prozesse zur Antwort auf Sicherheitskontrollfehler sollten Folgendes umfassen:
  - Wiederherstellung der Sicherheitskontrolle.
  - Identifizierung der Fehlerursache.
  - Identifizierung und Behebung von Sicherheitsproblemen, die während des Versagens der Sicherheitskontrolle aufgetreten sind.
  - Implementierung von Minderungsmaßnahmen, wie zum Beispiel Prozess- oder technische Kontrollen, um zu verhindern, dass die Ursache des Fehlers erneut auftritt.
  - Wiederaufnahme der Überwachung der Sicherheitskontrolle, möglicherweise mit verbesserter Überwachung für einen bestimmten Zeitraum, um zu überprüfen, ob die Kontrolle effektiv funktioniert.

- Überprüfung von Änderungen, die Sicherheitsrisiken für die Umgebung darstellen könnten (zum Beispiel das Hinzufügen neuer Systeme, Änderungen der System- oder Netzwerkkonfigurationen), bevor die Änderung abgeschlossen wird, einschließlich der folgenden Punkte:
  - Durchführung einer Risikobewertung durch, um die potenziellen Auswirkungen auf den PCI-DSS-Geltungsbereich zu bestimmen (zum Beispiel könnte eine neue Regel zur Kontrolle der Netzwerksicherheit, die die Konnektivität zwischen einem System in der CDE und einem anderen System zulässt, zusätzliche Systeme oder Netzwerke in den Geltungsbereich von PCI DSS bringen).
  - Identifizierung der PCI-DSS-Anforderungen, die für von den Änderungen betroffene Systeme und Netzwerke gelten (wenn beispielsweise ein neues System in den Geltungsbereich von PCI DSS fällt, müsste es gemäß den Systemkonfigurationsstandards konfiguriert werden, einschließlich Mechanismen zur Änderungserkennung, Anti-Malware-Software, Patches und Audit-Protokollierung. Diese neuen Systeme und Netzwerke müssten in das Inventar der untersuchten Systemkomponenten und in den vierteljährlichen Zeitplan für die Schwachstellenüberprüfung aufgenommen werden.)
  - Aktualisierung des PCI DSS-Geltungsbereichs und gegebenenfalls Implementierung von Sicherheitskontrollen.
  - Aktualisierung der Dokumentation, um die implementierten Änderungen widerzuspiegeln.
- Überprüfung der Auswirkungen auf den Geltungsbereich und die Anforderungen des PCI DSS bei Änderungen der Organisationsstruktur (zum Beispiel bei einer Unternehmensfusion oder -übernahme).
- Regelmäßige Überprüfung externer Verbindungen und des Zugriffs von Drittanbietern.
- Für Entitäten, die Dritte für die Softwareentwicklung einsetzen, regelmäßige Bestätigung, dass diese Softwareentwicklungsaktivitäten weiterhin die Softwareentwicklungsanforderungen in Anforderung 6 erfüllen.
- Durchführung regelmäßiger Überprüfungen, um zu bestätigen, dass die PCI-DSS-Anforderungen weiterhin bestehen und das Personal etablierte Prozesse einhält. Regelmäßige Überprüfungen sollten alle Einrichtungen und Standorte abdecken, einschließlich Einzelhandelsgeschäfte und Rechenzentren, unabhängig davon, ob sie selbst verwaltet werden oder ein TPSP verwendet wird. Beispielsweise können regelmäßige Überprüfungen verwendet werden, um zu bestätigen, dass Konfigurationsstandards auf die anwendbaren Systeme angewendet wurden, Standardanbieterkonten und Passwörter werden entfernt oder deaktiviert, Patches und Anti-Malware-Lösungen sind auf dem neuesten Stand, Audit-Protokolle werden überprüft und so weiter. Die Häufigkeit der regelmäßigen Überprüfungen sollte von der Entität entsprechend der Größe und Komplexität ihrer Umgebung festgelegt werden, sofern im PCI DSS nichts anderes angegeben ist.

Diese Überprüfungen können auch verwendet werden, um zu verifizieren, ob die erforderlichen Nachweise für eine PCI-DSS-Bewertung aufrechterhalten werden. Beispielsweise sind Nachweise von Audit-Protokollen, Schwachstellen-Scan-Berichten und Überprüfungen von Regelsätzen für die Netzwerksicherheitskontrolle erforderlich, um die Entität bei der Vorbereitung auf ihre nächste PCI-DSS-Bewertung zu unterstützen.

- Etablierung der Kommunikation mit allen betroffenen Parteien, sowohl extern als auch intern, über neu identifizierte Bedrohungen und Änderungen der Organisationsstruktur. Kommunikationsmaterialien sollten den Empfängern helfen, die Auswirkungen von Bedrohungen, Maßnahmen zur Schadensbegrenzung und Kontaktstellen für weitere Informationen oder Eskalationen zu verstehen.

- Überprüfung von Hardware- und Softwaretechnologien mindestens alle 12 Monate, um zu bestätigen, dass sie weiterhin vom Anbieter unterstützt werden und die Sicherheitsanforderungen der Entität, einschließlich PCI DSS, erfüllen können. Wenn Technologien vom Anbieter nicht mehr unterstützt werden oder die Sicherheitsanforderungen der Entität nicht erfüllen können, sollte die Entität einen Sanierungsplan erstellen, einschließlich des Austauschs der Technologie, falls erforderlich.

Hinweis: *Einige bewährte Praktiken in diesem Abschnitt sind auch als PCI DSS-Anforderungen für bestimmte Entitäten enthalten. Zum Beispiel diejenigen, die sich einer vollständigen PCI DSS-Bewertung unterziehen, Dienstleistungsanbieter, die nach den zusätzlichen „Nur-Dienstleistungsanbieter"-Anforderungen validieren, und bestimmte Entitäten, die gemäß Anhang A3 validieren müssen: Ergänzende Validierung für bestimmte Entitäten.*

Jede Entität sollte in Erwägung ziehen, diese bewährten Praktiken in ihre Umgebung zu implementieren, auch wenn die Entität nicht verpflichtet ist, sie zu validieren (zum Beispiel Händler, die sich einer Selbstbewertung unterziehen).

Siehe *Bewährte Praktiken zur Aufrechterhaltung der PCI DSS-Konformität* in der Dokumentenbibliothek auf der PCI SSC-Webseite für zusätzliche Anleitungen.

6 Für Bewerter: Stichproben für PCI-DSS-Bewertungen

Stichproben sind eine Option für Bewerter, die PCI DSS-Bewertungen durchführen, um den Bewertungsprozess zu erleichtern, wenn eine große Anzahl von Elementen in einer zu testenden Population vorhanden ist.

Es ist zwar akzeptabel, dass ein Bewerter im Rahmen seiner Überprüfung der PCI DSS-Konformität einer Entität Stichproben aus ähnlichen Elementen einer zu prüfenden Population zieht, es ist jedoch nicht akzeptabel, dass eine Entität die PCI DSS-Anforderungen nur auf eine Stichprobe seiner Umgebung anwendet (zum Beispiel gelten die Anforderungen für vierteljährliche Schwachstellen-Scans für alle Systemkomponenten). Ebenso ist es nicht akzeptabel, wenn ein Bewerter nur eine Stichprobe der PCI DSS-Anforderungen auf Konformität überprüft.

Obwohl die Bewerter bei Stichproben weniger als 100 % einer bestimmten Stichprobenpopulation testen können, sollten sie stets eine möglichst vollständige Überprüfung anstreben. Bewerter werden ermutigt, automatisierte Prozesse oder andere Mechanismen zu verwenden, wenn die gesamte Population, unabhängig von ihrer Größe, schnell und effizient mit minimalen Auswirkungen auf die Ressourcen der zu prüfenden Einheit getestet werden kann. Stehen keine automatisierten Verfahren zur Verfügung, um 100 % einer Population zu testen, sind Stichproben ein ebenso akzeptabler Ansatz.

Unter Berücksichtigung des gesamten Geltungsbereichs, der Komplexität und der Konsistenz der zu bewertenden Umgebung sowie der Art (automatisiert oder manuell) der Prozesse, die von einer Entität zur Erfüllung einer Anforderung eingesetzt werden, kann der Bewerter unabhängig repräsentative Stichproben aus den zu prüfenden Populationen auswählen, um die Konformität der PCI DSS-Anforderungen durch die Entität zu bewerten. Die Stichproben müssen eine repräsentative Auswahl aller Varianten der Population darstellen und ausreichend groß sein, um dem Bewerter die Gewissheit zu geben, dass die Kontrollen in der gesamten Population wie erwartet durchgeführt werden. Beim Testen der periodischen Leistung einer Anforderung (zum Beispiel wöchentlich, vierteljährlich oder in regelmäßigen Abständen) sollte der Bewerter versuchen, eine Stichprobe auszuwählen, die den gesamten Bewertungszeitraum abdeckt, so dass der Bewerter ein angemessenes Urteil darüber abgeben kann, dass die Anforderung während des gesamten Bewertungszeitraums erfüllt wurde. Testen derselben Stichprobe von Elementen Jahr für Jahr könnte dazu führen, dass unbekannte Schwankungen bei den nicht untersuchten Elementen unentdeckt bleiben. Bewerter müssen die Gründe für die Stichprobenziehung bei jeder Bewertung erneut überprüfen und frühere Stichprobenreihen berücksichtigen. Für jede Bewertung müssen unterschiedliche Proben ausgewählt werden.

Die geeignete Auswahl der Stichprobe hängt davon ab, was bei der Untersuchung der Stichprobenelemente berücksichtigt werden soll. Zum Beispiel, Bestimmen des Vorhandenseins von Anti-Malware auf Servern, von denen bekannt ist, dass sie von bösartiger Software betroffen sind, kann dazu führen, dass die Population alle Server in der Umgebung oder alle Server in der Umgebung ist, auf denen ein bestimmtes Betriebssystem ausgeführt wird, oder alle Server, die keine Mainframes sind usw. Die Auswahl einer geeigneten Stichprobe würde dann Vertreter ALLER Mitglieder der identifizierten Population umfassen, einschließlich aller Server, auf denen das ermittelte Betriebssystem einschließlich aller Versionen läuft, sowie der Server innerhalb der Population, die für unterschiedliche Funktionen verwendet werden (Webserver, Anwendungsserver, Datenbankserver usw.).

Wird ein spezifisches Konfigurationselement betrachtet, kann die Population in geeigneter Weise unterteilt und getrennte Stichprobengruppen festgelegt werden. Zum Beispiel ist eine Stichprobe aller Server möglicherweise nicht geeignet, wenn eine Betriebssystemkonfigurationseinstellung überprüft wird, wenn verschiedene Betriebssysteme in der Umgebung vorhanden sind. In diesem Fall

wären Stichproben von jedem Betriebssystemtyp geeignet, um zu identifizieren, ob die Konfiguration für jedes Betriebssystem richtig eingestellt wurde. Jeder Stichprobensatz sollte Server enthalten, die für jeden Betriebssystemtyp, einschließlich Version, sowie repräsentative Funktionen repräsentativ sind.

Andere Beispiele für Stichproben beinhalten die Auswahl von Personal mit ähnlichen oder unterschiedlichen Rollen, basierend auf der zu bewertenden Anforderung, zum Beispiel eine Stichprobe von Verwaltern im Vergleich zu einer Stichprobe aller Mitarbeiter.

Der Bewerter muss bei der Planung, Durchführung und Bewertung der Stichprobe professionelles Urteilsvermögen anwenden, um seine Schlussfolgerung darüber zu stützen, ob und wie die Entität eine Anforderung erfüllt hat. Das Ziel des Bewerters beim Stichprobenverfahren besteht darin, genügend Beweise zu erhalten, um eine vernünftige Grundlage für seine Meinung zu haben. Bei der unabhängigen Auswahl von Stichproben sollten Bewerter Folgendes berücksichtigen:

- Der Bewerter muss die Stichprobe aus der gesamten Population ohne Einflussnahme der bewerteten Entität auswählen.
- Verfügt die Entität über standardisierte Prozesse und Kontrollen, die Konsistenz gewährleisten und die auf jedes Element der Population angewendet werden, kann die Stichprobe kleiner sein, als wenn die Entität über keine standardisierten Prozesse/Kontrollen verfügt. Die Stichprobe muss groß genug sein, um dem Bewerter hinreichende Sicherheit bereitzustellen, dass die Elemente in der Population den standardisierten Prozessen entsprechen, die auf jedes Element in der Population angewendet werden. Der Assessor muss verifizieren, ob die standardisierten Kontrollen implementiert sind und effektiv funktionieren.
- Wenn die Entität über mehr als eine Art standardisierter Prozesse verfügt (zum Beispiel für verschiedene Arten von Geschäftseinrichtungen/Systemkomponenten), dann muss die Stichprobe Elemente enthalten, die jeder Prozessart unterliegen. Populationen könnten zum Beispiel in Untergruppen unterteilt werden, basierend auf Merkmalen, die sich auf die Konsistenz der bewerteten Anforderungen auswirken können, wie zum Beispiel die Verwendung verschiedener Prozesse oder Tools. Aus jeder Unterpopulation würden dann Stichproben ausgewählt.
- Wenn die Entität über keine standardisierten PCI-DSS-vorhandenen Prozesse/-Kontrollen verfügt und wenn jedes Element in der Grundgesamtheit durch nicht standardisierte Prozesse verwaltet wird, dann muss die Stichprobe größer sein, damit der Bewerter sicher sein kann, dass die PCI-DSS-Anforderungen auf jedes Element angemessen in der Population angewendet werden kann.
- Stichproben von Systemkomponenten müssen alle verwendeten Typen und Kombinationen beinhalten. Wenn eine Entität über mehr als ein CDE verfügt, müssen die Stichproben Populationen über alle Systemkomponenten im Geltungsbereich umfassen. Zum Beispiel, wenn von Anwendungen Stichproben gemacht werden, muss die Stichprobe alle Versionen und Plattformen für jeden Anwendungstyp enthalten.
- Die Stichprobengrößen müssen immer größer als eins sein, es sei denn, es gibt nur ein Element in der gegebenen Population, oder es wird eine automatisierte Kontrolle verwendet, bei der der Bewerter bestätigt hat, dass die Kontrolle für jede bewertete Stichprobenpopulation wie programmiert funktioniert.
- Wenn sich der Bewerter als Grundlage für die Auswahl einer Stichprobe auf standardisierte Prozesse und Kontrollen verlässt, dann aber während der Tests feststellt, dass standardisierte Prozesse und Kontrollen nicht vorhanden sind oder nicht effektiv funktionieren,

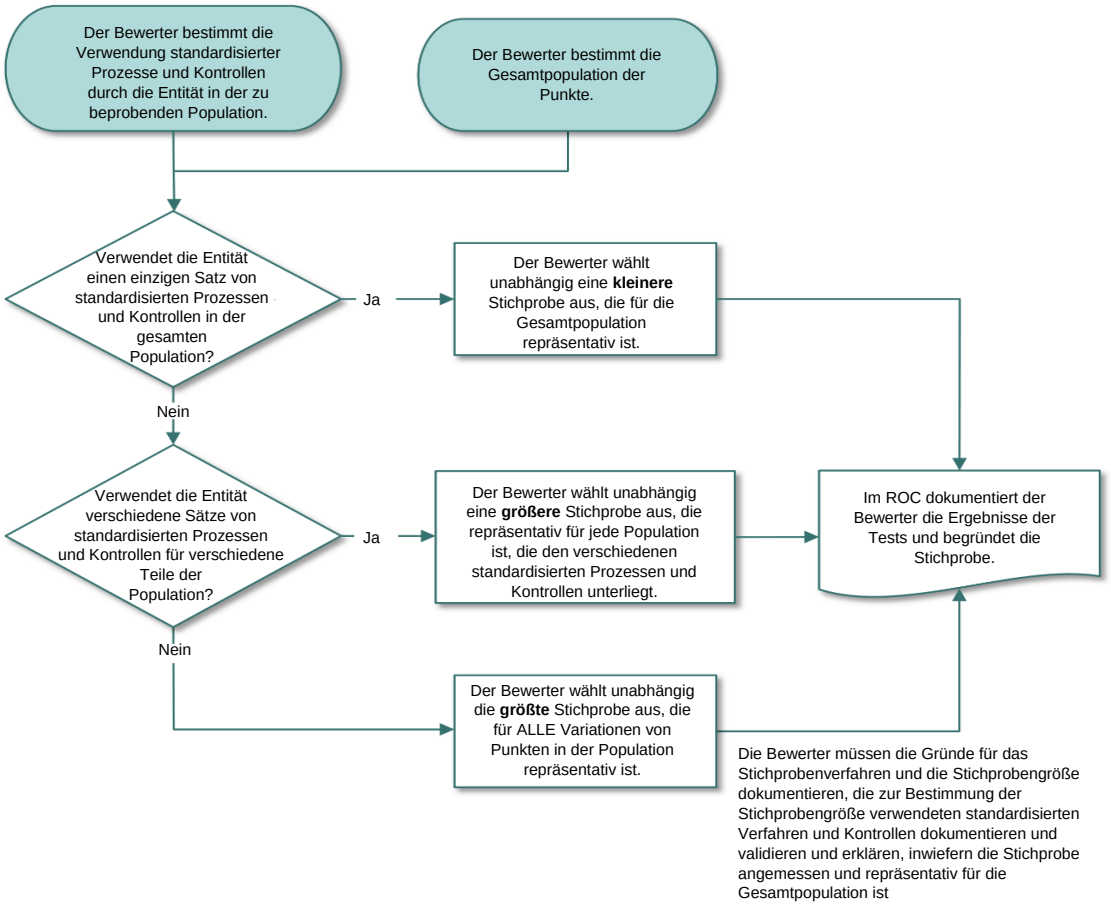
sollte der Bewerter die Stichprobengröße erhöhen, um zu versuchen, um sicherzustellen, dass die PCI-DSS-Anforderungen erfüllt werden.

Für jeden Fall, in dem Stichproben verwendet werden, muss der Bewerter:

- Die Gründe für das Stichprobenverfahren und die Stichprobengröße dokumentieren.
- Die standardisierten Prozesse und Kontrollen, die zur Bestimmung der Stichprobengröße verwendet werden, validieren und dokumentieren.
- Erklären, inwiefern die Stichprobe angemessen und repräsentativ für die Gesamtpopulation ist.

Figur 3 zeigt Überlegungen zur Bestimmung der Stichprobengröße.

Figur 3. Überlegungen zur PCI-DSS-Stichprobe



Hinweis: *In PCI DSS v4.0 wurden spezifische Referenzen auf die Stichprobenahme aus allen Testprozeduren entfernt. Diese Referenzen wurden entfernt, da das Aufrufen von Stichprobenahmen nur in einigen Testverfahren impliziert haben könnte, dass die Stichprobenahme für diese Testverfahren obligatorisch war (was nicht der Fall war) oder dass eine Stichprobenahme nur zulässig war, wenn dies ausdrücklich erwähnt wurde. Bewerter sollten Stichproben auswählen, wenn dies für die zu testende Population angemessen ist, und diese Entscheidungen gemäß den obigen Ausführungen unter Berücksichtigung des gesamten Geltungsbereichs und der Komplexität einer Umgebung treffen.*

7 Beschreibung der Zeitrahmen, die in den PCI-DSS-Anforderungen verwendet werden

Bestimmte PCI-DSS-Anforderungen wurden mit bestimmten Zeitrahmen für Aktivitäten festgelegt, die durch einen regelmäßig geplanten und wiederholten Prozess konsistent durchgeführt werden müssen. Die Absicht ist, dass die Aktivität in einem Intervall durchgeführt wird, das so nah wie möglich an diesem Zeitrahmen liegt, ohne ihn zu überschreiten. Es liegt im Ermessen der Entität, eine Aktivität häufiger als angegeben durchzuführen (zum Beispiel eine Aktivität monatlich durchzuführen, obwohl die PCI DSS-Anforderung vorschreibt, dass sie alle drei Monate durchzuführen ist).

Tabelle 4 skizziert die Häufigkeit für die verschiedenen Zeiträume, die in den PCI-DSS-Anforderungen verwendet werden.

Tabelle 4. PCI-DSS-Anforderungs-Zeitrahmen

Zeitrahmen in PCI-DSS-Anforderungen	Beschreibungen und Beispiele
Täglich	An jedem Tag des Jahres (nicht nur an Werktagen).
Wöchentlich	Mindestens einmal alle sieben Tage.
Monatlich	Mindestens einmal alle 30 bis 31 Tage oder am n-^{ten} Tag des Monats.
Alle drei Monate („vierteljährlich“)	Mindestens einmal alle 90 bis 92 Tage oder am n-^{ten} Tag von jedem dritten Monat.
Alle sechs Monate	Mindestens einmal alle 180 bis 184 Tage oder am n-^{ten} Tag von jedem sechsten Monat.
Alle 12 Monate („jährlich“)	Mindestens einmal alle 365 (oder 366 für Schaltjahre) Tage oder jedes Jahr am gleichen Datum.
Periodisch	Die Häufigkeit des Auftretens liegt im Ermessen der Entität und wird dokumentiert und durch die Risikoanalyse der Entität unterstützt. Die Entität muss demonstrieren, dass die Häufigkeit angemessen ist, damit die Aktivität effektiv ist und den Zweck der Anforderung erfüllt.
Sofort	Ohne Verzug In Echtzeit oder nahezu in Echtzeit.
Prompt	So schnell wie möglich.

Zeitrahmen in PCI-DSS-Anforderungen	Beschreibungen und Beispiele
Wesentliche Änderung	Es gibt bestimmte Anforderungen, für die die Leistung bei einer wesentlichen Änderung im Umfeld einer Entität festgelegt wird. Was eine signifikante Änderung darstellt, hängt zwar stark von der Konfiguration einer bestimmten Umgebung ab, aber mindestens jede der folgenden Aktivitäten hat potenzielle Auswirkungen auf die Sicherheit des CDE und muss im Kontext der entsprechenden PCI DSS-Anforderungen als signifikante Änderung betrachtet werden: • Neue Hardware, Software oder Netzwerkausrüstung zum CDE hinzugefügt. • Jeglicher Ersatz oder größere Aktualisierungen von Hardware und Software im CDE. • Alle Änderungen im Fluss oder der Speicherung von Kontodaten. • Alle Änderungen an der Grenze des CDE und/oder des Geltungsbereichs der PCI-DSS-Bewertung. • Alle Änderungen an der zugrunde liegenden unterstützenden Infrastruktur des CDE (einschließlich, aber nicht beschränkt auf Änderungen an Verzeichnisdienstleistungen, Zeitservern, Protokollierung und Überwachung). • Alle Änderungen an Drittanbietern/Dienstleistungsanbietern (oder bereitgestellten Dienstleistungen), die CDE unterstützen oder die PCI-DSS-Anforderungen im Namen der Entität erfüllen.

Bei anderen PCI-DSS-Anforderungen, bei denen der Standard keine Mindesthäufigkeit für wiederkehrende Aktivitäten festlegt, sondern stattdessen die „regelmäßige Erfüllung“ der Anforderung zulässt, wird erwartet, dass die Entität die Häufigkeit entsprechend seiner Geschäftstätigkeit festlegt. Die von der Entität definierte Häufigkeit muss durch die Sicherheitsrichtlinie der Entität und die gemäß PCI-DSS-Anforderung 12.3.1 durchgeführte Risikoanalyse unterstützt werden. Die Entität muss demonstrieren können, dass die Häufigkeit, die sie definiert hat, angemessen ist, damit die Aktivität effektiv ist und den Zweck der Anforderung erfüllt.

In beiden Fällen, in denen PCI DSS eine erforderliche Häufigkeit vorgibt und PCI DSS eine „regelmäßige“ Leistung zulässt, wird von der Entität erwartet, dass sie über dokumentierte und implementierte Prozesse verfügt, um sicherzustellen, dass die Aktivitäten innerhalb eines angemessenen Zeitrahmens durchgeführt werden, einschließlich mindestens eines der Folgenden:

- Die Entität wird jedes Mal umgehend benachrichtigt, wenn eine Aktivität nicht gemäß ihrem festgelegten Zeitplan ausgeführt wird,
- Die Entität bestimmt die Ereignisse, die dazu führten, dass eine geplante Aktivität verpasst wurde,
- Die Entität führt die Aktivität so schnell wie möglich durch, nachdem sie versäumt wurde, und kehrt entweder zum Zeitplan zurück oder legt einen neuen Zeitplan fest,
- Die Entität erstellt eine Dokumentation, die zeigt, dass die obigen Elemente aufgetreten sind,

Wenn die oben genannten Prozesse in einer Entität vorhanden sind, um das Versäumnis einer geplanten Aktivität zu erfassen und zu adressieren, dann ist ein angemessener Ansatz zulässig, d. h., wenn eine Aktivität mindestens alle drei Monate durchgeführt werden muss, dann ist das Entität nicht automatisch nicht-konform, wenn die Aktivität verspätet durchgeführt wird und der dokumentierte und implementierte Prozess der Entität (wie oben) befolgt wurde. Wenn jedoch kein solcher Prozess eingerichtet ist und/oder die Aktivität aufgrund von Aufsicht, Fehlverwaltung oder mangelnder Überwachung nicht termingerecht durchgeführt wurde, hat die Entität die Anforderung nicht erfüllt. In

solchen Fällen besteht die Anforderung nur, wenn die Entität 1) den oben beschriebenen Prozess dokumentiert (oder erneut bestätigt), um sicherzustellen, dass die geplante Aktivität pünktlich stattfindet, 2) den Zeitplan neu erstellt und 3) den Nachweis bereitstellt, dass die Entität die geplante Aktivität mindestens einmal gemäß ihrem Zeitplan ausgeführt hat.

Hinweis: *Bei einer anfänglichen PCI-DSS-Bewertung (d. h., dass eine Entität noch nie zuvor einer Bewertung unterzogen wurde), bei der eine Anforderung einen definierten Zeitrahmen hat, innerhalb dessen eine Aktivität erfolgen soll, ist es nicht erforderlich, dass die Aktivität für jeden dieser Zeitrahmen während des vorherigen Jahrs durchgeführt wurde, wenn der Bewerter Folgendes nachweist:*

- *Die Aktivität wurde gemäß den geltenden Anforderungen innerhalb des letzten Zeitrahmens (zum Beispiel der letzten Dreimonats- oder Sechsmonatsperiode) durchgeführt und*
- *Die Entität hat Richtlinien und Prozeduren für die Fortführung der Aktivität innerhalb des festgelegten Zeitrahmens dokumentiert.*

Für die folgenden Jahre nach der Erstbewertung muss die Aktivität innerhalb jedes geforderten Zeitrahmens mindestens einmal durchgeführt worden sein. Beispielsweise muss eine alle drei Monate erforderliche Aktivität im Vorjahr mindestens viermal in einem Abstand von höchstens 90-92 Tagen durchgeführt worden sein.

8 Ansätze zur Implementierung und Validierung von PCI DSS

Um die Flexibilität beim Erreichen der Sicherheitszielsetzungen zu unterstützen, gibt es zwei Ansätze für die Implementierung und Validierung von PCI DSS. Entitäten sollten den für ihre Sicherheitsimplementierung am besten geeigneten Ansatz identifizieren und diesen Ansatz zur Validierung der Kontrollen verwenden.

Definierter Ansatz

Folgt dem traditionellen Verfahren zur Implementierung und Validierung von PCI DSS und verwendet die im Standard definierten Anforderungen und Testprozeduren. Beim definierten Ansatz führt die Entität Sicherheitskontrollen durch, um die angegebenen Anforderungen zu erfüllen, und der Bewerter befolgt die definierten Testprozeduren, um zu verifizieren, dass die Anforderungen erfüllt wurden.

Der definierte Ansatz unterstützt Entitäten mit vorhandenen Kontrollen, die die PCI-DSS-Anforderungen wie angegeben erfüllen. Dieser Ansatz eignet sich auch für Entitäten, die mehr Anhaltspunkte für die Erfüllung von Sicherheitszielen wünschen, sowie für Entitäten, die neu im Bereich Informationssicherheit oder PCI DSS sind.

Kompensationskontrollen

Als Teil des definierten Ansatzes können Entitäten, die eine PCI-DSS-Anforderung aufgrund einer legitimen und dokumentierten technischen oder geschäftlichen Einschränkung nicht explizit erfüllen können, andere, oder *kompensierende, Kontrollen*, implementieren, die das mit der Anforderung verbundene Risiko ausreichend mindern. Jährlich müssen alle kompensierenden Kontrollen von der Stelle dokumentiert und vom Bewerter überprüft und validiert sowie dem Konformitätsbericht beigefügt werden.

Hinweis: *Weitere Details siehe Anhang B: Kompensationskontrollen und Anhang C: Arbeitsblatt für Kompensationskontrollen.*

Kundenspezifischer Ansatz

Konzentriert sich auf die Zielsetzung jeder PCI DSS-Anforderung (falls anwendbar) und erlaubt es Entitäten, Kontrollen zu implementieren, um das erklärte Ziel des angepassten Ansatzes der Anforderung auf eine Weise zu erfüllen, die nicht streng der definierten Anforderung folgt. Da jede kundenspezifische Implementierung unterschiedlich ist, gibt es keine definierten Testprozeduren; der Bewerter muss Testprozeduren ableiten, die für die spezifische Implementierung geeignet sind, um zu validieren, dass die implementierten Kontrollen die erklärte Zielsetzung erfüllen.

Hinweis: *Weitere Details siehe Anhang D: Benutzerdefinierter Ansatz und Anhang E: Stichprobenvorlagen zur Unterstützung des benutzerdefinierten Ansatzes.*

Der maßgeschneiderte Ansatz unterstützt Innovationen bei den Sicherheitspraktiken und ermöglicht es den Entitäten, flexibler zu zeigen, wie ihre aktuellen Sicherheitskontrollen die Zielsetzungen des PCI DSS erfüllen. Dieser Ansatz ist für risikoreife Entitäten gedacht, die ein solides Risikomanagementkonzept für die Sicherheit vorweisen können, einschließlich, aber nicht beschränkt auf eine spezielle Risikoverwaltungsabteilung oder ein organisationsweites Risikoverwaltungskonzept.

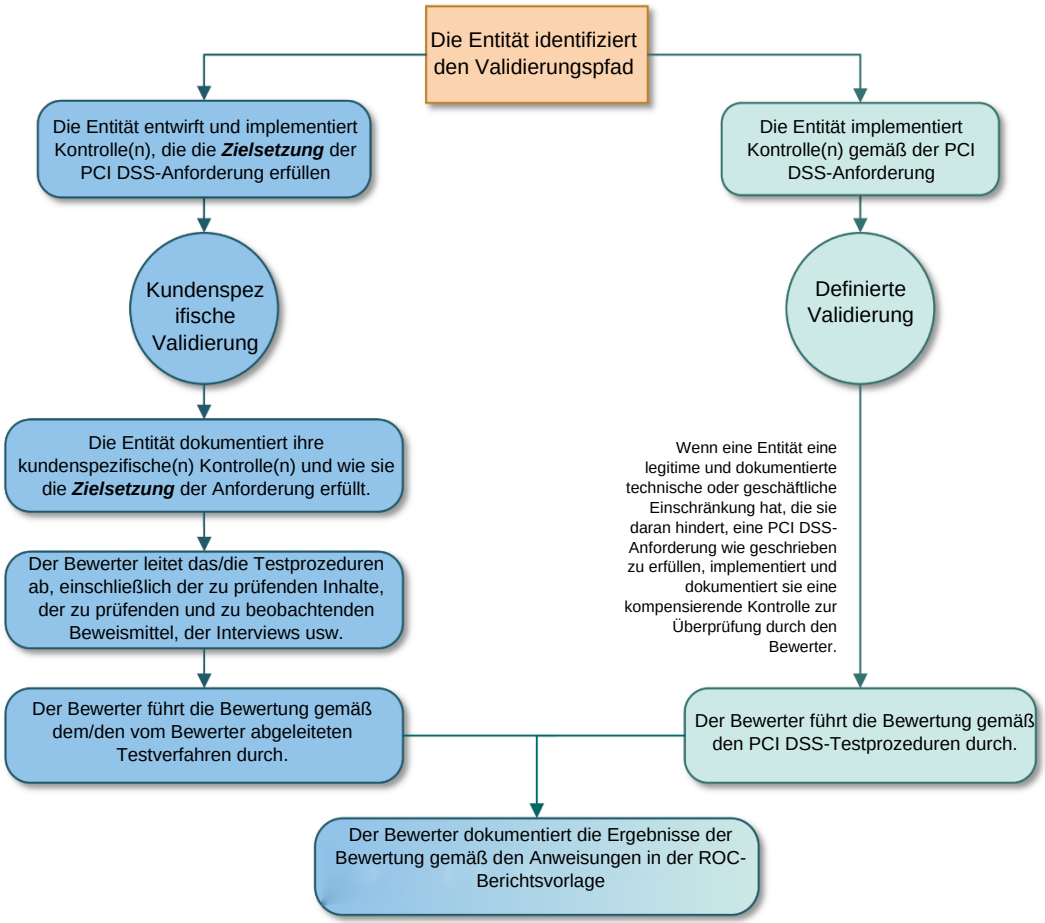
Es wird erwartet, dass die Kontrollen, die mit Hilfe des angepassten Ansatzes implementiert und validiert werden, die Sicherheit erfüllen oder übertreffen, die durch die Anforderungen des definierten Ansatzes gegeben ist. Der Dokumentation- und Arbeitsaufwand für die Validierung kundenspezifischer Implementierungen wird ebenfalls höher sein als bei dem definierten Ansatz.

Die meisten PCI DSS-Anforderungen können entweder mit dem definierten oder dem kundenspezifischen Ansatz erfüllt werden. Einige Anforderungen haben jedoch keine festgelegte Zielsetzung des kundenspezifischen Ansatzes; der kundenspezifische Ansatz ist für diese Anforderungen keine Option.

Die Entitäten können in ihrer Umgebung sowohl die definierten als auch die kundenspezifischen Ansätze verwenden. Das bedeutet, dass eine Entität den definierten Ansatz zur Erfüllung einiger Anforderungen und den kundenspezifischen Ansatz zur Erfüllung anderer Anforderungen verwenden könnte. Das bedeutet auch, dass eine Entität den definierten Ansatz verwenden könnte, um eine bestimmte PCI DSS-Anforderung für eine Systemkomponente oder in einer Umgebung zu erfüllen, und den angepassten Ansatz verwenden könnte, um dieselbe PCI DSS-Anforderung für eine andere Systemkomponente oder in einer anderen Umgebung zu erfüllen. Auf diese Weise kann eine PCI DSS-Bewertung sowohl definierte als auch kundenspezifische Testprozeduren umfassen.

Figur 4 zeigt die beiden Validierungsoptionen für PCI DSS v4.0.

Figur 4. PCI DSS-Validierungsansätze



9 Schutz von Informationen über die Sicherheitslage einer Entität

Die Prozesse, die mit dem Aufbau und der Wartung einer PCI DSS-konformen Umgebung verbunden sind, führen zu vielen Artefakten, die eine Entität als sensibel erachtet und als solche schützen möchte, einschließlich der folgenden Elemente:

- Der Bericht über die Konformität der Vorschriften oder der Fragebogen zur Selbsteinschätzung (die zugehörige Konformitätsbescheinigung der Vorschriften wird nicht als sensibel angesehen, und es wird erwartet, dass Drittdienstleistungsanbieter (TPSP) ihre AOC mit Kunden teilen).
- Netzwerkdiagramme und Kontodatenflussdiagramme sowie Sicherheitskonfigurationen und -regeln.
- Systemkonfigurationsstandards.
- Kryptographie und Schlüsselverwaltungsmethoden und -protokolle.

Entitäten sollten alle Artefakte, die sich auf die PCI DSS-Kontrollen oder die Bewertung beziehen, überprüfen und sie in Übereinstimmung mit den Sicherheitsrichtlinien der Entität für diese Art von Informationen schützen.

TPSPs sind verpflichtet (PCI DSS-Anforderung 12.9), ihre Kunden mit dem Folgenden zu unterstützen:

- Informationen, die Kunden benötigen, um den PCI DSS-Konformitätsstatus der TPSPs zu überwachen (damit der Kunde die Anforderung 12.8 erfüllen kann), und
- Nachweis, dass der TPSP die geltenden PCI DSS-Anforderungen erfüllt, wenn die Dienstleistungen des TPSP dazu bestimmt sind, die PCI DSS-Anforderungen eines Kunden zu erfüllen oder deren Erfüllung zu erleichtern, oder wenn diese Dienstleistungen die Sicherheit des CDE eines Kunden beeinflussen können.

Dieser Abschnitt hat keine Auswirkung auf die Verpflichtung eines TPSP, seine Kunden gemäß Anforderung 12.9 zu unterstützen und zu informieren.

Weitere Einzelheiten zu den Erwartungen an TPSPs und den Beziehungen zwischen TPSPs und Kunden siehe Verwendung von Drittanbieter von Dienstleistungen.

Schutz vertraulicher und sensibler Informationen durch qualifizierte Sicherheitsbewertungsunternehmen

Jedes qualifizierte Sicherheit-Bewertungs (QSA)-Unternehmen unterzeichnet eine Vereinbarung mit dem PCI SSC, dass es die Qualifizierungsanforderungen für QSAs einhalten wird. Der *Abschnitt zum Schutz vertraulicher und sensibler Informationen* dieses Dokuments enthält Folgendes:

> „Das QSA-Unternehmen muss über ein dokumentiertes Verfahren zum Schutz vertraulicher und sensibler Informationen verfügen und sich daranhalten. Dies muss angemessene physische, elektronische und verfahrenstechnische Sicherheitsvorkehrungen beinhalten, die den branchenüblichen Praktiken zum Schutz vertraulicher und sensibler Informationen vor Bedrohungen oder unbefugtem Zugriff während der Speicherung, Verarbeitung und/oder Übermittlung dieser Informationen entsprechen.

Das QSA-Unternehmen muss den Datenschutz und die Vertraulichkeit von Informationen wahren, die es im Rahmen der Erfüllung seiner Aufgaben und Pflichten als QSA-Unternehmen erhält, es sei denn, die Offenlegung ist gesetzlich vorgeschrieben."

10 Testverfahren für PCI-DSS-Anforderungen

Die in den Testverfahren für jede Anforderung angegebenen Testprozeduren beschreiben die zu erwartenden Aktivitäten, die vom Bewerter durchzuführen sind, um festzustellen, ob die Entität die Anforderung erfüllt hat. Die Absicht hinter jedem Testverfahren wird wie folgt beschrieben:

- Untersuchen: Die Datennachweise werden vom Bewerter kritisch beurteilt. Übliche Beispiele beinhalten Dokumente (elektronisch oder physisch), Screenshots, Konfigurationsdateien, Audit-Protokolle, und Datendateien.
- Beobachten: Der Bewerter beobachtet eine Handlung oder betrachtet etwas in der Umgebung. Beispiele für Beobachtungsthemen sind Personal, das Aufgaben oder Prozesse ausführt, Systemkomponenten, die eine Funktion ausführen oder auf Eingaben reagieren, Umgebungsbedingungen und physische Kontrollen.
- Interview: Der Bewerter führt Gespräche mit einzelnen Mitarbeitern. Interview-Zielsetzungen können die Bestätigung sein, ob eine Aktivität durchgeführt wird, Beschreibungen, wie eine Aktivität durchgeführt wird und ob das Personal über besondere Kenntnisse oder Verstehen verfügt.

Die Testverfahren sollen es der bewerteten Entität ermöglichen, zu demonstrieren, wie sie eine Anforderung erfüllt hat. Sie vermitteln der bewerteten Entität und dem Bewerter auch ein gemeinsames Verständnis der durchzuführenden Bewertungsaktivitäten. Die zu untersuchenden oder zu beobachtenden spezifischen Punkte und das zu befragende Personal sollten sowohl für die zu bewertende Anforderung als auch für die jeweilige Umsetzung der jeweiligen Stelle geeignet sein. Bei der Dokumentation der Bewertungsergebnisse identifiziert der Bewerter die durchgeführten Testaktivitäten und das Ergebnis jeder Tätigkeit.

11 Anleitungen und Inhalt für den Compliance-Bericht

Anleitungen und Inhalte für den Bericht der Konformität (ROC) werden in der *PCI DSS Bericht der Konformitäts(ROC)-Vorlage bereitgestellt*.

Die PCI DSS Bericht der Konformitäts(ROC)-Vorlage muss als Vorlage für die Erstellung eines PCI DSS-Bericht der Konformität verwendet werden.

Ob eine Entität verpflichtet ist, den PCI DSS einzuhalten oder seine Konformität zu bestätigen, liegt im Ermessen der Organisationen, die die Konformitätsprogramme verwalten (z. B. Zahlungsanbieter und Erwerber). Die Entitäten sollten sich mit den betreffenden Organisationen in Verbindung setzen, um etwaige Meldeanordnungen und Anweisungen zu erfahren.

12 PCI-DSS-Bewertungsprozess

Der PCI DSS-Bewertungsprozess beinhaltet die folgenden übergeordneten Schritte:[5]

1. Bestätigung des Geltungsbereichs der PCI DSS-Bewertung.
2. Durchführung der PCI DSS-Bewertung der Umgebung.
3. Ausfüllung des entsprechenden Berichtes für die Bewertung gemäß den PCI DSS-Richtlinien und -Anweisungen.
4. Ausfüllung der Konformitätsbescheinigung für Dienstleistungsanbieter oder Händler in seiner Gesamtheit. Offizielle Konformitätsbescheinigungen sind nur auf der Webseite des PCI SSC erhältlich.
5. Einreichung der entsprechenden PCI SSC-Dokumentation und der Konformitätsbescheinigung zusammen mit allen anderen angeforderten Unterlagen ein, wie ASV-Scan-Berichte – an die anfragende Organisation (diejenige, die Konformitätsprogramme wie Zahlungsmarken verwalten und Erwerber (für Händler) oder andere Anforderer (für Dienstleistungsanbieter)).
6. Falls erforderlich, Durchführung von Abhilfemaßnahmen, um nicht erfüllte Anforderungen zu erfüllen, und Bereitstellung eines aktualisierten Berichts.

Hinweis: *Die Anforderungen des PCI DSS gelten nicht als erfüllt, wenn die Kontrollen noch nicht implementiert sind oder zu einem späteren Zeitpunkt abgeschlossen werden sollen. Nachdem alle offenen oder nicht vorhandenen Punkte von der Entität adressiert wurden, nimmt der Bewerter eine erneute Bewertung vor, um zu validieren, ob die Abhilfemaßnahmen abgeschlossen sind und alle Anforderungen erfüllt werden. Zur Dokumentation der PCI DSS-Bewertung können Sie auf die folgenden Ressourcen zurückgreifen (verfügbar auf der PCI SSC-Webseite):*

- *Anweisungen zum Ausfüllen von Berichten über die Konformität der Vorschriften (ROC) finden Sie in der Vorlage für den PCI DSS-Bericht über die Konformität der Vorschriften (ROC).*
- *Anweisungen zum Ausfüllen von Fragebögen zur Selbstbewertung (SAQ) finden Sie in den PCI DSS SAQ Anweisungen und Richtlinien.*
- *Anweisungen zur Einreichung von Berichten zur Validierung der PCI DSS-Konformität finden Sie in der PCI DSS-Konformitätsbescheinigung.*

[5] Der PCI DSS-Bewertungsprozess und die Rollen und Verantwortlichkeiten für die Durchführung der einzelnen Schritte variieren je nach Art der Bewertung und der Konformitätsprogramme, die von Zahlungsmarken und Erwerbern verwaltet werden.

13 Zusätzliche Referenzen

Tabelle 5 führt externe Organisationen auf, auf die in den PCI DSS-Anforderungen oder den entsprechenden Leitlinien verwiesen wird. Diese externen Organisationen und ihre Referenzen werden nur zur Information bereitgestellt und ersetzen oder erweitern keine PCI DSS-Anforderungen.

Tabelle 5. Externe Organisationen, auf die in den PCI DSS-Anforderungen verwiesen wird

Referenz	Vollständiger Name	Quelle
ANSI	Amerikanisches Institut für Normung	www.ansi.org
CIS	Zentrum für Internetsicherheit	www.cisecurity.org
CSA	Allianz für Cloud-Sicherheit	www.csa.org
ENISA	Agentur der Europäischen Union für Cybersicherheit (vormals Europäische Agentur für Netz- und Informationssicherheit)	www.enisa.europa.eu
FIDO Alliance	Die FIDO-Allianz	www.fidoalliance.org
ISO	Internationale Organisation für Normung	www.iso.org
NCSC	Das britische Nationale Zentrum für Cybersicherheit	www.ncsc.gov.uk
NIST	Nationales Institut für Normen und Technologie	www.nist.gov
OWASP	Sicherheitsprojekt für offene Webanwendungen	www.owasp.org
SAFEcode	Software Garantie-Forum für Exzellenz im Code	www.safecode.org

14 PCI-DSS-Versionen

Ab dem Veröffentlichungsdatum dieses Dokuments ist PCI DSS v3.2.1 bis zum 31. März 2024 gültig und wird danach eingestellt. Alle PCI DSS-Validierungen nach diesem Datum müssen PCI DSS 4.0 oder höher sein.

Für Bewertungen zwischen März 2022 und 31. März 2024 kann entweder PCI DSS Version 3.2.1 oder 4.0 verwendet werden.

Tabelle 6 fasst PCI-DSS-Versionen und deren relevante Daten zusammen.[6]

Tabelle 6. PCI-DSS-Versionen

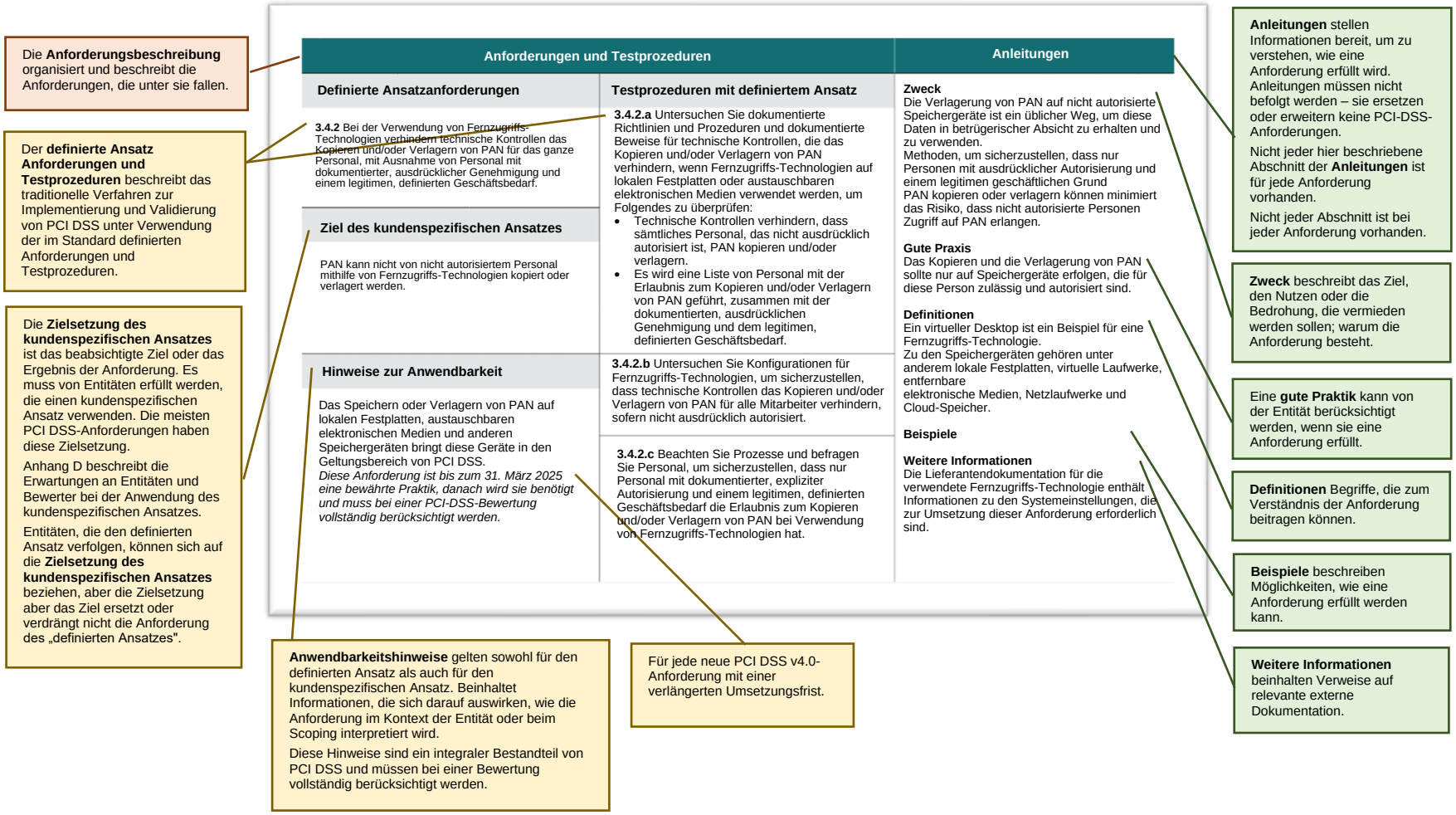
Version	Veröffentlicht	Zurückgezogen
PCI DSS v4.0 (dieses Dokument)	März 2022	Wird noch festgelegt
PCI DSS v3.2.1	Mai 2018	31. März 2024

[6] Änderung vorbehalten bei Veröffentlichung einer neuen Version von PCI DSS.

15 Detaillierte PCI-DSS-Anforderungen und Testprozeduren

Figur 5 beschreibt die Spaltenüberschriften und den Inhalt für die PCI-DSS-Anforderungen.

Figur 5. Verstehen der Teile der Anforderungen



Zusätzliche Anforderungen nur für Dienstleistungsanbieter

Einige Anforderungen gelten nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. Diese sind in der Anforderung als „*Zusätzliche Anforderung nur für Dienstleistungsanbieter" definiert* und gelten zusätzlich zu allen anderen geltenden Anforderungen. Handelt es sich bei der zu bewertenden Stelle sowohl um einen Händler als auch um einen Dienstleistungsanbieter, gelten die Anforderungen von „*Zusätzliche Anforderung nur für Dienstleistungsanbieter"* für den Dienstleistungsanbieteranteil des Geschäfts der Entität. Anforderungen, die mit „*Zusätzliche Anforderung nur für Dienstleistungsanbieter"* identifiziert werden, werden auch als bewährte Praktiken zur Berücksichtigung durch alle Entität empfohlen.

Anhänge mit zusätzlichen PCI-DSS-Anforderungen für verschiedene Arten von Entitäten

Zusätzlich zu den 12 Hauptanforderungen enthält PCI DSS Anhang A zusätzliche PCI DSS-Anforderungen für verschiedene Arten von Entitäten. Die Abschnitte in Anhang A beinhalten:

- Anhang A1: Zusätzliche PCI DSS-Anforderungen für Multi-Tenant-Dienstleistungsanbieter
- Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Entitäten, die SSL/Early TLS für Karte anwesend POS-POI-Terminalverbindungen verwenden.
- Anhang A3: Ergänzende Validierung für bestimmte Entitäten (DESV).

Ein sicheres Netzwerk und Sichere Systeme Aufbauen und Warten

Anforderung 1: Installation und Wartung von Netzwerksicherheitskontrollen

Abschnitte	
1.1	Prozesse und Mechanismen zur Installation und Wartung von Netzwerksicherheitskontrollen werden definiert und verstanden.
1.2	Netzwerksicherheitskontrollen (NSCs) werden konfiguriert und gewartet.
1.3	Der Netzwerkzugriff auf und von der Karteninhaberdatenumgebung ist eingeschränkt.
1.4	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert.
1.5	Risiken für die CDE durch Computergeräte, die sich sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbinden können, werden gemindert.

Übersicht

Netzwerksicherheitskontrollen (NSCs), wie Firewalls und andere Netzwerksicherheitstechnologien, sind Durchsetzungspunkte von Netzwerkrichtlinien, die normalerweise den Netzwerkverkehr zwischen zwei oder mehr logischen oder physischen Netzwerksegmenten (oder Subnetzen) basierend auf vordefinierten *Richtlinien* oder *Regeln* steuern.

NSCs untersuchen den gesamten Netzwerkverkehr, der einen Abschnitt betritt (Eintritt) und verlässt (Austritt), und entscheiden basierend auf den definierten Richtlinien, ob der Netzwerkverkehr passieren darf oder abgelehnt werden soll. Normalerweise werden NSCs zwischen Umgebungen mit unterschiedlichen Sicherheitsanforderungen oder Vertrauensstufen platziert, jedoch kontrollieren NSCs in einigen Umgebungen den Verkehr zu einzelnen Geräten unabhängig von Vertrauensgrenzen. Die Durchsetzung von Richtlinien erfolgt im Allgemeinen auf Schicht 3 des OSI-Modells, aber Daten, die in höheren Schichten vorhanden sind, werden auch oft verwendet, um Richtlinienentscheidungen zu treffen.

Diese Funktion wird traditionell von physischen Firewalls bereitgestellt; jetzt kann diese Funktionalität jedoch von virtuellen Geräten, Cloud-Zugriffskontrollen, Virtualisierungs-/Containersystemen und anderen softwaredefinierten Netzwerktechnologien bereitgestellt werden.

NSCs werden verwendet, um den Verkehr innerhalb der eigenen Netzwerke einer Entität zu kontrollieren – zum Beispiel zwischen hochsensiblen und weniger sensiblen Bereichen – und auch, um die Ressourcen der Entität vor der Gefährdung durch nicht vertrauenswürdige Netzwerke zu schützen. Die Karteninhaberdatenumgebung (CDE) ist ein Beispiel für einen sensibleren Bereich innerhalb des Netzwerks einer Entität. Scheinbar unbedeutende Pfade zu und von nicht vertrauenswürdigen Netzwerken können oft ungeschützte Wege in sensible Systeme bereitstellen. NSCs stellen einen wichtigen Schutzmechanismus für jedes Computernetzwerk bereit.

Häufige Beispiele für nicht vertrauenswürdige Netzwerke schließen das Internet, dedizierte Verbindungen wie Business-to-Business-Kommunikationskanäle, drahtlose Netzwerke, Carrier-Netzwerke (wie Mobilfunk), Drittanbieter-Netzwerke und andere Quellen außerhalb der Kontrolle der Entität ein. Darüber hinaus schließen nicht vertrauenswürdige Netzwerke auch Unternehmensnetzwerke ein, die als nicht vertrauenswürdig für PCI DSS gelten, da sie nicht bewertet werden und daher als nicht vertrauenswürdig behandelt werden müssen, da das Vorhandensein von Sicherheitskontrollen nicht verifiziert wurde. Während eine Entität ein internes Netzwerk aus der Sicht von Infrastruktur als vertrauenswürdig einstufen kann, muss dieses Netzwerk für PCI DSS als nicht vertrauenswürdig betrachtet werden, wenn ein Netzwerk außerhalb des Geltungsbereichs von PCI DSS liegt.

Finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
1.1 Prozesse und Mechanismen zur Installation und Wartung von Netzwerksicherheitskontrollen werden definiert und verstanden.		
Definierte Ansatzanforderungen **1.1.1** Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 1 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt. **Zielsetzung des kundenspezifischen Ansatzes** Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 1 werden vom betroffenen Personal definiert, verstanden und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht des Managements.	**Testprozeduren mit definiertem Ansatz** **1.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 1 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Bei Anforderung 1.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 1 angegeben sind. Während es wichtig ist, die in Anforderung 1 genannten spezifischen Richtlinien oder Verfahren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesen Gründen in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Verfahren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Verfahren und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen.

<table>
<tr><th colspan="2">Anforderungen und Testprozeduren</th><th>Anleitungen</th></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="4">Zweck
Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen sind, ist das Personal sich möglicherweise seiner täglichen Verantwortlichkeiten nicht bewusst und kritische Aktivitäten können nicht stattfinden.
Gute Praxis
Rollen und Verantwortlichkeiten können in Richtlinien und Verfahren dokumentiert oder in separaten Dokumenten gewartet werden.
Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen.
Beispiele
Ein Verfahren zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).</td></tr>
<tr><td rowspan="2">1.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 1 werden dokumentiert, zugewiesen und verstanden.</td><td>1.1.2.a Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 1 dokumentiert und zugewiesen sind.</td></tr>
<tr><td>1.1.2.b Befragung von Personal, das für die Durchführung von Aktivitäten in Anforderung 1 verantwortlich sind, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes</td><td colspan="2"></td></tr>
<tr><td>Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 1 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.</td><td colspan="2"></td></tr>
</table>

Anforderungen und Testprozeduren		Anleitungen
1.2 Netzwerksicherheitskontrollen (NSCs) werden konfiguriert und gewartet.		
Definierte Ansatzanforderungen **1.2.1** Konfigurationsstandards für NSC-Regelsätze sind: • Definiert. • Implementiert. • Gewartet. **Zielsetzung des kundenspezifischen Ansatzes** Die Art und Weise, wie NSCs konfiguriert und betrieben werden, ist definiert und wird konsequent angewendet.	**Testprozeduren mit definiertem Ansatz** **1.2.1.a** Konfigurationsstandards für NSC-Regelsätze untersuchen, um zu verifizieren, dass die Standards mit allen in dieser Anforderung angegebenen Elementen übereinstimmen. **1.2.1.b** Konfigurationseinstellungen für NSC-Regelsätze untersuchen, um sicherzustellen, dass Regelsätze gemäß den Konfigurationsstandards implementiert werden.	**Zweck** Die Implementierung dieser Konfigurationsstandards führt dazu, dass der NSC konfiguriert und verwaltet wird, um ihre Sicherheitsfunktionen (oft als Regelsatz bezeichnet) richtig durchzuführen. **Gute Praxis** Diese Standards definieren oft die Anforderungen an akzeptable Protokolle, Ports, die verwendet werden dürfen, und spezifische Konfigurationsanforderungen, die akzeptabel sind. Konfigurationsstandards können auch umreißen, was die Entität in ihrem Netzwerk für nicht akzeptabel oder nicht gestattet hält. **Definitionen** NSCs sind Schlüsselkomponenten einer Netzwerkarchitektur. Am häufigsten werden NSCs an den Grenzen der CDE verwendet, um den ein- und ausgehenden Netzwerkverkehr von der CDE zu steuern. Konfigurationsstandards umreißen die Mindestanforderungen einer Entität an die Konfiguration ihrer NSCs **Beispiele** Beispiele von NSCs, die von diesen Konfigurationsstandards abgedeckt werden, beinhalten, sind aber nicht beschränkt auf Firewalls, Router, die mit Zugriffskontrolllisten konfiguriert sind, und virtuelle Cloud-Netzwerke.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Gute Praxis** Änderungen sollten von Personen mit der entsprechenden Autorität und Kenntnissen genehmigt werden, um die Auswirkungen der Änderung zu verstehen. Die Verifizierung sollte hinreichende Gewähr dafür bieten, dass die Änderung die Sicherheit des Netzwerks nicht beeinträchtigt hat und dass die Änderung wie erwartet funktioniert. Um zu vermeiden, dass durch eine Änderung eingeführte Sicherheitsprobleme behoben werden müssen, sollten alle Änderungen vor der Implementierung genehmigt und nach der Implementierung der Änderung verifiziert werden. Nach der Genehmigung und Verifizierung sollte die Netzwerkdokumentation aktualisiert werden, um die Änderungen aufzunehmen, um Inkonsistenzen zwischen der Netzwerkdokumentation und der tatsächlichen Konfiguration zu vermeiden.
1.2.2 Alle Änderungen an Netzwerkverbindungen und an Konfigurationen von NSCs werden gemäß dem in Anforderung 6.5.1 definierten Änderungskontrollprozess genehmigt und verwaltet.	**1.2.2.a** Dokumentierte Prozeduren untersuchen, um zu verifizieren, dass Änderungen an Netzwerkverbindungen und Konfigurationen von NSCs in den formalen Änderungskontrollprozess gemäß Anforderung 6.5.1 eingeschlossen werden.	
	1.2.2.b Netzwerkkonfigurationseinstellungen untersuchen, um Änderungen an den Netzwerkverbindungen zu identifizieren. Verantwortliches Personal befragen und Änderungskontrollaufzeichnungen untersuchen, um zu verifizieren, dass identifizierte Änderungen an Netzwerkverbindungen genehmigt und gemäß Anforderung 6.5.1 verwaltet wurden.	
Zielsetzung des kundenspezifischen Ansatzes	**1.2.2.c** Netzwerkkonfigurationseinstellungen untersuchen, um Änderungen an den Konfigurationen von NSCs zu identifizieren. Verantwortliches Personal befragen und Änderungskontrollaufzeichnungen untersuchen, um zu verifizieren, dass identifizierte Änderungen an Konfigurationen von NSCs genehmigt und gemäß Anforderung 6.5.1 verwaltet wurden.	
Änderungen an Netzwerkverbindungen und NSCs können nicht zu Fehlkonfigurationen, Implementierung unsicherer Dienstleistungen oder nicht autorisierten Netzwerkverbindungen führen.		
Hinweise zur Anwendbarkeit		
Änderungen an Netzwerkverbindungen beinhalten das Hinzufügen, Entfernen oder Ändern einer Verbindung. Änderungen an NSC-Konfigurationen beinhalten solche, die sich auf die Komponente selbst beziehen, sowie solche, die sich darauf auswirken, wie sie ihre Sicherheitsfunktion ausführt.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Wartung eines genauen und aktuellen Netzwerkdiagramms verhindert, dass Netzwerkverbindungen und Geräte übersehen und unwissentlich ungesichert und anfällig für Kompromisse bleiben. Ein oder mehrere ordnungsgemäß gewartete Netzwerkdiagramm(e) helfen einer Organisation, ihren PCI DSS-Geltungsbereich zu verifizieren, indem Systeme identifiziert werden, die eine Verbindung zu und von der CDE herstellen. **Gute Praxis** Alle Verbindungen zu und von der CDE sollten identifiziert werden, einschließlich der Systeme, die Sicherheits-, Verwaltungs- oder Wartungsdienstleistungen für CDE-Systemkomponenten bereitstellen. Entitäten sollten in Erwägung ziehen, Folgendes in ihre Netzwerkdiagramme einzuschließen: • Alle Standorte, einschließlich Einzelhandelsstandorte, Rechenzentren, Unternehmensstandorte, Cloud-Anbieter usw. • Klare Kennzeichnung aller Netzwerksegmente. • Alle Sicherheitskontrollen, die eine Segmentierung bereitstellen, einschließlich eindeutiger Identifizierer für jede Kontrolle (z. B. Name der Kontrolle, Marke, Modell und Version). • Alle Systemkomponenten im Geltungsbereich, einschließlich NSCs, Web-App-Firewalls, Anti-Malware-Lösungen, Änderungsverwaltungs-Lösungen, IDS/IPS, Protokollaggregationssysteme, Zahlungsterminals, Zahlungsanwendungen, HSMs usw. *(Fortsetzung auf der nächsten Seite)*
1.2.3 Genaue Netzwerkdiagramme werden beibehalten, die alle Verbindungen zwischen der CDE und anderen Netzwerken, einschließlich aller drahtlosen Netzwerke, zeigen.	**1.2.3.a** Diagramme untersuchen und Netzwerkkonfigurationen, um zu verifizieren, dass ein oder mehrere genaue Netzwerkdiagramme gemäß allen in dieser Anforderung angegebenen Elementen vorhanden sind.	
	1.2.3.b Die Dokumentation untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass die Netzwerkdiagramme korrekt sind und aktualisiert werden, wenn Änderungen an der Umgebung vorgenommen werden.	
Zielsetzung des kundenspezifischen Ansatzes Eine Darstellung der Grenzen zwischen der CDE, allen vertrauenswürdigen Netzwerken und allen nicht vertrauenswürdigen Netzwerken wird gewartet und ist verfügbar.		
Hinweise zur Anwendbarkeit Ein aktuelles Netzwerkdiagramm oder eine andere technische oder topologische Lösung, die die Netzwerkverbindungen und -geräte identifiziert, kann zur Erfüllung dieser Anforderung verwendet werden.		

Anforderungen und Testprozeduren		Anleitungen
		• Klare Kennzeichnung von Bereichen außerhalb des Geltungsbereichs im Diagramm über ein schattiertes Kästchen oder einen anderen Mechanismus. • Datum der letzten Aktualisierung und Namen der Personen, die die Aktualisierungen vorgenommen und genehmigt haben. • Eine Legende oder ein Schlüssel, um das Diagramm zu erklären. Diagramme sollten von autorisiertem Personal aktualisiert werden, um sicherzustellen, dass Diagramme weiterhin eine genaue Beschreibung des Netzwerks bereitstellen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **1.2.4** Genaue Datenflussdiagramm(e) werden gewartet, die Folgendes erfüllen: • Zeigt alle Kontodatenflüsse über Systeme und Netzwerke an. • Wird bei Änderungen an der Umgebung nach Bedarf aktualisiert. **Zielsetzung des kundenspezifischen Ansatzes** Eine Darstellung aller Übertragungen von Kontodaten zwischen Systemkomponenten und über Netzwerksegmente hinweg wird aufrecht erhalten und zur Verfügung gestellt. **Hinweise zur Anwendbarkeit** Ein Datenflussdiagramm(e) oder eine andere technische oder topologische Lösung, die Flüsse von Kontodaten über Systeme und Netzwerke identifiziert, kann zur Erfüllung dieser Anforderung verwendet werden.	**Testprozeduren mit definiertem Ansatz** **1.2.4.a** Datenflussdiagramm(e) untersuchen und das Personal befragen, um zu verifizieren, dass das/die Diagramm(e) alle Kontodatenflüsse gemäß allen in dieser Anforderung spezifizierten Elementen zeigt. **1.2.4.b** Die Dokumentation untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass die Datenflussdiagramm(e) korrekt sind und aktualisiert werden, wenn Änderungen an der Umgebung vorgenommen werden.	**Zweck** Ein aktuelles, leicht verfügbares Datenflussdiagramm hilft einer Organisation, den Geltungsbereich seiner Umgebung zu verstehen und zu verfolgen, indem es zeigt, wie Kontodaten über Netzwerke und zwischen einzelnen Systemen und Geräten fließen. Die Wartung eines oder mehrerer aktueller Datenflussdiagramme verhindert, dass Kontodaten übersehen und unwissentlich ungesichert bleiben. **Gute Praxis** Das Datenflussdiagramm sollte alle Verbindungspunkte enthalten, an denen Kontodaten in das Netzwerk empfangen und aus dem Netzwerk gesendet werden, einschließlich Verbindungen zu offenen, öffentlichen Netzwerken, Anwendungsverarbeitungsflüssen, Speicherung, Übertragungen zwischen Systemen und Netzwerken und Dateibackups. Das Datenflussdiagramm ist als Ergänzung zum Netzwerkdiagramm gedacht und sollte mit dem Netzwerkdiagramm in Einklang stehen und es verbessern. Als bewährte Praktik können Entitäten Folgendes in ihre Datenflussdiagramme aufnehmen: • Alle Verarbeitungsprozesse von Kontodaten, einschließlich Autorisierung, Erfassung, Abrechnung, Rückbuchung und Erstattungen. • Alle unterschiedlichen Akzeptanzkanäle, einschließlich Karte vorhanden, Karte nicht vorhanden und E-Commerce. • Alle Arten von Datenempfang oder -übertragung, einschließlich aller, die Ausdrucke/Papiermedien betreffen. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		• Der Fluss der Kontodaten von dem Punkt, an dem sie in die Umgebung eintreten, bis zu ihrer endgültigen Bereitstellung. • Wo Kontodaten übertragen und verarbeitet werden, wo sie gespeichert werden und ob die Speicherung kurz- oder langfristig ist. • Die Quelle aller empfangenen Kontodaten (zum Beispiel Kunden, Dritte usw.) und alle Entitäten, mit denen Kontodaten geteilt werden. • Datum der letzten Aktualisierung und Namen der Personen, die die Aktualisierungen vorgenommen und genehmigt haben.
Definierte Ansatzanforderungen **1.2.5** Alle zulässigen Dienstleistungen, Protokolle und Ports werden identifiziert, genehmigt und haben einen definierten Geschäftsbedarf. **Zielsetzung des kundenspezifischen Ansatzes** Nicht autorisierter Netzwerkverkehr (Dienstleistungen, Protokolle oder Pakete, die für bestimmte Ports bestimmt sind) kann nicht in das Netz eingehen oder es verlassen.	**Testprozeduren mit definiertem Ansatz** **1.2.5.a** Dokumentation untersuchen, um zu verifizieren, dass eine Liste aller zulässigen Dienstleistungen, Protokolle und Ports vorhanden ist, einschließlich der geschäftlichen Begründung und Genehmigung für jedes. **1.2.5.b** Konfigurationseinstellungen für NSCs untersuchen, um zu verifizieren, dass nur genehmigte Dienstleistungen, Protokolle und Ports verwendet werden.	**Zweck** Kompromisse entstehen oft durch nicht verwendete oder unsichere Dienste (zum Beispiel Telnet und FTP), Protokolle und Ports, da diese dazu führen können, dass unnötige Zugriffspunkte in die CDE geöffnet werden. Zusätzlich werden Dienstleistungen, Protokolle und Ports, die aktiviert, aber nicht verwendet werden, oft übersehen und ungesichert und nicht gepatcht gelassen. Durch die Identifizierung der für das Geschäft erforderlichen Dienstleistungen, Protokolle und Ports können Entitäten sicherstellen, dass alle anderen Dienstleistungen, Protokolle und Ports deaktiviert oder entfernt werden. **Gute Praxis** Das mit jeder zugelassenen Dienstleistung, Protokoll und Port verbundene Sicherheitsrisiko sollte verstanden werden. Genehmigungen sollten von Personal erteilt werden, das von denjenigen, die die Konfiguration verwalten, unabhängig ist. Genehmigendes sollte über Kenntnisse und Verantwortlichkeit verfügen, die für das Treffen von Genehmigungsentscheidungen angemessen sind.

<table>
<tr><th colspan="2">Anforderungen und Testprozeduren</th><th>Anleitungen</th></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="4">Zweck
Kompromisse nutzen unsichere Netzwerkkonfigurationen aus.
Gute Praxis
Wenn unsichere Dienstleistungen, Protokolle oder Ports für das Geschäft erforderlich sind, sollte das von diesen Dienstleistungen, Protokollen und Ports ausgehende Risiko klar verstanden und von der Organisation akzeptiert werden, die Verwendung der Dienstleistung, des Protokolls oder Ports sollte gerechtfertigt sein und die Sicherheitsfunktionen, die das Risiko der Verwendung dieser Dienstleistungen, Protokolle und Ports mindern, sollten von der Entität definiert und implementiert werden.
Weitere Informationen
Anleitungen zu Dienstleistungen, Protokollen oder Ports, die als unsicher eingestuft werden, finden Sie in den Industriestandards und -anleitungen (zum Beispiel von NIST, ENISA usw.).</td></tr>
<tr><td rowspan="2">1.2.6 Für alle Dienstleistungen, Protokolle und Ports, die verwendet werden und als unsicher gelten, werden Sicherheitsfunktionen definiert und implementiert, sodass das Risiko gemindert wird.</td><td>1.2.6.a Dokumentation, die alle unsicheren Dienstleistungen, Protokolle und verwendeten Ports identifiziert, untersuchen, um zu verifizieren, dass für jeden Sicherheitsfunktionen definiert sind, um das Risiko zu mindern.</td></tr>
<tr><td>1.2.6.b Konfigurationseinstellungen für NSCs, um zu verifizieren, dass die definierten Sicherheitsfunktionen für jede identifizierte unsichere Dienstleistung, jedes Protokoll und jeden Port implementiert sind.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes</td><td></td></tr>
<tr><td>Die spezifischen Risiken im Zusammenhang mit der Nutzung unsicherer Dienstleistungen, Protokolle und Ports werden verstanden, bewertet und angemessen gemindert.</td><td></td><td></td></tr>
</table>

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Eine solche Überprüfung gibt der Organisation die Möglichkeit, unnötige, veraltete oder falsche Regeln und Konfigurationen zu bereinigen, die von einer nicht autorisierten Person verwendet werden könnten. Darüber hinaus stellt sie sicher, dass alle Regeln und Konfigurationen nur autorisierte Dienstleistungen, Protokolle und Ports zulassen, die den dokumentierten geschäftlichen Begründungen entsprechen. **Gute Praxis** Diese Überprüfung, die mit manuellen, automatisierten oder systembasierten Methoden implementiert werden kann, soll bestätigen, dass die Einstellungen, die Verkehrsregeln verwalten, was in und aus dem Netzwerk erlaubt ist, mit den genehmigten Konfigurationen übereinstimmen. Die Überprüfung sollte Bestätigung bereitstellen, dass alle zulässigen Zugriffe einen berechtigten geschäftlichen Grund haben. Alle Diskrepanzen oder Unsicherheiten bezüglich einer Regel oder Konfiguration sollten zur Lösung eskaliert werden. Obwohl diese Anforderung vorsieht, dass diese Überprüfung mindestens alle sechs Monate stattfindet, möchten Organisationen mit einem hohen Änderungsvolumen an ihren Netzwerkkonfigurationen jedoch möglicherweise häufiger Überprüfungen durchführen, um sicherzustellen, dass die Konfigurationen weiterhin den Anforderungen des Unternehmens entsprechen.
1.2.7 Konfigurationen von NSCs werden mindestens alle sechs Monate überprüft, um zu bestätigen, dass sie relevant und effektiv sind.	**1.2.7.a** Dokumentation untersuchen, um zu verifizieren, dass Prozeduren für die Überprüfung der Konfigurationen von NSCs mindestens alle sechs Monate definiert sind.	
	1.2.7.b Dokumentation der Überprüfungen von Konfigurationen für NSCs untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass Überprüfungen mindestens alle sechs Monate stattfinden.	
Zielsetzung des kundenspezifischen Ansatzes	**1.2.7.c** Konfigurationen für NSCs untersuchen, um zu verifizieren, dass Konfigurationen, die durch eine geschäftliche Begründung als nicht mehr unterstützt identifiziert wurden, entfernt oder aktualisiert werden.	
NSC-Konfigurationen, die den Zugriff auf vertrauenswürdige Netzwerke zulassen oder einschränken, werden regelmäßig verifiziert, um sicherzustellen, dass nur autorisierte Verbindungen mit einer aktuellen geschäftlichen Begründung zugelassen werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Um zu verhindern, dass nicht autorisierte Konfigurationen auf das Netzwerk angewendet werden, müssen gespeicherte Dateien mit Konfigurationen für Netzwerksteuerungen auf dem neuesten Stand gehalten und gegen nicht autorisierte Änderungen gesichert werden. Wenn die Konfigurationsinformationen aktuell und sicher gehalten werden, wird sichergestellt, dass bei jeder Ausführung der Konfiguration die richtigen Einstellungen für NSCs angewendet werden. **Beispiele** Wenn die sichere Konfiguration für einen Router im nichtflüchtigen Speicher gespeichert wird, sollten diese Kontrollen bei der Wiederaufnahme oder dem Neustart dieses Routers sicherstellen, dass seine sichere Konfiguration wiederhergestellt wird.
1.2.8 Konfigurationsdateien für NSCs sind: • Vor nicht autorisiertem Zugriff gesichert. • Werden konsistent mit aktiven Netzwerkkonfigurationen gehalten.	**1.2.8.** Konfigurationsdateien für NSCs untersuchen, um zu verifizieren, dass sie mit allen in dieser Anforderung angegebenen Elementen übereinstimmen.	
Zielsetzung des kundenspezifischen Ansatzes		
NSCs können nicht mit nicht vertrauenswürdigen Konfigurationsobjekten (einschließlich Dateien) definiert oder modifiziert werden.		
Hinweise zur Anwendbarkeit		
Jede Datei oder Einstellung, die zum Konfigurieren oder Synchronisieren von NSCs verwendet wird, wird als „Konfigurationsdatei“ betrachtet. Dies beinhaltet Dateien, automatisierte und systembasierte Kontrollen, Skripte, Einstellungen, Infrastruktur als Code oder andere Parameter, die gesichert, archiviert oder entfernt gespeichert werden.		

Anforderungen und Testprozeduren		Anleitungen
1.3 Der Netzwerkzugriff auf und von der Karteninhaberdatenumgebung ist eingeschränkt.		
Definierte Ansatzanforderungen **1.3.1** Der eingehende Verkehr zur CDE wird wie folgt eingeschränkt: • Nur auf Verkehr, der notwendig ist. • Jeder andere Verkehr wird gezielt verweigert. **Zielsetzung des kundenspezifischen Ansatzes** Nicht autorisierter Verkehr kann nicht in die CDE gelangen.	**Testprozeduren mit definiertem Ansatz** **1.3.1.a** Konfigurationen von NSCs untersuchen, um zu verifizieren, dass sie einschränkenden eingehenden Verkehr zur CDE gemäß allen in dieser Anforderung angegebenen Elementen ist. **1.3.1.b** Konfigurationen von NSCs untersuchen, um zu verifizieren, dass der eingehende Verkehr zur CDE gemäß allen in dieser Anforderung angegebenen Elementen eingeschränkt ist.	**Zweck** Diese Anforderung soll verhindern, dass böswillige Personen über nicht autorisierte IP-Adressen auf das Netzwerk der Entität zugreifen oder Dienstleistungen, Protokolle oder Ports auf nicht autorisierte Weise nutzen. **Gute Praxis** Der gesamte zur CDE eingehende Verkehr, unabhängig von seinem Ursprung, sollte bewertet werden, um sicherzustellen, dass er etablierten, autorisierten Regeln folgt. Verbindungen sollten inspiziert werden, um sicherzustellen, dass Verkehr nur auf autorisierte Kommunikation beschränkt ist – zum Beispiel durch Beschränkung von Quell-/Zieladressen und Ports und Sperren von Inhalten. **Beispiele** Das Implementieren einer Regel, die den gesamten ein- und ausgehenden Verkehr ablehnt, der nicht speziell benötigt wird – beispielsweise durch die Verwendung einer expliziten „Alles verweigern“ oder einer impliziten Verweigerung nach dem Erlauben – trägt dazu bei, unbeabsichtigte Lücken zu vermeiden, die unbeabsichtigten und potenziell schädlichen Verkehr ermöglichen würden.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Diese Anforderung soll verhindern, dass böswillige Personen und kompromittierte Systemkomponenten innerhalb des Netzwerks der Entität mit einem nicht vertrauenswürdigen externen Host kommunizieren. **Gute Praxis** Der gesamte zur CDE eingehende Verkehr, unabhängig von seinem Ziel, sollte bewertet werden, um sicherzustellen, dass er etablierten, autorisierten Regeln folgt. Verbindungen sollten inspiziert werden, um Verkehr nur auf autorisierte Kommunikationen zu beschränken – zum Beispiel durch Beschränkung von Quell-/Zieladressen und Ports und Sperren von Inhalten. **Beispiele** Das Implementieren einer Regel, die den gesamten ein- und ausgehenden Verkehr ablehnt, der nicht speziell benötigt wird – beispielsweise durch die Verwendung einer expliziten „Alles verweigern“ oder einer impliziten Verweigerung nach dem Erlauben – trägt dazu bei, unbeabsichtigte Lücken zu vermeiden, die unbeabsichtigten und potenziell schädlichen Verkehr ermöglichen würden.
1.3.2 Der ausgehende Verkehr von der CDE wird wie folgt eingeschränkt: • Nur auf Verkehr, der notwendig ist. • Jeder andere Verkehr wird gezielt verweigert.	**1.3.2.a** Konfigurationen für NSCs untersuchen, um zu verifizieren, dass sie einschränkenden ausgehenden Verkehr zur CDE gemäß allen in dieser Anforderung angegebenen Elementen definieren.	
Zielsetzung des kundenspezifischen Ansatzes Nicht autorisierter Verkehr kann die CDE nicht verlassen.	**1.3.2.b** Konfigurationen von NSCs untersuchen, um zu verifizieren, dass der ausgehende Verkehr von der CDE gemäß allen in dieser Anforderung angegebenen Elementen eingeschränkt ist.	
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die bekannte (oder unbekannte) Implementierung und Ausnutzung von drahtloser Technologie innerhalb eines Netzwerks ist ein üblicher Weg für böswillige Personen, um Zugriff auf das Netzwerk und die Kontodaten zu erhalten. Wenn ein drahtloses Gerät oder Netzwerk ohne Wissen der Entität installiert wird, könnte eine böswillige Person leicht und „unsichtbar“ in das Netzwerk eindringen. *(Fortsetzung auf der nächsten Seite)*
1.3.3 NSCs werden zwischen allen drahtlosen Netzwerken und der CDE installiert, unabhängig davon, ob es sich bei dem drahtlosen Netzwerk um ein CDE handelt, so dass: • Der gesamte drahtlose Verkehr von drahtlosen Netzwerken in die CDE wird standardmäßig abgelehnt. • Nur drahtloser Verkehr mit einem autorisierten Geschäftszweck ist in die CDE zugelassen.	**1.3.3.a** Konfigurationseinstellungen und Netzwerkdiagramme untersuchen, um zu verifizieren, dass NSCs zwischen allen drahtlosen Netzwerken und der CDE gemäß allen in dieser Anforderung angegebenen Elementen implementiert sind.	

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Nicht autorisierter Verkehr kann Netzwerkgrenzen zwischen drahtlosen Netzwerken und kabelgebundenen Umgebungen in der CDE nicht überqueren.		Wenn NSCs den Zugriff von drahtlosen Netzwerken auf die CDE nicht einschränken, können sich böswillige Personen, die sich nicht autorisierten Zugriff auf das drahtlose Netzwerk verschaffen, leicht mit der CDE verbinden und Kontoinformationen kompromittieren.

Anforderungen und Testprozeduren		Anleitungen
1.4 Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
1.4.1 NSCs werden zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken implementiert.	**1.4.1.a** Konfigurationsstandards und Netzwerkdiagramme untersuchen, um zu verifizieren, dass NSCs zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken definiert sind.	Die Implementierung von NSCs bei jeder Verbindung, die in vertrauenswürdige Netzwerke ein- und ausgeht, gestattet es der Entität, den Zugriff zu überwachen und zu kontrollieren, und minimiert die Chancen, dass eine böswillige Person über eine ungeschützte Verbindung Zugriff auf das interne Netzwerk erhält.
Zielsetzung des kundenspezifischen Ansatzes	**1.4.1.b** Netzwerkkonfigurationen untersuchen, um zu verifizieren, dass NSCs zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken gemäß den dokumentierten Konfigurationsstandards und Netzwerkdiagrammen vorhanden sind.	**Beispiele**
Nicht autorisierter Verkehr kann keine Netzwerkgrenzen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken überqueren.		Eine Entität könnte eine DMZ implementieren, die ein Teil des Netzwerks ist, das Verbindungen zwischen einem nicht vertrauenswürdigen Netzwerk (Beispiele für nicht vertrauenswürdige Netzwerke finden Sie in der Übersicht von Anforderung 1) und Dienstleistungen verwaltet, die eine Organisation der Öffentlichkeit zur Verfügung stellen muss, wie einen Webserver. Bitte Beobachten Sie, dass, wenn die DMZ einer Entität, die Kontodaten verarbeitet oder überträgt (zum Beispiel eine E-Commerce-Webseite), ebenfalls als CDE betrachtet wird.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Sicherstellung, dass der öffentliche Zugriff auf eine Systemkomponente ausdrücklich autorisiert ist, verringert das Risiko, dass Systemkomponenten unnötigerweise nicht vertrauenswürdigen Netzwerken ausgesetzt werden. **Gute Praxis** Systemkomponenten, die öffentlich zugängliche Dienste bereitstellen, wie E-Mail-, Web- und DNS-Server, sind am anfälligsten für Bedrohungen, die von nicht vertrauenswürdigen Netzwerken ausgehen. Idealerweise werden solche Systeme in ein dediziertes, vertrauenswürdiges Netzwerk platziert, das der Öffentlichkeit zugänglich ist (zum Beispiel einer DMZ), das jedoch über NSCs von sensibleren internen Systemen getrennt ist, was zum Schutz des restlichen Netzwerks beiträgt, falls diese von außen zugänglichen Systeme kompromittiert werden. Diese Funktionalität soll verhindern, dass böswillige Akteure über das Internet auf das interne Netzwerk der Organisation zugreifen oder Dienstleistungen, Protokolle oder Ports auf nicht autorisierte Weise verwenden. Wenn diese Funktionalität als integrierte Funktion eines NSC bereitgestellt wird, sollte die Entität sicherstellen, dass ihre Konfigurationen nicht dazu führen, dass die Funktionalität deaktiviert oder umgangen wird. **Definitionen** Das Aufrechterhalten des „Zustands“ (oder Status) für jede Verbindung zu einem Netzwerk bedeutet, dass der NSC „weiß“, ob eine scheinbare Antwort auf eine vorherige Verbindung eine gültige, autorisierte Antwort ist (da der NSC den Status jeder Verbindung beibehält) oder ob es sich um böswilligen Verkehr handelt, der versucht, den NSC dazu zu bringen, die Verbindung zuzulassen.
1.4.2 Eingehender Verkehr von nicht vertrauenswürdigen Netzwerken zu vertrauenswürdigen Netzwerken ist beschränkt auf: • Kommunikationen mit Systemkomponenten, die autorisiert sind, öffentlich zugängliche Dienste, Protokolle und Ports bereitzustellen. • Zustandsbehaftete Antworten auf Kommunikationen, die von Systemkomponenten in einem vertrauenswürdigen Netzwerk eingeleitet wurden. • Alle anderen Verkehre werden verweigert.	**1.4.2.** Anbieterkonfigurationen und Konfigurationen von NSCs untersuchen, um zu verifizieren, dass eingehender Verkehr von nicht vertrauenswürdigen Netzwerken zu vertrauenswürdigen Netzwerken gemäß allen in dieser Anforderung angegebenen Elementen eingeschränkt wird.	
Zielsetzung des kundenspezifischen Ansatzes Nur Verkehr, der autorisiert ist oder eine Reaktion auf eine Systemkomponente im vertrauenswürdigen Netzwerk ist, kann von einem nicht vertrauenswürdigen Netzwerk in ein vertrauenswürdiges Netzwerk eingehen.		
Hinweise zur Anwendbarkeit Die Absicht dieser Anforderung besteht darin, Kommunikationssitzungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken zu adressieren, anstatt die Besonderheiten von Protokollen. Diese Anforderung schränkt die Verwendung von UDP oder anderen verbindungslosen Netzwerkprotokollen nicht ein, wenn der Zustand vom NSC aufrechterhalten wird.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Filtern von Paketen, die in das vertrauenswürdige Netzwerk gelangen, hilft unter anderem sicherzustellen, dass Pakete nicht „parodiert" werden, um den Anschein zu erwecken, dass sie aus dem internen Netzwerk einer Organisation stammen. Zum Beispiel verhindern Anti-Spoofing-Maßnahmen, dass interne Adressen aus dem Internet in die DMZ gelangen. **Gute Praxis** Produkte werden normalerweise standardmäßig mit einem Anti-Spoofing-Satz geliefert und können möglicherweise nicht konfiguriert werden. Die Entitäten sollten die Anbieterdokumentation für weitere Informationen konsultieren. **Beispiele** Normalerweise enthält ein Paket die IP-Adresse des Computers, der es ursprünglich gesendet hat, damit andere Computer im Netzwerk wissen, woher das Paket stammt. Böswillige Personen versuchen oft, die sendende IP-Adresse zu parodieren (oder zu imitieren), um dem Zielsystem vorzutäuschen, dass das Paket von einer vertrauenswürdigen Quelle stammt.
1.4.3 Anti-Spoofing-Maßnahmen werden implementiert, um gefälschte Quell-IP-Adressen zu erkennen und daran zu hindern, in das vertrauenswürdige Netzwerk einzudringen.	**1.4.3** Anbieterdokumentation und Konfigurationen für NSCs untersuchen, um zu verifizieren, dass Anti-Spoofing-Maßnahmen implementiert sind, um gefälschte Quell-IP-Adressen zu erkennen und daran zu hindern, in das vertrauenswürdige Netzwerk einzudringen.	
Zielsetzung des kundenspezifischen Ansatzes		
Pakete mit gefälschten IP-Quelladressen können nicht in ein vertrauenswürdiges Netzwerk eintreten.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
1.4.4 Auf Systemkomponenten, die Karteninhaberdaten speichern, kann von nicht vertrauenswürdigen Netzwerken nicht direkt zugegriffen werden.	**1.4.4.a** Das Datenflussdiagramm und das Netzwerkdiagramm untersuchen, um zu verifizieren, dass dokumentiert ist, dass auf Systemkomponenten, die Karteninhaberdaten speichern, nicht direkt von nicht vertrauenswürdigen Netzwerken zugegriffen werden kann.	Karteninhaberdaten, auf die aus einem nicht vertrauenswürdigen Netzwerk direkt zugegriffen werden kann, beispielsweise weil sie auf einem System innerhalb der DMZ oder in einer Cloud-Datenbankdienstleistung gespeichert sind, sind für einen externen Angreifer leichter zugänglich, da weniger Verteidigungsschichten durchdrungen werden. Die Verwendung von NSCs, um sicherzustellen, dass auf Systemkomponenten, die Karteninhaberdaten speichern (wie eine Datenbank oder eine Datei), nur von vertrauenswürdigen Netzwerken direkt zugegriffen werden kann, kann verhindern, dass nicht autorisierter Netzwerkverkehr die Systemkomponente erreicht.
Zielsetzung des kundenspezifischen Ansatzes	**1.4.4.b** Konfigurationen von NSCs untersuchen, um zu verifizieren, dass Kontrollen so implementiert sind, dass Systemkomponenten, die Karteninhaberdaten speichern, nicht direkt von nicht vertrauenswürdigen Netzwerken aus zugänglich sind.	
Auf gespeicherte Karteninhaberdaten kann von nicht vertrauenswürdigen Netzwerken nicht zugegriffen werden.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nicht für die Speicherung von Kontodaten in flüchtigem Speicher, gilt jedoch dort, wo der Speicher als persistenter Speicher behandelt wird (z. B. RAM-Disk). Kontodaten können nur während der Zeit im flüchtigen Speicher gespeichert werden, die zur Unterstützung des zugehörigen Geschäftsprozesses erforderlich ist (zum Beispiel bis zum Abschluss der entsprechenden Zahlungskartentransaktion).		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Beschränkung der Offenlegung interner, privater und lokaler IP-Adressen ist nützlich, um zu verhindern, dass ein Hacker Kenntnis von diesen IP-Adressen erhält und diese Informationen für den Zugriff auf das Netzwerk verwendet. **Gute Praxis** Die zur Erfüllung dieser Anforderung verwendeten Methoden können je nach verwendeter Netzwerktechnologie variieren. Zum Beispiel, die zur Erfüllung dieser Anforderung verwendeten Steuerelemente können für IPv4-Netzwerke anders sein als für IPv6-Netzwerke. **Beispiele** Methoden zum Verschleiern der IP-Adressierung können beinhalten, sind aber nicht beschränkt auf: • IPv4-Netzwerkadressübersetzung (NAT). • Platzierung von Systemkomponenten hinter Proxyservern/NSCs. • Entfernen oder Filtern von Routenankündigungen für interne Netzwerke, die registrierte Adressierung verwenden. • Interne Verwendung von RFC 1918 (IPv4) oder Verwendung der IPv6-Datenschutzerweiterung (RFC 4941) beim Einleiten von ausgehenden Sitzungen zum Internet.
1.4.5 Die Offenlegung interner IP-Adressen und Routing-Informationen ist nur auf autorisierten Parteien beschränkt.	**1.4.5.a** Konfigurationen von NSCs untersuchen, um zu verifizieren, dass die Offenlegung interner IP-Adressen und Routing-Informationen nur auf autorisierten Parteien beschränkt ist.	
	1.4.5.b Das Personal befragen und die Dokumentation untersuchen, um zu verifizieren, dass Kontrollen implementiert sind, sodass die Offenlegung interner IP-Adressen und Routing-Informationen nur auf autorisierten Parteien beschränkt ist.	
Zielsetzung des kundenspezifischen Ansatzes		
Interne Netzwerkinformationen sind vor nicht autorisierter Offenlegung geschützt.		

Anforderungen und Testprozeduren		Anleitungen
1.5 Risiken für die CDE durch Computergeräte, die sich sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbinden können, werden gemindert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
1.5.1 Sicherheitskontrollen werden auf allen Computergeräten implementiert, einschließlich unternehmens- und mitarbeitereigenen Geräten, die sich mit nicht vertrauenswürdigen Netzwerken (einschließlich dem Internet) und der CDE wie folgt verbinden: • Spezifische Konfigurationseinstellungen werden definiert, um zu verhindern, dass Bedrohungen in das Netzwerk der Entität eingeführt werden. • Sicherheitskontrollen werden aktiv durchgeführt. • Sicherheitskontrollen können von Benutzern der Computergeräte nicht geändert werden, es sei denn, dies wird von der Geschäftsleitung im Einzelfall für einen begrenzten Zeitraum ausdrücklich dokumentiert und genehmigt.	**1.5.1.a** Richtlinien und Konfigurationsstandards untersuchen und das Personal befragen, um zu verifizieren, dass die Sicherheitskontrollen für Computergeräte, die sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit der CDE verbunden sind, gemäß allen in dieser Anforderung festgelegten Elementen implementiert sind.	Computergeräte, die sich von außerhalb der Unternehmensumgebung mit dem Internet verbinden dürfen – zum Beispiel Desktops, Laptops, Tablets, Smartphones und andere mobile Computergeräte, die von Mitarbeitern verwendet werden – sind für internetbasierte Bedrohungen anfälliger. Verwendung von Sicherheitskontrollen wie hostbasierte Kontrollen (z. B. persönliche Firewall-Software oder Endpunktschutzlösungen), netzwerkbasierte Sicherheitskontrollen (z. B. Firewalls, netzwerkbasierte heuristische Inspektion und Malware-Simulation) oder Hardware, trägt zum Schutz von Geräten vor internetbasierten Angriffen bei, die das Gerät verwenden könnten, um Zugriff auf die Systeme und Daten des Unternehmens zu erhalten, wenn das Gerät wieder mit dem Netzwerk verbunden wird. *(Fortsetzung auf der nächsten Seite)*
Zielsetzung des kundenspezifischen Ansatzes	**1.5.1.b** Konfigurationseinstellungen auf Computergeräten, die sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbunden sind, untersuchen, um zu verifizieren, dass die Einstellungen gemäß mit allen in dieser Anforderung angegebenen Elementen implementiert wurden.	
Geräte, die sich mit nicht vertrauenswürdigen Umgebungen verbinden und sich auch mit der CDE verbinden, können keine Bedrohung für die CDE der Entität einführen.		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Diese Sicherheitskontrollen dürfen nur dann vorübergehend deaktiviert werden, wenn ein berechtigter technischer Bedarf besteht, der von der Verwaltung im Einzelfall genehmigt wird. Wenn diese Sicherheitskontrollen für einen bestimmten Zweck deaktiviert werden müssen, muss dieses formell autorisiert werden. Für den Zeitraum, in dem diese Sicherheitskontrollen nicht aktiv sind, müssen möglicherweise zusätzliche Sicherheitsmaßnahmen implementiert werden. Diese Anforderung gilt für mitarbeiter- und unternehmenseigene Computergeräte. Systeme, die nicht durch Unternehmensrichtlinien verwaltet werden können, führen zu Schwachstellen und stellen Möglichkeiten bereit, die böswillige Personen ausnutzen können.		**Gute Praxis** Die spezifischen Konfigurationseinstellungen werden von der Entität festgelegt und sollten mit ihren Netzwerksicherheitsrichtlinien und -verfahren konsistent sein. Wenn eine berechtigte Notwendigkeit besteht, die Sicherheitskontrollen auf einem unternehmenseigenen oder mitarbeitereigenen Gerät, das sowohl mit einem nicht vertrauenswürdigen Netzwerk als auch mit der CDE verbunden ist, vorübergehend zu deaktivieren - zum Beispiel um eine bestimmte Wartungsaktivität oder Untersuchung eines technischen Problems zu unterstützen - dann wird der Grund für das Ergreifen solcher Maßnahmen von einem geeigneten Verwaltungsvertreter verstanden und genehmigt. Jede Deaktivierung oder Änderung dieser Sicherheitskontrollen, auch auf den Geräten der Administratoren, wird von autorisiertem Personal durchgeführt. Es wird anerkannt, dass Administratoren über Berechtigungen verfügen, die es ihnen ermöglichen können, Sicherheitskontrollen auf ihren eigenen Computern zu deaktivieren, aber es sollten Warnmechanismen vorhanden sein, wenn solche Kontrollen deaktiviert werden, und es werden Nachverfolgungsmaßnahmen durchgeführt, um sicherzustellen, dass Prozesse befolgt wurden. **Beispiele** Praktiken beinhalten das Verbot von Split-Tunneling von VPNs für mitarbeiter- oder unternehmenseigene Mobilgeräte und das Erfordernis, dass solche Geräte in einem VPN hochfahren.

Anforderung 2: Anwendung sicherer Konfigurationen auf alle Systemkomponenten

Abschnitte	
2.1	Prozesse und Mechanismen zum Anwenden sicherer Konfigurationen auf alle Systemkomponenten werden definiert und verstanden.
2.2	Systemkomponenten werden sicher konfiguriert und verwaltet.
2.3	Drahtlose Komponenten werden sicher konfiguriert und verwaltet.

Übersicht

Böswillige Personen, sowohl extern als auch intern, verwenden häufig Standardpasswörter und Standardeinstellungen anderer Anbieter, um Systeme zu kompromittieren. Diese Passwörter und Einstellungen sind bekannt und können leicht über öffentliche Informationen ermittelt werden.

Das Anwenden sicherer Konfigurationen auf Systemkomponenten verringert die Mittel, die einem Angreifer zur Verfügung stehen, um das System zu kompromittieren. Das Ändern von Standardpasswörtern, das Entfernen unnötiger Software, Funktionen und Konten, sowie das Deaktivieren oder Entfernen unnötiger Dienste tragen dazu bei, die potenzielle Angriffsfläche zu verringern.

Finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
2.1 Prozesse und Mechanismen zum Anwenden sicherer Konfigurationen auf alle Systemkomponenten werden definiert und verstanden.		
Definierte Ansatzanforderungen **2.1.1** Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 2 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt. **Zielsetzung des kundenspezifischen Ansatzes** Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 2 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht des Managements.	**Testprozeduren mit definiertem Ansatz** **2.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 2 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Bei Anforderung 2.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 2 angegeben sind. Während es wichtig ist, die in Anforderung 2 genannten spezifischen Richtlinien oder Verfahren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Verfahren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Verfahren und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen sind, ist das Personal sich möglicherweise seiner täglichen Verantwortlichkeiten nicht bewusst und kritische Aktivitäten können nicht stattfinden. **Gute Praxis** Rollen und Verantwortlichkeiten können in Richtlinien und Verfahren dokumentiert oder in separaten Dokumenten gewartet werden. Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen. **Beispiele** Ein Verfahren zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).
2.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 2 werden dokumentiert, zugewiesen und verstanden.	**2.1.2.a** Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 2 dokumentiert und zugewiesen sind.	
	2.1.2.b Befragung von Personal mit Verantwortlichkeit zur Durchführung von Aktivitäten in Anforderung 2, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 2 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
2.2 Systemkomponenten werden sicher konfiguriert und verwaltet.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Es gibt bekannte Schwachstellen bei vielen Betriebssystemen, Datenbanken, Netzwerkgeräten, Software, Anwendungen, Container-Images und anderen Geräten, die von einer Entität oder in der Umgebung einer Entität verwendet werden. Es gibt auch bekannte Wege, diese Systemkomponenten zu konfigurieren, um Schwachstellen zu beheben. Das Beheben von Schwachstellen verringert die Möglichkeiten, die einem Angreifer zur Verfügung stehen. Durch die Entwicklung von Standards stellen Entitäten sicher, dass ihre Systemkomponenten konsistent und sicher konfiguriert werden, und adressieren den Schutz von Geräten, für die eine vollständige Härtung möglicherweise schwieriger ist. **Gute Praxis** Sich über aktuelle Branchenrichtlinien auf dem Laufenden zu halten, hilft dem Unternehmen, sichere Konfigurationen aufrechtzuerhalten. Die auf ein System anzuwendenden spezifischen Kontrollen variieren und sollten für den Typ und die Funktion des Systems geeignet sein. Zahlreiche Sicherheitsorganisationen haben Richtlinien und Empfehlungen zur Systemhärtung etabliert, die Ratschläge zur Behebung allgemeiner, bekannter Schwachstellen geben. **Weitere Informationen** Quellen für Anleitungen zu Konfigurationsstandards sind unter anderem: Center for Internet Security (CIS), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Cloud Security Alliance, und Produktanbieter.
2.2.1 Konfigurationsstandards werden entwickelt, implementiert und gewartet, um: • Alle Systemkomponenten abzudecken. • Alle bekannten Schwachstellen zu adressieren. • Mit branchenübliche Standards für die Systemhärtung oder die Empfehlungen der Anbieter zur Härtung konsistent zu sein. • Wenn neue Schwachstellen identifiziert werden, wie in Anforderung 6.3.1 definiert, aktualisiert zu sein. • Wenn neue Systeme konfiguriert und verifiziert werden, wie sie bevor oder unmittelbar vorhanden sind, nachdem eine Systemkomponente mit einer Produktionsumgebung verbunden wird, angewandt zu sein.	**2.2.1.a** Systemkonfigurationsstandards untersuchen, um zu verifizieren, dass sie Prozesse definieren, die alle in dieser Anforderung angegebenen Elemente beinhalten.	
	2.2.1.b Richtlinien und Prozeduren untersuchen und das Personal befragen, um zu verifizieren, dass die Systemkonfigurationsstandards aktualisiert werden, wenn neue Schwachstellen identifiziert werden, wie in Anforderung 6.3.1 definiert.	
	2.2.1.c Konfigurationseinstellungen untersuchen und das Personal befragen, um zu verifizieren, dass die Systemkonfigurationsstandards angewendet werden, wenn neue Systeme konfiguriert und als vorhanden verifiziert werden, bevor oder unmittelbar nachdem eine Systemkomponente mit einer Produktionsumgebung verbunden wird.	
Zielsetzung des kundenspezifischen Ansatzes		
Alle Systemkomponenten werden sicher und konsistent und gemäß branchenüblichen Härtungsstandards oder Anbieterempfehlungen konfiguriert.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Böswillige Personen verwenden häufig die Standardkontonamen und -passwörter von Anbietern, um Betriebssysteme, Anwendungen, und die Systeme, auf denen sie installiert sind, zu kompromittieren. Da diese Standardeinstellungen häufig veröffentlicht und bekannt sind, werden die Systeme durch eine Änderung dieser Einstellungen weniger anfällig für Angriffe. **Gute Praxis** Alle Anbieter-Standardkonten sollten identifiziert, und ihr Zweck und ihre Verwendung sollten verstanden werden. Es ist wichtig, Kontrollen für Anwendungs- und Systemkonten einzurichten, einschließlich der Konten, die zur Bereitstellung und Wartung von Cloud-Diensten verwendet werden, damit diese keine Standardpasswörter verwenden und nicht von nicht autorisierten Personen verwendet werden können. Wenn kein Standardkonto verwendet werden soll, wird durch Ändern des Standardpassworts in ein eindeutiges Passwort, das die PCI DSS-Anforderung 8.3.6 erfüllt, das Entfernen des Zugriffs auf das Standardkonto und das anschließende Deaktivieren des Kontos verhindert, dass eine böswillige Person das Konto wieder aktivieren kann und Zugriff mit dem Standardpasswort erhalten kann. Die Verwendung eines isolierten Staging-Netzwerks, um neue Systeme zu installieren und zu konfigurieren wird empfohlen und kann auch verwendet werden, um zu bestätigen, dass Standardanmeldeinformationen in Produktionsumgebungen nicht eingeführt wurden. **Beispiele** Standardeinstellungen, die berücksichtigt werden sollen, beinhalten Benutzer-IDs, Passwörter und andere Authentifizierungsreferenzen, die üblicherweise von Anbietern in ihren Produkten verwendet werden.
2.2.2 Anbieterstandardkonten werden wie folgt verwaltet: • Wenn die Anbieter-Standardkonten verwendet werden, wird das Standardpasswort gemäß Anforderung 8.3.6 geändert. • Wenn die Anbieter-Standardkonten nicht verwendet werden, wird das Konto entfernt oder deaktiviert.	**2.2.2.a** Systemkonfigurationsstandards untersuchen, um zu verifizieren, dass sie die Verwaltung der Anbieter-Standardkonten gemäß allen in dieser Anforderung genannten Elementen beinhalten.	
	2.2.2.b Anbieterdokumentation untersuchen und einen Systemadministrator beobachten, der sich mit Verwendung der Anbieter-Standardkonten anmeldet, um zu verifizieren, dass die Konten gemäß allen in dieser Anforderung angegebenen Elementen implementiert sind.	
Zielsetzung des kundenspezifischen Ansatzes Auf Systemkomponenten kann nicht mit Standardpasswörtern zugegriffen werden.	**2.2.2.c** Konfigurationsdateien untersuchen und das Personal befragen, um zu verifizieren, dass alle nicht verwendeten Standardkonten des Anbieters entfernt oder deaktiviert wurden.	
Hinweise zur Anwendbarkeit Dies gilt für ALLE Anbieter-Standardkonten und -Passwörter, einschließlich, aber nicht beschränkt auf diejenigen, die von Betriebssystemen verwendet werden, Software, die Sicherheitsdienstleistungen bereitstellt, Anwendungs- und Systemkonten, Verkaufsstellen-Terminals (POS), Zahlungsanwendungen und Simple Network Standardeinstellungen für das einfache Netzwerkverwaltungsprotokoll (SNMP). Diese Anforderung gilt auch, wenn eine Systemkomponente nicht in der Umgebung einer Entität installiert ist, zum Beispiel Software und Anwendungen, die Teil der CDE sind und auf die über eine Cloud-Abonnementdienstleistung zugegriffen wird.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
2.2.3 Primäre Funktionen, die unterschiedliche Sicherheitsstufen erfordern, werden wie folgt verwaltet: • Auf einer Systemkomponente existiert nur eine primäre Funktion, **ODER** • Primäre Funktionen mit unterschiedlichen Sicherheitsstufen, die auf derselben Systemkomponente existieren, sind voneinander isoliert, **ODER** • Primäre Funktionen mit unterschiedlichen Sicherheitsstufen auf derselben Systemkomponente werden alle auf der Stufe gesichert, die die Funktion mit dem höchsten Sicherheitsbedürfnis erfordert.	**2.2.3.a** Systemkonfigurationsstandards untersuchen, um zu verifizieren, dass sie die Verwaltung von primären Funktionen umfassen, die unterschiedliche Sicherheitsstufen erfordern, wie in dieser Anforderung angegeben. **2.2.3.b** Systemkonfigurationsstandards untersuchen, um zu verifizieren, dass primäre Funktionen, die unterschiedliche Sicherheitsstufen erfordern, auf eine der in dieser Anforderung angegebenen Weisen verwaltet werden. **2.2.3.c** Wenn Virtualisierungstechnologien verwendet werden, Systemkonfigurationen untersuchen, um zu verifizieren, dass Systemfunktionen, die unterschiedliche Sicherheitsstufen erfordern, auf eine der folgenden Arten verwaltet werden: • Funktionen mit unterschiedlichen Sicherheitsanforderungen koexistieren nicht auf derselben Systemkomponente. • Funktionen mit unterschiedlichen Sicherheitsanforderungen, die auf derselben Systemkomponente existieren, sind voneinander isoliert. • Primäre Funktionen mit unterschiedlichen Sicherheitsbedürfnissen auf derselben Systemkomponente werden alle auf der Stufe gesichert, die die Funktion mit dem höchsten Sicherheitsbedürfnis erfordert.	Systeme, die eine Kombination aus Dienstleistungen, Protokollen und Dämonen für ihre Hauptfunktion enthalten, haben ein Sicherheitsprofil, das geeignet ist, um zu gestatten, dass diese Funktion effektiv arbeiten kann. Zum Beispiel Systeme, die direkt mit dem Internet verbunden sein müssen, würden ein bestimmtes Profil, wie einen DNS-Server, Webserver oder einen E-Commerce-Server haben. Umgekehrt können andere Systemkomponenten eine primär Funktion betreiben, die einen anderen Satz von Dienstleistungen, Protokollen und Dämonen umfasst, die Funktionen durchführt, die eine Entität nicht dem Internet zugänglich machen möchte. Diese Anforderung soll sicherstellen, dass unterschiedliche Funktionen die Sicherheitsprofile anderer Dienstleistungen nicht in einer Weise beeinflussen, die dazu führen kann, dass diese auf einer höheren oder niedrigeren Sicherheitsstufe betrieben werden. **Gute Praxis** Idealerweise sollte jede Funktion auf verschiedenen Systemkomponenten platziert werden. Dies kann erreicht werden, indem auf jeder Systemkomponente nur eine primäre Funktion implementiert wird. Eine andere Möglichkeit besteht darin, primäre Funktionen auf derselben Systemkomponente mit unterschiedlichen Sicherheitsstufen zu isolieren, zum Beispiel Webserver (die direkt mit dem Internet verbunden sein müssen) von Anwendungs- und Datenbankservern zu isolieren. *(Fortsetzung auf der nächsten Seite)*
Zielsetzung des kundenspezifischen Ansatzes		
Primäre Funktionen mit niedrigeren Sicherheitsanforderungen können die Sicherheit von primären Funktionen mit höheren Sicherheitsanforderungen auf derselben Systemkomponente nicht beeinträchtigen.		

Anforderungen und Testprozeduren		Anleitungen
		Wenn eine Systemkomponente primäre Funktionen enthält, die unterschiedliche Sicherheitsstufen benötigen, besteht eine dritte Möglichkeit darin, zusätzliche Kontrollen zu implementieren, um sicherzustellen, dass die resultierende Sicherheitsstufe der primären Funktion(en) mit höheren Sicherheitsanforderungen nicht durch das Vorhandensein der primären Funktionen mit niedrigerer Sicherheit verringert wird. Zusätzlich sollten die Funktionen mit einer niedrigeren Sicherheitsstufe isoliert und/oder gesichert werden, um sicherzustellen, dass sie nicht auf die Ressourcen einer anderen Systemfunktion zugreifen oder diese beeinflussen können und keine Sicherheitsschwächen in andere Funktionen auf demselben Server einführen. Funktionen unterschiedlicher Sicherheitsstufen können entweder durch physische oder logische Kontrollen isoliert werden. Zum Beispiel, ein Datenbanksystem sollte nicht auch Webdienstleistungen hosten, es sei denn, es werden Kontrollen wie Virtualisierungstechnologien verwendet, um die Funktionen zu isolieren und in separaten Subsystemen einzudämmen. Ein weiteres Beispiel ist die Verwendung virtueller Instanzen oder die Bereitstellung von dediziertem Speicherzugriff durch Systemfunktion. Wenn Virtualisierungstechnologien verwendet werden, sollten die Sicherheitsstufen für jede virtuelle Komponente identifiziert und verwaltet werden. Beispiele für Überlegungen für virtualisierte Umgebungen beinhalten: • Die Funktion jeder Anwendung, jedes Containers oder jeder virtuellen Serverinstanz. • Wie virtuelle Maschinen (VMs) oder Container gespeichert und gesichert werden.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
2.2.4 Nur notwendige Dienstleistungen, Protokolle, Dämonen und Funktionen werden aktiviert und jede unnötige Funktionalität wird entfernt oder deaktiviert.	**2.2.4.a** Systemkonfigurationsstandards untersuchen, um zu verifizieren, dass die erforderlichen Systemdienstleistungen, Protokolle und Dämonen identifiziert und dokumentiert werden.	Unnötige Dienstleistungen und Funktionen können böswilligen Personen zusätzliche Möglichkeiten bieten, Zugriff auf ein System zu erhalten. Durch das Entfernen oder Deaktivieren aller unnötigen Dienste, Protokolle, Dämonen und Funktionen können Organisationen sich auf die Sicherung der erforderlichen Funktionen konzentrieren und das Risiko verringern, dass unbekannte oder unnötige Funktionen ausgenutzt werden.
	2.2.4.b Systemenkonfigurationen untersuchen, um Folgendes zu verifizieren: • Jede unnötige Funktionalität wird entfernt oder gesperrt. • Nur die erforderliche Funktionalität, die in den Konfigurationsstandards dokumentiert ist, wird freigeschaltet.	**Gute Praxis** Es gibt viele Protokolle, die standardmäßig aktiviert werden könnten und die häufig von böswilligen Personen verwendet werden, um ein Netzwerk zu kompromittieren. Das Deaktivieren oder Entfernen aller nicht verwendeten Dienstleistungen, Funktionen und Protokolle minimiert die potenzielle Angriffsfläche – beispielsweise durch Entfernen oder Deaktivieren eines nicht verwendeten FTP- oder Webservers.
Zielsetzung des kundenspezifischen Ansatzes		**Beispiele** Unnötige Funktionalität kann unter anderem Skripte, Treiber, Funktionen, Subsysteme, Dateisysteme, Schnittstellen (USB und Bluetooth) und unnötige Webserver beinhalten.
Systemkomponenten können nicht kompromittiert werden, indem unnötige in der Systemkomponente vorhandene Funktionalität ausgenutzt wird.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Sicherstellung, dass alle unsicheren Dienstleistungen, Protokolle und Dämonen angemessen mit geeigneten Sicherheitsfunktionen gesichert sind, macht es böswilligen Personen schwieriger, gemeinsame Angriffspunkte innerhalb eines Netzwerks auszunutzen. **Gute Praxis** Ermöglichung von Sicherheitsfunktionen vor der Bereitstellung neuer Systemkomponenten verhindert, dass unsichere Konfigurationen in die Umgebung eingeführt werden. Einige Anbieterlösungen stellen möglicherweise zusätzliche Sicherheitsfunktionen bereit, um einen unsicheren Prozess abzusichern. **Weitere Informationen** Anleitungen zu Dienstleistungen, Protokollen oder Dämonen, die als unsicher gelten, finden Sie in den Industriestandards und Anleitungen (zum Beispiel wie von NIST, ENISA und OWASP veröffentlicht).
2.2.5 Wenn irgendwelche unsicheren Dienstleistungen, Protokolle oder Dämonen vorhanden sind: • Die geschäftliche Rechtfertigung wird dokumentiert. • Zusätzliche Sicherheitsfunktionen werden dokumentiert und implementiert, die das Risiko der Verwendung unsicherer Dienstleistungen, Protokollen oder Dämonen reduzieren.	**2.2.5.a** Wenn irgendwelche unsicheren Dienstleistungen, Protokolle oder Dämonen vorhanden sind, Systemkonfigurationsstandards untersuchen und das Personal befragen, um zu verifizieren, dass sie gemäß allen in dieser Anforderung festgelegten Elementen verwaltet und implementiert werden.	
	2.2.5.b Wenn irgendwelche unsicheren Dienstleistungen, Protokolle oder Dämonen vorhanden sind, die Konfigurationsstandards untersuchen, um zu verifizieren, dass zusätzliche Sicherheitsfunktionen implementiert sind, um das Risiko der Verwendung von unsicheren Dienstleistungen, Protokollen oder Dämonen zu reduzieren.	
Zielsetzung des kundenspezifischen Ansatzes		
Systemkomponenten können nicht durch die Ausnutzung von unsicheren Dienstleistungen, Protokollen oder Dämonen kompromittiert werden.		

<table>
<tr><th colspan="2">Anforderungen und Testprozeduren</th><th>Anleitungen</th></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="5">Zweck
Die korrekte Konfiguration von Sicherheitsparametern, die in Systemkomponenten bereitgestellt sind, nutzt die Fähigkeiten der Systemkomponente, um böswillige Angriffe abzuwehren.
Gute Praxis
Systemkonfigurationsstandards und zugehörige Prozesse sollten speziell Sicherheitseinstellungen und Parameter adressieren, die bekannte Auswirkungen auf die Sicherheit für jeden verwendeten Systemtyp haben.
Damit Systeme sicher konfiguriert werden, sollte das für die Konfiguration und/oder die Verwaltung der Systeme verantwortliche Personal mit den spezifischen Sicherheitsparametern und -einstellungen vertraut sein, die für das System gelten. Überlegungen sollten auch sichere Einstellungen für Parameter beinhalten, die verwendet werden, um auf Cloud-Portale zuzugreifen.
Weitere Informationen
Siehe die in Anforderung 2.2.1 vermerkte Anbieterdokumentation und Branchenreferenz für Informationen über geltende Sicherheitsparameter für jede Systemart.</td></tr>
<tr><td rowspan="3">2.2.6 Systemsicherheitsparameter werden konfiguriert, um Missbrauch zu verhindern.</td><td>2.2.6.a Systemkonfigurationsstandards untersuchen, um zu verifizieren, dass sie die Konfiguration von Systemsicherheitsparametern beinhalten, um Missbrauch zu verhindern.</td></tr>
<tr><td>2.2.6.b Systemadministratoren und/oder Sicherheitsmanager befragen, um zu verifizieren, dass sie Kenntnisse über allgemeine Sicherheitsparametereinstellungen für Systemkomponenten haben.</td></tr>
<tr><td rowspan="2">2.2.6.c Systemenkonfigurationen untersuchen, um zu verifizieren, dass allgemeine Sicherheitsparameter richtig und gemäß den Systemkonfigurationsstandards eingestellt sind.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes</td></tr>
<tr><td>Systemkomponenten können wegen einer falschen Konfiguration der Sicherheitsparameter nicht kompromittiert werden.</td><td></td></tr>
</table>

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn die Nicht-Konsolen- (einschließlich Fern-)Administration nicht verschlüsselte Kommunikation verwendet, können administrative Autorisierungsfaktoren (wie IDs und Passwörter) einem Lauscher offenbart werden. Eine böswillige Person könnte diese Informationen verwenden, um auf das Netzwerk zuzugreifen, Administrator zu werden und Daten zu stehlen. **Gute Praxis** Welches Sicherheitsprotokoll auch immer verwendet wird, es sollte so konfiguriert werden, dass nur sichere Versionen und Konfigurationen verwendet werden, um die Verwendung einer unsicheren Verbindung zu verhindern – zum Beispiel, indem nur vertrauenswürdige Zertifikate verwendet werden, nur starke Verschlüsselung unterstützt wird, und kein Rückfall auf schwächere, unsichere Protokolle oder Methoden unterstützt wird **Beispiele** Klartextprotokolle (wie HTTP, Telnet usw.) verschlüsseln weder den Verkehr noch die Anmeldedaten, sodass ein Lauscher diese Informationen leicht abfangen kann. Nicht-Konsolenzugriff kann durch Technologien erleichtert werden, die alternativen Zugriff auf Systeme bereitstellen, einschließlich, aber nicht beschränkt auf Außerhalb des Bandes (OOB), Licht-aus-Verwaltung (LOM), Intelligente Plattform-Verwaltungs-Schnittstelle (IPMI) und Tastatur, Video-, Maus-(KVM)-Schalter mit Fernfunktionen. Diese und andere Nicht-Konsolen-Zugriffstechnologien und -Methoden müssen mit starker Kryptographie gesichert werden. **Weitere Informationen** Beziehen Sie sich auf Industriestandards und bewährte Praktiken wie *NIST SP 800-52 und SP 800-57*.
2.2.7 Alle administrativen Nicht-Konsolen-Zugriffe werden mit Verwendung von starker Kryptographie verschlüsselt.	**2.2.7.a** Systemkonfigurationsstandards untersuchen, um zu verifizieren, dass sie die Verschlüsselung des gesamten Nicht-Konsolen-administrativen Zugriffs mit starker Kryptografie beinhalten.	
	2.2.7.b Eine Administratoranmeldung bei den Systemkomponenten beachten und Systemkonfigurationen untersuchen, um zu verifizieren, ob der Nichtkonsolen-Administratorzugriff gemäß dieser Anforderung verwaltet wird.	
	2.2.7.c Einstellungen für Systemkomponenten und Authentifizierungsdienstleistungen untersuchen, um zu verifizieren, dass unsichere Fern-Anmeldedienstleistungen für den Nichtkonsolen-Administratorzugriff nicht verfügbar sind.	
Zielsetzung des kundenspezifischen Ansatzes Die administrativen Autorisierungsfaktoren von Klartext können von Netzwerkübertragungen nicht gelesen oder abgefangen werden.	**2.2.7.d** Anbieterdokumentation untersuchen und das Personal befragen, um zu verifizieren, dass eine starke Kryptographie für die verwendete Technologie gemäß den bewährten Praktiken der Branche und/oder den Empfehlungen des Anbieters implementiert ist.	
Hinweise zur Anwendbarkeit Dies beinhaltet den administrativen Zugriff über browserbasierte Schnittstellen und Anwendungsprogrammierschnittstellen (APIs).		

Anforderungen und Testprozeduren		Anleitungen
2.3 Drahtlose Komponenten werden sicher konfiguriert und verwaltet.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn drahtlose Netzwerke nicht mit ausreichenden Sicherheitskonfigurationen (einschließlich der Änderung von Standardeinstellungen) implementiert werden, können drahtlose Schnüffler den Verkehr belauschen, Daten und Passwörter leicht erfassen und problemlos in das Netzwerk eindringen und es angreifen. **Gute Praxis** Drahtlose Passwörter sollten so konstruiert sein, dass sie gegen Offline-Brutale-Gewalt-Angriffe resistent sind.
2.3.1 Für drahtlose Umgebungen, die mit der CDE verbunden sind oder Kontodaten, übertragen, werden alle drahtlosen Anbieter-Standardeinstellungen bei der Installation geändert oder als sicher bestätigt, einschließlich, aber nicht beschränkt auf: • Standardmäßige drahtlose Verschlüsselungsschlüssel. • Passwörter auf drahtlose Zugriffspunkte. • SNMP-Standardeinstellungen. • Alle anderen sicherheitsrelevanten drahtlosen Anbieter-Standardeinstellungen.	**2.3.1.a** Richtlinien und Verfahren untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass Prozesse für die drahtlose Anbieter-Standardeinstellungen definiert sind, um sie entweder bei der Installation zu ändern oder um zu bestätigen, dass sie gemäß allen Elementen dieser Anforderung sicher sind.	
	2.3.1.b Anbieterdokumentation untersuchen und einen Systemadministrator beobachten, der sich bei drahtlosen Geräten anmeldet, um zu verifizieren, dass: • SNMP-Standardeinstellungen nicht verwendet werden. • Standardpasswörter/Passphrasen der drahtlosen Zugangspunkte nicht verwendet werden.	
Zielsetzung des kundenspezifischen Ansatzes Auf drahtlose Netzwerke kann nicht mit Standardpasswörtern oder Standardkonfigurationen des Anbieters zugegriffen werden.	**2.3.1.c** Anbieterdokumentation und drahtlose Konfigurationseinstellungen untersuchen, um zu verifizieren, dass andere sicherheitsrelevante drahtlose Standardeinstellungen geändert wurden, falls zutreffend.	
Hinweise zur Anwendbarkeit Dies beinhaltet, ist aber nicht beschränkt auf standardmäßige drahtlose Verschlüsselungsschlüssel, Passwörter für drahtlose Zugriffspunkte, SNMP-Standardeinstellungen und alle anderen sicherheitsrelevanten drahtlosen Anbieter-Standardeinstellungen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Änderung von drahtlosen Verschlüsselungsschlüsseln, wenn jemand mit Kenntnis des Schlüssels die Organisation verlässt oder in eine Rolle wechselt, die Kenntnis des Schlüssels nicht mehr erfordert, trägt dazu bei, dass das Wissen über die Schlüssel auf diejenigen beschränkt bleibt, die es aus geschäftlichen Gründen wissen müssen. Auch die Änderung von drahtlosen Verschlüsselungsschlüsseln, wenn vermutet wird oder wenn bekannt ist, dass ein Schlüssel kompromittiert ist, macht ein drahtloses Netzwerk widerstandsfähiger gegen Kompromisse. **Gute Praxis** Dieses Ziel kann auf verschiedene Weise erreicht werden, einschließlich regelmäßiger Schlüsselwechsel, Schlüsselwechsel über einen definierten „Beitreter-Beweger-Abgänger“ (JML)-Prozess, Implementierung zusätzlicher technischer Kontrollen und Nicht-Verwendung von festen vorher geteilten Schlüsseln. Zusätzlich sollten alle Schlüssel, von denen bekannt ist oder vermutet wird, dass sie kompromittiert sind, gemäß dem Vorfallreaktionsplan der Entität bei Anforderung 12.10.1 verwaltet werden.
2.3.2 Für drahtlose Umgebungen, die mit der CDE verbunden sind oder Kontodaten übertragen, werden die drahtlosen Verschlüsselungsschlüssel wie folgt geändert:: • Immer dann, wenn Personal mit Kenntnis des Schlüssels das Unternehmen oder die Funktion verlassen, für die die Kenntnis notwendig war. • Immer dann, wenn vermutet wird oder bekannt ist, dass ein Schlüssel kompromittiert wurde.	**2.3.2** Verantwortliches Personal befragen und die Schlüsselverwaltungsdokumentation untersuchen, um zu verifizieren, dass drahtlose Verschlüsselungsschlüssel gemäß allen in dieser Anforderung angegebenen Elementen geändert wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Kenntnis von drahtlosen Verschlüsselungsschlüsseln kann keinen unbefugten Zugriff auf drahtlose Netzwerke ermöglichen.		

Schutz von Kontodaten

Anforderung 3: Schutz von Gespeicherten Kontodaten

Abschnitte	
3.1	Prozesse und Mechanismen zum Schutz gespeicherter Kontodaten sind definiert und verstanden.
3.2	Speicherung von Kontendaten wird auf einem Minimum gehalten.
3.3	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert.
3.4	Der Zugang zur Anzeige der vollständigen PAN und die Möglichkeit, Karteninhaberdaten zu kopieren, sind eingeschränkt.
3.5	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist.
3.6	Kryptografische Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, sind gesichert.
3.7	Wenn Kryptographie zum Schutz gespeicherter Kontodaten verwendet wird, werden Schlüsselverwaltungsprozesse und -prozeduren definiert und implementiert, die alle Aspekte des Schlüssellebenszyklus abdecken.

Übersicht

Schutzverfahren wie Verschlüsselung, Kürzung, Maskierung und Haschierung sind kritische Komponenten des Kontodatenschutzes. Wenn ein Eindringling andere Sicherheitskontrollen umgeht und Zugriff auf verschlüsselte Kontodaten erhält, sind die Daten ohne die richtigen kryptografischen Schlüssel unlesbar und für diesen Eindringling unbrauchbar. Andere effektive Methoden zum Schutz gespeicherter Daten sollten ebenfalls als potenzielle Möglichkeiten zur Risikominderung in Betracht gezogen werden. Zum Beispiel, Methoden zur Risikominimierung beinhalten das Nichtspeichern von Kontodaten, sofern dies nicht erforderlich ist, das Abschneiden von Karteninhaberdaten, wenn keine vollständige PAN benötigt wird, und das Versenden ungeschützter PANs unter Verwendung von Messaging-Technologien für Endbenutzer wie E-Mail und Instant Messaging.

Wenn Kontodaten in einem nicht persistenten Speicher vorhanden sind (zum Beispiel RAM, flüchtigen Speicher), ist eine Verschlüsselung der Kontodaten nicht erforderlich. Es müssen jedoch geeignete Kontrollen vorhanden sein, um sicherzustellen, dass der Speicher einen nicht persistenten Zustand beibehält. Daten sollten aus dem flüchtigen Speicher entfernt werden, sobald der Geschäftszweck (zum Beispiel die zugehörige Transaktion) abgeschlossen ist. Für den Fall, dass die Datenspeicherung persistent wird, gelten alle geltenden PCI DSS-Anforderungen, einschließlich der Verschlüsselung der gespeicherten Daten.

Anforderung 3 gilt für den Schutz gespeicherter Kontodaten, es sei denn, dies wird in einer individuellen Anforderung ausdrücklich genannt.

Siehe Anhang G für Definitionen von „starker Kryptographie“ und anderen PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
3.1 Prozesse und Mechanismen zum Schutz gespeicherter Kontodaten sind definiert und verstanden.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
3.1.1 Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 3 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	**3.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 3 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	Bei Anforderung 3.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 3 angegeben sind. Während es wichtig ist, die in Anforderung 3 genannten spezifischen Richtlinien oder Verfahren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Verfahren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Verfahren und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen.
Zielsetzung des kundenspezifischen Ansatzes		
Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 3 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht des Managements.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen sind, ist das Personal sich möglicherweise seiner täglichen Verantwortlichkeiten nicht bewusst und kritische Aktivitäten können nicht stattfinden. **Gute Praxis** Rollen und Verantwortlichkeiten können in Richtlinien und Verfahren dokumentiert oder in separaten Dokumenten gewartet werden. Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen. **Beispiele** Ein Verfahren zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).
3.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 3 werden dokumentiert, zugewiesen und verstanden.	**3.1.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten, die Aktivitäten in Anforderung 3 durchführen, dokumentiert und zugewiesen sind.	
	3.1.2.b Befragung von Personal mit Verantwortlichkeit zur Durchführung von Aktivitäten in Anforderung 3, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 3 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
3.2 Speicherung von Kontendaten wird auf einem Minimum gehalten.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	
3.2.1 Die Speicherung von Kontodaten wird durch die Implementierung von Richtlinien, Verfahren und Prozessen zur Datenaufbewahrung und -entsorgung auf ein Minimum beschränkt, die mindestens Folgendes beinhalten: • Abdeckung für alle Speicherorte von gespeicherten Kontodaten. • Abdeckung aller sensiblen Authentifizierungsdaten (SAD), die vor Abschluss der Autorisierung gespeichert wurden. *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens einer bewährten Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.* • Begrenzung der Datenspeichermenge und -aufbewahrungszeit auf das, was für gesetzliche oder behördliche und/oder Geschäfsanforderungen erforderlich ist. • Spezifische Aufbewahrungsanforderungen für gespeicherte Kontodaten, die die Länge der Aufbewahrungsfrist definieren und eine dokumentierte geschäftliche Begründung beinhalten. • Prozesse zum sicheren Löschen von Kontodaten oder wodurch Kontodaten nicht wiederhergestellt werden können, wenn sie gemäß der Aufbewahrungsrichtlinie nicht mehr benötigt werden. • Ein Verfahren, um mindestens alle drei Monate zu verifizieren, ob gespeicherte Kontodaten, die die definierte Aufbewahrungsfrist überschreiten, sicher gelöscht oder nicht wiederhergestellt werden können.	**3.2.1.a** Richtlinien, Prozeduren und Prozesse zur Datenaufbewahrung und -entsorgung untersuchen und das Personal befragen, um zu verifizieren, dass die Prozesse so definiert sind, dass sie alle in dieser Anforderung angegebenen Elemente enthalten. **3.2.1.b** Dateien und Systemdatensätze auf Systemkomponenten untersuchen, in denen Kontodaten gespeichert sind, um zu verifizieren, dass die Datenspeichermenge und die Aufbewahrungszeit die in der Datenaufbewahrungsrichtlinie definierten Anforderungen nicht überschreiten. **3.2.1.c** Beachtung der Mechanismen, die verwendet werden, um Kontodaten nicht wiederherstellbar zu machen, um zu verifizieren, dass Daten nicht wiederhergestellt werden können.	**Zweck** Eine formelle Richtlinie zur Datenaufbewahrung legt fest, welche Daten wie lange aufbewahrt werden müssen und wo sich diese Daten befinden, damit sie sicher vernichtet oder gelöscht werden können, sobald sie nicht mehr benötigt werden. Die einzigen Kontodaten, die nach der Autorisierung gespeichert werden können, sind die primäre Kontonummer oder PAN (unlesbar gemacht), das Ablaufdatum, der Name des Karteninhabers und der Dienstleistungscode. Die Speicherung von SAD-Daten vor Abschluss des Autorisierungsprozesses ist auch in der Datenaufbewahrungs- und Entsorgungsrichtlinie enthalten, so dass die Speicherung dieser sensiblen Daten auf ein Minimum beschränkt und nur für die definierte Zeitdauer aufbewahrt wird. **Gute Praxis** Wenn Speicherorte gespeicherter Kontodaten identifiziert werden, Berücksichtigung aller Prozesse und jegliches Personal mit Zugriff auf die Daten, da die Daten möglicherweise verschoben und an anderen Speicherorten als ursprünglich definiert gespeichert wurden. Speicherorte, die oft übersehen werden, schließen Backup- und Archivsysteme, entfernbare Datenspeichergeräte, papierbasierte Medien und Audioaufzeichnungen ein. Um angemessene Aufbewahrungsanforderungen zu definieren, muss eine Entität zunächst ihre eigenen Geschäftsanforderungen sowie alle rechtlichen oder behördlichen Verpflichtungen verstehen, die für ihre Branche oder die Art der aufbewahrten Daten gelten. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Kontodaten werden nur bei Bedarf und für die kürzeste benötigte Zeit aufbewahrt und sicher gelöscht oder nicht wiederherstellbar gemacht, wenn sie nicht mehr benötigt werden. **Hinweise zur Anwendbarkeit** Wenn Kontodaten von einem TPSP gespeichert werden (zum Beispiel in einer Cloud-Umgebung), sind Entitäten dafür verantwortlich, mit ihren Dienstleistungsanbietern zusammenzuarbeiten, um zu verstehen, wie der TPSP diese Anforderung für die Entität erfüllt. Die Überlegungen beinhalten, sicherzustellen, dass alle geografischen Instanzen eines Datenelements sicher gelöscht werden. *Der obige Aufzählungspunkt (für die Abdeckung von SAD, die vor Abschluss der Autorisierung gespeichert wurden) ist eine bewährte Praktik bis zum 31. März 2025, danach ist er als Teil von Anforderung 3.2.1 erforderlich und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		Die Implementierung eines automatisierten Prozesses, um sicherzustellen, dass Daten automatisch und sicher nach ihrer festgelegten Aufbewahrungsfrist gelöscht werden, kann dabei helfen, sicherzustellen, dass Kontodaten nicht über das für geschäftliche, rechtliche oder behördliche Zwecke erforderliche Maß hinaus aufbewahrt werden. Methoden zur Beseitigung von Daten, wenn sie die Aufbewahrungsfrist überschreiten, beinhalten die sichere Löschung, um die Entfernung der Daten abzuschließen oder sie nicht wiederherstellbar und nicht rekonstruierbar zu machen. Identifizierung und sichere Löschung von gespeicherten Daten, die ihre angegebene Aufbewahrungsfrist überschritten haben, verhindert eine unnötige Aufbewahrung nicht mehr benötigter Daten. Dieser Prozess kann automatisiert, manuell oder eine Kombination von beiden sein. Die Löschfunktion in den meisten Betriebssystemen ist kein „sicheres Löschen“, da sie Wiederherstellung gelöschter Daten ermöglicht, stattdessen muss eine dedizierte sichere Löschfunktion oder Anwendung verwendet werden, um Daten nicht wiederherstellbar zu machen. *Denken Sie daran, wenn Sie sie nicht benötigen, speichern Sie sie nicht!* **Beispiele** Eine automatisierte, programmatische Prozedur könnte ausgeführt werden, um Daten aufzufinden und zu entfernen, oder eine manuelle Überprüfung der Datenspeicherbereiche könnte durchgeführt werden. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Unabhängig davon, welche Methode verwendet wird, ist es eine gute Idee, den Prozess zu überwachen, um sicherzustellen, dass er erfolgreich abgeschlossen wird und dass die Ergebnisse aufgezeichnet und als abgeschlossen validiert werden. Die Implementierung sicherer Löschmethoden stellt sicher, dass die Daten nicht wiederhergestellt werden können, wenn sie nicht mehr benötigt werden. **Weitere Informationen** Siehe *NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization*.

Anforderungen und Testprozeduren		Anleitungen
3.3 Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert.		
Definierte Ansatzanforderungen **3.3.1** SAD werden nach der Autorisierung nicht aufbewahrt, selbst wenn sie verschlüsselt sind. Alle empfangenen sensiblen Authentifizierungsdaten werden nach Abschluss des Autorisierungsprozesses nicht wiederherstellbar gemacht. **Zielsetzung des kundenspezifischen Ansatzes** Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet. **Hinweise zur Anwendbarkeit** Diese Anforderung gilt nicht für Aussteller und Unternehmen, die Ausstellungsdienstleistungen unterstützen (wo SAD für einen legitimen ausstellenden Geschäftsbedarf erforderlich sind) und die eine geschäftliche Begründung für die Speicherung der sensiblen Authentifizierungsdaten haben. Siehe Anforderung 3.3.3 für zusätzliche Anforderungen speziell für Aussteller. Sensible Authentifizierungsdaten beinhalten die in den Anforderungen 3.3.1.1 bis 3.3.1.3 genannten Daten.	**Testprozeduren mit definiertem Ansatz** **3.3.1.a** Wenn SAD empfangen werden, die dokumentierten Richtlinien, Prozeduren und Systemkonfigurationen untersuchen, um zu verifizieren, dass die Daten nach der Autorisierung nicht aufbewahrt werden. **3.3.1.b** Wenn SAD empfangen werden, die dokumentierten Verfahren untersuchen und die sicheren Datenlöschprozesse beachten, um zu verifizieren, dass die Daten nach Abschluss des Autorisierungsprozesses nicht wiederherstellbar gemacht werden.	**Zweck** SAD sind sehr wertvoll für böswillige Personen, da sie ihnen die Generierung gefälschter Zahlungskarten und die Erstellung betrügerischer Transaktionen ermöglicht. Daher ist die Speicherung von SAD nach Abschluss des Autorisierungsprozesses verboten. **Definitionen** Der Autorisierungsprozess ist abgeschlossen, wenn ein Händler eine Transaktionsantwort erhält (zum Beispiel eine Genehmigung oder Ablehnung).

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **3.3.1.1** Der vollständige Inhalt einer Spur wird nach Abschluss des Autorisierungsprozesses nicht aufbewahrt. **Zielsetzung des kundenspezifischen Ansatzes** Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet. **Hinweise zur Anwendbarkeit** Im normalen Geschäftsverlauf müssen möglicherweise folgende Datenelemente von der Spur aufbewahrt werden: • Name des Karteninhabers. • Primäre Kontonummer (PAN). • Ablaufdatum. • Dienstleistungscode. Um das Risiko zu minimieren, nur diese Datenelemente sicher speichern, die für den Geschäftsverkehr erforderlich sind.	**Testprozeduren mit definiertem Ansatz** **3.3.1.1** Datenquellen untersuchen, um zu verifizieren, dass der vollständige Inhalt einer jeden Spur nach Abschluss des Autorisierungsprozesses nicht gespeichert werden.	**Zweck** Wenn der vollständige Inhalt einer Spur (vom Magnetstreifen auf der Rückseite einer Karte, falls vorhanden, gleichwertige Daten auf einem Chip oder anderswo) gespeichert wird, können böswillige Personen, die diese Daten erhalten, diese verwenden, um Zahlungskarten zu reproduzieren und betrügerische Transaktionen durchzuführen. **Definitionen** Vollständige Spurdaten werden alternativ vollständige Spur-, Spur-, Spur-1-, Spur-2- und Magnetstreifendaten genannt. Jede Spur enthält eine Reihe von Datenelementen, und diese Anforderung gibt nur diejenigen an, die nach der Autorisierung behalten werden können. **Beispiele** Datenquellen, die überprüft werden müssen, um sicherzustellen, dass der vollständige Inhalt einer jeden Spur nach Abschluss des Autorisierungsprozesses nicht aufbewahrt werden, schließen Folgende, aber nicht darauf beschränkte ein: • Eingehende Transaktionsdaten. • Sämtliche Protokolle (z. B. Transaktionen, Verlauf, Debugging, Fehler). • Verlaufsdateien. • Spurdateien. • Datenbankschemata. • Inhalte von Datenbanken und vor Ort- und Cloud-Datenspeichern. • Alle vorhandenen Speicher-/Crash-Dump-Dateien.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **3.3.1.2** Der Kartenverifizierungscode wird nach Abschluss des Autorisierungsprozesses nicht aufbewahrt. **Zielsetzung des kundenspezifischen Ansatzes** Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet. **Hinweise zur Anwendbarkeit** Der Kartenverifizierungscode ist die drei- oder vierstellige Zahl, die auf der Vorder- oder Rückseite einer Zahlungskarte aufgedruckt ist, die verwendet wird, um Transaktionen ohne Karte zu verifizieren.	**Testprozeduren mit definiertem Ansatz** **3.3.1.2** Datenquellen untersuchen, um zu verifizieren, dass der Kartenverifizierungscode nach Abschluss des Autorisierungsprozesses nicht gespeichert werden.	**Zweck** Wenn Kartenverifizierungscodes gestohlen werden, können böswillige Personen betrügerische Internet- und Versand-/Telefon-Order-Transaktionen (MO/TO) ausführen. Wenn diese Daten nicht gespeichert werden, verringert sich die Wahrscheinlichkeit, dass sie kompromittiert werden. **Beispiele** Wenn Kartenverifizierungscodes vor Abschluss der Autorisierung auf Papiermedien gespeichert werden, sollte ein Verfahren zum Löschen oder Abdecken der Codes verhindern, dass sie nach Abschluss der Autorisierung gelesen werden können. Beispielverfahren, um die Codes unlesbar zu machen, umfassen das Entfernen des Codes mit einer Schere und das Anbringen einer geeignet undurchsichtigen und nicht entfernbaren Markierung über dem Code. Datenquellen, die überprüft werden müssen, um sicherzustellen, dass der Kartenverifizierungscode nach Abschluss des Autorisierungsprozesses nicht aufbewahrt werden, schließen Folgende, aber nicht darauf beschränkte ein: • Eingehende Transaktionsdaten. • Sämtliche Protokolle (z. B. Transaktionen, Verlauf, Debugging, Fehler). • Verlaufsdateien. • Spurdateien. • Datenbankschemata. • Inhalte von Datenbanken und vor Ort- und Cloud-Datenspeichern. • Alle vorhandenen Speicher-/Crash-Dump-Dateien.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **3.3.1.3** Die persönliche Identifikationsnummer (PIN) und die PIN-Sperre werden nach Abschluss des Autorisierungsprozesses nicht aufbewahrt. **Zielsetzung des kundenspezifischen Ansatzes** Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet. **Hinweise zur Anwendbarkeit** PIN-Sperren werden während des natürlichen Ablaufs von Transaktionsprozessen verschlüsselt, aber selbst wenn eine Entität die PIN-Sperre erneut verschlüsselt, darf er nach Abschluss des Autorisierungsprozesses nicht gespeichert werden.	**Testprozeduren mit definiertem Ansatz** **3.3.1.3** Datenquellen untersuchen, um zu verifizieren, dass PINs und PIN-Sperren nach Abschluss des Autorisierungsprozesses nicht gespeichert werden.	**Zweck** PIN und PIN-Sperren sollten nur dem Karteninhaber oder der kartenausstellenden Entität bekannt sein. Wenn diese Daten gestohlen werden, können böswillige Personen betrügerische PIN-basierte Transaktionen ausführen (z. B. Einkäufe in Geschäften und Abhebungen an Geldautomaten). Wenn diese Daten nicht gespeichert werden, verringert sich die Wahrscheinlichkeit, dass sie kompromittiert werden. **Beispiele** Datenquellen, die überprüft werden müssen, um sicherzustellen, dass PIN und PIN-Sperren nach Abschluss des Autorisierungsprozesses nicht aufbewahrt werden, schließen Folgende, aber nicht darauf beschränkte ein: • Eingehende Transaktionsdaten. • Sämtliche Protokolle (z. B. Transaktionen, Verlauf, Debugging, Fehler). • Verlaufsdateien. • Spurdateien. • Datenbankschemata. • Inhalte von Datenbanken und vor Ort- und Cloud-Datenspeichern. • Alle vorhandenen Speicher-/Crash-Dump-Dateien.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
3.3.2 SAD, die elektronisch vor dem Abschluss der Autorisierung gespeichert werden, sind mit starker Kryptographie verschlüsselt.	**3.3.2** Datenspeicher, Systemkonfigurationen und/oder Anbieterdokumentation untersuchen, um zu verifizieren, dass alle SADs, die vor Abschluss der Autorisierung elektronisch gespeichert werden, mit starker Kryptographie verschlüsselt sind.	SAD kann von böswilligen Personen verwendet werden, um die Wahrscheinlichkeit zu erhöhen, erfolgreich gefälschte Zahlungskarten zu generieren und betrügerische Transaktionen durchzuführen. **Gute Praxis** Entitäten sollten erwägen, SAD mit einem anderen kryptografischen Schlüssel zu verschlüsseln, als er zum Verschlüsseln von PAN verwendet wird. Beachten, dass dies nicht bedeutet, dass die in den SAD (als Teil der Spurdaten) vorhandene PAN separat verschlüsselt werden muss. **Definitionen** Der Autorisierungsprozess ist abgeschlossen, sobald die Antwort auf eine Autorisierungsanfrageantwort – also eine Genehmigung oder Ablehnung – empfangen wurde.
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		
Hinweise zur Anwendbarkeit		
Ob SAD vor der Autorisierung gespeichert werden dürfen, wird von den Organisationen bestimmt, die Einhaltungsprogramme verwalten (zum Beispiel Zahlungsmarken und Erwerber) verwalten. Erkundigen Sie sich bei den Organisationen, die Sie interessieren, nach zusätzlichen Kriterien. Diese Anforderung gilt für die gesamte Speicherung von SAD, auch wenn kein PAN in der Umgebung vorhanden ist. Siehe Anforderung 3.2.1 für eine zusätzliche Anforderung, die gilt, wenn SAD vor Abschluss der Autorisierung gespeichert wird. Diese Anforderung gilt nicht für Aussteller und Unternehmen, die Ausstellungsdienstleistungen unterstützen, bei denen eine legitime Begründung für die Speicherung von SAD besteht. Siehe Anforderung 3.3.3 für Anforderungen speziell für Aussteller. Diese Anforderung ersetzt weder die erforderliche Verwaltung von PIN-Sperren, noch bedeutet sie, dass eine ordnungsgemäß verschlüsselte PIN-Sperre erneut verschlüsselt werden muss. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI-DSS-Bewertung vollständig berücksichtigt werden.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
3.3.3 ***Zusätzliche Anforderung für Aussteller und Unternehmen, die Ausstellungsdienstleistungen unterstützen und sensible Authentifizierungsdaten speichern:*** Jegliche Speicherung sensibler Authentifizierungsdaten ist: • Beschränkt auf das, was für einen legitimen Ausstellungsgeschäftsverkehr erforderlich und gesichert ist. • Mit starker Kryptographie verschlüsselt. *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens einer bewährten Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.*	**3.3.3.a** ***Zusätzliche Testprozedur für Aussteller und Unternehmen, die Ausstellungsdienstleistungen unterstützen und sensible Authentifizierungsdaten speichern:*** Dokumentierte Richtlinien untersuchen und das Personal befragen, um zu verifizieren, dass es eine dokumentierte geschäftliche Rechtfertigung für die Speicherung sensibler Authentifizierungsdaten gibt. **3.3.3.b** ***Zusätzliche Testprozedur für Aussteller und Unternehmen, die Ausstellungsdienstleistungen unterstützen und sensible Authentifizierungsdaten speichern:*** Datenspeicher und Systemkonfigurationen untersuchen, um zu verifizieren, dass die vertraulichen Authentifizierungsdaten sicher gespeichert sind.	SAD können von böswilligen Personen verwendet werden, um die Wahrscheinlichkeit zu erhöhen, erfolgreich gefälschte Zahlungskarten zu generieren und betrügerische Transaktionen durchzuführen**.** **Gute Praxis** Entitäten sollten erwägen, SAD mit einem anderen kryptografischen Schlüssel zu verschlüsseln, als er zum Verschlüsseln von PAN verwendet wird. Beachten, dass dies nicht bedeutet, dass die in den SAD (als Teil der Spurdaten) vorhandene PAN separat verschlüsselt werden muss. **Definitionen** Legitime Anforderungen an den Ausstellungsgeschäftsverkehr bedeutet, dass die Daten benötigt werden, um den ausstellenden Geschäftsprozess zu erleichtern. **Weitere Informationen** Siehe *ISO/DIS 9564-5 Finanzdienstleistungen — persönliche Identifikationsnummer (PIN)-Verwaltung und Sicherheit — Teil 5: Verfahren zur Erzeugung, Änderung und Verifizierung von PINs und Kartensicherheitsdaten unter Verwendung des fortschrittlichen Verschlüsselungsstandards.*
Zielsetzung des kundenspezifischen Ansatzes Sensible Authentifizierungsdaten werden nur gespeichert, wenn dies zur Unterstützung der Ausstellungsfunktionen erforderlich ist, und sind vor unbefugtem Zugriff geschützt. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur für Aussteller und Unternehmen, die Ausstellungsdienstleistungen unterstützen und sensible Authentifizierungsdaten speichern. Entitäten, die Zahlungskarten ausstellen oder Ausstellungsdienstleistungen erbringen oder unterstützen, erstellen und kontrollieren im Rahmen der Ausstellungsfunktion häufig sensible Authentifizierungsdaten. Es ist Unternehmen, die Ausstellungsdienstleistungen durchführen, erleichtern oder unterstützen, erlaubt, sensible Authentifizierungsdaten NUR DANN zu speichern, WENN sie einen legitimen geschäftlichen Bedarf an der Speicherung dieser Daten haben. Die PCI-DSS-Anforderungen sind für alle Entitäten gedacht, die Kontodaten speichern, verarbeiten oder übertragen, einschließlich Ausstellern. Die einzige Ausnahme für Aussteller und Ausstellerverarbeiter besteht darin, dass sensible Authentifizierungsdaten aufbewahrt werden können, wenn ein legitimer Grund dafür vorliegt. Alle diese Daten müssen sicher und gemäß allen PCI DSS- und spezifischen Zahlungsmarkenanforderungen gespeichert werden. *Der obige Aufzählungspunkt (für die Verschlüsselung gespeicherter SAD mit starker Kryptographie) ist eine bewährte Praktik bis zum 31. März 2025, danach ist er als Teil von Anforderung 3.3.3 erforderlich und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
3.4 Der Zugriff auf die Anzeigen des vollständigen PAN und die Möglichkeit zum Kopieren von PAN ist eingeschränkt.		
Definierte Ansatzanforderungen **3.4.1** Die PAN wird bei der Anzeige maskiert (die BIN und die letzten vier Ziffern **sind die maximale Anzahl** anzuzeigender Ziffern), sodass nur Personal mit einem legitimen Geschäftsbedarf **mehr als** die BIN und die letzten vier Ziffern der PAN sehen kann. **Zielsetzung des kundenspezifischen Ansatzes** PAN-Anzeigen sind auf die Mindestanzahl von Ziffern beschränkt, die erforderlich ist, um einen definierten Geschäftsbedarf zu erfüllen. **Hinweise zur Anwendbarkeit** Diese Anforderung ersetzt nicht die vorhandenen strengeren Anforderungen für Anzeigen von Karteninhaberdaten – zum Beispiel gesetzliche Anforderungen oder Anforderungen an Zahlungsmarken für Kassenbelege (POS). Diese Anforderung bezieht sich auf den Schutz von PAN, wenn sie auf Bildschirmen, Papierbelegen, Ausdrucken usw. angezeigt wird, und darf nicht mit Anforderung 3.5.1 zum Schutz von PAN bei der Speicherung, Verarbeitung oder Übertragung verwechselt werden.	**Testprozeduren mit definiertem Ansatz** **3.4.1.a** Dokumentierte Richtlinien und Prozeduren untersuchen, um die Anzeige von PANs zu maskieren, um Folgendes zu verifizieren: • Es wird eine Liste von Rollen dokumentiert, die Zugriff auf mehr als die BIN und die letzten vier Ziffern der PAN (einschließlich der vollständigen PAN) benötigen, zusammen mit einem legitimen Geschäftsbedarf für jede Rolle, einen solchen Zugriff zu haben. • Die PAN wird bei der Anzeige maskiert, sodass nur Personal mit legitimen Geschäftsbedarf mehr als die BIN und die letzten vier Ziffern der PAN sehen kann. • Alle Rollen, die nicht speziell zum Anzeigen der vollständigen PAN autorisiert sind, dürfen nur maskierte PANs sehen. **3.4.1.b** Systemkonfigurationen untersuchen, um zu verifizieren, dass die vollständige PAN nur für Rollen mit einem dokumentierten Geschäftsbedarf angezeigt wird und dass die PAN für alle anderen Anforderungen maskiert ist.	**Zweck** Die Anzeige vollständiger PANs auf Computerbildschirmen, Zahlungskartenbelegen, usw. kann dazu führen, dass unautorisierte Personen an diese Daten gelangen und sie zu betrügerischen Zwecken verwenden. Sicherstellung, dass die vollständige PAN nur für Personen mit einem legitimen Geschäftsbedarf angezeigt minimiert das Risiko, dass nicht autorisierte Personen Zugriff auf PAN-Daten erlangen. **Gute Praxis** Die Anwendung von Zugriffskontrollen gemäß definierten Rollen ist eine Möglichkeit, den Zugriff auf die Anzeige des vollständigen PAN auf Personen mit einem definierten Geschäftsbedarf zu beschränken. Der Maskierungsansatz sollte stets nur die für die Ausführung einer bestimmten Geschäftsfunktion erforderliche Anzahl von Ziffern anzeigen. Zum Beispiel, wenn nur die letzten vier Ziffern zum Durchführen einer Geschäftsfunktion benötigt werden, sollte PAN maskiert werden, um nur die letzten vier Ziffern anzuzeigen. As weiteres Beispiel, wenn eine Funktion die Bankleitzahl (BIN) für Routingzwecke anzeigen muss, nur Bloßstellen der BIN-Ziffern für diese Funktion. **Definitionen** Maskierung ist nicht gleichbedeutend mit Abschneiden und diese Begriffe können nicht austauschbar verwendet werden. Maskierung bezieht sich auf das Verbergen bestimmter Ziffern während der Anzeige oder des Druckens, selbst wenn die gesamte PAN auf einem System gespeichert ist. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
	3.4.1.c Die PAN-Anzeigen (zum Beispiel auf dem Bildschirm, auf Papierbelegen) untersuchen, um zu verifizieren, dass PANs maskiert sind, wenn sie angezeigt werden und dass nur Personen mit einem legitimen Geschäftsbedarf mehr als die BIN und/oder die letzten vier Ziffern der PAN sehen können	Dies unterscheidet sich vom Abschneiden, wo die abgeschnittenen Ziffern entfernt werden und nicht innerhalb des Systems abgerufen werden können. Maskierte PAN könnten „unmaskiert" werden, aber es gibt keine „Aufhebung des Abschneidens", ohne die PAN aus einer anderen Quelle neu zu erstellen. **Weitere Informationen** Weitere Informationen zum Maskieren und Abschneiden finden Sie in den FAQs von PCI SSC zu diesen Themen.
Definierte Ansatzanforderungen **3.4.2** Bei der Verwendung von Fernzugriffs-Technologien verhindern technische Kontrollen das Kopieren und/oder Verlagern von PAN für das ganze Personal, mit Ausnahme von Personal mit dokumentierter, ausdrücklicher Autorisierung und einem legitimen, definierten Geschäftsbedarf. **Zielsetzung des kundenspezifischen Ansatzes** PAN kann nicht von nicht autorisiertem Personal mithilfe von Fernzugriffs-Technologien kopiert oder verlagert werden. **Hinweise zur Anwendbarkeit** Das Speichern oder Verlagern von PAN auf lokalen Festplatten, austauschbaren elektronischen Medien und anderen Speichergeräten bringt diese Geräte in den Geltungsbereich von PCI DSS.	**Testprozeduren mit definiertem Ansatz** **3.4.2.a** Untersuchen Sie dokumentierte Richtlinien und Prozeduren und dokumentierte Beweise für technische Kontrollen, die das Kopieren und/oder Verlagern von PAN verhindern, wenn Fernzugriffs-Technologien auf lokalen Festplatten oder austauschbaren elektronischen Medien verwendet werden, um Folgendes zu überprüfen: • Technische Kontrollen verhindern, dass sämtliches Personal, das nicht ausdrücklich autorisiert ist, PAN kopieren und/oder verlagern. • Es wird eine Liste von Personal mit der Erlaubnis zum Kopieren und/oder Verlagern von PAN geführt, zusammen mit der dokumentierten, ausdrücklichen Genehmigung und dem legitimen, definierten Geschäftsbedarf. **3.4.2.b** Konfigurationen für Fernzugriffs-Technologien untersuchen, um zu verifizieren, dass technische Kontrollen das Kopieren und/oder Verlagern von PAN für alle Mitarbeiter verhindern, sofern nicht ausdrücklich autorisiert.	**Zweck** Die Verlagerung von PAN auf nicht autorisierte Speichergeräte ist ein üblicher Weg, um diese Daten in betrügerischer Absicht zu erhalten und zu verwenden. Verfahren, um sicherzustellen, dass nur Personen mit ausdrücklicher Autorisierung und einem legitimen geschäftlichen Grund PAN kopieren oder verlagern können minimiert das Risiko, dass nicht autorisierte Personen Zugriff auf PAN erlangen. **Gute Praxis** Das Kopieren und die Verlagerung von PAN sollte nur auf Speichergeräte erfolgen, die für diese Person zulässig und autorisiert sind. **Definitionen** Ein virtueller Desktop ist ein Beispiel für eine Fernzugriffs-Technologie. Zu den Speichergeräten gehören unter anderem lokale Festplatten, virtuelle Laufwerke, entfernbare elektronische Medien, Netzlaufwerke und Cloud-Speicher. **Weitere Informationen** Die Lieferantendokumentation für die verwendete Fernzugriffs-Technologie enthält Informationen zu

Anforderungen und Testprozeduren		Anleitungen
Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI-DSS-Bewertung vollständig berücksichtigt werden.	**3.4.2.c** Prozesse beachten und das Personal befragen, um zu verifizieren, dass nur Personal mit dokumentierter, expliziter Autorisierung und einem legitimen, definierten Geschäftsbedarf die Erlaubnis zum Kopieren und/oder Verlagern von PAN bei Verwendung von Fernzugriffs-Technologien hat.	den Systemeinstellungen, die zur Umsetzung dieser Anforderung erforderlich sind.

Anforderungen und Testprozeduren		Anleitungen
3.5 Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
3.5.1 PAN wird überall dort, wo sie gespeichert wird, unlesbar gemacht, indem eine der folgenden Vorgehensweisen verwendet wird: • Einweg-Hashes basierend auf starker Kryptographie der gesamten PAN. • Abschneiden (Hashing kann nicht verwendet werden, um das abgeschnittene Segment von PAN zu ersetzen). – Wenn in einer Umgebung gehashte und abgeschnittene Versionen derselben PAN oder unterschiedliche Abschneidungsformate derselben PAN vorhanden sind, werden zusätzliche Kontrollen durchgeführt, damit die verschiedenen Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren. • Verzeichnistoken. • Starke Kryptographie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren.	**3.5.1.a** Die Dokumentation über das System, das verwendet wird, untersuchen, um die PAN unlesbar zu machen, einschließlich des Anbieters, des System-/Prozesstyps und der Verschlüsselungsalgorithmen (sofern zutreffend), um zu verifizieren, dass die PAN mit einer der in dieser Anforderung angegebenen Methoden unlesbar gemacht wird. **3.5.1.b** Datenbestände und Audit-Protokolle untersuchen, einschließlich von Zahlungsanwendungsprotokollen, um zu verifizieren, ob die PAN mit einer der in dieser Anforderung angegebenen Methoden unlesbar gemacht wurde. **3.5.1.c** Wenn gehashte und abgeschnittene Versionen derselben PAN in der Umgebung vorhanden sind, implementierte Kontrollen untersuchen, um zu verifizieren, dass die gehashten und abgeschnittenen Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.	Das Entfernen von im Klartext gespeicherten PAN ist eine tiefgreifende Abwehrkontrolle zum Schutz der Daten, wenn eine nicht autorisierte Person Zugriff auf gespeicherte Daten erhält, indem sie eine Schwachstelle oder Fehlkonfiguration der primären Zugriffskontrolle einer Entität ausnutzt. Sekundäre unabhängige Kontrollsysteme (zum Beispiel, die den Zugriff auf und die Verwendung von Kryptographie- und Entschlüsselungsschlüsseln regeln) verhindern den Ausfall eines primären Zugriffskontrollsystems, der zu einer Verletzung der Vertraulichkeit der gespeicherten PAN führt. Wenn ein Streuspeicherverfahren verwendet wird, um gespeicherte Klartext-PAN zu entfernen, indem haschierte und verkürzte Versionen einer bestimmten PAN korreliert werden, kann eine böswillige Person leicht den ursprünglichen PAN-Wert ableiten. Kontrollen, die die Korrelation dieser Daten verhindern, tragen dazu bei, dass die ursprüngliche PAN unlesbar bleibt.
Zielsetzung des kundenspezifischen Ansatzes		**Weitere Informationen**
Klartext-PAN kann von Speichermedien nicht gelesen werden.		Informationen zu Abschneideformaten und Abschneidungen im Allgemeinen finden Sie in den FAQs von PCI SSC zu diesem Thema. Informationsquellen zu Verzeichnistoken beinhalten: • PCI SSC's Sicherheitsrichtlinien für Tokenisierungsprodukte (https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf)
(Fortsetzung auf der nächsten Seite)		(Fortsetzung auf der nächsten Seite)

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Für eine böswillige Person ist es relativ trivial, die ursprünglichen PAN-Daten zu rekonstruieren, wenn sie sowohl auf die abgeschnittene als auch auf die gehashte Version einer PAN zugreifen kann. Diese Anforderung gilt sowohl für PANs, die im primären Speicher (Datenbanken oder flachen Dateien wie Tabellenkalkulationen für Textdateien) gespeichert sind, als auch im nicht primären Speicher (Backup-, Audit-Protokolle, Ausnahme- oder Fehlerbehebungsprotokolle) müssen alle geschützt werden. Diese Anforderung schließt die Verwendung temporärer Dateien mit Klartext-PAN beim Ver- und Entschlüsseln von PAN nicht aus.		• ANSI X9.119-2-2017: Finanzdienstleistungen für Einzelhandel – Anforderungen zum Schutz sensibler Zahlungskartendaten – Teil 2: Implementieren von Tokenisierungssystemen nach der Autorisierung

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Entfernen von im Klartext gespeicherten PAN ist eine tiefgreifende Abwehrkontrolle zum Schutz der Daten, wenn eine nicht autorisierte Person Zugriff auf gespeicherte Daten erhält, indem sie eine Schwachstelle oder Fehlkonfiguration der primären Zugriffskontrolle einer Entität ausnutzt. Sekundäre unabhängige Kontrollsysteme (zum Beispiel, die den Zugriff auf und die Verwendung von Kryptographie- und Entschlüsselungsschlüsseln regeln) verhindern den Ausfall eines primären Zugriffskontrollsystems, der zu einer Verletzung der Vertraulichkeit der gespeicherten PAN führt. **Gute Praxis** Eine Hashing-Funktion, die einen zufällig generierten geheimen Schlüssel enthält, stellt brutale Gewalt-Angriffs-Widerstand und die Integrität der geheimen Authentifizierung bereit. **Weitere Informationen** Geeignete verschlüsselte kryptografische Hashing-Algorithmen beinhalten, sind aber nicht beschränkt auf: HMAC, CMAC und GMAC mit einer effektiven kryptografischen Stärke von mindestens 128 Bit (*NIST SP 800-131Ar2)*. Im Folgenden finden Sie weitere Informationen über HMAC, CMAC und GMAC: *NIST SP 800-107r1, NIST SP 800-38B, und NIST SP 800-38D).* Siehe *NIST SP 800-107 (Revision 1): Empfehlung für Anwendungen, die zugelassene Hash-Algorithmen verwenden §5.3.*
3.5.1.1 Hashes, die verwendet werden, um PAN unlesbar zu machen (gemäß dem ersten Aufzählungspunkt von Anforderung 3.5.1) sind verschlüsselte kryptografische Hashes der gesamten PAN mit zugehörigen Schlüsselverwaltungsprozessen und -prozeduren gemäß den Anforderungen 3.6 und 3.7.	**3.5.1.1.a** Dokumentation über das Hashing-Verfahren untersuchen, das verwendet wird, um PAN unlesbar zu machen, einschließlich des Anbieters, der Art des Systems/Prozesses und der Verschlüsselungsalgorithmen (sofern zutreffend) um zu verifizieren, dass das Hashing-Verfahren zu verschlüsselten kryptografischen Hashes der gesamten PANs führt, mit zugehöriger Schlüsselverwaltungsprozessen und -prozeduren.	
Hinweise zur Anwendbarkeit	**3.5.1.1.b** Dokumentation über die Schlüsselverwaltungsprozeduren und -prozesse, die den verschlüsselten kryptografischen Hashes zugeordnet sind, untersuchen, um zu verifizieren, dass Schlüssel gemäß den Anforderungen 3.6 und 3.7 verwaltet werden.	
Diese Anforderung gilt sowohl für PANs, die im primären Speicher (Datenbanken oder flachen Dateien wie Tabellenkalkulationen für Textdateien) gespeichert sind, als auch im nicht primären Speicher (Backup-, Audit-Protokolle, Ausnahme- oder Fehlerbehebungsprotokolle) müssen alle geschützt werden. Diese Anforderung schließt die Verwendung temporärer Dateien mit Klartext-PAN beim Ver- und Entschlüsseln von PAN nicht aus. *Diese Anforderung wird bis zum 31. März 2025 als bewährte Praktik betrachtet, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**3.5.1.1.c** Datenbestände untersuchen, um zu verifizieren, dass die PAN unlesbar gemacht wurde.	
	3.5.1.1.d Audit-Protokolle, einschließlich Zahlungsanwendungsprotokolle untersuchen, um zu verifizieren, dass die PAN unlesbar gemacht wurde.	

<table>
<tr><th colspan="2">Anforderungen und Testprozeduren</th><th>Anleitungen</th></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="4">Zweck
Verschlüsselung auf Festplatten- und Partitionsebene verschlüsselt normalerweise die gesamte Festplatte oder Partition mit demselben Schlüssel, wobei alle Daten automatisch entschlüsselt werden, wenn das System ausgeführt wird oder ein autorisierter Benutzer dies anfordert. Aus diesem Grund ist die Verschlüsselung auf Festplattenebene nicht geeignet, um gespeicherte PANs auf Computern, Laptops, Servern, Speicherarrays oder anderen Systemen zu schützen, die eine transparente Entschlüsselung bei der Benutzerauthentifizierung bereitstellt.
Weitere Informationen
Sofern verfügbar, kann die Einhaltung der Härtungsanl;eitungen der Anbieter und der branchenüblichen bewährte Praktiken-Anleitungen dazu beitragen, PAN auf diesen Geräten zu sichern.</td></tr>
<tr><td rowspan="2">3.5.1.2 Wenn eine Verschlüsselung auf Festplatten- oder Partitionsebene (anstatt einer Datenbankverschlüsselung auf Datei-, Spalten- oder Feldebene) verwendet wird, um PAN unlesbar zu machen, wird sie nur wie folgt implementiert:
• Auf entfernbaren elektronischen Medien
ODER
• Bei Verwendung für nicht entfernbare elektronische Medien wird PAN auch über einen anderen Mechanismus, der die Anforderung 3.5.1 erfüllt, unlesbar gemacht.</td><td>3.5.1.2.a Verschlüsselungsprozesse untersuchen, um zu verifizieren, dass, wenn Verschlüsselung auf Festplatten- oder Partitionsebene verwendet wird, um PAN unlesbar zu machen, diese nur wie folgt implementiert wird:
• Auf entfernbaren elektronischen Medien,
ODER
• Bei Verwendung für nicht entfernbare elektronische Medien, Verschlüsselungsprozesse untersuchen, die verwendet werden, um zu verifizieren, dass PAN auch durch eine andere Methode, die die Anforderung 3.5.1 erfüllt, unlesbar gemacht wird.</td></tr>
<tr><td>3.5.1.2.b Konfigurationen und/oder Herstellerdokumentation untersuchen, und Verschlüsselungsprozesse beobachten, um zu verifizieren, dass das System gemäß Anbieterdokumentation konfiguriert ist, führt dies dazu, dass die Festplatte oder die Partition unlesbar gemacht wird.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes</td><td colspan="2"></td></tr>
<tr><td>Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.
(Fortsetzung auf der nächsten Seite)</td><td colspan="2"></td></tr>
</table>

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit		
Obwohl die Festplattenverschlüsselung auf diesen Gerätetypen noch vorhanden sein kann, kann sie nicht der einzige Mechanismus sein, der verwendet wird, um auf diesen Systemen gespeicherte PANs zu schützen. Jede gespeicherte PAN muss außerdem gemäß Anforderung 3.5.1 unlesbar gemacht werden – zum Beispiel durch Abschneiden oder einen Verschlüsselungsmechanismus auf Datenebene. Die vollständige Festplattenverschlüsselung trägt zum Schutz der Daten bei einem physischen Verlust einer Festplatte bei und ist daher nur für entfernbare elektronische Medienspeichergeräte geeignet. Medien, die Teil einer Rechenzentrumsarchitektur sind (zum Beispiel Hot-Swap-fähige Laufwerke, Massensicherungen auf Band) gelten als nicht entfernbare elektronische Medien, für die Anforderung 3.5.1 gilt. Implementierungen der Festplatten- oder Partitionsverschlüsselung müssen auch alle anderen PCI DSS-Verschlüsselungs- und Schlüsselverwaltungsanforderungen erfüllen. Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Verschlüsselung auf Festplattenebene verschlüsselt normalerweise die gesamte Festplatte oder Partition mit demselben Schlüssel, wobei alle Daten automatisch entschlüsselt werden, wenn das System ausgeführt wird oder ein autorisierter Benutzer dies anfordert. Viele Lösungen zur Festplattenverschlüsselung fangen Lese-/Schreibvorgänge des Betriebssystems ab und führen die entsprechenden kryptografischen Transformationen durch, ohne dass der Benutzer außer der Eingabe eines Passworts oder einer Passphrase beim Systemstart oder zu Beginn einer Sitzung besondere Maßnahmen ergreifen muss. Dies stellt keinen Schutz vor einer böswilligen Person bereit, die sich bereits Zugriff auf ein gültiges Benutzerkonto verschafft hat. **Gute Praxis** Die vollständige Festplattenverschlüsselung trägt zum Schutz der Daten bei einem physischen Verlust einer Festplatte bei und daher beschränkt sich ihre Verwendung am besten nur auf entfernbare elektronische Medienspeichergeräte.
3.5.1.3 Wenn eine Verschlüsselung auf Festplatten- oder Partitionsebene (anstatt einer Datenbankverschlüsselung auf Datei-, Spalten- oder Feldebene) verwendet wird, um PAN unlesbar zu machen, wird sie folgt verwaltet: • Der logische Zugriff wird separat und unabhängig von nativen Betriebssystem-Authentifizierungs- und Zugriffskontrollmechanismen verwaltet. • Entschlüsselungsschlüssel sind nicht mit Benutzerkonten assoziiert. • Authentifizierungsfaktoren (Passwörter, Passphrasen, oder kryptografische Schlüssel), die Zugriff auf nicht verschlüsselte Daten gestatten, werden sicher gespeichert.	**3.5.1.3.a** Wenn eine Verschlüsselung auf Festplatten- oder Partitionsebene verwendet wird, um PAN unlesbar zu machen, die Systemkonfiguration untersuchen und der Authentifizierungsprozess beobachten, um zu verifizieren, dass der logische Zugriff gemäß allen in dieser Anforderung angegebenen Elementen implementiert ist.	
Zielsetzung des kundenspezifischen Ansatzes Implementierungen der Festplattenverschlüsselung sind so konfiguriert, dass sie eine unabhängige Authentifizierung und logische Zugriffskontrollen für die Entschlüsselung erfordern.	**3.5.1.3.b** Dateien, die Authentifizierungsfaktoren (Passwörter, Passphrasen, oder kryptografische Schlüssel) untersuchen und das Personal befragen, um zu verifizieren, dass Authentifizierungsfaktoren, die den Zugriff auf unverschlüsselte Daten ermöglichen, sicher gespeichert werden und unabhängig von den Authentifizierungs- und Zugriffskontrollmethoden des nativen Betriebssystems sind.	
Hinweise zur Anwendbarkeit Implementierungen der Festplatten- oder Partitionsverschlüsselung müssen auch alle anderen PCI DSS-Verschlüsselungs- und Schlüsselverwaltungsanforderungen erfüllen.		

Anforderungen und Testprozeduren		Anleitungen
3.6 Kryptografische Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, sind gesichert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
3.6.1 Prozeduren werden definiert und implementiert, um kryptografische Schlüssel zu schützen, die verwendet werden, um gespeicherte Kontodaten vor Offenlegung und Missbrauch zu schützen, darunter: • Der Zugriff auf Schlüssel ist auf die erforderliche Anzahl von Verwahrern beschränkt. • Schlüsselverschlüsselungsschlüssel sind mindestens so stark wie die Datenverschlüsselungsschlüssel, die sie schützen. • Schlüsselverschlüsselungsschlüssel werden getrennt von Datenverschlüsselungsschlüsseln gespeichert. • Schlüssel werden an möglichst wenigen Orten und Formularen gespeichert.	**3.6.1** Dokumentierte Richtlinien und Prozeduren zur Schlüsselverwaltung untersuchen, um zu verifizieren, dass Prozesse zum Schutz von kryptografischen Schlüsseln zum Schutz gespeicherter Kontodaten vor Offenlegung und Missbrauch so definiert sind, dass sie alle in dieser Anforderung angegebenen Elemente enthalten.	Kryptografische Schlüssel müssen stark geschützt werden, da diejenigen, die Zugriff erhalten, in der Lage sind, Daten zu entschlüsseln. **Gute Praxis** Für die Verwaltung kryptografischer Schlüssel wird ein zentrales Schlüsselverwaltungssystem auf Basis von Industriestandards empfohlen. **Weitere Informationen** Die Schlüsselverwaltungsprozeduren der Entität werden von der Anpassung an die Branchenanforderungen profitieren, Quellen für Informationen zu den Lebenszyklen der kryptografischen Schlüsselverwaltung sind: • *ISO 11568-1 Banking — Schlüsselverwaltung (Einzelhandel) — Teil 1*: Grundsätze (insbesondere Kapitel 10 und die referenzierten Teile 2 und 4) • *NIST SP 800-57 Teil 1, Revision 5 – Empfehlung für die Schlüsselverwaltung: Allgemein*.
Zielsetzung des kundenspezifischen Ansatzes 3.6.1 Prozesse, die kryptografische Schlüssel schützen, die verwendet werden, um gespeicherte Kontodaten vor Offenlegung und Missbrauch zu schützen, werden definiert und implementiert.		
Hinweise zur Anwendbarkeit Diese Anforderung gilt für Schlüssel, die zum Verschlüsseln gespeicherter Kontodaten verwendet werden, und für Schlüssel zum Verschlüsseln von Schlüsseln, die zum Schutz von datenverschlüsselnden Schlüsseln verwendet werden. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Die Anforderung zum Schutz von Schlüsseln, die zum Schutz gespeicherter Kontodaten vor Offenlegung und Missbrauch verwendet werden, gilt sowohl für datenverschlüsselnde Schlüssel als auch für schlüsselverschlüsselnde Schlüssel. Da ein Schlüssel zum Verschlüsseln von Daten Zugriff auf viele Schlüssel zum Verschlüsseln von Daten gewähren kann, erfordern die Schlüssel zum Verschlüsseln von Schlüsseln starke Schutzmaßnahmen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Wartung einer aktuellen Dokumentation der kryptografischen Architektur ermöglicht es einer Entität, die Algorithmen, Protokolle und kryptografischen Schlüssel zu verstehen, die zum Schutz gespeicherter Kontodaten verwendet werden, sowie die Geräte, die die Schlüssel generieren, verwenden und schützen. Dies ermöglicht einer Entität, mit sich entwickelnden Bedrohungen ihrer Architektur Schritt zu halten und Aktualisierungen zu planen, wenn sich das Sicherheitsniveau, das von verschiedenen Algorithmen und Schlüsselstärken bereitgestellt wird, ändert. Die Wartung einer solchen Dokumentation ermöglicht es einer Entität auch, verlorene oder fehlende Schlüssel oder Schlüsselverwaltungsgeräte zu erkennen und unbefugte Ergänzungen ihrer kryptografischen Architektur zu identifizieren. Die Verwendung derselben kryptografischen Schlüssel in Produktions- und Testumgebungen führt das Risiko der Offenlegung des Schlüssels ein, wenn die Testumgebung nicht dieselbe Sicherheitsstufe wie die Produktionsumgebung aufweist. **Gute Praxis** Ein automatisierter Berichtsmechanismus kann die Wartung der kryptografischen Attribute unterstützen.
3.6.1.1 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Es wird eine dokumentierte Beschreibung der kryptografischen Architektur beibehalten, die Folgendes beinhaltet: • Details zu allen Algorithmen, Protokollen und Schlüsseln, die zum Schutz gespeicherter Kontodaten verwendet werden, einschließlich Schlüsselstärke und Ablaufdatum. • Verhinderung der Verwendung derselben kryptografischen Schlüssel in Produktions- und Testumgebungen. *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens einer bewährten Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.* • Beschreibung der Schlüsselverwendung für jeden Schlüssel. • Inventar aller Hardware-Sicherheitsmodule (HSMs), Schlüsselverwaltungssysteme (KMS) und anderer sicherer kryptografischer Geräte (SCDs), die für die Schlüsselverwaltung verwendet werden, einschließlich Art und Standort der Geräte, wie in Anforderung 12.3.4 beschrieben.	**3.6.1.1** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Verantwortliches Personal befragen und Dokumentation untersuchen, um zu verifizieren, dass ein Dokument existiert, um die kryptografische Architektur zu beschreiben, die alle in dieser Anforderung angegebenen Elemente enthält.	
Zielsetzung des kundenspezifischen Ansatzes		
Genaue Details der kryptografischen Architektur werden beibehalten und sind verfügbar. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. Bei Cloud-HSM-Implementierungen wird die Verantwortung für die kryptografische Architektur gemäß dieser Anforderung zwischen dem Cloud-Anbieter und dem Cloud-Kunden aufgeteilt. *Der obige Aufzählungspunkt (für die Aufnahme in die Kryptografiearchitektur, dass die Verwendung der gleichen kryptografischen Schlüssel in Produktion und Test verhindert wird) ist eine bewährte Praktik bis zum 31. März 2025, danach wird er als Teil von Anforderung 3.6.1.1 benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das sichere Speichern von kryptografischen Schlüsseln verhindert unbefugten oder unnötigen Zugriff, der zur Aufdeckung gespeicherter Kontodaten führen könnte. Das getrennte Speichern von Schlüsseln bedeutet, dass sie so gespeichert werden, dass, wenn der Standort eines Schlüssels kompromittiert wird, der zweite Schlüssel nicht auch kompromittiert wird. **Gute Praxis** Wenn Datenverschlüsselungsschlüssel in einem HSM gespeichert werden, sollte der HSM-Interaktionskanal geschützt werden, um das Abfangen von Verschlüsselungs- oder Entschlüsselungsvorgängen zu verhindern.
3.6.1.2 Geheime und private Schlüssel, die zum Verschlüsseln/Entschlüsseln gespeicherter Kontodaten verwendet werden, werden jederzeit in einem (oder mehreren) der folgenden Formate gespeichert: • Verschlüsselt mit einem Schlüssel zum Verschlüsseln, der mindestens so stark ist wie der Schlüssel zum Verschlüsseln von Daten, und der getrennt vom Schlüssel zum Verschlüsseln von Daten gespeichert wird. • In einem sicheren kryptografischen Gerät (SCD), wie einem Hardware-Sicherheitsmodul (HSM) oder einem PTS-zugelassenen Ort der Interaktion-Gerät. • Als mindestens zwei Schlüsselkomponenten voller Länge oder Schlüsselanteile, gemäß einer in der Branche anerkannten Methode.	**3.6.1.2.a** Dokumentierte Prozeduren untersuchen, um zu verifizieren, dass definiert ist, dass kryptografische Schlüssel, die zum Verschlüsseln/Entschlüsseln gespeicherter Kontodaten verwendet werden, nur in einer (oder mehreren) der in dieser Anforderung angegebenen Formen existieren dürfen. **3.6.1.2.b** Systemkonfigurationen und wichtige Speicherorte untersuchen, um zu verifizieren, dass kryptografische Schlüssel, die zum Verschlüsseln/Entschlüsseln gespeicherter Kontodaten verwendet werden, nur in einer (oder mehreren) der in dieser Anforderung angegebenen Formen existieren. **3.6.1.2.c** Überall dort, wo schlüsselverschlüsselnde Schlüssel verwendet werden, Systemkonfigurationen und Schlüsselspeicherorte untersuchen, um zu verifizieren, dass: • Schlüsselverschlüsselungsschlüssel mindestens so stark wie die Datenverschlüsselungsschlüssel sind, die sie schützen. • Schlüsselverschlüsselungsschlüssel getrennt von Datenverschlüsselungsschlüsseln gespeichert werden.	
Zielsetzung des kundenspezifischen Ansatzes Geheime und private Schlüssel werden in einer sicheren Form gespeichert, die einen nicht autorisierten Abruf oder Zugriff verhindert.		
Hinweise zur Anwendbarkeit Es ist nicht erforderlich, dass öffentliche Schlüssel in einer dieser Formen gespeichert werden. Kryptografische Schlüssel, die als Teil eines Schlüsselverwaltungssystems (KMS) gespeichert werden, das SCDs verwendet, sind akzeptabel. Ein kryptografischer Schlüssel, der in zwei Teile geteilt ist, erfüllt diese Anforderung nicht. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Als Schlüsselkomponenten oder Schlüsselanteile gespeicherte geheime oder private Schlüssel müssen über einen der Folgenden generiert werden: • Verwendung eines zugelassenen Zufallszahlengenerators und innerhalb einer SCD, **ODER** • Gemäß ISO 19592 oder einem gleichwertigen Industriestandard für die Generierung geheimer Schlüsselanteile.		
Definierte Ansatzanforderungen **3.6.1.3** Zugriff auf kryptografische Schlüsselkomponenten im Klartext ist auf die geringste Anzahl von Verwahrern beschränkt. **Zielsetzung des kundenspezifischen Ansatzes** Der Zugriff auf kryptografische Schlüsselkomponenten im Klartext ist auf das erforderliche Personal beschränkt.	**Testprozeduren mit definiertem Ansatz** **3.6.1.3** Benutzerzugriffslisten untersuchen, um zu verifizieren, dass der Zugriff auf kryptografische Schlüsselkomponenten im Klartext auf die geringste Anzahl von Verwahrern beschränkt ist.	**Zweck** Die Beschränkung der Anzahl von Personen, die Zugriff auf kryptografische Schlüsselkomponenten im Klartext haben, verringert das Risiko, dass gespeicherte Kontodaten von nicht autorisierten Parteien abgerufen oder sichtbar gemacht werden. **Gute Praxis** Nur Personal mit definierten Verantwortlichkeiten für die Schlüsselverwahrung (Erstellen, Ändern, Rotieren, Verteilen oder anderweitige Wartung von Verschlüsselungsschlüsseln) sollte Zugriff auf Schlüsselkomponenten erhalten. Idealerweise handelt es sich dabei um eine sehr kleine Anzahl von Personen.
Definierte Ansatzanforderungen **3.6.1.4** Kryptografische Schlüssel werden an möglichst wenigen Orten gespeichert. **Zielsetzung des kundenspezifischen Ansatzes** Kryptografische Schlüssel werden nur bei Bedarf aufbewahrt.	**Testprozeduren mit definiertem Ansatz** **3.6.1.4** Schlüsselspeicherorte untersuchen und Prozesse beobachten, um zu verifizieren, dass Schlüssel an möglichst wenigen Orten gespeichert werden.	**Zweck** Das Speichern von kryptografischen Schlüsseln an den wenigsten Orten hilft einer Organisation, alle Schlüsselorte zu verfolgen und zu überwachen, und minimiert das Risiko, dass Schlüssel nicht autorisierten Parteien preisgegeben werden.

Anforderungen und Testprozeduren		Anleitungen
3.7 Wenn Kryptographie zum Schutz gespeicherter Kontodaten verwendet wird, werden Schlüsselverwaltungsprozesse und -prozeduren definiert und implementiert, die alle Aspekte des Schlüssellebenszyklus abdecken.		
Definierte Ansatzanforderungen **3.7.1** Richtlinien und Prozeduren zur Schlüsselverwaltung werden implementiert, um die Generierung von starken sicheren kryptografischen Schlüsseln zum Schutz gespeicherter Kontodaten einzuschließen. **Zielsetzung des kundenspezifischen Ansatzes** Es werden starke kryptografische Schlüssel generiert.	**Testprozeduren mit definiertem Ansatz** **3.7.1.a** Die dokumentierten Richtlinien und Prozeduren zur Schlüsselverwaltung für Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, untersuchen, um zu verifizieren, dass sie die Generierung von starken kryptografischen Schlüsseln definieren. **3.7.1.b** Die Methode zum Generieren von Schlüsseln beobachten, um zu verifizieren, dass starke Schlüssel generiert werden.	**Zweck** Die Verwendung starker kryptografischer Schlüssel erhöht die Sicherheitsstufe verschlüsselter Kontodaten erheblich. **Weitere Informationen** Siehe die Quellen, auf die unter „Kryptografische Schlüsselgenerierung" in Anhang G verwisen wird.
Definierte Ansatzanforderungen **3.7.2** Richtlinien und Prozeduren zur Schlüsselverwaltung werden implementiert, um sichere Verteilung von kryptografischen Schlüsseln zum Schutz gespeicherter Kontodaten einzuschließen. **Zielsetzung des kundenspezifischen Ansatzes** Kryptografische Schlüssel werden während der Verteilung gesichert.	**Testprozeduren mit definiertem Ansatz** **3.7.2.a** Die dokumentierten Richtlinien und Prozeduren zur Schlüsselverwaltung für Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, untersuchen, um zu verifizieren, dass sie die sichere Verteilung von kryptografischen Schlüsseln definieren. **3.7.2.b** Die Methode zum Verteilen von Schlüsseln beachten, um zu verifizieren, dass die Schlüssel sicher verteilt werden.	**Zweck** Die sichere Verteilung oder Übermittlung geheimer oder privater kryptografischer Schlüssel bedeutet, dass Schlüssel nur an autorisierte Verwahrer, wie in Anforderung 3.6.1.2 angegeben, und niemals unsicher verteilt werden.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Speichern von Schlüsseln ohne angemessenen Schutz könnte Angreifern Zugriff verschaffen, was zur Entschlüsselung und Offenlegung von Kontodaten führt. **Gute Praxis** Datenverschlüsselungsschlüssel können geschützt werden, indem sie mit einem Schlüsselverschlüsselungsschlüssel verschlüsselt werden. Schlüssel können in einem Hardwaresicherheitsmodul (HSM) gespeichert werden. Geheime oder private Schlüssel, die Daten entschlüsseln können, sollten niemals im Quellcode vorhanden sein.
3.7.3 3.7.3 Richtlinien und Prozeduren zur Schlüsselverwaltung werden implementiert, um sichere Speicherung von kryptografischen Schlüsseln zum Schutz gespeicherter Kontodaten einzuschließen.	**3.7.3.a** Die dokumentierten Richtlinien und Prozeduren zur Schlüsselverwaltung für Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, untersuchen, um zu verifizieren, dass sie die sichere Speicherung von kryptografischen Schlüsseln definieren.	
	3.7.3.b Die Methode zum Speichern von Schlüsseln beobachten, um zu verifizieren, dass die Schlüssel sicher gespeichert werden.	
Zielsetzung des kundenspezifischen Ansatzes		
Kryptografische Schlüssel werden während der Speicherung gesichert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Ändern von Verschlüsselungsschlüsseln am Ende ihrer Kryptozeitperiode ist zwingend erforderlich, um das Risiko zu minimieren, dass jemand die Verschlüsselungsschlüssel erhält und sie zum Entschlüsseln von Daten verwendet. **Definitionen** Eine Kryptoperiode ist die Zeitspanne, in der ein kryptografischer Schlüssel für seinen definierten Zweck verwendet werden kann. Kryptoperioden werden oft in Bezug auf die Periode definiert, für die der Schlüssel aktiv ist und/oder die Menge an verschlüsseltem Text, die durch den Schlüssel erzeugt wurde. Überlegungen zum Definieren der Kryptozeitdauer beinhalten, sind aber nicht beschränkt auf, die Stärke des zugrunde liegenden Algorithmus, die Größe oder Länge des Schlüssels, das Risiko einer *(Fortsetzung auf der nächsten Seite)*
3.7.4 Richtlinien und Verfahren zur Schlüsselverwaltung werden für kryptografische Schlüsseländerungen für Schlüssel implementiert, die das Ende ihrer Verschlüsselungszeitdauer erreicht haben, wie vom jeweiligen Anwendungsanbieter oder Schlüsselbesitzer definiert ist und auf den bewährten Praktiken und Richtlinien der Branche basiert, einschließlich der folgenden: • Eine definierte Kryptozeitdauer für jeden verwendeten Schlüsseltyp. • Einen Prozess für Schlüsseländerungen am Ende der definierten Kryptozeitdauer. *(Fortsetzung auf der nächsten Seite)*	**3.7.4.a** Die dokumentierten Schlüsselverwaltungsrichtlinien und -prozeduren für Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, untersuchen, um zu verifizieren, dass sie Änderungen an kryptografischen Schlüsseln definieren, die das Ende ihrer Kryptozeitdauer erreicht haben, und alle Elemente enthalten, die in dieser Anforderung angegeben sind.	
	3.7.4.b Das Personal befragen, Dokumentation untersuchen, und Schlüsselspeicherorte beobachten, um zu verifizieren, dass Schlüssel am Ende der definierten Kryptozeitdauer(n) geändert werden.	

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Kryptografische Schlüssel werden nicht über ihre definierte Kryptozeitdauer hinaus verwendet.		Schlüsselkompromittierung und die Sensibilität der zu verschlüsselnden Daten. **Weitere Informationen** *NIST SP 800-57 Part 1, Revision 5, Abschnitt 5.3 Kryptozeitdauern* - stellt Anleitungen zum Etablieren der Zeitspanne bereit, während der ein bestimmter Schlüssel zur Verwendung durch berechtigte Entitäten autorisiert ist oder die Schlüssel für ein bestimmtes System gültig bleiben. Siehe Tabelle 1 von *SP 800-57* Teil 1 für vorgeschlagene Kryptozeitdauern für verschiedene Schlüsseltypen.
Definierte Ansatzanforderungen **3.7.5** Prozeduren zur Schlüsselverwaltung werden implementiert, um die Aussonderung, den Ersatz oder die Zerstörung von Schlüsseln, die zum Schutz gespeicherter Kontodaten verwendet werden, nach Bedarf zu umfassen, wenn: • Der Schlüssel das Ende seiner definierten Kryptozeitdauer erreicht hat. • Die Integrität des Schlüssels geschwächt wurde, auch wenn Personal mit Kenntnis einer Klartext-Schlüsselkomponente das Unternehmen verlässt oder die Rolle, für die die Schlüsselkomponente bekannt war, verlässt. • Es wird vermutet oder es ist bekannt, dass Schlüssel kompromittiert wurden. Zurückgezogene oder ersetzte Schlüssel werden nicht für Verschlüsselungsbetriebe verwendet.	**Testprozeduren mit definiertem Ansatz** **3.7.5.a** Die dokumentierten Schlüsselverwaltungsrichtlinien und -prozeduren für Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, untersuchen und verifizieren, dass sie die Aussonderung, den Ersatz oder die Zerstörung von Schlüsseln gemäß allen in dieser Anforderung angegebenen Elementen definieren. **3.7.5.b** Personal befragen, um zu verifizieren, dass die Verfahren gemäß allen in dieser Anforderung angegebenen Elementen implementiert werden.	**Zweck** Nicht mehr benötigte Schlüssel, Schlüssel mit geschwächter Integrität und Schlüssel, von denen bekannt ist oder vermutet wird, dass sie kompromittiert sind, sollten archiviert, widerrufen und/oder zerstört werden, um sicherzustellen, dass die Schlüssel nicht mehr verwendet werden können. Wenn solche Schlüssel aufbewahrt werden müssen (zum Beispiel um archivierte verschlüsselte Daten zu unterstützen), sollten sie stark geschützt werden. **Gute Praxis** Archivierte kryptografische Schlüssel sollten nur zu Entschlüsselungs-/Verifizierungszwecken verwendet werden. Die Verschlüsselungslösung sollte einen Prozess zum Ersetzen von Schlüsseln, die ersetzt werden müssen oder von denen bekannt ist oder vermutet wird, dass sie kompromittiert sind, bereitstellen und erleichtern. Darüber hinaus sollten alle Schlüssel, von denen bekannt ist oder vermutet wird, dass sie kompromittiert sind, gemäß dem Vorfallreaktionsplan der Entität gemäß Anforderung 12.10.1 verwaltet werden.
Zielsetzung des kundenspezifischen Ansatzes Schlüssel werden aus der aktiven Verwendung entfernt, wenn der Verdacht besteht oder es bekannt ist, dass die Integrität des Schlüssels geschwächt ist.		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Wenn ausgesonderte oder ersetzte kryptografische Schlüssel aufbewahrt werden müssen, müssen diese Schlüssel sicher archiviert werden (zum Beispiel mithilfe eines Schlüsselverschlüsselungsschlüssels).		**Weitere Informationen** Bewährte Praktiken der Branche für die Archivierung ausgesonderter Schlüssel sind in *NIST SP 800-57 Teil 1, Revision 5, Abschnitt 8.3.1* beschrieben und beinhalten die Wartung des Archivs bei einem vertrauenswürdigen Dritten und die getrennte Speicherung archivierter Schlüsselinformationen von Betriebsdaten.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
3.7.6 Wenn manuelle Betriebe zur Verwaltung von kryptografischen Klartextschlüsseln von Personal durchgeführt werden, werden Richtlinien und Prozeduren zur Schlüsselverwaltung implementiert, die die Verwaltung dieser Betriebe unter Verwendung von geteiltem Wissen und doppelter Kontrolle beinhalten.	**3.7.6.a** Die dokumentierten Richtlinien und Prozeduren zur Schlüsselverwaltung für Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, untersuchen, und verifizieren, dass sie mit geteiltem Wissen und doppelter Kontrolle definiert werden.	Gespaltenes Wissen und die doppelte Kontrolle von Schlüsseln werden verwendet, um die Möglichkeit auszuschließen, dass eine einzelne Person Zugriff auf den gesamten Schlüssel hat und sich daher nicht autorisierten Zugriff auf die Daten verschaffen kann.
Zielsetzung des kundenspezifischen Ansatzes	**3.7.6.b** Personal befragen und/oder Prozesse beobachten, um zu verifizieren, dass manuelle Klartextschlüssel mit gespaltenem Wissen und Vier-Augen-Prinzip verwaltet werden.	**Definitionen**
Geheime oder private Klartextschlüssel können niemandem bekannt sein. Betriebe, die Klartextschlüssel einbeziehen, können nicht von einer einzelnen Person durchgeführt werden.		Gespaltenes Wissen ist eine Methode, bei der zwei oder mehr Personen getrennt über Schlüsselkomponenten verfügen, wobei jede Person nur ihre eigene Schlüsselkomponente kennt und die einzelnen Schlüsselkomponenten kein Wissen über andere Komponenten oder den ursprünglichen kryptographischen Schlüssel vermitteln. Doppelte Kontrolle erfordert, dass zwei oder mehr Personen die Verwendung eines kryptografischen Schlüssels authentifizieren oder eine Schlüsselverwaltungsfunktion ausführen. Keine einzelne Person kann auf den Authentifizierungsfaktor (zum Beispiel Passwort, PIN oder Schlüssel) einer anderen zugreifen oder diesen verwenden.
Hinweise zur Anwendbarkeit		**Gute Praxis**
Diese Kontrolle gilt für manuelle Schlüsselverwaltungsbetriebe oder wenn die Schlüsselverwaltung nicht vom Verschlüsselungsprodukt kontrolliert wird. Ein kryptografischer Schlüssel, der einfach in zwei Teile geteilt ist, erfüllt diese Anforderung nicht. Als Schlüsselkomponenten oder Schlüsselanteile gespeicherte geheime oder private Schlüssel müssen über einen der Folgenden generiert werden: • Verwendung eines zugelassenen Zufallszahlengenerators und in einem sicheren kryptografischen Gerät (SCD), wie einem Hardware-Sicherheitsmodul (HSM) oder einem PTS-zugelassenen Ort der Interaktion-Gerät, **ODER** • Gemäß ISO 19592 oder einem gleichwertigen Industriestandard für die Generierung geheimer Schlüsselanteile.		Wenn Schlüsselkomponenten oder Schlüsselanteile verwendet werden, sollten Prozeduren sicherstellen, dass kein einzelner Verwahrer jemals Zugriff auf ausreichende Schlüsselkomponenten oder Schlüsselanteile hat, um den kryptografischen Schlüssel zu rekonstruieren. Zum Beispiel darf in einem m-aus-n-Schema (zum Beispiel Shamir), bei dem nur zwei von drei beliebigen Komponenten erforderlich sind, um den kryptografischen *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Schlüssel zu rekonstruieren, ein Verwahrer nicht über aktuelle oder vorherige Kenntnisse von mehr als einer Komponente verfügen. Wenn einem Verwahrer zuvor Komponente A zugewiesen wurde, die dann neu zugewiesen wurde, sollte dem Verwahrer dann nicht Komponente B oder C zugewiesen werden, da dies dem Verwahrer Kenntnisse über zwei Komponenten und die Möglichkeit geben würde, den Schlüssel neu zu erstellen. **Beispiele** Schlüsselverwaltungsbetriebe, die manuell durchgeführt werden können, beinhalten, sind aber nicht beschränkt auf, die Schlüsselerzeugung, -übertragung, -ladung, -speicherung und -zerstörung. **(Weitere Informationen** Industriestandards für die Verwaltung von Schlüsselkomponenten beinhalten: • *NIST SP 800-57* Teil 2, Revision 1 – Empfehlung für die Schlüsselverwaltung: Part 2 – Bewährte Praktiken für Schlüsselverwaltungsorganisationen [4.6 Schlüsselmaterialverteilung] • *ISO 11568-2 Banking — Schlüsselverwaltung (Einzelhandel) — Teil 2*: Symmetrische Chiffren, ihre Schlüsselverwaltung und ihr Lebenszyklus [4.7.2.3 Schlüsselkomponenten und 4.9.3 Schlüsselkomponenten] *European Payments Council EPC342-08 Guidelines on Cryptographic Algorithms Usage and Key Management* [insbesondere 4.1.4 Schlüsselinstallation].

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn ein Angreifer den Schlüssel einer Entität durch einen ihm bekannten Schlüssel ersetzen kann, kann der Angreifer alle mit diesem Schlüssel verschlüsselten Daten entschlüsseln. **Gute Praxis** Die Verschlüsselungslösung sollte das Ersetzen von Schlüsseln aus nicht autorisierten Quellen oder unerwarteten Prozessen nicht zulassen oder akzeptieren. Kontrollen sollten sicherstellen, dass Personen mit Zugriff auf Schlüsselkomponenten oder Anteile keinen Zugriff auf andere Komponenten oder Anteile haben, die die erforderliche Schwelle bilden, um den zur Schlüssel abzuleiten.
3.7.7 Richtlinien und Prozeduren zur Schlüsselverwaltung werden implementiert, um die Verhinderung eines nicht autorisierten Austauschs kryptographischer Schlüssel einzuschließen.	**3.7.7.a** Die dokumentierten Richtlinien und Prozeduren zur Schlüsselverwaltung für Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, untersuchen, und verifizieren, dass sie die Verhinderung von nicht autorisiertem Ersatz kryptografischer Schlüsseln definieren.	
Zielsetzung des kundenspezifischen Ansatzes	**3.7.7.b** Personal befragen und/oder Prozesse beachten, um zu verifizieren, dass ein nicht autorisierter Austausch von Schlüsseln verhindert wird.	
Kryptografische Schlüssel können nicht durch nicht autorisiertes Personal ersetzt werden.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Dieser Prozess wird dazu beitragen, sicherzustellen, dass sich Personen, die als Schlüsselverwahrer fungieren, auf die Rolle der Schlüsselverwahrer verpflichten und die Verantwortlichkeiten verstehen und akzeptieren. Eine jährliche erneute Bestätigung kann dabei helfen, wichtige Schlüsselverwahrer an ihre Verantwortung zu erinnern. **Weitere Informationen** Die Branchenanleitungen für Schlüsselverwahrer und ihre Rollen und Verantwortlichkeiten umfassen: • *NIST SP 800-130 Ein Rahmenwerk zum Entwerfen von kryptografischen Schlüsselverwaltungssystemen* [5. Rollen und Verantwortlichkeiten (insbesondere) für Schlüsselverwahrer] • *ISO 11568-1 Banking — Schlüsselverwaltung (Einzelhandel) — Teil 1*: Grundsätze [5 Grundsätze der Schlüsselverwaltung (insbesondere b)]
3.7.8 Richtlinien und Verfahren zur Schlüsselverwaltung werden implementiert, um zu enthalten, dass die Verwahrer von kryptografischen Schlüsseln formell bestätigen (schriftlich oder elektronisch), dass sie ihre Verantwortlichkeiten als Schlüsselverwahrer verstehen und akzeptieren.	**3.7.8.a** Die dokumentierten Schlüsselverwaltungsrichtlinien und -prozeduren für Schlüssel, die zum Schutz gespeicherter Kontodaten verwendet werden, untersuchen, und verifizieren, dass sie Bestätigungen für Schlüsselverwahrer gemäß allen in dieser Anforderung angegebenen Elementen definieren.	
Zielsetzung des kundenspezifischen Ansatzes	**3.7.8.b** Dokumentation oder andere Nachweise untersuchen, die zeigen, dass die Schlüsselverwahrer Bestätigungen gemäß allen in dieser Anforderung angegebenen Elementen bereitgestellt haben.	
Schlüsselverwahrer kennen ihre Verantwortlichkeiten in Bezug auf kryptografische Betriebe und können bei Bedarf auf Unterstützung und Anleitungen zugreifen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Bereitstellung von Anleitungen für Kunden zum sicheren Übertragen, Speichern und Aktualisieren von kryptografischen Schlüsseln kann dabei helfen, dass Schlüssel falsch verwaltet oder an nicht autorisierte Entitäten weitergegeben werden. **Weitere Informationen** Zahlreiche Industriestandards für die Schlüsselverwaltung sind oben in den Anleitungen für Anforderungen 3.7.1-3.7.8 aufgeführt.
3.7.9 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Wenn ein Dienstanbieter kryptografische Schlüssel mit seinen Kunden zur Übertragung oder Speicherung von Kontodaten teilt, werden Anleitungen zur sicheren Übertragung, Speicherung und Aktualisierung dieser Schlüssel dokumentiert und an die Kunden des Dienstleistungsanbieters verteilt.	**3.7.9** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Wenn der Dienstleistungsanbieter kryptografische Schlüssel mit seinen Kunden zur Übertragung oder Speicherung von Kontodaten teilt, die Dokumentation untersuchen, die der Dienstleistungsanbieter seinen Kunden bereitstellt, um zu verifizieren, dass sie Anleitungen zur sicheren Übertragung, Speicherung und Aktualisierung der Schlüssel der Kunden gemäß allen Elementen, die in den Anforderungen 3.7.1 bis 3.7.8 oben angegeben sind, enthält.	
Zielsetzung des kundenspezifischen Ansatzes		
Den Kunden werden angemessene Anleitungen zur Schlüsselverwaltung bereitgestellt, wenn sie gemeinsame kryptografische Schlüssel erhalten.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist.		

Anforderung 4: Schutz von Karteninhaberdaten mit Starker Kryptographie Während der Übertragung über Offene, öffentliche Netzwerke

Abschnitte	
4.1	Prozesse und Mechanismen zum Schutz von Karteninhaberdaten mit starker Kryptographie bei der Übertragung über offene, öffentliche Netze werden definiert und dokumentiert.
4.2	PAN wird während der Übertragung mit starker Kryptographie geschützt

Übersicht

Die Verwendung einer starken Kryptographie stellt eine größere Sicherheit bei der Wahrung der Vertraulichkeit, Integrität und Nichtabstreitbarkeit der Daten bereit.

Zum Schutz vor Kompromittierung muss PAN während der Übertragung über Netzwerke verschlüsselt werden, auf die böswillige Personen leicht zugreifen können, einschließlich nicht vertrauenswürdiger und öffentlicher Netzwerke. Falsch konfigurierte drahtlose Netzwerke und Schwachstellen in alten Verschlüsselungs- und Authentifizierungsprotokollen werden weiterhin von böswilligen Personen angegriffen, die diese Schwachstellen ausnutzen wollen, um privilegierten Zugriff auf Karteninhaberdatenumgebungen (CDE) zu erhalten. Alle Übertragungen von Karteninhaberdaten über das/die interne(n) Netzwerk(e) einer Entität wird dieses Netzwerk natürlich in den Anwendungsbereich von PCI DSS bringen, da dieses Netzwerk Karteninhaberdaten speichert, verarbeitet oder überträgt. Alle derartigen Netzwerke müssen anhand der geltenden PCI DSS-Anforderungen bewertet und beurteilt werden.

Anforderung 4 gilt für Übertragungen von PAN, es sei denn, dies wird in einer individuellen Anforderung ausdrücklich genannt.

PAN-Übertragungen können durch Verschlüsseln der Daten vor der Übertragung oder durch Verschlüsseln der Sitzung, über die Daten übertragen werden, oder durch beides geschützt werden. Es ist nicht erforderlich, sowohl auf Daten- als auch auf Sitzungsebene eine starke Kryptographie anzuwenden, es wird jedoch empfohlen.

Siehe Anhang G für Definitionen von „starker Kryptographie“ und anderen PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
4.1 Prozesse und Mechanismen zum Schutz von Karteninhaberdaten mit starker Kryptographie bei der Übertragung über offene, öffentliche Netze werden definiert und dokumentiert.		
Definierte Ansatzanforderungen **4.1.1** Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 4 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	**Testprozeduren mit definiertem Ansatz** **4.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 4 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Bei Anforderung 4.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 4 angegeben sind. Während es wichtig ist, die in Anforderung 4 genannten spezifischen Richtlinien oder Verfahren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Prozeduren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Verfahren und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen. Richtlinien und Prozeduren, einschließlich Aktualisierungen, werden jeglichem betroffenen Personal aktiv mitgeteilt und durch Betriebsprozeduren unterstützt, die beschreiben, wie Aktivitäten durchgeführt werden.
Zielsetzung des kundenspezifischen Ansatzes Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 4 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht des Managements.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen sind, ist das Personal sich möglicherweise seiner täglichen Verantwortlichkeiten nicht bewusst und kritische Aktivitäten können nicht stattfinden. **Gute Praxis** Rollen und Verantwortlichkeiten können in Richtlinien und Verfahren dokumentiert oder in separaten Dokumenten gewartet werden. Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen. **Beispiele** Ein Verfahren zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).
4.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 4 werden dokumentiert, zugewiesen und verstanden.	**4.1.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 4 dokumentiert und zugewiesen sind.	
	4.1.2.b Personal mit Verantwortlichkeit zur Durchführung von Aktivitäten in Anforderung 4 befragen, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 4 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
4.2 PAN wird während der Übertragung mit starker Kryptographie geschützt.		
Definierte Ansatzanforderungen **4.2.1** Starke Kryptographie- und Sicherheitsprotokolle werden wie folgt implementiert, um PAN während der Übertragung über offene, öffentliche Netzwerke zu schützen: • Es werden nur vertrauenswürdige Schlüssel und Zertifikate akzeptiert. • Zertifikate, die zum Schutz von PAN während der Übertragung über offene, öffentliche Netzwerke verwendet werden, werden als gültig bestätigt und sind nicht abgelaufen oder widerrufen. *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens einer bewährten Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.* • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen und unterstützt keinen Rückfall auf oder die Verwendung von unsicheren Versionen, Algorithmen, Schlüsselgrößen oder Implementierungen. • Die Verschlüsselungsstärke ist für die verwendete Verschlüsselungsmethodik angemessen. **Zielsetzung des kundenspezifischen Ansatzes** Klartext-PAN kann bei Übertragungen über offene, öffentliche Netzwerke nicht gelesen oder abgefangen werden.	**Testprozeduren mit definiertem Ansatz** **4.2.1.a** Dokumentierte Richtlinien und Prozeduren untersuchen und das Personal befragen, um zu verifizieren, dass die Prozesse so definiert sind, dass sie alle in dieser Anforderung angegebenen Elemente enthalten. **4.2.1.b** Systemkonfigurationen untersuchen, um zu verifizieren, dass starke Kryptografie- und Sicherheitsprotokolle in Übereinstimmung mit allen in dieser Anforderung angegebenen Elementen implementiert sind. **4.2.1.c** Datenübertragungen von Karteninhabern untersuchen, um zu verifizieren, dass alle PANs mit starker Kryptographie verschlüsselt sind, wenn sie über offene, öffentliche Netzwerke übertragen werden. **4.2.1.d** Systemkonfigurationen untersuchen, um zu verifizieren, dass Schlüssel und/oder Zertifikate, die nicht als vertrauenswürdig verifiziert werden können, abgelehnt werden.	**Zweck** Sensible Informationen müssen während der Übertragung über öffentliche Netzwerke verschlüsselt werden, da es für eine böswillige Person einfach und üblich ist, Daten während des Transports abzufangen und/oder umzuleiten. **Gute Praxis** Die in Anforderung 1 definierten Netzwerkdiagramme und Datenfluss- sind eine nützliche Ressource, um alle Verbindungspunkte zu identifizieren, an denen Kontodaten über offene, öffentliche Netzwerke übertragen oder empfangen werden. Obwohl dies nicht erforderlich ist, wird es als gute Praxis für Entitäten angesehen, PAN auch über ihre internen Netzwerke zu verschlüsseln, und für Entitäten, neue Netzwerkimplementierungen mit verschlüsselter Kommunikation zu etablieren. PAN-Übertragungen können durch Verschlüsseln der Daten vor der Übertragung oder durch Verschlüsseln der Sitzung, über die Daten übertragen werden, oder durch beides geschützt werden. Es ist nicht erforderlich, sowohl auf Daten- als auch auf Sitzungsebene eine starke Kryptographie anzuwenden, es wird jedoch besonders empfohlen. Bei Verschlüsselung auf Datenebene können die zum Schutz der Daten verwendeten kryptografischen Schlüssel gemäß Anforderungen 3.6 und 3.7 verwaltet werden. Wenn die Daten auf Sitzungsebene verschlüsselt werden, sollte benannten Schlüsselverwahrern die Verantwortung für die Verwaltung von Übertragungsschlüsseln und Zertifikaten zugewiesen werden. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Es kann vorkommen, dass eine Entität Karteninhaberdaten unaufgefordert über einen unsicheren Kommunikationskanal erhält, der nicht für den Empfang sensibler Daten vorgesehen ist. In dieser Situation kann die Entität entweder den Kanal in den Geltungsbereich ihrer CDE aufnehmen und ihn gemäß PCI DSS sichern oder Maßnahmen implementieren, um zu verhindern, dass der Kanal für Karteninhaberdaten verwendet wird. Ein selbstsigniertes Zertifikat kann auch akzeptabel sein, wenn das Zertifikat von einer internen CA innerhalb der Organisation ausgestellt wird, der Autor des Zertifikats bestätigt und das Zertifikat verifiziert ist – zum Beispiel per Hash oder Unterschrift – und nicht abgelaufen ist. Beachten Sie, dass selbstsignierte Zertifikate, bei denen das Anerkannter Name (DN)-Feld in den Feldern „Ausgestellt von“ und „Ausgestellt an“ identisch ist, nicht akzeptabel sind. *Der obige Aufzählungspunkt (zur Bestätigung, dass Zertifikate, die zum Schutz von PAN während der Übertragung über offene, öffentliche Netzwerke verwendet werden, gültig sind und nicht abgelaufen oder widerrufen sind) ist eine bewährte Praktik bis zum 31. März 2025, danach wird er als Teil von Anforderung 4.2.1 benötigt und muss bei einer PCI-DSS-Bewertung vollständig berücksichtigt werden.*		Einige Protokollimplementierungen (wie SSL, SSH v1.0 und frühe TLS) weisen bekannte Schwachstellen auf, die ein Angreifer verwenden kann, um Zugriff auf die Klartextdaten zu erhalten. Es ist wichtig, dass Entitäten die branchendefinierten Verfallsdaten für die von ihnen verwendeten Verschlüsselungspakete im Auge behalten und bereit sind, auf neuere Versionen oder Protokolle zu migrieren, wenn ältere als nicht mehr sicher gelten. Die Verifizierung, dass Zertifikate vertrauenswürdig sind, hilft dabei, die Integrität der sicheren Verbindung zu sicherzustellen. Um als vertrauenswürdig betrachtet zu werden, sollte ein Zertifikat von einer vertrauenswürdigen Quelle, wie einer vertrauenswürdigen Zertifizierungsbehörde (CA), ausgestellt werden und nicht abgelaufen sein. Aktuelle Zertifikatswiderrufslisten (CRLs) oder das Online Zertifikatsstatusprotokoll (OCSP) können verwendet werden, um Zertifikate zu validieren. Techniken, um Zertifikate zu validieren können das Anheften von Zertifikaten und öffentlichen Schlüsseln beinhalten, wobei das vertrauenswürdige Zertifikat oder ein öffentlicher Schlüssel entweder während der Entwicklung oder bei seiner ersten Verwendung angeheftet wird. Entitäten können sich auch bei Entwicklern bestätigen oder den Quellcode überprüfen, um sicherzustellen, dass Kunden und Server Verbindungen ablehnen, wenn das Zertifikat schlecht ist. Bei browserbasierten TLS-Zertifikaten kann das Zertifikatsvertrauen oft durch Klicken auf das Schlosssymbol neben der Adressleiste verifiziert werden. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Beispiele Offene, öffentliche Netzwerke be4inhalten, sind aber nicht beschränkt auf: • Das Interne und • Drahtlose Technologien, einschließlich Wi-Fi, Bluetooth, Mobilfunktechnologien und Satellitenkommunikationen. **Weitere Informationen** Informationen über die richtige Verschlüsselungsstärke speziell für die verwendete Verschlüsselungsmethode finden Sie in den Empfehlungen von Anbietern und den bewährten Praktiken der Branche. Weitere Informationen zu starker Kryptografie und sicheren Protokollen finden Sie unter Industriestandards und bewährte Praktiken wie *NIST SP 800-52* und *SP 800-57*. Weitere Informationen zu vertrauenswürdigen Schlüsseln und Zertifikaten siehe *NIST Cybersecurity Practice Guide Special Publication 1800-16*, *Securing Web Transactions: Transport Layer Security (TLS) Server Certificate Management.*

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Inventar der vertrauenswürdigen Schlüssel hilft der Entität, den Überblick über Algorithmen, Protokolle, Schlüsselstärke, Schlüsselverwahrer und Schlüsselablaufdaten zu behalten. Dadurch kann die Entität schnell auf Schwachstellen reagieren, die in Verschlüsselungssoftware, Zertifikaten und kryptografischen Algorithmen entdeckt werden. **Gute Praxis** Bei Zertifikaten sollte das Inventar die ausstellende CA und das Ablaufdatum der Zertifizierung enthalten.
4.2.1.1 Es wird ein Inventar der vertrauenswürdigen Schlüssel und Zertifikate der Entität geführt, die zum Schutz von PAN während der Übertragung verwendet werden.	**4.2.1.1.a** Dokumentierte Richtlinien und Verfahren untersuchen, um zu verifizieren, ob Prozesse für die Entität definiert sind, um eine Bestandsaufnahme ihrer vertrauenswürdigen Schlüssel und Zertifikate beizubehalten.	
	4.2.1.1.b Das Inventar von vertrauenswürdigen Schlüsseln und Zertifikaten untersuchen, um zu verifizieren, dass es auf dem neuesten Stand ist.	
Zielsetzung des kundenspezifischen Ansatzes Alle Schlüssel und Zertifikate, die zum Schutz der PAN während der Übertragung verwendet werden, werden als vertrauenswürdig identifiziert und bestätigt.		
Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Da drahtlose Netzwerke keine physischen Medien für die Verbindung benötigen, ist es wichtig, Kontrollen zu etablieren, die einschränken, wer eine Verbindung herstellen kann und welche Übertragungsprotokolle verwendet werden. Böswillige Benutzer verwenden kostenlose und weit verbreitete Tools, um die drahtlose Kommunikation abzuhören. Die Verwendung einer starken Kryptographie kann dabei helfen, die Offenlegung sensibler Informationen in drahtlosen Netzwerken einzuschränken. Drahtlose Netzwerke stellen einzigartige Risiken für eine Organisation dar; daher müssen sie gemäß den Branchenanforderungen identifiziert und geschützt werden. Eine starke Kryptographie für die Authentifizierung und Übertragung von PAN ist erforderlich, um zu verhindern, dass böswillige Benutzer Zugriff auf das drahtlose Netzwerk erhalten oder drahtlose Netzwerke verwenden, um auf andere interne Netzwerke oder Daten zuzugreifen. **Gute Praxis** Drahtlose Netzwerke sollten keinen Drahtlose Netze sollten keinen Rückfall oder Herabstufung auf ein unsicheres Protokoll oder eine geringere Verschlüsselungsstärke zulassen, die nicht der Absicht einer starken Kryptografie entspricht. **Weitere Informationen** Weitere Informationen zur Auswahl von Protokollen, Konfigurationen und Einstellungen im Zusammenhang mit der Kryptographie finden Sie in der spezifischen Dokumentation des Anbieters.
4.2.1.2 Drahtlose Netzwerke, die PAN übertragen oder mit der CDE verbunden sind, verwenden bewährte Praktiken der Branche, um eine starke Kryptographie für die Authentifizierung und Übertragung zu implementieren.	**4.2.1.2** Systemkonfigurationen untersuchen, um zu verifizieren, dass drahtlose Netzwerke, die PAN übertragen oder mit der CDE verbunden sind, bewährte Praktiken der Branche verwenden, um eine starke Kryptographie für die Authentifizierung und Übertragung zu implementieren.	
Zielsetzung des kundenspezifischen Ansatzes		
Klartext-PAN kann von drahtlosen Netzwerken nicht gelesen oder abgefangen werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
4.2.2 PAN wird immer mit starker Kryptographie gesichert, wenn es über Messaging-Technologien für Endbenutzer gesendet wird.	**4.2.2.a** Dokumentierte Richtlinien und Verfahren untersuchen, um zu verifizieren, dass Prozesse definiert sind, um PAN mit starker Kryptographie zu sichern, wenn sie über Messaging-Technologien für Endbenutzer gesendet werden.	Messaging-Technologien für Endbenutzer können in der Regel leicht durch Paket-Schnüffeln während der Zustellung über interne und öffentliche Netzwerke abgefangen werden. **Gute Praxis** Die Verwendung von Endbenutzer-Messaging-Technologie zum Senden von PAN sollte nur in Betracht gezogen werden, wenn ein definierter Geschäftsbedarf besteht. **Beispiele** E-Mail, Instant Messaging, SMS und Chat sind Beispiele für die Art der Messaging-Technologie für Endbenutzer, auf die sich diese Anforderung bezieht.
Zielsetzung des kundenspezifischen Ansatzes	**4.2.2.b** Systemkonfigurationen und Herstellerdokumentation untersuchen, um zu verifizieren, dass PAN mit starker Kryptographie gesichert ist, wenn sie über Messaging-Technologien für Endbenutzer gesendet wird.	
Klartext-PAN kann von Übertragungen mit Endbenutzer-Messaging-Technologien nicht gelesen oder abgefangen werden.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt auch, wenn ein Kunde oder ein anderer Dritter die Zusendung von PAN über Endbenutzer-Messaging-Technologien anfordert. Es kann vorkommen, dass eine Entität unaufgeforderte Karteninhaberdaten über einen unsicheren Kommunikationskanal erhält, der nicht für Übertragungen sensibler Daten vorgesehen ist. In dieser Situation kann die Entität entweder den Kanal in den Geltungsbereich ihrer CDE aufnehmen und ihn gemäß PCI DSS sichern oder die Karteninhaberdaten löschen und Maßnahmen implementieren, um zu verhindern, dass der Kanal für Karteninhaberdaten verwendet wird.		

Wartung Eines Programms zur Verwaltung von Schwachstellen

Anforderung 5: Schutz aller Systeme und Netzwerke vor Bösartiger Software

Abschnitte	
5.1	Prozesse und Mechanismen zum Schutz aller Systeme und Netzwerke vor böswilliger Software sind definiert und verstanden.
5.2	Böswillige Software (Malware) wird verhindert oder erfasst und beseitigt.
5.3	Anti-Malware-Mechanismen und Prozesse sind aktiv, werden gewartet und überwacht.
5.4	Anti-Phishing-Mechanismen schützen Benutzer vor Phishing-Angriffen.

Übersicht

Bei böswilliger Software (Malware) handelt es sich um Software oder Firmware, die darauf abzielt, ein Computersystem ohne das Wissen oder die Zustimmung des Besitzers zu infiltrieren oder zu beschädigen, um die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen, oder des Betriebssystems des Besitzers zu beeinträchtigen.

Beispiele umfassen Viren, Würmer, Trojaner, Spyware, Ransomware, Keylogger und Rootkits, böswilligen Code, Skripte und Links.

Malware kann bei vielen vom Unternehmen genehmigten Aktivitäten in das Netzwerk eindringen, einschließlich durch E-Mails von Mitarbeitern (z. B. über Phishing) und Verwendung des Internets, mobile Computer und Speichergeräte, was zur Ausnutzung von Systemschwachstellen führt.

Die Verwendung von Anti-Malware-Lösungen, die alle Arten von Malware adressieren, hilft bei, Systeme vor aktuellen und sich entwickelnden Malware-Bedrohungen zu schützen.

Finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
5.1 Prozesse und Mechanismen zum Schutz aller Systeme und Netzwerke vor böswilliger Software sind definiert und verstanden.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
5.1.1 Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 5 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	**5.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 5 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	Bei Anforderung 5.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 5 angegeben sind. Während es wichtig ist, die in Anforderung 5 genannten spezifischen Richtlinien oder Verfahren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Prozeduren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Verfahren und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen.
Zielsetzung des kundenspezifischen Ansatzes		
Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 5 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar konsequent angewendet, und entsprechen der Absicht der Verwaltung.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen werden, sind Netzwerke und Systeme möglicherweise nicht ordnungsgemäß vor Malware geschützt. **Gute Praxis** Rollen und Verantwortlichkeiten können in Richtlinien und Verfahren dokumentiert oder in separaten Dokumenten gewartet werden. Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen. **Beispiele** Ein Verfahren zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).
5.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 5 werden dokumentiert, zugewiesen und verstanden.	**5.1.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 5 dokumentiert und zugewiesen sind.	
	5.1.2.b Personal mit Verantwortlichkeit zur Durchführung von Aktivitäten in Anforderung 5 befragen, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 5 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
5.2 Böswillige Software (Malware) wird verhindert oder erfasst und beseitigt.		
Definierte Ansatzanforderungen **5.2.1** Eine Anti-Malware Lösung(en) werden auf allen Systemkomponenten bereitgestellt, mit Ausnahme der Systemkomponenten, die in regelmäßigen Bewertungen gemäß Anforderung 5.2.3 identifiziert wurden, die zu dem Schluss kommen, dass die Systemkomponenten nicht durch Malware gefährdet sind. **Zielsetzung des kundenspezifischen Ansatzes** Es werden automatisierte Mechanismen implementiert, um zu verhindern, dass Systeme zum Angriffsvektor für Malware werden.	**Testprozeduren mit definiertem Ansatz** **5.2.1.a** Systemkomponenten untersuchen, um zu verifizieren, dass eine oder mehrere Anti-Malware-Lösungen auf allen Systemkomponenten bereitgestellt werden, mit Ausnahme derer, die aufgrund regelmäßiger Bewertungen gemäß Anforderung 5.2.3 als nicht durch Malware gefährdet eingestuft wurden. **5.2.1.b** Für alle Systemkomponenten ohne Anti-Malware-Lösung die regelmäßigen Bewertungen untersuchen, um zu verifizieren, dass die Komponente bewertet wurde und die Bewertung zu dem Schluss kommt, dass die Komponente nicht durch Malware gefährdet ist.	**Zweck** Es gibt einen ständigen Strom von Angriffen, die auf neu entdeckte Schwachstellen in Systemen abzielen, die zuvor als sicher galten. Ohne eine regelmäßig aktualisierte Anti-Malware-Lösung können neue Formen von Malware verwendet werden, um Systeme anzugreifen, ein Netzwerk zu deaktivieren oder Daten zu kompromittieren. **Gute Praxis** Für Entitäten ist es von Vorteil, sich über „Zero-Day“-Angriffe (solche, die eine zuvor unbekannte Schwachstelle ausnutzen) bewusst zu sein und Lösungen in Betracht zu ziehen, die sich auf Verhaltensmerkmale konzentrieren und auf unerwartetes Verhalten aufmerksam machen und darauf reagieren. **Definitionen** Systemkomponenten, von denen bekannt ist, dass sie von Malware betroffen sind, verfügen über aktive Malware-Ausnutzungen, die in der realen Welt verfügbar sind (nicht nur theoretische Ausnutzungen).
Definierte Ansatzanforderungen **5.2.2** Die eingesetzte(n) Anti-Malware-Lösung(en): • Erkennt alle bekannten Arten von Malware. • Entfernt, sperrt oder dämmt alle bekannten Arten von Malware ein. **Zielsetzung des kundenspezifischen Ansatzes** Malware kann andere Systemkomponenten nicht ausführen oder infizieren.	**Testprozeduren mit definiertem Ansatz** **5.2.2** Anbieterdokumentation und Konfigurationen der Anti-Malware-Lösung(en) untersuchen, um zu verifizieren, dass die Lösung: • Alle bekannten Arten von Malware erkennt. • Alle bekannten Arten von Malware entfernt, sperrt oder eindämmt.	**Zweck** Es ist wichtig, sich vor allen Arten und Formen von Malware zu schützen, um unbefugten Zugriff zu verhindern. **Gute Praxis** Anti-Malware-Lösungen können eine Kombination aus netzwerkbasierten Kontrollen, hostbasierten Kontrollen und Endpunktsicherheitslösungen enthalten. Zusätzlich zu signaturbasierten Tools enthalten die Funktionen moderner Anti-Malware-Lösungen Sandboxing, Kontrollen zur Rechteausweitung und maschinelles Lernen. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Lösungstechniken beinhalten das Verhindern des Eindringens von Malware in das Netzwerk und das Entfernen oder Eindämmen von Malware, die in das Netzwerk eindringt. **Beispiele** Die Arten von Malware beinhalten, sind aber nicht beschränkt auf Viren, Trojaner, Würmer, Spyware, Ransomware, Keylogger, Rootkits, böswilligen Code, Skripte und Links.
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
5.2.3 Alle Systemkomponenten, die nicht durch Malware gefährdet sind, werden regelmäßig bewertet, um Folgendes zu beinhalten: • Eine dokumentierte Liste aller Systemkomponenten, die nicht durch Malware gefährdet sind. • Identifizierung und Bewertung von sich entwickelnden Malware-Bedrohungen für diese Systemkomponenten. • Bestätigung, ob solche Systemkomponenten weiterhin keinen Anti-Malware-Schutz benötigen.	**5.2.3.a** Dokumentierte Richtlinien und Prozeduren untersuchen, um zu verifizieren, ob ein Prozess für die regelmäßige Bewertung aller Systemkomponenten definiert ist, die nicht durch Malware gefährdet sind, die alle in dieser Anforderung angegebenen Elemente beinhalten.	Bestimmte Systeme werden zu einem bestimmten Zeitpunkt möglicherweise derzeit nicht häufig von Malware anvisiert oder betroffen. Branchentrends für Malware können sich jedoch schnell ändern, daher ist es für Organisationen wichtig, sich neuer Malware bewusst zu sein, die ihre Systeme betreffen könnte – zum Beispiel durch die Überwachung von Sicherheitshinweisen der Anbieter und Anti-Malware-Foren, um zu bestimmen, ob ihre Systeme möglicherweise durch neue und sich entwickelnde Malware gefährdet sind.
	5.2.3.b Personal befragen, um zu verifizieren, dass die Bewertungen alle in dieser Anforderung angegebenen Elemente enthalten.	**Gute Praxis** Wenn eine Entität feststellt, dass ein bestimmtes System nicht anfällig für Malware ist, sollte die Feststellung durch Branchennachweise, Anbieterressourcen und bewährte Praktiken unterstützt werden. Die folgenden Schritte können Entitäten bei ihren regelmäßigen Bewertungen helfen:
Zielsetzung des kundenspezifischen Ansatzes Die Entität hält das Bewusstsein für sich entwickelnde Malware-Bedrohungen aufrecht, um sicherzustellen, dass Systeme, die nicht vor Malware geschützt sind, keiner Infektionsgefahr ausgesetzt sind.	**5.2.3.c** Die Liste der Systemkomponenten, die als nicht von Malware gefährdet identifiziert wurden, untersuchen und sie mit den Systemkomponenten ohne eine gemäß Anforderung 5.2.1 eingesetzte Anti-Malware-Lösung vergleichen, um zu verifizieren, dass die Systemkomponenten beiden Anforderungen entsprechen.	

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Von dieser Anforderung abgedeckte Systemkomponenten sind diejenigen, für die keine Anti-Malware-Lösung gemäß Anforderung 5.2.1 eingesetzt wurde.		• Identifizierung aller Systemtypen, bei denen zuvor festgestellt wurde, dass kein Malware-Schutz erforderlich ist. • Überprüfung von branchenspezifischen Schwachstellenwarnungen und -hinweisen, um festzustellen, ob für ein identifiziertes System neue Bedrohungen vorhanden sind. • Eine dokumentierte Schlussfolgerung, ob die Systemtypen nicht anfällig für Malware bleiben. • Eine Strategie zum Hinzufügen von Malware-Schutz für alle Systemtypen, für die Malware-Schutz erforderlich wurde. Trends bei Malware sollten bei der Identifizierung neuer Sicherheitsschwachstellen in Anforderung 6.3.1 berücksichtigt werden, und Methoden zur Behebung neuer Trends sollten bei Bedarf in die Konfigurationsstandards und Schutzmechanismen der Entität integriert werden.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
5.2.3.1 Die Häufigkeit der regelmäßigen Bewertungen von Systemkomponenten, die als nicht gefährdet für Malware identifiziert wurden, wird in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird.	**5.2.3.1.a** Die gezielte Risikoanalyse der Entität für die Häufigkeit regelmäßiger Bewertungen von Systemkomponenten, die als nicht gefährdet für Malware identifiziert sind, untersuchen, um zu verifizieren, dass die Risikoanalyse gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wurde.	Entitäten bestimmen die optimale Zeitdauer, um die Bewertung anhand von Kriterien wie der Komplexität der Umgebung der einzelnen Entitäten und der Anzahl der zu bewertenden Systemtypen durchzuführen.
Zielsetzung des kundenspezifischen Ansatzes	**5.2.3.1.b** Dokumentierte Ergebnisse der regelmäßigen Bewertungen von Systemkomponenten, die als nicht gefährdet für Malware identifiziert sind, untersuchen und das Personal befragen, um zu verifizieren, dass Bewertungen in der Häufigkeit durchgeführt werden, die in der für diese Anforderung durchgeführten gezielten Risikoanalyse der Entität angegeben ist.	
Systeme, von denen nicht bekannt ist, dass sie durch Malware gefährdet sind, werden in einer Häufigkeit neu bewertet, die das Risiko der Entitäten adressiert.		
Hinweise zur Anwendbarkeit		
Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.		

Anforderungen und Testprozeduren		Anleitungen
5.3 Anti-Malware-Mechanismen und Prozesse sind aktiv, werden gewartet und überwacht.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Damit eine Anti-Malware-Lösung wirksam bleibt, muss sie über die neuesten Sicherheitsaktualisierungen, Signaturen, Bedrohungsanalyse-Engines und andere Malware-Schutzmechanismen verfügen, auf die sich die Lösung stützt. Ein automatisierter Aktualisierungsprozess vermeidet die Belastung der Endbenutzer mit der Verantwortung für die manuelle Installation von Aktualisierungen und stellt eine größere Sicherheit bereit, dass Anti-Malware-Schutzmechanismen nach der Freigabe einer Aktualisierung so schnell wie möglich aktualisiert werden. **Gute Praxis** Anti-Malware-Mechanismen sollten so schnell wie möglich über eine vertrauenswürdige Quelle aktualisiert werden, nachdem eine Aktualisierung verfügbar ist. Die Verwendung einer vertrauenswürdigen gemeinsamen Quelle, um Aktualisierungen an Endbenutzersysteme zu verteilen, hilft dabei, die Integrität und Konsistenz der Lösungsarchitektur sicherzustellen. Aktualisierungen können automatisch an einen zentralen Ort heruntergeladen werden, um zum Beispiel Tests zu gestatten, bevor sie auf einzelnen Systemkomponenten eingesetzt werden.
5.3.1 Die Anti-Malware-Lösung(en) wird (werden) durch automatische Aktualisierungen auf dem neuesten Stand gehalten.	**5.3.1.a** Anti-Malware-Lösungs-Konfigurationen einschließlich einer Master-Installation der Software untersuchen, um zu verifizieren, dass die Lösung konfiguriert ist, um automatische Aktualisierungen durchzuführen.	
	5.3.1.b Systemkomponenten und Protokolle untersuchen, um zu verifizieren, dass die Anti-Malware-Lösung(en) und Definitionen aktuell sind und umgehend bereitgestellt wurden	
Zielsetzung des kundenspezifischen Ansatzes		
Anti-Malware-Mechanismen können die neuesten Malware-Bedrohungen erkennen und adressieren.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Regelmäßige Scans können Malware identifizieren, die in der Umgebung vorhanden, aber derzeit inaktiv ist. Manche Malware, wie -Malware, kann in eine Umgebung eindringen, bevor die Scan-Lösung in der Lage ist, sie zu erkennen. Die Durchführung regelmäßiger Scans oder kontinuierlicher Verhaltensanalysen von Systemen oder Prozessen hilft dabei, sicherzustellen, dass bisher unentdeckte Malware identifiziert, entfernt und untersucht werden kann, um festzustellen, wie sie Zugriff auf die Umgebung erhalten hat. **Gute Praxis** Die Verwendung einer Kombination aus regelmäßigen Scans (geplant und bei Bedarf) und aktiven Echtzeit-Scans (bei Zugriff) hilft dabei, sicherzustellen, dass Malware, die sich sowohl in statischen als auch in dynamischen Elementen der CDE befindet, adressiert wird. Benutzer sollten auch Scans auf Verlangen auf ihren Systemen durchführen können, wenn verdächtige Aktivitäten erkannt werden – dies kann bei der Früherkennung von Malware hilfreich sein. Scans sollten das gesamte Dateisystem umfassen, einschließlich aller Festplatten, Arbeitsspeicher und Startdateien und Boot-Records (beim Neustart des Systems), um alle Malware bei der Dateiausführung zu erkennen, einschließlich jeglicher Software, die möglicherweise auf einem System resident, aber derzeit nicht aktiv ist. Der Scan-Geltungsbereich sollte alle Systeme und Software in der CDE umfassen, einschließlich derer, die oft übersehen werden, wie E-Mail-Server, Webbrowser und Instant Messaging-Software. *(Fortsetzung auf der nächsten Seite)*
5.3.2 Die Anti-Malware-Lösung(en): • Führt regelmäßige Scans und aktive oder Echtzeit-Scans durch. **ODER** • Führt eine kontinuierliche Verhaltensanalyse von Systemen oder Prozessen durch.	**5.3.2.a** Anti-Malware-Lösung(en)-Konfigurationen einschließlich einer Master-Installation der Software untersuchen, um zu verifizieren, dass die Lösung(en) konfiguriert ist (sind), um mindestens eines der in dieser Anforderung angegebenen Elemente durchzuführen.	
	5.3.2.b Systemkomponenten untersuchen, einschließlich aller als Schadsoftware gefährdeten Betriebssystemarten, um zu verifizieren, dass die Lösung(en) gemäß mindestens einem der in dieser Anforderung angegebenen Elemente aktiviert ist (sind).	
Zielsetzung des kundenspezifischen Ansatzes	**5.3.2.c** Protokolle und Scanergebnisse untersuchen, um zu verifizieren, dass die Lösung(en) gemäß mindestens einem der in dieser Anforderung angegebenen Elemente aktiviert ist.	
Malware kann die Ausführung nicht abschließen.		

Anforderungen und Testprozeduren		Anleitungen
		Definitionen Aktives oder Echtzeit-Scannen überprüft Dateien auf Malware bei jedem Versuch, eine Datei zu öffnen, zu schließen, umzubenennen oder auf andere Weise mit ihr zu interagieren, wodurch verhindert wird, dass die Malware aktiviert wird.
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Entitäten können die optimale Zeitdauer für die Durchführung regelmäßiger Scans basierend auf ihrer eigenen Einschätzung der Risiken für ihre Umgebung bestimmen.
5.3.2.1 Wenn regelmäßige Malware-Scans durchgeführt werden, um Anforderung 5.3.2 zu erfüllen, wird die Häufigkeit der Scans in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird.	**5.3.2.1.a** Die gezielte Risikoanalyse der Entität für die Häufigkeit regelmäßiger Malware-Scans untersuchen, um zu verifizieren, dass die Risikoanalyse gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wurde.	
	5.3.2.1.b Dokumentierte Ergebnisse der regelmäßigen Malware-Scans untersuchen und das Personal befragen, um zu verifizieren, dass Scans in der Häufigkeit durchgeführt werden, die in der für diese Anforderung durchgeführten gezielten Risikoanalyse der Entität angegeben ist.	
Zielsetzung des kundenspezifischen Ansatzes		
Scans durch die Malware-Lösung werden mit einer Häufigkeit durchgeführt, die das Risiko der Entität adressiert.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt für Entitäten, die regelmäßige Malware-Scans durchführen, um Anforderung 5.3.2 zu erfüllen. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **5.3.3** Für entfernbare elektronische Medien führt die Anti-Malware-Lösung(en): • automatische Scans durch, wenn die Medien eingelegt, verbunden oder logisch angebracht werden, **ODER** • eine kontinuierliche Verhaltensanalyse von Systemen oder Prozessen durch, wenn die Medien eingelegt, verbunden oder logisch angebracht werden. **Zielsetzung des kundenspezifischen Ansatzes** Malware kann nicht über externe entfernbare Medien in Systemkomponenten eingeführt werden. **Hinweise zur Anwendbarkeit** *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**Testprozeduren mit definiertem Ansatz** **5.3.3.a** Die Konfigurationen der Anti-Malware-Lösung untersuchen, um zu verifizieren, dass die Lösung für entfernbare elektronische Medien konfiguriert ist, um mindestens eines der in dieser Anforderung angegebenen Elemente durchzuführen. **5.3.3.b** Systemkomponenten mit angeschlossenen entfernbaren elektronischen Medien untersuchen, um zu verifizieren, dass die Lösung(en) gemäß mindestens einem der in dieser Anforderung angegebenen Elemente aktiviert ist. **5.3.3.c** Protokolle und Scanergebnisse untersuchen, um zu verifizieren, dass die Lösung(en) gemäß mindestens einem der in dieser Anforderung angegebenen Elemente aktiviert ist.	**Zweck** Tragbare Mediengeräte werden oft als Eintrittsmethode für Malware übersehen. Angreifer laden häufig Malware auf tragbare Geräte wie USB- und Flash-Laufwerke; das Anschließen eines infizierten Geräts an einen Computer löst dann die Malware aus und bringt neue Bedrohungen in die Umgebung ein.
Definierte Ansatzanforderungen **5.3.4** Audit-Protokolle für die Anti-Malware-Lösung(en) sind aktiviert und werden gemäß Anforderung 10.5.1 aufbewahrt. **Zielsetzung des kundenspezifischen Ansatzes** Historische Aufzeichnungen von Anti-Malware-Aktionen sind sofort verfügbar und werden mindestens 12 Monate aufbewahrt.	**Testprozeduren mit definiertem Ansatz** **5.3.4** Anti-Malware-Lösung(en) konfigurationen untersuchen, um zu verifizieren, dass Protokolle gemäß Anforderung 10.5.1 aktiviert und aufbewahrt werden.	**Zweck** Es ist wichtig, die Wirksamkeit der Anti-Malware-Mechanismen zu verfolgen, indem zum Beispiel bestätigt wird, dass Aktualisierungen und Scans wie erwartet durchgeführt werden und dass Malware identifiziert und adressiert wird. Audit-Protokolle gestatten einer Entität auch, festzustellen, wie Malware in die Umgebung eingedrungen ist, und ihre Aktivität innerhalb des Netzwerks der Entität zu verfolgen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wichtig ist, dass Abwehrmechanismen immer laufen, damit Malware in Echtzeit erkannt wird. Das Ad-hoc-Starten und -Stoppen von Anti-Malware-Lösungen könnte es Malware ermöglichen, sich ungeprüft und unentdeckt zu verbreiten. **Gute Praxis** Wenn eine berechtigte Notwendigkeit besteht, die Anti-Malware eines Systems vorübergehend zu deaktivieren - zum Beispiel um eine bestimmte Wartungsaktivität oder Untersuchung eines technischen Problems zu unterstützen - dann sollte der Grund für das Ergreifen solcher Maßnahmen von einem geeigneten Verwaltungsvertreter verstanden und genehmigt werden. Jede Deaktivierung oder Änderung von Anti-Malware-Mechanismen, auch auf den Geräten der Administratoren, wird von autorisiertem Personal durchgeführt. Es wird anerkannt, dass Administratoren über Berechtigungen verfügen, die es ihnen ermöglichen können, Anti-Malware auf ihren eigenen Computern zu deaktivieren, aber es sollten Warnmechanismen vorhanden sein, wenn eine solche Software deaktiviert wird, und dann werden Nachverfolgungsmaßnahmen durchgeführt, um sicherzustellen, dass richtige Prozesse befolgt wurden. **Beispiele** Zusätzliche Sicherheitsmaßnahmen, die möglicherweise für die Zeitdauer implementiert werden müssen, in dem der Anti-Malware-Schutz nicht aktiv ist, umfassen das Trennen des ungeschützten Systems vom Internet, während der Anti-Malware-Schutz deaktiviert ist, und das Ausführen eines vollständigen Scans, sobald er wieder aktiviert ist.
5.3.5 Anti-Malware-Mechanismen können von Benutzern nicht deaktiviert oder geändert werden, es sei denn, dies wird von der Geschäftsleitung im Einzelfall für eine begrenzten Zeitdauer ausdrücklich dokumentiert und genehmigt.	**5.3.5.a** Anti-Malware-Konfigurationen untersuchen, um zu verifizieren, dass die Anti-Malware-Mechanismen nicht von Benutzern deaktiviert oder geändert werden können.	
Zielsetzung des kundenspezifischen Ansatzes	**5.3.5.b** Verantwortliches Personal befragen und Prozesse beachten, um sicherzustellen, dass alle Anfragen zur Deaktivierung oder Änderung von Anti-Malware-Mechanismen von Fall zu Fall für eine begrenzte Zeitdauer von der Verwaltung speziell dokumentiert und genehmigt werden.	
Anti-Malware-Mechanismen können von nicht autorisiertem Personal nicht geändert werden.		
Hinweise zur Anwendbarkeit		
Anti-Malware-Lösungen dürfen nur dann vorübergehend deaktiviert werden, wenn ein berechtigter technischer Bedarf besteht, der von der Verwaltung im Einzelfall genehmigt wird. Wenn der Anti-Malware-Schutz für einen bestimmten Zweck deaktiviert werden muss, muss dieses formell autorisiert werden. Für die Zeitdauer, in dem der Anti-Malware-Schutz nicht aktiv ist, müssen möglicherweise zusätzliche Sicherheitsmaßnahmen implementiert werden.		

Anforderungen und Testprozeduren		Anleitungen
5.4 Anti-Phishing-Mechanismen schützen Benutzer vor Phishing-Angriffen.		
Definierte Ansatzanforderungen **5.4.1** Prozesse und automatisierte Mechanismen sind vorhanden, um Phishing-Angriffe zu erkennen und das Personal davor zu schützen. **Zielsetzung des kundenspezifischen Ansatzes** Mechanismen zum Schutz vor und zur Risikominderung durch Phishing-Angriffe sind vorhanden. **Hinweise zur Anwendbarkeit** Diese Anforderung gilt für den automatisierten Mechanismus. Es ist nicht beabsichtigt, dass die Systeme und Dienstleistungen, die solche automatisierten Mechanismen bereitstellen (wie E-Mail-Server), in den Geltungsbereich von PCI DSS gebracht werden. Der Schwerpunkt dieser Anforderung liegt auf dem Schutz des Personals mit Zugriff auf Systemkomponenten im Geltungsbereich von PCI DSS. Die Erfüllung dieser Anforderung an technische und automatisierte Kontrollen zur Erkennung und zum Schutz des Personals vor Phishing ist nicht dasselbe wie Anforderung 12.6.3.1 für Schulung zum Sicherheitsbewusstsein. Die Erfüllung dieser Anforderung erfüllt auch nicht die Anforderung, das Personal mit Sicherheitsbewusstsein zu schulen und umgekehrt. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**Testprozeduren mit definiertem Ansatz** **5.4.1** Implementierte Prozesse beobachten und Mechanismen untersuchen, um zu verifizieren, dass Kontrollen vorhanden sind, um Phishing-Angriffe zu erkennen und das Personal davor zu schützen.	**Zweck** Technische Kontrollen können die Anzahl der Gelegenheiten begrenzen, in denen das Personal den Wahrheitsgehalt einer Kommunikation überprüfen muss, und können auch die Auswirkungen individueller Reaktionen auf Phishing begrenzen. **Gute Praxis** Wenn Anti-Phishing-Kontrollen entwickelt werden, dann werden Entitäten ermutigt, eine Kombination von Ansätzen in Betracht zu ziehen. Zum Beispiel, die Verwendung von Anti-Spoofing-Kontrollen wie domänenbasierte Nachrichtenauthentifizierung, Berichterstattung und Konformität (DMARC), Absenderrichtlinien-Rahmenwerk (SPF) und mit Domänenschlüssel identifizierte Mail (DKIM) hilft Phishern, die Domäne des Unternehmens zu fälschen und sich als Personal auszugeben. Der Einsatz von Technologien zum Blockieren von Phishing-E-Mails und Malware, bevor sie das Personal erreichen, wie Link-Schrubber und serverseitige Anti-Malware, kann Vorfälle reduzieren und die Zeit verkürzen, die das Personal für die Überprüfung und Meldung von Phishing-Angriffen benötigt. Zusätzlich kann Schulung von Personal, um Phishing-E-Mails zu erkennen und zu melden, gestatten, dass ähnliche E-Mails identifiziert und vor dem Öffnen entfernt werden. Es wird empfohlen (ist aber nicht erforderlich), dass Anti-Phishing-Kontrollen in der gesamten Organisation einer Entität angewendet werden. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Definitionen Phishing ist eine Form von Social Engineering und beschreibt die verschiedenen Methoden, die von Angreifern verwendet werden, um Personal dazu zu bringen, sensible Informationen wie Kontonamen und Passwörter, und Kontodaten von Benutzern preiszugeben. Angreifer tarnen sich normalerweise und versuchen, als echte oder vertrauenswürdige Quelle aufzutreten, indem sie das Personal anweisen, eine E-Mail-Antwort zu senden, auf einen Weblink zu klicken oder Daten in eine kompromittierte Website einzugeben. In Anti-Malware-Lösungen sind häufig Mechanismen enthalten, die Phishing-Versuche erkennen und verhindern können. **Weitere Informationen** Weitere Informationen zum Phishing finden Sie im Folgenden: *National Cyber Security Centre - Phishing Attacks: Defending your Organization*. *US Cybersecurity & Infrastructure Security Agency - Report Phishing Sites.*

Anforderung 6: Entwicklung und Wartung Sicherer Systeme und Software

Abschnitte	
6.1	Prozesse und Mechanismen zur Entwicklung und Wartung von sicheren Systemen und Software werden definiert und verstanden.
6.2	Maßgeschneiderte und kundenspezifische Software werden sicher entwickelt.
6.3	Sicherheitsschwachstellen werden identifiziert und behoben.
6.4	Öffentlich zugängliche Webanwendungen sind gegen Angriffe geschützt.
6.5	Änderungen an allen Systemkomponenten werden sicher verwaltet.

Übersicht

Akteure mit bösen Absichten können Sicherheitsschwachstellen nutzen, um sich privilegierten Zugriff auf Systeme zu verschaffen. Viele dieser Schwachstellen werden durch vom Anbietern bereitgestellte Sicherheitspatches behoben, die von den Entitäten installiert werden müssen, die die Systeme verwalten. Alle Systemkomponenten müssen über alle geeigneten Software-Patches verfügen, um vor der Ausnutzung und Kompromittierung von Kontodaten durch böswillige Personen und böswillige Software zu schützen.

Geeignete Software Patches sind Patches, die ausreichend evaluiert und getestet wurden, um festzustellen, dass die Patches nicht mit bestehenden Sicherheitskonfigurationen in Konflikt stehen. Bei maßgeschneiderter und kundenspezifischer Software können zahlreiche Schwachstellen durch die Anwendung von Software-Lebenszyklus (SLC)-Prozessen und sicheren Codierungstechniken vermieden werden.

Code-Bestände, die Anwendungscode, Systemkonfigurationen oder andere Konfigurationsdaten speichern, die sich auf die Sicherheit von Kontodaten oder die CDE auswirken können, sind Gegenstand von PCI DSS-Beurteilungen.

Siehe Beziehung zwischen PCI DSS- und PCI SSC-Softwarestandards auf Seite 7 betreffs Informationen zur Verwendung von PCI SSC-validierter Software und Softwareanbietern und wie die Verwendung der Softwarestandards von PCI SSC bei der Erfüllung der Kontrollen in Anforderung 6 helfen kann.

Finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

Hinweis: *Anforderung 6 gilt für alle Systemkomponenten, mit Ausnahme von Abschnitt 6.2 zur sicheren Entwicklung von Software, der nur für maßgeschneiderte und kundenspezifische Software gilt, die auf einer Systemkomponente verwendet wird, die in der CDE enthalten oder mit ihr verbunden ist.*

Anforderungen und Testprozeduren		Anleitungen
6.1 Prozesse und Mechanismen zur Entwicklung und Wartung von sicheren Systemen und Software werden definiert und verstanden.		
Definierte Ansatzanforderungen **6.1.1** Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 6 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt. **Zielsetzung des kundenspezifischen Ansatzes** Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 6 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht der Verwaltung.	**Testprozeduren mit definiertem Ansatz** **6.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 6 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Bei Anforderung 6.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 6 angegeben sind. Während es wichtig ist, die in Anforderung 6 genannten spezifischen Richtlinien oder Verfahren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Prozeduren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Verfahren und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen.

<table>
<tr><th colspan="2">Anforderungen und Testprozeduren</th><th>Anleitungen</th></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="3">Zweck
Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen werden, werden Systeme nicht sicher gewartet und ihre Sicherheitsstufe wird reduziert.
Gute Praxis
Rollen und Verantwortlichkeiten können in Richtlinien und Verfahren dokumentiert oder in separaten Dokumenten gewartet werden.
Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen.
Beispiele
Ein Verfahren zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).</td></tr>
<tr><td>6.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 6 werden dokumentiert, zugewiesen und verstanden.</td><td>6.1.2.a Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 6 dokumentiert und zugewiesen sind.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 6 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.</td><td>6.1.2.b Personal, das für die Durchführung von Aktivitäten in Anforderung 6 verantwortlich sind, befragen um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.</td></tr>
</table>

Anforderungen und Testprozeduren		Anleitungen
6.2 Maßgeschneiderte und kundenspezifische Software werden sicher entwickelt.		
Definierte Ansatzanforderungen **6.2.1** Maßgeschneiderte und kundenspezifische Software werden sicher wie folgt entwickelt: • Basierend auf Industriestandards und/oder bewährten Praktiken für eine sichere Entwicklung. • Gemäß PCI DSS (zum Beispiel sichere Authentifizierung und Protokollierung). • Einbeziehung von Berücksichtigung von Fragen der Informationssicherheit in jeder Phase des Softwareentwicklungs-Lebenszyklus. **Zielsetzung des kundenspezifischen Ansatzes** Maßgeschneiderte und kundenspezifische Software wird gemäß PCI DSS und sicheren Entwicklungsprozessen während des gesamten Software-Lebenszyklus entwickelt. **Hinweise zur Anwendbarkeit** Dies gilt für alle Software, die für oder von der Entität für den eigenen Gebrauch entwickelt wurde. Dies beinhaltet sowohl maßgeschneiderte als auch kundenspezifische Software. Dies gilt nicht für Software von Drittanbietern.	**Testprozeduren mit definiertem Ansatz** **6.2.1** Dokumentierte Softwareentwicklungsprozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, die alle in dieser Anforderung angegebenen Elemente enthalten.	**Zweck** Ohne die Einbeziehung von Sicherheit während der Anforderungsdefinitions-, Design-, Analyse- und Testphasen der Softwareentwicklung können Sicherheitsschwachstellen versehentlich oder böswillig in die Produktionsumgebung eingeführt werden. **Gute Praxis** Das Verständnis, wie sensible Daten von der Anwendung gehandhabt werden – einschließlich beim Speichern, Übertragen und im Speicher – kann dabei helfen, zu identifizieren, wo Daten geschützt werden müssen. PCI DSS-Anforderungen müssen bei der Entwicklung von Software berücksichtigt werden, um diese Anforderungen absichtlich zu erfüllen, anstatt zu versuchen, die Software später nachzurüsten. **Beispiele** Sichere Software-Lebenszyklus-Verwaltungs-Methoden und -Rahmenwerke beinhalten PCI Sicheres Software-Rahmenwerk, BSIMM, OPENSAMM und Werke von NIST, ISO und SAFECode.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Mitarbeiter mit sicheren Codierungsmethoden, einschließlich der in Anforderung 6.2.4 definierten Techniken, vertraut sind, kann die Anzahl der Sicherheitsschwachstellen minimieren, die durch schlechte Codierungspraktiken eingeführt werden. **Gute Praxis** Schulung für Entwickler kann intern oder von Dritten bereitgestellt werden. Die Schulung sollte beinhalten, ist aber nicht beschränkt auf, verwendete Entwicklungssprachen, sicheres Softwaredesign, sichere Codierungstechniken, Verwendung von Techniken/Methoden zum Auffinden von Schwachstellen im Code, Verfahren zur Verhinderung der Wiedereinführung bereits behobener Schwachstellen und Verwendung automatischer Sicherheitstesttools zum Erkennen von Schwachstellen in Software. Da sich branchenübliche sichere Codierungspraktiken ändern, müssen möglicherweise die Codierungspraktiken der Organisation und die Entwicklerschulung aktualisiert werden, um neue Bedrohungen zu adressieren.
6.2.2 Softwareentwicklungspersonal, das an maßgeschneiderter und kundenspezifischer Software arbeitet, wird mindestens einmal alle 12 Monate wie folgt geschult: • über Softwaresicherheit, die für ihre Tätigkeitsfunktion und Entwicklungssprachen relevant ist. • Einschließlich sicheres Softwaredesign und sichere Codierungstechniken. • Einschließlich, wenn Sicherheitstesttools verwendet werden, wie die Tools zum Erkennen von Schwachstellen in Software verwendet werden.	**6.2.2.a** Softwareentwicklungsverfahren untersuchen, um zu verifizieren, dass Prozesse für die Schulung von Softwareentwicklungspersonal definiert sind, das maßgeschneiderte und kundenspezifische Software entwickelt, die alle in dieser Anforderung angegebenen Elemente beinhaltet.	
Zielsetzung des kundenspezifischen Ansatzes	**6.2.2.b** Schulungsunterlagen untersuchen und das Personal befragen, um zu verifizieren, dass das Softwareentwicklungspersonal, das an maßgeschneiderter und kundenspezifischer Software arbeitet, eine Softwaresicherheitsschulung erhalten hat, die für ihre berufliche Funktion und ihre Entwicklungssprachen gemäß allen in dieser Anforderung angegebenen Elementen relevant ist.	
Das Softwareentwicklungspersonal bleibt über sichere Entwicklungspraktiken informiert; Softwaresicherheit; und Angriffe gegen die Sprachen, Rahmenwerke oder Anwendungen, die sie entwickeln. Das Personal kann bei Bedarf auf Hilfe und Anleitungen zugreifen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Sicherheitslücken in maßgeschneiderter und benutzerdefinierter Software werden häufig von böswilligen Personen ausgenutzt, um sich Zugang zu einem Netzwerk zu verschaffen und Kontodaten zu kompromittieren. Anfälliger Code ist weitaus schwieriger und teurer zu adressieren, nachdem er bereitgestellt oder in Produktionsumgebungen freigegeben wurde. Das Erfordern einer formellen Überprüfung und Freigabe durch die Verwaltung vor der Freigabe hilft dabei, sicherzustellen, dass der Code genehmigt und gemäß Richtlinien und Prozeduren entwickelt wurde. **Gute Praxis** Die folgenden Punkte sollten für die Aufnahme in Code-Reviews berücksichtigt werden: • Suche nach undokumentierten Merkmalen (Implantationstools, Hintertüren). • Bestätigung, dass die Software die Funktionen externer Komponenten (Bibliotheken, Rahmenwerke, APIs usw.) sicher verwendet. Zum Beispiel, wenn eine Drittanbieterbibliothek verwendet wird, die kryptografische Funktionen bereitstellt, verifizieren, ob diese sicher integriert wurde. • Überprüfung der korrekten Verwendung der Protokollierung, um zu verhindern, dass sensible Daten in Protokolle gelangen. • Analyse unsicherer Codestrukturen, die potenzielle Schwachstellen im Zusammenhang mit gängigen Softwareangriffen enthalten können, die in Anforderungen 6.2.5 identifiziert wurden. • Überprüfung des Verhaltens der Anwendung, um logische Schwachstellen zu erkennen.
6.2.3 Maßgeschneiderte und kundenspezifische Software wird vor der Freigabe für die Produktion oder für Kunden überprüft, um potenzielle Codierungsschwachstellen wie folgt zu identifizieren und zu korrigieren: • Code-Überprüfungen stellen sicher, dass Code gemäß den Richtlinien für sichere Codierung entwickelt wird. • Code-Überprüfungen suchen sowohl nach bestehenden als auch nach neuen Software-Schwachstellen. • Entsprechende Korrekturen werden vor der Freigabe implementiert.	**6.2.3.a** Dokumentierte Softwareentwicklungsverfahren untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass Prozesse definiert sind, die eine Überprüfung der gesamten maßgeschneiderten und kundenspezifischen Software auf allen in dieser Anforderung angegebenen Elemente erfordern.	
	6.2.3.b Nachweis von Änderungen an maßgeschneiderter und kundenspezifischer Software untersuchen, um zu verifizieren, dass die Codeänderungen gemäß allen in dieser Anforderung angegebenen Elementen überprüft wurden.	
Zielsetzung des kundenspezifischen Ansatzes Maßgeschneiderte und kundenspezifische Software kann nicht durch Codierungs-Schwachstellen ausgenutzt werden.		
Hinweise zur Anwendbarkeit Diese Anforderung für Code-Überprüfungen gilt für alle maßgeschneiderte und kundenspezifische Software (sowohl intern als auch öffentlich zugänglich) als Teil des Systementwicklungslebenszyklus. Öffentlich zugängliche Webanwendungen unterliegen ebenfalls zusätzlichen Kontrollen, um laufende Bedrohungen und Schwachstellen nach der Implementierung zu adressieren, wie in der PCI-DSS-Anforderung 6.4 definiert. Code-Überprüfungen entweder mit manuellen oder automatisierten Prozessen oder einer Kombination aus beiden durchgeführt werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
6.2.3.1 Wenn für maßgeschneiderte und benutzerdefinierte Software vor der Freigabe für die Produktion manuelle Code-Überprüfungen durchgeführt werden, dann werden Codeänderungen: • Von anderen Personen als dem ursprünglichen Code-Autor überprüft, und die sich mit Code-Überprüfungs-Techniken und sicheren Codierungspraktiken auskennen. • Vor der Freigabe von der Geschäftsleitung geprüft und genehmigt.	**6.2.3.1.a** Wenn für maßgeschneiderte und kundenspezifische Software vor der Freigabe für die Produktion manuelle Code-Überprüfungen durchgeführt werden, dokumentierte Softwareentwicklungsprozeduren untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass Prozesse für manuelle Code-Überprüfungen definiert sind, die gemäß allen in dieser Anforderung angegebenen Elementen durchgeführt werden sollen. **6.2.3.1.b** Nachweis von Änderungen an maßgeschneiderter und kundenspezifischer Software untersuchen, und Personal befragen, um zu verifizieren, dass manuelle Code-Überprüfungen gemäß allen in dieser Anforderung angegebenen Elementen durchgeführt wurden.	Die Überprüfung des Codes durch eine andere Person als den ursprünglichen Autor, die sowohl Erfahrung mit Code-Überprüfungen als auch mit sicheren Codierungspraktiken vertraut ist, minimiert die Möglichkeit, dass Code mit Sicherheits- oder Logikfehlern, die die Sicherheit der Karteninhaberdaten beeinträchtigen könnten, in eine Produktionsumgebung freigegeben wird. Das Erfordernis der Genehmigung durch die Verwaltung, dass der Code überprüft wurde, schränkt die Möglichkeit ein, den Prozess zu umgehen. **Gute Praxis** Es hat sich gezeigt, dass eine formale Überprüfungs-Methodik und Überprüfungs-Checklisten die Qualität des Code-Überprüfungs-Prozesses verbessern. Code-Überprüfung ist ein ermüdender Prozess, und aus diesem Grund ist sie am effektivsten, wenn Prüfer jeweils nur kleine Codemengen überprüfen. Um die Effektivität der Code-Überprüfung aufrechtzuerhalten, ist es von Vorteil, die allgemeine Arbeitsbelastung der Prüfer zu überwachen und sie die Anwendungen überprüfen zu lassen, mit denen sie vertraut sind. Code-Überprüfungen können entweder mit manuellen oder automatisierten Prozessen oder einer Kombination aus beiden durchgeführt werden. Entitäten, die ausschließlich auf manueller Codeüberprüfung beruhen, sollten sicherstellen, dass die Überprüfer ihre Fähigkeiten durch regelmäßige Schulungen aufrechterhalten, wenn neue Schwachstellen gefunden werden, und neue sichere Codierungsmethoden werden empfohlen. **Weitere Informationen** Siehe den *OWASP Code Review Guide*.
Zielsetzung des kundenspezifischen Ansatzes		
Der manuelle Code-Überprüfungsprozess kann nicht umgangen werden und ist beim Aufdecken von Sicherheitsschwachstellen effektiv.		
Hinweise zur Anwendbarkeit		
Manuelle Code-Überprüfungen können durch sachkundiges internes Personal oder sachkundiges Personal Dritter durchgeführt werden. Eine Person, der formell die Verantwortung für die Freigabekontrolle übertragen wurde und die weder der ursprüngliche Code-Autor noch der Code-Überprüfer ist, erfüllt die Kriterien der Verwaltung.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	
6.2.4 Softwareentwicklungstechniken oder andere Methoden werden von Softwareentwicklungspersonal für maßgeschneiderte und kundenspezifische Software definiert und verwendet, um übliche Softwareangriffe und damit verbundene Schwachstellen in maßgeschneiderter und kundenspezifischer Software zu verhindern oder abzuschwächen, einschließlich, aber nicht beschränkt auf Folgendes: • Injektionsangriffe, einschließlich SQL-, LDAP-, XPath- oder andere Befehls-, Parameter-, Objekt-, Fehler- oder injektionsartige Mängel. • Angriffe auf Daten und Datenstrukturen, einschließlich Versuche, Puffer, Zeiger, Eingabedaten oder gemeinsam genutzte Daten zu manipulieren. • Angriffe auf die Kryptografienutzung, einschließlich Versuche, schwache, unsichere oder unangemessene kryptografische Implementierungen, Algorithmen, Verschlüsselungssammlungen oder Betriebsmodi auszunutzen. • Angriffe auf die Geschäftslogik, einschließlich Versuche, Anwendungsmerkmale und -funktionen durch die Manipulation von APIs, Kommunikationsprotokollen und -kanälen, kundenseitigen Funktionen oder anderen System-/Anwendungsfunktionen und -ressourcen zu missbrauchen oder zu umgehen. Dazu gehören Cross-Site-Scripting (XSS) und Cross-Site-Request-Forgery (CSRF). *(Fortsetzung auf der nächsten Seite)*	**6.2.4** Dokumentierte Prozeduren untersuchen und verantwortliches Softwareentwicklungspersonal befragen, um zu verifizieren, dass Software-Engineering-Techniken oder andere Methoden definiert sind und von Entwicklern von maßgeschneiderter und benutzerdefinierter Software verwendet werden, um alle in dieser Anforderung angegebenen gängigen Softwareangriffe zu verhindern oder abzuschwächen.	**Zweck** Häufige Fehler, die zu anfälligem Code führen, so früh wie möglich im Softwareentwicklungsprozess zu erkennen oder zu verhindern, verringert die Wahrscheinlichkeit, dass solche Fehler in die Produktion gelangen und zu einer Kompromittierung führen. Durch die Einbettung formaler Engineering-Techniken und -Tools in den Entwicklungsprozess werden diese Fehler frühzeitig erkannt. Diese Philosophie wird manchmal als „Sicherheitsverlagerung nach links“ bezeichnet. **Gute Praxis** Sowohl für maßgeschneiderte als auch für kundenspezifische Software muss die Entität sicherstellen, dass ein Code entwickelt wird, der sich auf die Verhinderung oder Abwehr gängiger Softwareangriffe konzentriert, einschließlich: • Versuche, gängige Codierungsschwachstellen (Bugs) auszunutzen. • Versuche, Software-Designfehler auszunutzen. • Versuche, Implementierungs-/Konfigurationsfehler auszunutzen. • Aufzählungsangriffe – automatisierte Angriffe, die aktiv im Zahlungsverkehr ausgenutzt werden und Identifizierungs-, Authentifizierungs- oder Autorisierungsmechanismen missbrauchen. Siehe den *PCI Perspectives-Blog-Artikel „Hüten Sie sich vor Kontotest-Angriffen“*.” *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
• Angriffe auf Zugangskontrollmechanismen, einschließlich Versuche, Identifizierungs-, Authentifizierungs-, oder Autorisierungsmechanismen zu umgehen oder zu missbrauchen, oder Versuche, Schwachstellen bei der Implementierung solcher Mechanismen auszunutzen. • Angriffe über alle „Hochrisiko“-Schwachstellen, die im Schwachstellenidentifizierungsprozess identifiziert wurden, wie in Anforderung 6.3.1 definiert.		Die Recherche und Dokumentation von Software-Engineering-Techniken oder anderen Methoden hilft dabei, zu definieren, wie Softwareentwickler verschiedene Softwareangriffe durch Funktionen oder Gegenmaßnahmen, die sie in die Software integrieren, verhindern oder abschwächen. Dies kann Identifizierungs-/Authentifizierungsmechanismen, Zugriffskontrolle, Eingabevalidierungsroutinen usw. beinhalten. Entwickler sollten mit verschiedenen Arten von Schwachstellen und möglichen Angriffen vertraut sein und Maßnahmen verwenden, um potenzielle Angriffsvektoren bei der Entwicklung von Code zu vermeiden.
Zielsetzung des kundenspezifischen Ansatzes Maßgeschneiderte und kundenspezifische Software kann nicht durch übliche Angriffe und damit verbundene Schwachstellen ausgenutzt werden.		**Beispiele** Die Techniken beinhalten automatisierte Prozesse und Praktiken, die Code früh im Entwicklungszyklus scannen, wenn Code eingecheckt wird, um zu bestätigen, dass keine Schwachstellen vorhanden sind.
Hinweise zur Anwendbarkeit Dies gilt für alle Software, die für oder von der Entität für den eigenen Gebrauch entwickelt wurde. Dies beinhaltet sowohl maßgeschneiderte als auch kundenspezifische Software. Dies gilt nicht für Software von Drittanbietern.		

Anforderungen und Testprozeduren		Anleitungen
6.3 Sicherheitsschwachstellen werden identifiziert und behoben.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Klassifizierung der Risiken (zum Beispiel als kritisch, hoch, mittel oder gering) gestattet Organisationen, die Elemente mit dem höchsten Risiko schneller zu identifizieren, zu priorisieren und zu adressieren und die Wahrscheinlichkeit zu verringern, dass Schwachstellen mit dem größten Risiko ausgenutzt werden. **Gute Praxis** Die Methoden zur Bewertung von Schwachstellen und zur Zuweisung von Risikoeinstufungen variieren je nach Umgebung und Risikobewertungsstrategie einer Organisation. Wenn eine Entität ihre Risikoeinstufungen zuweist, sollte sie in Erwägung ziehen, eine formale, objektive und vertretbare Methodik zu verwenden, die die Risiken der für die Organisation relevanten Schwachstellen genau abbildet und in eine angemessene, der Entität zugewiesene Priorität für die Behebung umsetzt. Die Prozesse einer Organisation zur Verwaltung von Schwachstellen sollten in andere Verwaltungsprozesse integriert werden – zu Beispiel Risikoverwaltung, Änderungsverwaltung, Patch-Verwaltung, Reaktion auf Vorfälle, Anwendungssicherheit sowie die ordnungsgemäßez Überwachung und Protokollierung dieser Prozesse. Dadurch wird sichergestellt, dass alle Schwachstellen ordnungsgemäß identifiziert und adressiert werden. Prozesse sollten die laufende Bewertung von Schwachstellen unterstützen. Zum Beispiel kann aus einer anfänglich als risikoarm identifizierten Schwachstelle später ein höheres Risiko werden. *(Fortsetzung auf der nächsten Seite)*
6.3.1 Sicherheitsschwachstellen werden identifiziert und wie folgt verwaltet: • Neue Sicherheitsschwachstellen werden mithilfe von branchenweit anerkannten Quellen für Sicherheitsschwachstelleninformationen identifiziert, einschließlich Warnungen von internationalen und nationalen Computer-Notfallteams (CERTs). • Schwachstellen werden basierend auf den bewährten Praktiken der Branche und der Berücksichtigung potenzieller Auswirkungen einer Risikoeinstufung zugewiesen. • Risikoeinstufungen identifizieren mindestens alle Schwachstellen, die als hochriskant oder kritisch für die Umgebung angesehen werden. • Schwachstellen für maßgeschneiderte und kundenspezifische Software von Drittanbietern (zum Beispiel Betriebssysteme und Datenbanken) werden abgedeckt.	**6.3.1.a** Richtlinien und Prozeduren untersuchen, um Sicherheitsschwachstellen zu identifizieren und verwalten, um zu verifizieren, dass Prozesse gemäß allen in dieser Anforderung angegebenen Elementen definiert sind. **6.3.1.b** Verantwortliches Personal befragen, die Dokumentation untersuchen und Prozesse beobachten, um zu verifizieren, dass identifizierte Sicherheitsschwachstellen gemäß allen in dieser Anforderung angegebenen Elementen identifiziert und verwaltet werden.	
Zielsetzung des kundenspezifischen Ansatzes		
Neue System- und Softwareschwachstellen, die sich auf die Sicherheit von Kontodaten oder der CDE auswirken können, werden überwacht, katalogisiert und auf Risiken geprüft.		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Diese Anforderung wird weder durch die für die Anforderungen 11.3.1 und 11.3.2 durchgeführten Schwachstellen-Scans erfüllt, noch ist sie mit diesen identisch. Diese Anforderung gilt für einen Prozess zur aktiven Überwachung von Branchenquellen auf Schwachstelleninformationen und für die Entität, um die mit jeder Schwachstelle verbundene Risikoeinstufung zu bestimmen.		Zusätzlich, können Schwachstellen, die einzeln als niedriges oder mittleres Risiko eingestuft werden, zusammen ein hohes oder kritisches Risiko darstellen, wenn sie auf demselben System vorhanden sind oder wenn sie auf einem System mit geringem Risiko ausgenutzt werden, was zum Zugriff auf die CDE führen könnte. **Beispiele** Einige Organisationen, die Warnungen ausgeben, um Entitäten über dringende Schwachstellen zu informieren, die sofortige Patches/Aktualisierungen erfordern, sind nationale Computer Emergency Readiness/Response Teams (CERTs) und Anbieter. Kriterien für die Einstufung von Schwachstellen können die Kritikalität einer Schwachstelle sein, die in einer Warnung des Forums der Vorfallsreaktions- und Sicherheitsteams (FIRST) oder eines CERT identifiziert wurde, die Berücksichtigung der CVSS-Wertung, die Klassifizierung durch den Anbieter und/oder die Art der betroffenen Systeme. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Weitere Informationen Vertrauenswürdige Quellen für Informationen zu Schwachstellen sind Anbieter-Websites, Branchen-News-Gruppen, Mailinglisten usw. Wenn Software intern entwickelt wird, sollte das interne Entwicklungsteam auch Informationsquellen zu neuen Schwachstellen in Betracht ziehen, die sich auf intern entwickelte Anwendungen auswirken können. Andere Methoden, um sicherzustellen, dass neue Schwachstellen identifiziert werden, umfassen Lösungen, die automatisch ungewöhnliches Verhalten erkennen und alarmieren. Prozesse sollten sowohl weit verbreitete Ausnutzungen als auch „Zero-Day"-Angriffe erfassen, die auf bisher unbekannte Schwachstellen abzielen. Für maßgeschneiderte und kundenspezifische Software kann die Organisation Informationen über Bibliotheken, Rahmenwerken, Compiler, Programmiersprachen usw. von öffentlichen vertrauenswürdigen Quellen erhalten (zum Beispiel spezielle Ressourcen und Ressourcen von Komponentenentwicklern). Die Organisation kann auch unabhängig Komponenten von Dritten analysieren und Schwachstellen identifizieren. Zur Kontrolle der intern entwickelten Software kann die Organisation solche Informationen von externen Quellen erhalten. Die Organisation kann erwägen, ein „Bug-Bounty"-Programm zu verwenden, bei dem sie Informationen veröffentlicht (um Beispiel auf ihrer Website), damit Dritte die Organisation mit Informationen zu Schwachstellen kontaktieren können. Externe Quellen können unabhängige Ermittler oder Unternehmen sein, die der Organisation über identifizierte Schwachstellen berichten, und können Quellen wie das Gemeinsame System zur Bewertung von Schwachstellen (CVSS) oder die OWASP Methodik der Risikoeinstufung umfassen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Identifizieren und Auflisten der gesamten maßgeschneiderten und benutzerdefinierten Software der Entität sowie jeglicher Software von Dritten, die in die maßgeschneiderte und benutzerdefinierte Software der Entität integriert ist, ermöglicht der Entität, Schwachstellen und Patches zu verwalten. Schwachstellen in Drittanbieterkomponenten (einschließlich Bibliotheken, APIs usw.), die in die Software einer Entität eingebettet sind, machen solche Anwendungen ebenfalls anfällig für Angriffe. Das Wissen, welche Komponenten von Drittanbietern in der Software der Entität verwendet werden, und die Überwachung der Verfügbarkeit von Sicherheitspatches, um bekannte Schwachstellen zu adressieren, ist entscheidend für die Sicherstellung der Sicherheit der Software. **Gute Praxis** Das Inventar einer Entität sollte alle Komponenten und Abhängigkeiten der Zahlungssoftware, einschließlich unterstützte Ausführungsplattformen oder -umgebungen, Dritt- und Open-Source-Bibliotheken, Dienstleistungen und andere erforderliche Funktionalitäten erfassen. Es gibt viele verschiedene Arten von Lösungen, die bei der Verwaltung von Softwareinventaren helfen können, wie Tools zur Analyse der Softwarezusammensetzung, Tools zur Anwendungserkennung und Verwaltung mobiler Geräte.
6.3.2 Ein Inventar von maßgeschneiderter und kundenspezifischer Software und Softwarekomponenten von Dritten, die in maßgeschneiderte und kundenspezifische Software integriert sind, wird gepflegt, um das Schwachstellen- und die Patch-Verwaltung zu erleichtern.	**6.3.2.a** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass ein Inventar von maßgeschneiderter und kundenspezifischer Software und Softwarekomponenten von Dritten, die in maßgeschneiderte und kundenspezifische Software integriert sind, gepflegt wird und dass das Inventar verwendet wird, um Schwachstellen zu identifizieren und zu adressieren.	
Zielsetzung des kundenspezifischen Ansatzes Bekannte Schwachstellen in Softwarekomponenten von Dritten können in maßgeschneiderter und kundenspezifischer Software nicht ausgenutzt werden.	**6.3.2.b** Softwaredokumentation, einschließlich für maßgeschneiderte und kundenspezifische Software, die Softwarekomponenten von Dritten integriert, untersuchen, und sie mit dem Inventar vergleichen, um zu verifizieren, dass das Inventar die maßgeschneiderte und kundenspezifische Software und Softwarekomponenten von Dritten enthält.	
Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ständig werden neue Ausnutzungen entdeckt, die Angriffe auf bisher als sicher geltende Systeme erlauben können. Wenn die neuesten Sicherheitspatches/Aktualisierungen nicht so schnell wie möglich auf kritischen Systemen implementiert werden, kann ein böswilliger Akteur diese Ausnutzungen verwenden, um ein System anzugreifen oder zu deaktivieren oder sich Zugriff auf sensible Daten zu verschaffen. **Gute Praxis** Durch die Priorisierung von Sicherheitspatches/Aktualisierungen für kritische Infrastrukturen wird sichergestellt, dass Systeme und Geräte mit hoher Priorität so schnell wie möglich nach der Veröffentlichung eines Patches vor Schwachstellen geschützt sind. Der Patch-Rhythmus einer Entität sollte jede Neubewertung von Schwachstellen und nachfolgende Änderungen der Kritikalität einer Schwachstelle gemäß Anforderung 6.3.1 berücksichtigen. Zum Beispiel kann aus einer anfänglich als risikoarm identifizierten Schwachstelle später ein höheres Risiko werden. Zusätzlich können Schwachstellen, die einzeln als niedriges oder mittleres Risiko eingestuft werden, zusammen ein hohes oder kritisches Risiko darstellen, wenn sie auf demselben System vorhanden sind oder wenn sie auf einem System mit geringem Risiko ausgenutzt werden, was zum Zugriff auf die CDE führen könnte.
6.3.3 Alle Systemkomponenten werden vor bekannten Schwachstellen geschützt, indem anwendbare Sicherheitspatches/Aktualisierungen wie folgt installiert werden: • Kritische oder hochsichere Patches/Aktualisierungen werden gemäß dem Risikoeinstufungsprozess in Anforderung 6.3.1 identifiziert, werden innerhalb eines Monats der Veröffentlichung installiert. • Alle anderen anwendbaren Sicherheitspatches/Aktualisierungen werden innerhalb eines angemessenen Zeitrahmens installiert, der von der Entität bestimmt wird (zum Beispiel innerhalb von drei Monaten nach Freigabe).	**6.3.3.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse zum Adressieren von Schwachstellen durch Installieren von anwendbaren Sicherheitspatches-/Aktualisierungen gemäß allen in dieser Anforderung angegebenen Elementen definiert sind.	
	6.3.3.b Systemkomponenten und verwandte Software untersuchen und die Liste der installierten Sicherheitspatches/Aktualisierungen mit den neuesten Sicherheitspatch-/Aktualisierungsinformationen vergleichen, um zu verifizieren, dass Schwachstellen gemäß allen in dieser Anforderung angegebenen Elementen adressiert werden.	
Zielsetzung des kundenspezifischen Ansatzes		
Systemkomponenten können nicht durch die Ausnutzung einer bekannten Schwachstelle kompromittiert werden.		

Anforderungen und Testprozeduren		Anleitungen
6.4 Öffentlich zugängliche Webanwendungen sind gegen Angriffe geschützt.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Öffentlich zugängliche Webanwendungen sind solche, die der Öffentlichkeit zugänglich sind (nicht nur für den internen Gebrauch). Diese Anwendungen sind primäre Ziele für Angreifer, und schlecht codierte Webanwendungen bieten Angreifern einen einfachen Weg, um auf sensible Daten und Systeme zuzugreifen. **Gute Praxis** Manuelle oder automatisierte Tools oder Methoden zur Sicherheitsbewertung von Schwachstellen überprüfen und/oder testen die Anwendung auf Schwachstellen. Zu den gängigen Bewertungstools gehören spezialisierte Webscanner, die eine automatische Analyse des Schutzes von Webanwendungen durchführen. Wenn automatisierte technische Lösungen verwendet werden, ist es wichtig, Prozesse einzubeziehen, die eine rechtzeitige Reaktion auf von den Lösungen generierte Warnungen erleichtern, damit erkannte Angriffe abgewehrt werden können. **Beispiele** Eine Webanwendungs-Firewall (WAF), die vor öffentlich zugänglichen Webanwendungen installiert wird, um den gesamten Verkehr zu überprüfen, ist ein Beispiel für eine automatisierte technische Lösung, die webbasierte Angriffe erkennt und verhindert (zum Beispiel die in Anforderung 6.2.4 enthaltenen Angriffe). WAFs filtern und blockieren unwesentlichen Datenverkehr auf der Anwendungsebene. Eine ordnungsgemäß konfigurierte WAF hilft, *(Fortsetzung auf der nächsten Seite)*
6.4.1 Für öffentlich zugängliche Webanwendungen werden laufend neue Bedrohungen und Schwachstellen adressiert und diese Anwendungen werden wie folgt vor bekannten Angriffen geschützt: • Überprüfung öffentlich zugänglicher Webanwendungen mit manuellen oder automatisierten Tools oder Methoden zur Sicherheitsbeurteilung von Anwendungsschwachstellen wie folgt: – Mindestens einmal alle 12 Monate und nach bedeutenden Änderungen. – Von einer Entität, die auf Anwendungssicherheit spezialisiert ist. – Einschließlich mindestens aller gängigen Softwareangriffe in Anforderung 6.2.4. – Alle Schwachstellen werden gemäß Anforderung 6.3.1 eingestuft. – Alle Schwachstellen werden korrigiert. – Die Anwendung wird nach den Korrekturen erneut evaluiert **ODER** • Eine automatisierte technische Lösung(en) wird installiert, die webbasierte Angriffe wie folgt kontinuierlich erkennt und verhindert: – Wird vor öffentlich zugänglichen Webanwendungen installiert, um webbasierte Angriffe zu erkennen und zu verhindern. – Aktiv laufend und gegebenenfalls auf dem neuesten Stand. – Generieren von Audit-Protokollen. – Konfiguriert, um entweder webbasierte Angriffe zu blockieren oder eine Warnung zu generieren, die sofort untersucht wird.	**6.4.1** Stellen Sie für öffentlich zugängliche Webanwendungen sicher, dass eine der folgenden erforderlichen Methoden vorhanden ist: • Wenn manuelle oder automatisierte Schwachstellen-Sicherheitsbewertungstools oder -methoden verwendet werden, dokumentierte Prozesse untersuchen, das Personal befragen, und Aufzeichnungen von Anwendungssicherheitsbewertungen untersuchen, um zu verifizieren, dass öffentlich zugängliche Webanwendungen gemäß allen Elementen dieser Anforderung, die für das Tool/die Methode spezifisch sind, überprüft werden. **ODER** Wenn eine automatisierte technische Lösung(en) installiert ist/sind, die webbasierte Angriffe kontinuierlich erkennt und verhindert, die Systemkonfigurationseinstellungen und Audit-Protokolle untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass die automatisierte(n) technische(n) Lösung(en) gemäß allen Elementen dieser für die Lösung(en) angegebenen Anforderung installiert ist/sind.	

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Öffentlich zugängliche Webanwendungen sind gegen böswillige Angriffe geschützt. **Hinweise zur Anwendbarkeit** Diese Beurteilung ist nicht dasselbe wie die für Anforderung 11.3.1 und 11.3.2 durchgeführten Schwachstellen-Scans. Diese Anforderung wird durch Anforderung 6.4.2 nach dem 31. März 2025 ersetzt, wenn Anforderung 6.4.2 in Kraft tritt.		Angriffe auf Anwendungsebene auf Anwendungen zu verhindern, die nicht ordnungsgemäß codiert oder konfiguriert sind. Ein weiteres Beispiel für eine automatisierte technische Lösung sind Laufzeitanwendungs-Selbstschutz (RASP)-Technologien. Bei korrekter Implementierung können RASP-Lösungen anomales Verhalten der Software während der Ausführung erkennen und blockieren. Während WAFs normalerweise den Anwendungsumkreis überwachen, überwachen und blockieren RASP-Lösungen das Verhalten innerhalb der Anwendung.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Öffentlich zugängliche Webanwendungen sind primäre Ziele für Angreifer, und schlecht codierte Webanwendungen bieten Angreifern einen einfachen Weg, um auf sensible Daten und Systeme zuzugreifen. **Gute Praxis** Wenn automatisierte technische Lösungen verwendet werden, ist es wichtig, Prozesse einzubeziehen, die eine rechtzeitige Reaktion auf von den Lösungen generierte Warnungen erleichtern, damit erkannte Angriffe abgewehrt werden können. Solche Lösungen können auch verwendet werden, um eine Abschwächung zu automatisieren, zum Beispiel Ratenbegrenzungskontrollen, die implementiert werden können, um brutale Gewalt-Angriffe und Aufzählungsangriffe abzuschwächen. **Beispiele** Eine Webanwendungs-Firewall (WAF), die entweder lokal oder cloudbasiert sein kann, die vor öffentlich zugänglichen Webanwendungen installiert wird, um den gesamten Verkehr zu überprüfen, ist ein Beispiel für eine automatisierte technische Lösung, die webbasierte Angriffe erkennt und verhindert (zum Beispiel die in Anforderung 6.2.4 enthaltenen Angriffe). WAFs filtern und blockieren unwesentlichen Datenverkehr auf der Anwendungsebene. Eine ordnungsgemäß konfigurierte WAF hilft, Angriffe auf Anwendungsebene auf Anwendungen zu verhindern, die nicht ordnungsgemäß codiert oder konfiguriert sind.
6.4.2 Für öffentlich zugängliche Webanwendungen wird eine automatisierte technische Lösung eingesetzt, die webbasierte Angriffe kontinuierlich erkennt und verhindert, mit mindestens den folgenden: • Wird vor öffentlich zugänglichen Webanwendungen installiert, und ist konfiguriert, um webbasierte Angriffe zu erkennen und zu verhindern. • Aktiv laufend und gegebenenfalls auf dem neuesten Stand. • Generieren von Audit-Protokollen. • Konfiguriert, um entweder webbasierte Angriffe zu blockieren oder eine Warnung zu generieren, die sofort untersucht wird.	**6.4.2** Für öffentlich zugängliche Webanwendungen die Systemkonfigurationseinstellungen und Audit-Protokolle untersuchen, und verantwortliches Personal befragen, um zu verifizieren, dass eine automatisierte technische Lösung, die webbasierte Angriffe entdeckt und verhindert, gemäß allen Elementen dieser für die Lösung(en) angegebenen Anforderung installiert ist/sind	
Zielsetzung des kundenspezifischen Ansatzes Öffentlich zugängliche Webanwendungen sind in Echtzeit gegen böswillige Angriffe geschützt.		
Hinweise zur Anwendbarkeit Diese neue Anforderung wird Anforderung 6.4.1 ersetzen, sobald ihr effektives Datum erreicht ist. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
6.4.3 Alle Zahlungsseitenskripte, die im Browser des Verbrauchers geladen und ausgeführt werden, werden wie folgt verwaltet: • Es wird eine Methode implementiert, um zu bestätigen, dass jedes Skript autorisiert ist. • Es wird eine Methode implementiert, um die Integrität jedes Skripts sicherzustellen. • Es wird ein Inventar aller Skripte mit schriftlicher Begründung geführt, warum jedes benötigt wird.	**6.4.3.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse für die Verwaltung aller Zahlungsseitenskripte definiert sind, die in den Browser des Verbrauchers geladen und ausgeführt werden, gemäß allen in dieser Anforderung angegebenen Elementen. **6.4.3.b** Verantwortliches Personal befragen und Inventaraufzeichnungen und Systemkonfigurationen untersuchen, um zu verifizieren, dass alle Zahlungsseitenskripte, die im Browser des Verbrauchers geladen und ausgeführt werden, gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	Auf der Zahlungsseite geladene und ausgeführte Skripte können ohne Wissen der Entität in ihrer Funktionalität geändert werden und können auch die Funktionalität haben, zusätzliche externe Skripte zu laden (zum Beispiel Werbung und Verfolgung, Tag-Verwaltungs-Systeme). Solche scheinbar harmlosen Skripte können von potenziellen Angreifern verwendet werden, um böswillige Skripte hochzuladen, die Karteninhaberdaten aus dem Verbraucherbrowser lesen und exfiltrieren können. Die Sicherstellung, dass die Funktionalität aller solcher Skripte als notwendig für den Betrieb der Zahlungsseite verstanden wird, minimiert die Anzahl von Skripten, die manipuliert werden könnten. Die Sicherstellung, dass Skripte ausdrücklich autorisiert wurden, verringert die Wahrscheinlichkeit, dass unnötige Skripte ohne entsprechende Genehmigung der Verwaltung zur Zahlungsseite hinzugefügt werden. Durch die Verwendung von Techniken zur Verhinderung von Manipulationen am Skript wird die Wahrscheinlichkeit minimiert, dass das Skript geändert wird, um ein nicht autorisiertes Verhalten auszuführen, wie das Skimmen der Karteninhaberdaten von der Zahlungsseite. *(Fortsetzung auf der nächsten Seite)*
Zielsetzung des kundenspezifischen Ansatzes Nicht autorisierter Code darf nicht auf der Zahlungsseite vorhanden sein, da sie im Browser des Verbrauchers gerendert wird.		
Hinweise zur Anwendbarkeit Diese Anforderung gilt für alle Skripte, die aus der Umgebung der Entität geladen werden und für Skripte, die von Dritten und Vierten geladen werden. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
		Gute Praxis Skripte können durch manuelle oder automatisierte (zum Beispiel Arbeitsablauf-)Prozesse autorisiert werden. Wenn die Zahlungsseite in einen Inline-Frame (IFRAME) geladen wird, kann die Einschränkung des Ortes, von dem aus die Zahlungsseite geladen werden kann, unter Verwendung der Inhaltssicherheitsrichtlinie (CSP) der übergeordneten Seite dabei helfen, dass die Zahlungsseite nicht durch nicht autorisierte Inhalte ersetzt wird. **Definitionen** „Notwendig“ für diese Anforderung bedeutet, dass die Überprüfung jedes Skripts durch die Entität begründet und bestätigt, warum es für die Funktionalität der Zahlungsseite erforderlich ist, um eine Zahlungstransaktion zu akzeptieren. **Beispiele** Die Integrität von Skripten kann durch verschiedene Mechanismen erzwungen werden, einschließlich, aber nicht beschränkt auf: • Sub-Ressourcen-Integrität (SRI), die es dem Verbraucher-Browser ermöglicht, zu validieren, ob ein Skript nicht manipuliert wurde. • Eine CSP, die die Standorte begrenzt, von denen der Verbraucher-Browser ein Skript von Kontodaten laden und zu ihnen übertragen kann • Proprietäre Skript- oder Tag-Verwaltungs-Systeme, die die Ausführung böswilliger Skripts verhindern können.

Anforderungen und Testprozeduren		Anleitungen
6.5 Änderungen an allen Systemkomponenten werden sicher verwaltet.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Änderungsmanagementprozeduren müssen auf alle Änderungen – einschließlich Hinzufügen, Entfernen oder Ändern von Systemkomponenten – in der Produktionsumgebung angewendet werden. Es ist wichtig, den Grund für eine Änderung und die Änderungsbeschreibung zu dokumentieren, damit die relevanten Parteien verstehen und zustimmen, dass die Änderung erforderlich ist. Ebenso ermöglicht die Dokumentation der Auswirkungen der Änderung allen betroffenen Parteien, etwaige Verarbeitungsänderungen angemessen zu planen. **Gute Praxis** Die Genehmigung durch autorisierte Parteien bestätigt, dass die Änderung legitim ist und von der Organisation sanktioniert wird. Änderungen sollten von Personen mit der entsprechenden Autorität und Kenntnissen genehmigt werden, um die Auswirkungen der Änderung zu verstehen. Gründliches Testen durch die Entität bestätigt, dass die Sicherheit der Umgebung durch die Implementierung einer Änderung nicht verringert wird und dass alle bestehenden Sicherheitskontrollen entweder bestehen bleiben oder nach der Änderung durch gleichwertige oder stärkere Sicherheitskontrollen ersetzt werden. Die durchzuführenden spezifischen Tests variieren je nach Art der Änderung und der betroffenen Systemkomponente(n). *(Fortsetzung auf der nächsten Seite)*
6.5.1 Änderungen an allen Systemkomponenten in der Produktionsumgebung werden gemäß etablierter Prozeduren vorgenommen, die Folgende beinhalten: • Grund für und Beschreibung der Änderung. • Dokumentation der Auswirkung auf die Sicherheit. • Dokumentierte Änderungsgenehmigung durch autorisierte Parteien. • Testen um zu verifizieren, dass die Änderung die Systemsicherheit nicht beeinträchtigt. • Für maßgeschneiderte und kundenspezifische Softwareänderungen werden alle Aktualisierungen auf Einhaltung von Anforderung 6.2.4 getestet, bevor sie in der Produktion eingesetzt werden. • Prozeduren, um Versagen zu adressieren und in einen sicheren Zustand zuückzukehren.	**6.5.1.a** Dokumentierte Änderungskontrollprozeduren untersuchen, um zu verifizieren, dass Prozeduren für Änderungen an allen Systemkomponenten in der Produktionsumgebung definiert sind, um alle in dieser Anforderung angegebenen Elemente einzuschließen.	
Zielsetzung des kundenspezifischen Ansatzes	**6.5.1.b** Kürzliche Änderungen an Systemkomponenten untersuchen und diese Änderungen zurück zu der zugehörigen Änderungskontrolldokumentation verfolgen. Für jede untersuchte Änderung, verifizieren, dass die Änderung gemäß allen in dieser Anforderung angegebenen Elementen implementiert wird.	
Alle Änderungen werden nachverfolgt, autorisiert und auf Auswirkung und Sicherheit bewertet, und Änderungen werden verwaltet, um unbeabsichtigte Effekte auf die Sicherheit von Systemkomponenten zu vermeiden.		

Anforderungen und Testprozeduren		Anleitungen
		Für jede Änderung ist es wichtig, über dokumentierte Prozeduren zu verfügen, die Fehler adressieren und Anweisungen zur Rückkehr in einen sicheren Zustand bereitstellen, falls die Änderung fehlschlägt oder die Sicherheit einer Anwendung oder eines Systems beeinträchtigt. Diese Prozeduren werden der Anwendung oder dem System gestatten, in ihren vorherigen sicheren Zustand zurückversetzt zu werden.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **6.5.2** Nach Abschluss einer bedeutenden Änderung wird bestätigt, dass alle anwendbaren PCI DSS-Anforderungen auf allen neuen oder geänderten Systemen und Netzwerken vorhanden sind, und die Dokumentation wird gegebenenfalls aktualisiert. **Zielsetzung des kundenspezifischen Ansatzes** Alle Systemkomponenten werden nach einer bedeutenden Änderung auf Einhaltung der geltenden PCI DSS-Anforderungen verifiziert. **Hinweise zur Anwendbarkeit** Diese bedeutenden Änderungen sollten auch erfasst und in der jährlichen PCI DSS-Geltungsbereichs-Bestätigungsaktivität der Entität gemäß Anforderung 12.5.2 widergespiegelt werden.	**Testprozeduren mit definiertem Ansatz** **6.5.2** Dokumentation auf bedeutende Änderungen untersuchen, das Personal befragen, und die betroffenen Systeme/Netzwerke beobachten, um zu verifizieren, dass die Entität bestätigt hat, dass anwendbare PCI DSS-Anforderungen auf allen neuen oder geänderten Systemen und Netzwerken vorhanden sind, und dass die Dokumentation wie zutreffend aktualisiert wurde.	**Zweck** Prozesse zur Analyse bedeutender Änderungen helfen dabei, sicherzustellen, dass alle angemessenen PCI DSS-Kontrollen auf alle Systeme oder Netzwerke angewendet werden, die in der Umgebung im Geltungsbereich hinzugefügt oder geändert werden, und dass die PCI DSS-Anforderungen weiterhin erfüllt werden, um die Umgebung zu sichern. **Gute Praxis** Der Einbau dieser Validierung in Veränderungsmanagementprozesse hilft dabei, sicherzustellen, dass Geräteinventare und Konfigurationsstandards auf dem neuesten Stand gehalten werden und Sicherheitskontrollen bei Bedarf angewendet werden. **Beispiele** Anwendbare PCI DSS-Anforderungen, die betroffen sein könnten, umfassen, sind aber nicht beschränkt auf: • Netzwerk- und Datenflussdiagramme werden aktualisiert, um Änderungen widerzuspiegeln. • Systeme werden gemäß Konfigurationsstandards konfiguriert, wobei alle Standardpasswörter geändert und unnötige Dienste deaktiviert werden. • Systeme werden mit den erforderlichen Kontrollen geschützt – zum Beispiel durch Überwachung der Dateiintegrität (FIM), Anti-Malware, Patches und Audit-Protokollierung. • Sensible Authentifizierungsdaten werden nicht gespeichert, und die gesamte Kontodatenspeicherung wird dokumentiert und in die Richtlinien und Prozeduren zur Datenaufbewahrung aufgenommen. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		• Neue Systeme werden in den vierteljährlichen Schwachstellen-Scan-Prozess aufgenommen. • Systeme werden nach wesentlichen Änderungen gemäß den Anforderungen 11.3.1.3 und 11.3.2.1 auf interne und externe Schwachstellen gescannt.
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Aufgrund des sich ständig ändernden Zustands von Vorproduktionsumgebungen sind sie oft weniger sicher als die Produktionsumgebung. **Gute Praxis** Organisationen müssen klar verstehen, welche Umgebungen Testumgebungen oder Entwicklungsumgebungen sind und wie diese Umgebungen auf der Ebene von Netzwerken und Anwendungen interagieren. **Definitionen** Vorproduktionsumgebungen umfassen Entwicklung, Tests, Benutzerakzeptanztests (UAT) usw. Selbst wenn die Produktionsinfrastruktur verwendet wird, um Tests oder Entwicklung zu erleichtern, müssen Produktionsumgebungen (logisch oder physisch) von der Vorproduktionsfunktionalität getrennt werden, sodass Schwachstellen, die als Ergebnis von Vorproduktionsaktivitäten eingeführt werden, Produktionssysteme nicht gegenteilig beeinträchtigen.
6.5.3 Vorproduktionsumgebungen werden von Produktionsumgebungen getrennt und die Trennung wird mit Zugriffskontrollen erzwungen.	**6.5.3.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse zur Trennung der Vorproduktionsumgebung von der Produktionsumgebung über Zugriffskontrollen definiert sind, die die Trennung erzwingen.	
	6.5.3.b Netzwerkdokumentation und Konfigurationen von Netzwerksicherheitskontrollen untersuchen, um zu verifizieren, dass die Vorproduktionsumgebung von der/den Produktionsumgebung(en) getrennt ist.	
Zielsetzung des kundenspezifischen Ansatzes	**6.5.3.c** Zugriffskontrolleinstellungen untersuchen, um zu verifizieren, dass Zugriffskontrollen vorhanden sind, um eine Trennung zwischen der(den) Vorproduktions- und der Produktionsumgebung(en) zu erzwingen.	
Vorproduktionsumgebungen können keine Risiken und Schwachstellen in Produktionsumgebungen einführen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
6.5.4 Rollen und Funktionen sind zwischen Produktions- und Vorproduktionsumgebungen getrennt, um Rechenschaftspflicht bereitzustellen, sodass nur überprüfte und genehmigte Änderungen eingesetzt werden.	**6.5.4.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse zur Trennung von Rollen und Funktionen definiert sind, um Rechenschaftspflicht bereitzustellen, sodass nur überprüfte und genehmigte Änderungen eingesetzt werden.	Das Ziel der Trennung von Rollen und Funktionen zwischen Produktions- und Vorproduktionsumgebungen besteht darin, die Anzahl des Personals mit Zugriff auf die Produktionsumgebung und Kontodaten zu reduzieren und dadurch das Risiko eines nicht autorisierten, unbeabsichtigten oder unangemessenen Zugriffs auf Daten und Systemkomponenten zu minimieren und dabei zu helfen, sicherzustellen, dass Zugriff auf solche Personen beschränkt ist, die einen solchen Zugriff aus geschäftlichen Gründen benötigen.
Zielsetzung des kundenspezifischen Ansatzes	**6.5.4.b** Prozesse beobachten und Personal befragen, um zu verifizieren, dass implementierte Kontrollen Rollen und Funktionen trennen und Rechenschaftspflicht bereitstellen, sodass nur überprüfte und genehmigte Änderungen eingesetzt werden.	Die Absicht dieser Kontrolle besteht darin, kritische Aktivitäten zu trennen, um eine Übersicht und Überprüfung bereitzustellen, um Fehler abzufangen und die Chancen von Betrug oder Diebstahl zu minimieren (da zwei Personen konspirieren müssten, um eine Aktivität zu verbergen).
Arbeitsrollen und Verantwortlichkeiten, die zwischen Vorproduktions- und Produktionsaktivitäten unterscheiden, werden definiert und verwaltet, um das Risiko nicht autorisierter, unbeabsichtigter oder unangemessener Handlungen zu minimieren.		Die Trennung von Rollen und Funktionen, auch als Aufgabentrennung oder Funktionstrennung bezeichnet, ist ein zentrales internes Kontrollkonzept zum Schutz der Assets einer Entität.
Hinweise zur Anwendbarkeit		
In Umgebungen mit begrenztem Personal, in denen Personen mehrere Rollen oder Funktionen durchführen, kann dasselbe Ziel mit zusätzlichen prozessuralen Kontrollen erreicht werden, die Rechenschaftspflicht bereitstellen. Zum Beispiel kann ein Entwickler auch ein Administrator sein, der ein Konto auf Administratorebene mit erhöhten Privilegien in der Entwicklungsumgebung verwendet und für seine Entwicklerrolle ein separates Konto mit Zugriff auf Benutzerebene auf die Produktionsumgebung verwendet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Verwendung von Live-PANs außerhalb geschützter CDEs stellt böswilligen Personen die Möglichkeit bereit, sich nicht autorisierten Zugriff auf Karteninhaberdaten zu verschaffen. **Gute Praxis** Entitäten können ihre Speicherung von Live-PANs minimieren, indem sie diese nur dann in der Vorproduktion speichern, wenn dies für einen bestimmten und definierten Testzweck unbedingt erforderlich ist, und diese Daten nach der Verwendung sicher löschen. Wenn eine Entität PANs benötigt, die speziell für Testzwecke konzipiert sind, können diese von Erwerbern bezogen werden. **Definitionen** Live-PANs beziehen sich auf gültige PANs (keine Test-PANs), die das Potenzial haben, zur Ausführung von Zahlungstransaktionen verwendet zu werden. Zusätzlich, wenn Zahlungskarten ablaufen, wird dieselbe PAN oft mit einem anderen Ablaufdatum wiederverwendet. Alle PANs müssen verifiziert werden, sodass sie keine Zahlungstransaktionen ausführen können, bevor sie vom Geltungsbereich des PCI DSS ausgeschlossen werden. Es liegt in der Verantwortung der Entität, zu bestätigen, dass PANs nicht live sind.
6.5.5 Live-PANs werden nicht in Vorproduktionsumgebungen verwendet, es sei denn, diese Umgebungen sind in der CDE enthalten und gemäß allen anwendbaren PCI DSS-Anforderungen geschützt.	**6.5.5.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, um Live-PANs nicht in Vorproduktionsumgebungen zu verwenden, es sei denn, diese Umgebungen befinden sich in einer CDE und sind gemäß allen anwendbaren PCI DSS-Anforderungen geschützt.	
	6.5.5.b Testprozesse beobachten und das Personal befragen, um zu verifizieren, dass Prozeduren vorhanden sind, um sicherzustellen, dass Live-PANs nicht in Vorproduktionsumgebungen verwendet werden, es sei denn, diese Umgebungen befinden sich in einer CDE und sind gemäß allen geltenden PCI DSS-Anforderungen geschützt.	
Zielsetzung des kundenspezifischen Ansatzes	**6.5.5.c** Testdaten aus der Vorproduktion untersuchen, um zu verifizieren, dass Live-PANs nicht in Vorproduktionsumgebungen verwendet werden, es sei denn, diese Umgebungen sind in einer CDE und gemäß allen anwendbaren PCI DSS-Anforderungen geschützt.	
Live-PANs können nicht in Vorproduktionsumgebungen außerhalb der CDE vorhanden sein.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Diese Daten können Informationen über die Funktionsweise einer Anwendung oder eines Systems preisgeben und sind ein leichtes Ziel für nicht autorisierte Personen, um auszunutzen, um Zugriff auf Systeme zu erhalten. Der Besitz solcher Informationen könnte die Kompromittierung des Systems und der verwandten Kontodaten erleichtern.
6.5.6 Testdaten und Testkonten werden von Systemkomponenten entfernt, bevor das System in Produktion geht.	**6.5.6.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse zum Entfernen von Testdaten und Testkonten aus Systemkomponenten definiert sind, bevor das System in Produktion geht.	
	6.5.6.b Testprozesse sowohl für Standardsoftware als auch für interne Anwendungen beobachten, und das Personal befragen, um zu verifizieren, dass Testdaten und Testkonten entfernt worden sind, bevor ein System in Produktion geht	
	6.5.6.c Daten und Konten für kürzlich installierte oder aktualisierte Standardsoftware und interne Anwendungen untersuchen, um zu verifizieren, dass keine Testdaten oder Testkonten auf Systemen in der Produktion vorhanden sind.	
Zielsetzung des kundenspezifischen Ansatzes		
Testdaten und Testkonten können in Produktionsumgebungen nicht existieren.		

Implementierung Starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten nach Geschäftlichem Bedarf

Abschnitte	
7.1	Prozesse und Mechanismen zur Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten durch geschäftlichen Bedarf werden definiert und verstanden.
7.2	Der Zugriff auf Systemkomponenten und Daten wird entsprechend definiert und zugewiesen.
7.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsystem(e) verwaltet.

Übersicht

Nicht autorisierte Personen können aufgrund ineffektiver Zugriffskontrollregeln und -definitionen Zugriff auf kritische Daten oder Systeme erhalten. Um sicherzustellen, dass nur autorisiertes Personal auf kritische Daten zugreifen kann, müssen Systeme und Prozesse vorhanden sein, um den Zugriff je nach Bedarf und entsprechend den Job-Verantwortlichkeiten zu beschränken.

„Zugriff“ oder „Zugriffsrechte“ werden durch Regeln erstellt, die Benutzern Zugriff auf Systeme, Anwendungen, Anwendungen und Daten bereitstellen, während „Privilegien“ es einem Benutzer erlauben, eine bestimmte Aktion oder Funktion in Bezug auf dieses System, diese Anwendung oder diese Daten durchzuführen Zum Beispiel kann ein Benutzer Zugriffsrechte auf bestimmte Daten haben, aber ob er diese Daten nur lesen oder auch ändern oder löschen kann, wird durch die dem Benutzer zugewiesenen Privilegien bestimmt.

„Nach Wissensbedarf“ bezieht sich darauf, nur Zugriff auf die geringste Menge an Daten bereitzustellen, die für die Durchführung eines Jobs erforderlich sind.

„Geringste Privilegien“ bezieht sich darauf, nur die minimalen Privilegien bereitzustellen, die zum Durchführen eines Jobs erforderlich sind.

Diese Anforderungen gelten für Benutzerkonten und Zugriff für Mitarbeiter, Auftragnehmer, Berater, und internen und externen Anbietern und anderen Dritten (zum Beispiel, um Unterstützungs- oder Wartungsdienstleistungen bereitzustellen). Bestimmte Anforderungen gelten auch für Anwendungs- und Systemkonten, die von der Entität verwendet werden (auch „Dienstleistungskonten“ genannt).

Diese Anforderungen gelten nicht für Verbraucher (Karteninhaber).

Finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
7.1 Prozesse und Mechanismen zur Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten durch geschäftlichen Bedarf werden definiert und verstanden.		
Definierte Ansatzanforderungen **7.1.1** Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 7 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt. **Zielsetzung des kundenspezifischen Ansatzes** Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 7 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht der Verwaltung.	**Testprozeduren mit definiertem Ansatz** **7.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 7 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Bei Anforderung 7.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 7 angegeben sind. Während es wichtig ist, die in Anforderung 7 genannten spezifischen Richtlinien oder Prozeduren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Prozeduren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Methoden und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen sind, ist das Personal sich möglicherweise seiner täglichen Verantwortlichkeiten nicht bewusst und kritische Aktivitäten können nicht stattfinden. **Gute Praxis** Rollen und Verantwortlichkeiten können in Richtlinien und Prozeduren dokumentiert oder in separaten Dokumenten gewartet werden. Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen. **Beispiele** Eine Methode zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).
7.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 7 werden dokumentiert, zugewiesen und verstanden.	**7.1.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 7 dokumentiert und zugewiesen sind.	
	7.1.2.b Personal mit Verantwortlichkeit zur Durchführung von Aktivitäten in Anforderung 7 befragen, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 7 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
7.2 Der Zugriff auf Systemkomponenten und Daten wird entsprechend definiert und zugewiesen.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Definition eines Zugriffskontrollmodells, das für die Technologie und die Zugriffskontrollphilosophie der Entität angemessen ist, unterstützt eine konsistente und einheitliche Art der Zugriffszuweisung und reduziert die Möglichkeit von Fehlern wie der Vergabe übermäßiger Rechte. **Gute Praxis** Ein Faktor, der bei der Definition des Zugriffsbedarfs zu berücksichtigen ist, ist das Prinzip der Aufgabentrennung. Dieses Prinzip soll Betrug und Missbrauch oder Diebstahl von Ressourcen verhindern. Zum Beispiel 1) Aufteilen von missionskritischen Funktionen und Informationssystem-Unterstützungsfunktionen auf verschiedene Personen und/oder Funktionen, 2) Etablieren von Rollen, so dass Informationssystem-Unterstützungsaktivitäten von verschiedenen Funktionen/Personen durchgeführt werden (zum Beispiel Systemverwaltung, Programmierung, Konfigurationsverwaltung, Qualitätssicherung und -testen, und Netzwerksicherheit) und 3) Sicherzustellen, dass Sicherheitspersonal, das Zugriffskontrollfunktionen verwaltet, nicht auch Auditfunktionen verwaltet. In Umgebungen, in denen eine Person mehrere Funktionen durchführt, wie Administrations- und Sicherheitsbetriebe, können Aufgaben zugewiesen werden, sodass keine einzelne Person ohne einen unabhängigen Kontrollpunkt die durchgehende Kontrolle eines Prozesses hat. Zum Beispiel könnten die Verantwortung für die Konfiguration und die Verantwortung für die Genehmigung von Änderungen getrennten Personen zugewiesen werden. *(Fortsetzung auf der nächsten Seite)*
7.2.1 Ein Zugriffskontrollmodell wird definiert und umfasst die Zugriffsgewährung wie folgt: • Angemessener Zugriff abhängig von den Geschäfts- und Zugriffsanforderungen der Entität. • Zugriff auf Systemkomponenten und Datenressourcen, die auf der Jobklassifizierung und den Funktionen der Benutzer basieren. • Die geringsten erforderlichen Privilegien (zum Beispiel Benutzer, Administrator), um eine Jobfunktion durchzuführen.	**7.2.1.a** Dokumentierte Richtlinien und Prozeduren untersuchen und das Personal befragen, um zu verifizieren, dass das Zugriffskontrollmodell gemäß allen in dieser Anforderung angegebenen Elementen definiert ist.	
Zielsetzung des kundenspezifischen Ansatzes	**7.2.1.b** Zugriffskontrollmodelleinstellungen untersuchen und verifizieren, dass die Zugriffsanforderungen gemäß allen in dieser Anforderung angegebenen Elementen angemessen definiert sind.	
Zugriffsanforderungen werden gemäß den Jobfunktionen nach den Prinzipien der geringsten Privilegien und der Notwendigkeit, sie zu kennen, festgelegt.		

Anforderungen und Testprozeduren		Anleitungen
		Definitionen Schlüsselelementen eines Zugriffskontrollmodells beinhalten: • Zu schützende Ressourcen (die Systeme/Geräte/Daten, auf die Zugriff benötigt wird), • Jobfunktionen, die Zugriff auf die Ressource benötigen (z. B. Systemadministrator, Call-Center-Personal, Verkäufer) und • Welche Aktivitäten jede Jobfunktion ausführen muss (zum Beispiel Lesen/Schreiben oder Abfragen). Sobald Jobfunktionen, Ressourcen und Aktivitäten pro Jobfunktion definiert sind, kann Personen entsprechend Zugriff gewährt werden. **Beispiele** Zugriffskontrollmodelle, die Entitäten berücksichtigen können, umfassen rollenbasierte Zugriffskontrolle (RBAC) und attributbasierte Zugriffskontrolle (ABAC). Das von einer bestimmten Entität verwendete Zugriffskontrollmodell hängt von ihren Geschäfts- und Zugriffsanforderungen ab.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Zuweisung von den geringsten Privilegien hilft Benutzern ohne ausreichende Kenntnisse über die Anwendung, die Anwendungskonfiguration falsch oder versehentlich zu ändern oder ihre Sicherheitseinstellungen zu ändern. Die Erzwingung der geringsten Privilegien trägt auch dazu bei, das Ausmaß des Schadens zu minimieren, wenn eine nicht autorisierte Person Zugriff auf eine Benutzer-ID erhält. **Gute Praxis** Zugriffsrechte werden einem Benutzer durch Zuweisung zu einer oder mehreren Funktionen erteilt. Zugriff wird abhängig von den spezifischen Benutzerfunktionen und mit dem für die Aufgabe erforderlichen Mindestumfang zugewiesen. Bei der Zuweisung von privilegiertem Zugriff ist es wichtig, Personen nur die Berechtigungen zuzuweisen, die sie für ihren Job benötigen (die „geringsten Privilegien“). Zum Beispiel sollten dem Datenbankadministrator oder Backup-Administrator nicht die gleichen Privilegien wie dem allgemeinen Systemadministrator zugewiesen werden. Sobald die Bedürfnisse für Benutzerfunktionen definiert sind (gemäß PCI DSS-Anforderung 7.2.1), ist es einfach, Personen gemäß ihrer Jobklassifizierung und Funktion Zugriff zu gewähren, indem die bereits erstellten Rollen verwendet werden. Entitäten möchten möglicherweise die Verwendung von der Verwaltung des privilegierten Zugriffs (PAM) in Betracht ziehen, das eine Methode ist, um auf privilegierte Konten nur dann Zugriff zu gewähren, wenn diese Privilegien erforderlich sind, und diesen Zugriff sofort zu widerrufen, wenn sie nicht mehr benötigt werden.
7.2.2 Der Zugriff wird Benutzern, einschließlich privilegierten Benutzern, basierend auf Folgendem zugewiesen: • Jobklassifizierung und Funktion. • Geringste Privilegien, die zur Erfüllung der beruflichen Aufgaben erforderlich sind.	**7.2.2.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass sie die Zuweisung des Zugriffs auf Benutzer gemäß allen in dieser Anforderung angegebenen Elementen abdecken.	
	7.2.2.b Benutzerzugriffseinstellungen, einschließlich für privilegierte Benutzer untersuchen, und verantwortliches Verwaltungspersonal befragen, um zu verifizieren, dass die zugewiesenen Privilegien mit allen in dieser Anforderung angegebenen Elementen übereinstimmen.	
Zielsetzung des kundenspezifischen Ansatzes	**7.2.2.c** Das für die Zugriffszuweisung zuständige Personal befragen, um zu verifizieren, dass der privilegierte Benutzerzugriff gemäß allen in dieser Anforderung angegebenen Elementen zugewiesen wird.	
Der Zugriff auf Systeme und Daten ist auf den Zugriff beschränkt, der zum Ausführen von Jobfunktionen erforderlich ist, wie in den zugehörigen Zugriffsrollen definiert.		

<table>
<tr><th colspan="2">Anforderungen und Testprozeduren</th><th>Anleitungen</th></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="4">Zweck
Eine dokumentierte Genehmigung (zum Beispiel schriftlich oder elektronisch) stellt sicher, dass die Personen mit Zugang und Privilegien bekannt und von der Verwaltung autorisiert sind und dass ihr Zugriff für ihre Aufgaben erforderlich ist.</td></tr>
<tr><td rowspan="2">7.2.3 Erforderliche Privilegien werden von autorisiertem Personal genehmigt.</td><td>7.2.3.a Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass sie Prozesse zur Genehmigung aller Privilegien durch autorisiertes Personal definieren.</td></tr>
<tr><td>7.2.3.b Benutzer-IDs und zugewiesene Privilegien untersuchen, und sie mit dokumentierten Genehmigungen vergleichen, um zu verifizieren, dass:
• Für die zugewiesenen Privilegien liegt eine dokumentierte Genehmigung vor.
• Die Genehmigung erfolgte durch autorisiertes Personal.
• Angegebene Privilegien stimmen mit den Rollen überein, die der Person zugewiesen sind.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes</td><td colspan="2"></td></tr>
<tr><td>Zugriffsprivilegien können Benutzern ohne entsprechende, dokumentierte Autorisierung nicht gewährt werden.</td><td colspan="2"></td></tr>
</table>

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die regelmäßige Überprüfung der Zugriffsrechte hilft, übermäßige Zugriffsrechte zu erkennen, die verbleiben, nachdem sich die Jobverantwortlichkeiten der Benutzer geändert haben, Systemfunktionen sich geändert haben oder andere Änderungen. Wenn übermäßige Benutzerrechte nicht zeitgerecht widerrufen werden, können sie von böswilligen Benutzern für nicht autorisierten Zugriff verwendet werden. Diese Überprüfung stellt eine weitere Gelegenheit bereit, um sicherzustellen, dass Konten für alle gekündigten Benutzer entfernt wurden (falls zum Zeitpunkt der Kündigung welche übersehen wurden), sowie um sicherzustellen, dass der Zugriff von Dritten, die keinen Zugriff mehr benötigen, beendet wurde. **Gute Praxis** Wenn ein Benutzer in eine neue Rolle oder eine neue Abteilung wechselt, sind die mit seiner früheren Rolle verbundenen Privilegien und Zugriffe in der Regel nicht mehr erforderlich. Fortgesetzter Zugriff auf Privilegien oder Funktionen, die nicht mehr benötigt werden, kann das Risiko von Missbrauch oder Fehlern mit sich bringen. Wenn sich die Verantwortlichkeiten ändern, helfen daher Prozesse, die den Zugriff erneut validieren, sicherstellen, dass der Benutzerzugriff für die neuen Verantwortlichkeiten des Benutzers geeignet ist. Entitäten können erwägen, einen regelmäßigen, wiederholbaren Prozess zur Durchführung von Überprüfungen der Zugriffsrechte zu implementieren und „Dateneigentümer“ zuzuweisen, *(Fortsetzung auf der nächsten Seite)*
7.2.4 Alle Benutzerkonten und zugehörigen Zugriffsrechte, einschließlich Konten von Dritten/Anbietern, werden wie folgt überprüft: • Mindestens einmal alle sechs Monate. • Um sicherzustellen, dass Benutzerkonten und Zugriff je nach Jobfunktion angemessen bleiben. • Jeder unangemessene Zugriff wird adressiert. • Die Verwaltung bestätigt, dass der Zugriff weiterhin angemessen ist.	**7.2.4.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass sie Prozesse definieren, um alle Benutzerkonten und verwandte Zugriffsprivilegien zu überprüfen, einschließlich Konten von Dritten/Anbietern, gemäß allen in dieser Anforderung angegebenen Elementen.	
	7.2.4.b Verantwortliches Personal befragen und dokumentierte Ergebnisse regelmäßiger Überprüfungen von Benutzerkonten untersuchen, um zu verifizieren, dass alle Ergebnisse gemäß allen in dieser Anforderung angegebenen Elementen erfolgen.	
Zielsetzung des kundenspezifischen Ansatzes Zuweisungen von Kontoprivilegien werden regelmäßig von der Verwaltung auf Korrektheit verifiziert, und Abweichungen werden behoben.		
Hinweise zur Anwendbarkeit Diese Anforderung gilt für alle Benutzerkonten und verwandte Zugriffspivilegien, einschließlich derjenigen, die von Mitarbeitern und Dritten/Anbietern verwendet werden, und für Konten, die für den Zugriff auf Cloud-Dienstleistungen von Dritten verwendet werden. Siehe Anforderungen 7.2.5 und 7.2.5.1 und 8.6.1 bis 8.6.3 für Kontrollen für Anwendungs- und Systemkonten. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
		die für die Verwaltung und Überwachung des Zugriffs auf Daten im Zusammenhang mit ihrer beruflichen Funktion verantwortlich sind und die auch sicherstellen, dass der Benutzerzugriff aktuell und angemessen bleibt. Beispielsweise könnte ein direkter Manager den Teamzugriff monatlich überprüfen, während der leitende Manager den Zugriff seiner Gruppen vierteljährlich überprüft, wobei beide bei Bedarf Aktualisierungen für den Zugriff vornehmen. Die Absicht dieser bewährten Praktiken besteht darin, die Ausführung der Überprüfungen mindestens einmal alle 6 Monate zu unterstützen und zu erleichtern.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Es ist wichtig, die entsprechende Zugriffsebene für Anwendungs- oder Systemkonten zu etablieren. Wenn solche Konten kompromittiert werden, erhalten böswillige Benutzer dieselbe Zugriffsebene wie der Anwendung oder dem System gewährt wird. Daher ist es wichtig sicherzustellen, dass System- und Anwendungskonten auf der gleichen Grundlage wie Benutzerkonten eingeschränkter Zugriff gewährt wird. **Gute Praxis** Entitäten sollten beim Etablieren dieser Anwendungs- und Systemkonten möglicherweise die Etablierung einer Baseline in Betracht ziehen, einschließlich der folgenden, die für die Organisation gelten: • Sicherstellen, dass das Konto kein Mitglied einer privilegierten Gruppe wie Domänenadministratoren, lokale Administratoren oder Root ist. • Einschränken, auf welchen Computern das Konto verwendet werden kann. • Einschränken der Verwendungszeiten. • Entfernen aller zusätzlichen Einstellungen wie VPN-Zugriff und Fernzugriff.
7.2.5 Alle Anwendungs- und Systemkonten und verwandte Zugriffsrechte werden wie folgt zugewiesen und verwaltet: • Basierend auf den geringsten Berechtigungen, die für die Betriebsfähigkeit des Systems oder der Anwendung erforderlich sind. • Der Zugriff ist auf die Systeme, Anwendungen oder Prozesse beschränkt, die ihre Verwendung ausdrücklich erfordern.	**7.2.5.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass sie Prozesse definieren, um Anwendungs- und Systemkonten und verwandte Zugriffsprivilegien gemäß allen in dieser Anforderung angegebenen Elementen zu verwalten und zuzuweisen.	
Zielsetzung des kundenspezifischen Ansatzes Zugriffsrechte, die Anwendungs- und Systemkonten gewährt werden, sind auf den Zugriff beschränkt, der für die Funktionsfähigkeit dieser Anwendung oder dieses Systems erforderlich ist.	**7.2.5.b** Privilegien, die mit System- und Anwendungskonten verbunden sind untersuchen, und verantwortliches Personal befragen, um zu verifizieren, dass Anwendungs- und Systemkonten und verwandte Zugriffsprivilegien gemäß allen in dieser Anforderung angegebenen Elementen zugewiesen und verwaltet werden.	
Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
7.2.5.1 Jeder Zugriff von Anwendungs- und Systemkonten und verwandten Zugriffsprivilegien werden wie folgt überprüft: • Regelmäßig (in der Häufigkeit, die in der gezielten Risikoanalyse der Entität definiert ist, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird. • Der Anwendungs-/Systemzugriff bleibt für die durchgeführte Funktion angemessen. • Jeder unangemessene Zugriff wird adressiert. • Die Verwaltung bestätigt, dass der Zugriff weiterhin angemessen bleibt.	**7.2.5.1.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass sie Prozesse definieren, um alle Anwendungs- und Systemkonten und verwandte Zugriffsprivilegien gemäß allen in dieser Anforderung angegebenen Elementen zu überprüfen. **7.2.5.1.b** Die gezielte Risikoanalyse der Entität für die Häufigkeit regelmäßiger Protokollüberprüfungen von Anwendungs- und Systemkonten und verwandte Zugriffsprivilegien untersuchen, um zu verifizieren, dass die Risikoanalyse gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wurde. **7.2.5.1.c** Verantwortliches Personal befragen und dokumentierte Ergebnisse regelmäßiger Überprüfungen von System- und Anwendungskonten und verwandten Privilegien untersuchen, um zu verifizieren, dass die Überprüfungen gemäß allen in dieser Anforderung angegebenen Elementen erfolgen.	Die regelmäßige Überprüfung der Zugriffsrechte hilft, übermäßige Zugriffsrechte zu erkennen, die verbleiben, nachdem Systemfunktionen sich geändert haben oder andere Anwendungs- oder Systemänderungen vorgenommen wurden. Wenn übermäßige Rechte nicht entfernt werden, wenn sie nicht mehr benötigt werden, können sie von böswilligen Benutzern für nicht autorisierten Zugriff verwendet werden.
Zielsetzung des kundenspezifischen Ansatzes		
Zuweisungen von Anwendungs- und Systemkontoprivilegien werden regelmäßig von der Verwaltung auf Korrektheit verifiziert, und Abweichungen werden behoben.		
Hinweise zur Anwendbarkeit		
Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
7.2.6 Jeglicher Benutzerzugriff auf Abfrage-Repositorien von gespeicherter Karteninhaberdaten ist wie folgt beschränkt: • Über Anwendungen oder andere programmatische Methoden, mit Zugriff und zulässigen Aktionen basierend auf Benutzerrollen und geringsten Privilegien. • Nur der/die verantwortliche(n) Administrator(en) kann/können direkt auf Repositorien gespeicherter CHD zugreifen oder diese abfragen.	**7.2.6.a** Richtlinien und Prozeduren untersuchen und das Personal befragen, um zu verifizieren, dass Prozesse definiert sind, um Benutzern Zugriff auf Abfrage-Repositorien gespeicherter Karteninhaberdaten zu gewähren, gemäß allen in dieser Anforderung angegebenen Elementen.	Der Missbrauch des Abfragezugriffs auf Repositorien mit Karteninhaberdaten war eine regelmäßige Ursache für Datenschutzverletzungen. Die Beschränkung eines solchen Zugriffs auf Administratoren verringert das Risiko, dass dieser Zugriff von nicht autorisierten Benutzern missbraucht wird.
Zielsetzung des kundenspezifischen Ansatzes	**7.2.6.b** Konfigurationseinstellungen zum Abfragen von Repositorien gespeicherter Karteninhaberdaten untersuchen, um zu verifizieren, dass sie mit allen in dieser Anforderung angegebenen Elementen übereinstimmen.	**Definitionen**
Direkter ungefilterter (Ad-hoc-)Abfragezugriff auf Karteninhaberdatenspeicher ist verboten, es sei denn, dies wird von einem autorisierten Administrator durchgeführt.		„Programmatische Methoden“ bedeutet das Gewähren des Zugriffs durch Mittel wie gespeicherte Datenbankprozeduren, die es Benutzern ermöglichen, kontrollierte Aktionen an Daten in einer Tabelle durchzuführen, anstatt durch direkten, ungefilterten Zugriff auf das Datenrepository durch Endbenutzer (mit Ausnahme des/der verantwortlichen Administratoren), die für ihre administrativen Aufgaben direkten Zugriff auf die Datenbank benötigen).
Hinweise zur Anwendbarkeit		**Gute Praxis**
Diese Anforderung gilt für Kontrollen für den Benutzerzugriff auf Abfrage-Repositorien gespeicherter Karteninhaberdaten. Siehe Anforderungen 7.2.5 und 7.2.5.1 und 8.6.1 bis 8.6.3 für Kontrollen für Anwendungs- und Systemkonten.		Typische Benutzeraktionen beinhalten das Verschieben, Kopieren und Löschen von Daten. Auch den Geltungsbereich der erforderlichen Privilegien berücksichtigen, wenn Zugriff gewährt wird. Zum Beispiel kann Zugriff auf bestimmte Objekte wie Datenelemente, Dateien, Tabellen, Indizes, Ansichten und gespeicherte Routinen gewährt werden. Die Gewährung des Zugriffs auf Repositorien mit Karteninhaberdaten sollte dem gleichen Prozess folgen wie alle anderen gewährten Zugriffe, d. h., sie basiert auf Rollen, wobei jedem Benutzer nur die Privilegien zugewiesen werden, die zur Durchführung seiner Aufgaben erforderlich sind.

Anforderungen und Testprozeduren		Anleitungen
7.3 Der logische Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsystem(e) verwaltet.		
Definierte Ansatzanforderungen **7.3.1** Ein oder mehrere Zugriffskontrollsysteme sind vorhanden, die den Zugriff basierend auf den Informationsbedürfnissen eines Benutzers einschränken und alle Systemkomponenten abdecken. **Zielsetzung des kundenspezifischen Ansatzes** Zugriffsrechte und Privilegien werden über dafür vorgesehene Mechanismen verwaltet.	**Testprozeduren mit definiertem Ansatz** **7.3.1** Anbieterdokumentation und Systemeinstellungen untersuchen, um zu verifizieren, dass der Zugriff für jede Systemkomponente über ein Zugriffskontrollsystem(e) verwaltet wird, das den Zugriff basierend auf den Anforderungen des Benutzers einschränkt und alle Systemkomponenten abdeckt.	**Zweck** Ohne einen Mechanismus zur Beschränkung des Zugriffs basierend auf dem Wissensbedarf des Benutzers kann einem Benutzer unwissentlich Zugriff auf Karteninhaberdaten gewährt werden. Zugriffskontrollsysteme automatisieren den Prozess der Zugriffsbeschränkung und der Zuweisung von Privilegien.
Definierte Ansatzanforderungen **7.3.2** Das/die Zugriffskontrollsystem(e) ist/sind so konfiguriert, dass es Berechtigungen erzwingt, die Personen, Anwendungen, und Systemen basierend auf Jobklassifizierung und Funktion zugewiesen wurden. **Zielsetzung des kundenspezifischen Ansatzes** Individuelle Kontozugriffsrechte und Privilegien auf Systeme, Anwendungen und Daten werden nur von der Gruppenmitgliedschaft geerbt.	**Testprozeduren mit definiertem Ansatz** **7.3.2** Anbieterdokumentation und Systemeinstellungen untersuchen, um zu verifizieren, dass das/die Zugriffskontrollsystem(e) so konfiguriert ist/sind, dass Berechtigungen erzwungen werden, die Personen, Anwendungen, und Systemen basierend auf Jobklassifizierung und Funktion zugewiesen wurden.	**Zweck** Das Einschränken des privilegierten Zugriffs mit einem Zugriffskontrollsystem verringert die Wahrscheinlichkeit von Fehlern bei der Zuweisung von Berechtigungen an Personen, Anwendungen und Systeme.
Definierte Ansatzanforderungen **7.3.3** Das/die Zutrittskontrollsystem(e) ist/sind standardmäßig auf „Alles verweigern“ eingestellt.	**Testprozeduren mit definiertem Ansatz** **7.3.3** Anbieterdokumentation und Systemeinstellungen untersuchen, um zu verifizieren, ob das/die Zugriffskontrollsystem(e) standardmäßig auf „Alles verweigern“ eingestellt ist/sind.	**Zweck** Eine Standardeinstellung „Alles verweigern“ stellt sicher, dass niemandem Zugriff gewährt wird, es sei denn, es wurde eine Regel etabliert, die diesen Zugriff ausdrücklich gewährt.

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Zugriffsrechte und Privilegien sind verboten, sofern nicht ausdrücklich erlaubt.		**Gute Praxis** Es ist wichtig, die Standardkonfiguration von Zugriffskontrollsystemen zu überprüfen, da einige standardmäßig auf „Alles gestatten“ eingestellt sind und somit Zugriff erlauben, es sei denn/bis eine Regel geschrieben wird, die ihn ausdrücklich verweigert.

Anforderung 8: Identifizierung von Benutzern und Authentisierung von Zugriff auf Systemkomponenten

Abschnitte	
8.1	Prozesse und Mechanismen zur Identifizierung von Benutzern und zur Authentifizierung des Zugriffs auf Systemkomponenten werden definiert und verstanden.
8.2	Die Benutzeridentifizierung und verwandte Konten für Benutzer und Administratoren werden während des gesamten Lebenszyklus eines Kontos streng verwaltet.
8.3	Starke Authentifizierung für Benutzer und Administratoren wird etabliert und verwaltet.
8.4	Multi-Faktor-Authentifizierung (MFA) Die (MFA) wird implementiert, um den Zugriff auf die CDE zu sichern.
8.5	Multi-Faktor-Authentifizierungssysteme (MFA) sind so konfiguriert, dass sie Missbrauch verhindern.
8.6	Die Verwendung von Anwendungs- und Systemkonten und zugeordneten Authentifizierungsfaktoren werden streng verwaltet.

Übersicht

Zwei Grundprinzipien der Identifizierung und Authentifizierung von Benutzern sind 1) Feststellung der Identität einer Person oder eines Prozesses auf einem Computersystem und 2) Nachweis oder Verifizierung, dass der Benutzer, der der Identität zugeordnet ist, derjenige ist, für den sich der Benutzer ausgibt.

Die Identifizierung einer Person oder eines Prozesses auf einem Computersystem erfolgt durch Zuordnung einer Identität zu einer Person oder einem Prozess durch einen Identifizierer, wie einer Benutzer-, System- oder Anwendungs-ID. Diese IDs (auch als „Konten“ bezeichnet) etablieren grundsätzlich die Identität einer Person oder eines Prozesses fest, indem sie jeder Person oder jedem Prozess eine eindeutige Identifizierung zuweisen, um einen Benutzer oder Prozess von einem anderen zu unterscheiden. Wenn jeder Benutzer oder Prozess eindeutig identifiziert werden kann, stellt dies sicher, dass für die von dieser Identität durchgeführten Aktionen Rechenschaft abgelegt wird. Wenn eine solche Rechenschaftspflicht besteht, können die durchgeführten Aktionen bekannten und autorisierten Benutzern und Prozessen nachverfolgt werden.

Das Element, das zum Nachweis oder zur Verifizierung der Identität verwendet wird, wird als Authentifizierungsfaktor bezeichnet. Authentifizierungsfaktoren sind 1) etwas, das Sie wissen, wie ein Passwort oder eine Passphrase, 2) etwas, das Sie haben, wie ein Token-Gerät oder eine Smartcard, oder 3) etwas, das Sie sind, wie ein biometrisches Element.

Die ID und der Authentifizierungsfaktor gelten zusammen als Authentifizierungs-Anmeldeinformationen und werden verwendet, um Zugriff auf die Rechte und Privilegien zu erhalten, die einem Benutzer-, Anwendungs-, System- oder Dienstleistungskonten zugeordnet sind.

(Fortsetzung auf der nächsten Seite)

Diese Anforderungen für Identität und Authentifizierung basieren auf branchenweit akzeptablen Sicherheitsprinzipien und bewährten Praktiken zur Unterstützung des Zahlungsökosystems. *NIST Special Publication 800-63, Digital Identity Guidelines* stellt zusätzliche Informationen zu akzeptablen Rahmenbedingungen für digitale Identität und Authentifizierungsfaktoren bereit. Es ist wichtig zu beachten, dass die *NIST Digital Identity Guidelines* für US-Bundesbehörden bestimmt sind und in ihrer Gesamtheit betrachtet werden sollten. Von vielen der in diesen Anleitungen definierten Konzepte und Ansätze wird erwartet, dass sie miteinander und nicht als eigenständige Parameter funktionieren.

Hinweis: *Sofern in der Anforderung nicht anders angegeben, gelten diese Anforderungen für* ***alle Konten auf allen Systemkomponenten****, sofern in einer individuellen Anforderung nicht ausdrücklich darauf hingewiesen wird, einschließlich, aber nicht beschränkt auf:*

- *Konten an den Verkaufsstellen*
- *Konten mit administrativen Funktionen*
- *System- und Anwendungskonten*
- *Alle Konten, die zum Anzeigen oder Zugreifen auf Karteninhaberdaten oder zum Zugreifen auf Systeme mit Karteninhaberdaten verwendet werden.*

Dieses schließt Konten ein, die von Mitarbeitern, Auftragnehmern, Beratern, und internen und externen Anbietern und anderen Dritten verwendet werden (zum Beispiel, um Unterstützungs- oder Wartungsdienstleistungen bereitzustellen).

Bestimmte Anforderungen sollen nicht für Benutzerkonten gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs). Wenn Elemente nicht zutreffen, werden sie direkt in der spezifischen Anforderung vermerkt.

Diese Anforderungen gelten nicht für Benutzeraktivitäten, die von Verbrauchern (Karteninhabern) verwendet werden.

Finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
8.1 Prozesse und Mechanismen zur Identifizierung von Benutzern und zur Authentifizierung des Zugriffs auf Systemkomponenten werden definiert und verstanden.		
Definierte Ansatzanforderungen **8.1.1** Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 8 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt. **Zielsetzung des kundenspezifischen Ansatzes** Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 8 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht der Verwaltung.	**Testprozeduren mit definiertem Ansatz** **8.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 8 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Bei Anforderung 8.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 8 angegeben sind. Während es wichtig ist, die in Anforderung 8 genannten spezifischen Richtlinien oder Prozeduren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Prozeduren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Methoden und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen sind, ist das Personal sich möglicherweise seiner täglichen Verantwortlichkeiten nicht bewusst und kritische Aktivitäten können nicht stattfinden. **Gute Praxis** Rollen und Verantwortlichkeiten können in Richtlinien und Prozeduren dokumentiert oder in separaten Dokumenten gewartet werden. Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen. **Beispiele** Eine Methode zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).
8.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 8 werden dokumentiert, zugewiesen und verstanden.	**8.1.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 8 dokumentiert und zugewiesen sind.	
	8.1.2.b Personal mit Verantwortlichkeit zur Durchführung von Aktivitäten in Anforderung 8 befragen, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 8 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
8.2 Die Benutzeridentifizierung und verwandte Konten für Benutzer und Administratoren werden während des gesamten Lebenszyklus eines Kontos streng verwaltet.		
Definierte Ansatzanforderungen **8.2.1** Allen Benutzern wird eine eindeutige ID zugewiesen, bevor der Zugriff auf Systemkomponenten oder Karteninhaberdaten zugelassen wird. **Zielsetzung des kundenspezifischen Ansatzes** Alle Aktionen aller Benutzer sind einer Person zuzurechnen. **Hinweise zur Anwendbarkeit** Diese Anforderung soll nicht für Benutzerkonten im Rahmen von Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs).	**Testprozeduren mit definiertem Ansatz** **8.2.1.a** Verantwortliches Personal befragen, um zu verifizieren, dass allen Benutzern eine eindeutige ID für den Zugriff auf Systemkomponenten und Karteninhaberdaten zugewiesen wird. **8.2.1.b** Audit-Protokolle und andere Nachweise untersuchen, um zu verifizieren, dass der Zugriff auf Systemkomponenten und Karteninhaberdaten eindeutig identifiziert und Personen zugeordnet werden kann.	**Zweck** Die Fähigkeit, auf einem Computersystem ausgeführte Aktionen zu einer Person zurückzuverfolgen, schafft Verantwortlichkeit und Rückverfolgbarkeit und ist grundlegend für die Etablierung effektiver Zugriffskontrollen. Indem sichergestellt wird, dass jeder Benutzer eindeutig identifiziert wird, anstatt eine ID für mehrere Mitarbeiter zu verwenden, kann eine Organisation die individuelle Verantwortung für Aktionen und eine effektive Aufzeichnung im Audit-Protokoll pro Mitarbeiter aufrechterhalten. Darüber hinaus wird dies bei der Problemlösung und -eindämmung bei Missbrauch oder böswilliger Absicht helfen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Gruppen-, gemeinsam genutzte oder generische (oder Standard-)Konten werden normalerweise mit Software oder Betriebssystemen geliefert – zum Beispiel Root oder mit Privilegien, die einer bestimmten Funktion zugeordnet sind, wie einem Administrator. Wenn mehrere Benutzer dieselben Authentifizierungsdaten verwenden (zum Beispiel Benutzerkonto und Passwort), ist es unmöglich, den Systemzugriff und die Aktivitäten einer Person zuzuordnen. Dies wiederum hindert eine Entität daran, die Rechenschaftspflicht für die Aktionen einer Person zuzuweisen oder diese effektiv zu protokollieren, da eine bestimmte Aktion von jedem in der Gruppe mit Kenntnis der Benutzer-ID und den zugehörigen Authentifizierungsfaktoren hätte ausgeführt werden können. Die Fähigkeit, Personen den mit einem Konto durchgeführten Aktionen zuzuordnen, ist wesentlich, um eine individuelle Rechenschaftspflicht und Rückverfolgbarkeit darüber zu gewährleisten, wer eine Aktion durchgeführt hat, welche Aktion durchgeführt wurde und wann diese Aktion stattgefunden hat. **Gute Praxis** Wenn aus irgendeinem Grund gemeinsame Konten verwendet werden, müssen strenge Verwaltungskontrollen eingerichtet werden, um die Verantwortlichkeit und Rückverfolgbarkeit der Person beizubehalten. **Beispiele** Tools und Techniken können sowohl die Verwaltung als auch die Sicherheit dieser Arten von Konten erleichtern und die Identität einzelner Benutzer bestätigen, bevor der Zugriff auf ein Konto gewährt wird. *(Fortsetzung auf der nächsten Seite)*
8.2.2 Gruppen-, gemeinsame oder generische Konten, oder andere gemeinsame Authentifizierungs-Anmeldeinformationen werden nur in Ausnahmefällen verwendet und wie folgt verwaltet: • Die Verwendung des Kontos wird verhindert, es sei denn, es liegt ein außergewöhnlicher Umstand vor. • Die Verwendung ist auf die für den außergewöhnlichen Umstand erforderliche Zeit beschränkt. • Die geschäftliche Rechtfertigung zur Verwendung wird dokumentiert. • Die Verwendung wird ausdrücklich von der Geschäftsleitung genehmigt. • Die individuelle Benutzeridentität wird bestätigt, bevor der Zugriff auf ein Konto gewährt wird. • Jede durchgeführte Aktion ist einem einzelnen Benutzer zuzuordnen.	**8.2.2.a** Benutzerkontenlisten auf Systemkomponenten und anwendbare Dokumentation untersuchen, um zu verifizieren, dass gemeinsame Authentifizierungs-Anmeldeinformationen nur bei Bedarf und in Ausnahmefällen verwendet werden und gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	
	8.2.2.b Authentifizierungsrichtlinien und -prozeduren untersuchen, um zu verifizieren, dass Prozesse für gemeinsame Authentifizierungs-Anmeldeinformationen definiert sind, sodass sie nur bei Bedarf und in Ausnahmefällen verwendet werden und gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	
Zielsetzung des kundenspezifischen Ansatzes Alle Aktionen, die von Benutzern mit generischen, System- oder gemeinsamen IDs durchgeführt werden, sind einer einzelnen Person zuzuordnen.	**8.2.2.c** Systemadministratoren befragen, um zu verifizieren, dass gemeinsame Authentifizierungs-Anmeldeinformationen nur bei Bedarf und in Ausnahmefällen verwendet werden und gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	
Hinweise zur Anwendbarkeit Diese Anforderung soll nicht für Benutzerkonten im Rahmen von Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs).		

Anforderungen und Testprozeduren		Anleitungen
		Entitäten können Passworttresore oder andere vom System verwaltete Kontrollen wie den Befehl *sudo* in Betracht ziehen. Ein Beispiel für einen außergewöhnlichen Umstand ist, dass alle anderen Authentifizierungsmethoden fehlgeschlagen sind und ein gemeinsames Konto für den Notfall oder den Administratorzugriff benötigt wird.
Definierte Ansatzanforderungen **8.2.3 *Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Dienstleistungsanbieter mit Fernzugriff auf Kundenstandorte verwenden eindeutige Authentifizierungsfaktoren für jeden Kundenstandort. **Zielsetzung des kundenspezifischen Ansatzes** Die Anmeldeinformationen eines Dienstleistungsanbieters, die für einen Kunden verwendet werden, können nicht für andere Kunden verwendet werden. **Hinweise zur Anwendbarkeit** Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. Diese Anforderung gilt nicht für Dienstleistungsanbieter, die auf ihre eigenen gemeinsamen Dienstleistungsumgebungen zugreifen, in denen mehrere Kundenumgebungen gehostet werden. Wenn Mitarbeiter von Dienstleistungsanbietern gemeinsam genutzte Authentifizierungsfaktoren für den Fernzugriff auf Kundenstandorte verwenden, müssen diese Faktoren pro Kunde eindeutig sein und gemäß Anforderung 8.2.2 verwaltet werden.	**Testprozeduren mit definiertem Ansatz** **8.2.3 *Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Authentifizierungsrichtlinien und -prozeduren untersuchen und Personal befragen, um zu verifizieren, dass Dienstleistungsanbieter mit Fernzugriff auf Kundenstandorte eindeutige Authentifizierungsfaktoren für den Fernzugriff auf jeden Kundenstandort verwenden.	**Zweck** Dienstleistungsanbieter mit Fernzugriff auf Kundenstandorte verwenden diesen Zugriff normalerweise, um POS-POI-Systeme zu unterstützen oder andere Ferndienstleistungen bereitzustellen. Wenn ein Dienstleistungsanbieter dieselben Authentifizierungsfaktoren verwendet, um auf mehrere Kunden zuzugreifen, können alle Kunden des Dienstleistungsanbieters leicht kompromittiert werden, wenn ein Angreifer diesen einen Faktor kompromittiert. Kriminelle wissen das und zielen bewusst auf Dienstleistungsanbieter ab, die nach einem gemeinsamen Authentifizierungsfaktor suchen, der ihnen über diesen einzigen Faktor Fernzugriff auf viele Händler ermöglicht. **Beispiele** Technologien wie Multi-Faktor-Mechanismen, die eindeutige Anmeldeinformationen für jede Verbindung bereitstellen (wie ein Einmalpasswort), könnten ebenfalls die Absicht dieser Anforderung erfüllen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Es ist zwingend erforderlich, dass der Lebenszyklus einer Benutzer-ID (Hinzufügen, Löschen und Ändern) kontrolliert wird, damit nur autorisierte Konten Funktionen ausführen können, Aktionen überprüfbar sind und Privilegien nur auf das Erforderliche beschränkt sind. Angreifer kompromittieren oft ein bestehendes Konto und eskalieren dann die Privilegien dieses Kontos, um nicht autorisierte Handlungen durchzuführen, oder sie können neue IDs erstellen, um ihre Aktivität im Hintergrund fortzusetzen. Es ist wesentlich, zu erkennen und zu reagieren, wenn Benutzerkonten außerhalb des normalen Änderungsprozesses oder ohne entsprechende Autorisierung erstellt oder geändert werden.
8.2.4 Das Hinzufügen, Löschen und Ändern von Benutzer-IDs, Authentifizierungsfaktoren, Authentifizierungsfaktoren und anderen Identifiziererobjekten wird wie folgt verwaltet: • Autorisiert mit entsprechender Zulassung. • Implementiert nur mit den Privilegien, die in der dokumentierten Genehmigung angegeben sind.	**8.2.4** Dokumentierte Autorisierungen in verschiedenen Phasen des Kontolebenszyklus (Hinzufügungen, Änderungen und Löschungen) untersuchen und die Systemeinstellungen untersuchen, um zu verifizieren, dass die Aktivität gemäß allen in dieser Anforderung angegebenen Elementen verwaltet wurde.	
Zielsetzung des kundenspezifischen Ansatzes Lebenszyklusereignisse für Benutzer-IDs und Authentifizierungsfaktoren können nicht ohne entsprechende Autorisierung stattfinden.		
Hinweise zur Anwendbarkeit Diese Anforderung gilt für alle Benutzerkonten, einschließlich Mitarbeiter, Auftragnehmer, Berater, Zeitarbeiter und Drittanbieter.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn ein Mitarbeiter oder ein Dritter/Anbieter das Unternehmen verlassen hat und weiterhin über sein Benutzerkonto Zugriff auf das Netzwerk hat, könnte ein unnötiger oder böswilliger Zugriff auf Karteninhaberdaten erfolgen – entweder durch den ehemaligen Mitarbeiter oder durch einen böswilligen Benutzer, der das alte und/oder nicht verwendete Konto ausnutzt.
8.2.5 Der Zugriff für gekündigte Benutzer wird sofort widerrufen.	**8.2.5.a** Informationsquellen für gekündigte Benutzer untersuchen und die aktuellen Benutzerzugriffslisten überprüfen – sowohl für den lokalen als auch für den Fernzugriff – um zu verifizieren, dass gekündigte Benutzer-IDs deaktiviert oder aus den Zugriffslisten entfernt wurden.	
	8.2.5.b Verantworliches Personal befragen um zu verifizieren, dass alle physischen Authentifizierungsfaktoren— wie Smartcards, Token usw. – für beendete Benutzer zurückgegeben oder deaktiviert wurden.	
Zielsetzung des kundenspezifischen Ansatzes Die Konten gekündigter Benutzer können nicht verwendet werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **8.2.6** Inaktive Benutzerkonten werden innerhalb von 90 Tagen nach Inaktivität entfernt oder deaktiviert. **Zielsetzung des kundenspezifischen Ansatzes** Inaktive Benutzerkonten können nicht verwendet werden.	**Testprozeduren mit definiertem Ansatz** **8.2.6** Benutzerkonten und letzte Anmeldeinformationen untersuchen, und das Personal befragen, um zu verifizieren, dass alle inaktiven Benutzerkonten innerhalb von 90 Tagen nach Inaktivität entfernt oder deaktiviert werden.	**Zweck** Nicht regelmäßig genutzte Konten sind häufig Angriffsziele, da Änderungen, wie beispielsweise ein geändertes Passwort, mit geringerer Wahrscheinlichkeit bemerkt werden. Daher können diese Konten leichter ausgenutzt und für den Zugriff auf Karteninhaberdaten verwendet werden. **Gute Praxis** Wenn vernünftigerweise davon ausgegangen werden kann, dass ein Konto über einen längeren Zeitraum nicht verwendet wird, beispielsweise bei einer längeren Beurlaubung, sollte das Konto sofort zu Beginn des Urlaubs deaktiviert werden, anstatt 90 Tage zu warten.
Definierte Ansatzanforderungen **8.2.7** Konten, die von Dritten verwendet werden, um per Fernzugriff auf Systemkomponenten zuzugreifen, sie zu unterstützen oder zu warten, werden wie folgt verwaltet: • Nur während des erforderlichen Zeitraums aktiviert, und deaktiviert, wenn sie nicht verwendet werden. • Die Verwendung wird auf unerwartete Aktivitäten überwacht. **Zielsetzung des kundenspezifischen Ansatzes** Der Fernzugriff durch Dritte kann nicht verwendet werden, es sei denn, dies wurde ausdrücklich autorisiert und die Verwendung wird von der Verwaltung überwacht.	**Testprozeduren mit definiertem Ansatz** **8.2.7.** Das Personal befragen, Dokumentation zur Kontoverwaltung untersuchen, und Nachweis untersuchen, um zu verifizieren, dass Konten, die von Dritten für den Fernzugriff verwendet werden, gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Wenn Dritten rund um die Uhr Zugriff auf Systeme und Netzwerke einer Entität gewährt wird, wenn sie Unterstützung bereitstellen müssen, erhöht sich die Wahrscheinlichkeit eines nicht autorisierten Zugriffs. Dieser Zugriff könnte dazu führen, dass ein nicht autorisierter Benutzer in der Umgebung des Dritten oder eine böswillige Person den immer verfügbaren externen Eintrittspunkt in das Netzwerk einer Entität verwendet. Wenn Dritte rund um die Uhr Zugriff benötigen, sollte dies dokumentiert, begründet, überwacht und an bestimmte Dienstleistungsgründe gebunden werden **Gute Praxis** Den Zugriff nur für die benötigte Zeit freizugeben und zu deaktivieren, sobald er nicht mehr benötigt wird, hilft dabei, einen Missbrauch dieser Verbindungen zu verhindern. Ziehen Sie zusätzlich in Erwägung, Dritten gemäß ihrem Dienstleistungsvertrag ein Start- und Enddatum für ihren Zugriff zuzuweisen. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Die Überwachung des Zugriffs Dritter hilft dabei, sicherzustellen, dass Dritte nur auf die erforderlichen Systeme und nur in genehmigten Zeiträumen zugreifen. Jede ungewöhnliche Aktivität, die Konten von Dritten verwendet, sollte verfolgt und behoben werden.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Benutzer eine offene Maschine mit Zugriff auf Systemkomponenten oder Karteninhaberdaten verlassen, besteht das Risiko, dass die Maschine in Abwesenheit des Benutzers von anderen verwendet wird, was zu nicht autorisiertem Kontozugriff und/oder Missbrauch führt. **Gute Praxis** Die erneute Authentifizierung kann entweder auf Systemebene angewendet werden, um alle Sitzungen zu schützen, die auf diesem Computer ausgeführt werden, oder auf Anwendungsebene. Entitäten können auch die aufeinander folgenden Staging-Kontrollen in Betracht ziehen, um den Zugriff einer unbeaufsichtigten Sitzung im Laufe der Zeit weiter einzuschränken. Zum Beispiel kann der Bildschirmschoner nach 15 Minuten aktiviert und der Benutzer nach einer Stunde abgemeldet werden. Zeitüberschreitungskontrollen müssen jedoch das Risiko des Zugriffs und der Exposition mit den Auswirkungen auf den Benutzer und dem Zweck des Zugriffs abwägen. Wenn ein Benutzer ein Programm von einem unbeaufsichtigten Computer ausführen muss, kann sich der Benutzer beim Computer anmelden, um das Programm einzuleiten, und dann den Computer „sperren“, sodass niemand anderes die Anmeldung des Benutzers verwenden kann, während der Computer unbeaufsichtigt ist. **Beispiele** Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, einen automatischen Bildschirmschoner zu konfigurieren, der immer dann gestartet wird, wenn die Konsole 15 Minuten lang inaktiv ist und der angemeldete Benutzer zum Entsperren des Bildschirms sein Passwort eingeben muss.
8.2.8 Wenn eine Benutzersitzung länger als 15 Minuten inaktiv war, muss sich der Benutzer erneut authentifizieren, um das Terminal oder die Sitzung erneut zu aktivieren.	**8.2.8** Systemkonfigurationseinstellungen untersuchen, um zu verifizieren, dass die Auszeitfunktionen für System-/Sitzungsleerlauf für Benutzersitzungen auf 15 Minuten oder weniger eingestellt wurden.	
Zielsetzung des kundenspezifischen Ansatzes Eine Benutzersitzung kann nur von dem autorisierten Benutzer verwendet werden.		
Hinweise zur Anwendbarkeit Diese Anforderung soll nicht für Benutzerkonten an Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs). Diese Anforderung soll nicht verhindern, dass legitime Aktivitäten durchgeführt werden, während die Konsole/der PC unbeaufsichtigt ist.		

Anforderungen und Testprozeduren		Anleitungen
8.3 Starke Authentifizierung für Benutzer und Administratoren wird etabliert und verwaltet.		
Definierte Ansatzanforderungen **8.3.1** Der gesamte Benutzerzugriff auf Systemkomponenten für Benutzer und Administratoren wird über mindestens eine der folgenden Authentifizierungsfaktoren authentifiziert: • Etwas, das Sie wissen, wie ein Passwort oder eine Passphrase. • Etwas, das Sie besitzen, wie ein Token-Gerät oder eine Smartcard. • Etwas Persönliches, wie ein biometrisches Element. **Zielsetzung des kundenspezifischen Ansatzes** Auf ein Konto kann nur mit einer Kombination aus Benutzeridentität und einem Authentifizierungsfaktor zugegriffen werden. **Hinweise zur Anwendbarkeit** Diese Anforderung soll nicht für Benutzerkonten an Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs). Diese Anforderung ersetzt nicht die Anforderungen an die mehrstufige Authentifizierung (MFA), gilt jedoch für die im Geltungsbereich enthaltenen Systeme, die ansonsten nicht den MFA-Anforderungen unterliegen. Ein digitales Zertifikat ist eine gültige Option für „etwas, das Sie besitzen“, wenn es für einen bestimmten Benutzer eindeutig ist.	**Testprozeduren mit definiertem Ansatz** **8.3.1.a** Die Dokumentation untersuchen, die den/die Authentifizierungsfaktor(en) beschreibt, die verwendet werden, um zu verifizieren, dass Benutzerzugriff auf Systemkomponenten über mindestens einen in dieser Anforderung angegebenen Authentifizierungsfaktor authentifiziert wird. **8.3.1.b** Für jede Authentifizierungsfaktorart, die mit jeder Art von Systemkomponente verwendet wird, eine Authentifizierung beobachten, um zu verifizieren, dass die Authentifizierung konsistent mit dem (den) dokumentierten Authentifizierungsfaktor(en) funktioniert.	**Zweck** Wenn ein Authentifizierungsfaktor zusätzlich zu eindeutigen IDs verwendet wird, trägt er dazu bei, Benutzer-IDs vor Kompromittierung zu schützen, da der Angreifer über die eindeutige ID und die damit verbundenen Authentifizierungsfaktor(en) verfügen muss. **Gute Praxis** Ein üblicher Ansatz für eine böswillige Person, ein System zu kompromittieren, besteht darin, schwache oder nicht vorhandene Authentifizierungsfaktoren (zum Beispiel Passwörter/Passphrasen) auszunutzen. Die Anforderung starker Authentifizierungsfaktoren hilft dabei, gegen diesen Angriff zu schützen. **Weitere Informationen** Siehe *fidoalliance.org* für weitere Informationen zur Verwendung von Token, Smartcards oder Biometrie als Authentifizierungsfaktoren.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Von Netzwerkgeräten und Anwendungen ist bekannt, dass sie unverschlüsselte, lesbare Authentifizierungsfaktoren (wie Passwörter und Passphrasen) über das Netzwerk übertragen und/oder diese Werte ohne Verschlüsselung speichern Infolgedessen kann eine böswillige Person diese Informationen während der Übertragung mit einem „Schnüffler“ leicht abfangen oder direkt auf unverschlüsselte Authentifizierungsfaktoren in Dateien zugreifen, in denen sie gespeichert sind, und diese Daten dann verwenden, um nicht autorisierten Zugriff zu erhalten.
8.3.2 Starke Kryptographie wird verwendet, um alle Authentifizierungsfaktoren während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar zu machen.	**8.3.2.a** Die Herstellerdokumentation und die Systemkonfigurationseinstellungen untersuchen, um zu verifizieren, dass Authentifizierungsfaktoren während der Übertragung und Speicherung durch starke Kryptographie unlesbar gemacht werden.	
Zielsetzung des kundenspezifischen Ansatzes	**8.3.2.b** Repositorien mit Authentifizierungsfaktoren untersuchen, um zu verifizieren, dass sie während der Speicherung nicht lesbar sind.	
Klartext-Authentifizierungsfaktoren können nicht aus dem Abfangen von Kommunikationen oder aus gespeicherten Daten erhalten, abgeleitet oder wiederverwendet werden.	**8.3.2.c** Datenübertragungen untersuchen, um zu verifizieren, dass Authentifizierungsfaktoren während der Übertragung nicht lesbar sind.	
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Böswillige Personen verwenden „Social Engineering"-Techniken, um sich als Benutzer eines Systems auszugeben – zum Beispiel, indem sie einen Help Desk anrufen und als legitimer Benutzer auftreten – um einen Authentifizierungsfaktor ändern zu lassen, damit sie eine gültige Benutzer-ID verwenden können. Die Anforderung einer positiven Identifizierung eines Benutzers verringert die Wahrscheinlichkeit, dass diese Art von Angriff erfolgreich ist. **Gute Praxis** Änderungen an Authentifizierungsfaktoren, für die die Benutzeridentität verifiziert werden sollte, umfassen, sind aber nicht beschränkt auf Durchführen von Kennwortzurücksetzungen, das Bereitstellen neuer Hardware- oder Software-Token und das Generieren neuer Schlüssel. **Beispiele** Methoden zum Verifizieren der Identität eines Benutzers beinhalten eine geheime Frage/Antwort, wissensbasierte Informationen und den Rückruf des Benutzers unter einer bekannten und zuvor festgelegten Telefonnummer.
8.3.3 Die Benutzeridentität wird verifiziert, bevor ein Authentifizierungsfaktor geändert wird.	**8.3.3** Prozeduren zum Ändern von Authentifizierungsfaktoren untersuchen und das Sicherheitspersonal beobachten, um zu verifizieren, dass, wenn ein Benutzer eine Änderung eines Authentifizierungsfaktors anfordert, die Identität des Benutzers verifiziert wird, bevor der Authentifizierungsfaktor geändert wird.	
Zielsetzung des kundenspezifischen Ansatzes		
Nicht autorisierte Personen können keinen Systemzugriff erlangen, indem sie die Identität eines autorisierten Benutzers imitieren.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **8.3.4** Ungültige Authentifizierungsversuche werden eingeschränkt durch: • Sperren der Benutzer-ID nach nicht mehr als 10 Versuchen. • Einstellen der Sperrdauer auf mindestens 30 Minuten oder bis die Identität des Benutzers bestätigt ist. **Zielsetzung des kundenspezifischen Ansatzes** Ein Authentifizierungsfaktor kann bei einem Online-Angriff mit brutaler Gewalt nicht erraten werden. **Hinweise zur Anwendbarkeit** Diese Anforderung soll nicht für Benutzerkonten an Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs).	**Testprozeduren mit definiertem Ansatz** **8.3.4.a** Systemkonfigurationseinstellungen untersuchen, um zu verifizieren, dass die Authentifizierungsparameter so eingestellt sind, um zu erfordern, dass Benutzerkonten nach nicht mehr als 10 ungültigen Anmeldeversuchen gesperrt werden. **8.3.4.b** Systemkonfigurationseinstellungen untersuchen, um zu verifizieren, dass Passwortparameter so eingestellt sind, dass ein einmal gesperrtes Benutzerkonto für mindestens 30 Minuten oder bis zur Bestätigung der Identität des Benutzers gesperrt bleibt.	**Zweck** Ohne Mechanismen zur Kontosperrung kann ein Angreifer kontinuierlich versuchen, ein Passwort durch manuelle oder automatisierte Tools (zum Beispiel Passwort-Knacken) zu erraten, bis der Angreifer erfolgreich ist und Zugriff auf das Konto eines Benutzers erhält. Wenn ein Konto gesperrt wird, weil jemand ständig versucht, ein Passwort zu erraten, verhindern Kontrollen zum Verzögern der Reaktivierung des gesperrten Kontos die böswillige Person, das Passwort zu erraten, da sie mindestens 30 Minuten unterbrechen muss, bis das Konto reaktiviert wird **Gute Praxis** Vor der Reaktivierung eines gesperrten Kontos sollte die Identität des Benutzers bestätigt werden. Zum Beispiel kann der Administrator oder das Helpdesk-Personal validieren, dass der tatsächliche Kontoinhaber eine Reaktivierung anfordert, oder es können Selbstbedienungsmechanismen zum Zurücksetzen des Passworts vorhanden sein, die der Kontoinhaber verwendet, um seine Identität zu verifizieren.
Definierte Ansatzanforderungen **8.3.5** Wenn Passwörter/Passphrasen als Authentifizierungsfaktoren verwendet werden, um Anforderung 8.3.1 zu erfüllen, sie werden für jeden Benutzer wie folgt eingestellt und neu eingestellt: • Einstellung auf einen eindeutigen Wert für die erstmalige Verwendung und bei Neueinstellung. • Muss sofort nach der ersten Verwendung geändert werden. *(Fortsetzung auf der nächsten Seite)*	**Testprozeduren mit definiertem Ansatz** **8.3.5** Prozeduren zum Einstellen und Zurücksetzen von Passwörtern/Passphrasen (falls als Authentifizierungsfaktoren verwendet, um Anforderung 8.3.1 zu erfüllen und das Sicherheitspersonal beobachten, um zu verifizieren, dass Passwörter/Passphrasen gemäß allen in dieser Anforderung angegebenen Elementen festgelegt und zurückgesetzt werden.	**Zweck** Wenn das gleiche Passwort/die gleiche Passphrase für jeden neuen Benutzer verwendet wird, kann ein interner Benutzer, ehemaliger Mitarbeiter oder eine böswillige Person den Wert kennen oder leicht entdecken und ihn verwenden, um Zugriff auf Konten zu erhalten, bevor der autorisierte Benutzer versucht, das Passwort zu verwenden.

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes		
Ein einem Benutzer zugewiesenes anfängliches oder zurückgesetztes Passwort/eine Passphrase kann nicht von einem nicht autorisierten Benutzer verwendet werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Starke Passwörter/Passphrasen können die erste Verteidigungslinie in einem Netzwerk sein, da eine böswillige Person oft zuerst versucht, Konten mit schwachen, statischen oder nicht vorhandenen Passwörtern zu finden. Wenn Passwörter kurz oder leicht zu erraten sind, ist es für eine böswillige Person relativ einfach, diese schwachen Konten zu finden und ein Netzwerk unter dem Deckmantel einer gültigen Benutzer-ID zu kompromittieren. **Gute Praxis** Die Stärke von Passwörtern/Passphrasen hängt von der Komplexität, Länge und Zufälligkeit des Passworts/der Passphrase ab. Passwörter/Passphrasen sollten ausreichend komplex sein, damit ein Angreifer ihren Wert nicht erraten oder auf andere Weise entdecken kann. Entitäten können eine Erhöhung der Komplexität erwägen, indem sie die Verwendung von Sonderzeichen und Groß- und Kleinbuchstaben zusätzlich zu den in dieser Anforderung genannten Mindeststandards vorschreiben. Zusätzliche Komplexität erhöht die Zeit, die für Offline-brutale Gewalt-Angriffe auf gehashte Passwörter/Passphrasen benötigt wird. Eine andere Möglichkeit zur Erhöhung der Widerstandsfähigkeit von Passwörtern gegen Erraten von Angriffen besteht darin, vorgeschlagene Passwörter/Passphrasen mit einer Liste mit schlechten Passwörtern zu vergleichen und Benutzer dazu zu bringen, neue Passwörter für alle in der Liste gefundenen Passwörter bereitzustellen.
8.3.6 Wenn Passwörter/Passphrasen als Authentifizierungsfaktoren verwendet werden, um Anforderung 8.3.1 zu erfüllen, erfüllen sie die folgende Mindestkomplexitätsebene: • Eine Mindestlänge von 12 Zeichen (oder wenn das System 12 Zeichen nicht unterstützt, eine Mindestlänge von acht Zeichen). • Enthält sowohl numerische als auch alphabetische Zeichen.	**8.3.6** Systemkonfigurationseinstellungen untersuchen, um zu verifizieren, dass die Parameter für die Komplexität des Benutzerpassworts/der Benutzerpassphrase gemäß allen in dieser Anforderung angegebenen Elementen festgelegt werden.	
Zielsetzung des kundenspezifischen Ansatzes Ein erratenes Passwort/eine erratene Passphrase kann weder durch einen Online- noch durch einen Offline-brutale Gewalt-Angriff verifiziert werden.		
Hinweise zur Anwendbarkeit Diese Anforderung gilt nicht für: • Benutzerkonten an Kassenterminals, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs). • Anwendungs- oder Systemkonten, die den Anforderungen in Abschnitt 8.6 unterliegen. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.* Bis zum 31. März 2025 müssen Passwörter gemäß PCI DSS v3.2.1 Anforderung 8.2.3 eine Mindestlänge von sieben Zeichen aufweisen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
8.3.7 Personen ist es nicht gestattet, ein neues Passwort/eine neue Passphrase vorzulegen, das/die mit den letzten vier verwendeten Passwörtern/Passwörtern identisch ist.	**8.3.7** Systemkonfigurationseinstellungen untersuchen, um zu verifizieren, dass Passwortparameter so eingestellt sind, um anzufordern, dass neue Passwörter/Passphrasen nicht mit den vier zuvor verwendeten Passwörtern/Passphrasen identisch sein dürfen.	Wenn die Passworthistorie nicht beibehalten wird, wird die Effektivität der Passwortänderung verringert, da frühere Kennwörter immer wieder verwendet werden können. Die Anforderung, dass Passwörter für eine bestimmte Zeitdauer nicht wiederverwendet werden können, verringert die Wahrscheinlichkeit, dass erratene oder brutal erzwungene Passwörter in Zukunft wiederverwendet werden. Passwörter oder Passphrasen wurden möglicherweise zuvor aufgrund des Verdachts einer Kompromittierung geändert oder weil das Passwort oder die Passphrase ihre effektive Nutzungsdauer überschritten hat, beides sind Gründe, warum zuvor verwendete Passwörter nicht wiederverwendet werden sollten.
Zielsetzung des kundenspezifischen Ansatzes		
Ein zuvor verwendetes Passwort kann mindestens 12 Monate lang nicht für den Zugriff auf ein Konto verwendet werden.		
Hinweise zur Anwendbarkeit		
Diese Anforderung soll nicht für Benutzerkonten an Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs).		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Kommunikation von Authentifizierungsrichtlinien und -prozeduren an alle Benutzer hilft ihnen, die Richtlinien zu verstehen und einzuhalten. **Gute Praxis** Anleitungen zur Auswahl starker Passwörter kann Vorschläge enthalten, die dem Personal helfen, schwer zu erratenden Passwörtern auszuwählen, die keine Wörter aus dem Wörterbuch oder Informationen über den Benutzer enthalten, wie die Benutzer-ID, Namen von Familienmitgliedern, Geburtsdatum usw. Anleitungen zum Schutz von Authentifizierungsfaktoren können beinhalten, Passwörter nicht aufzuschreiben oder in unsicheren Dateien zu speichern und auf böswillige Personen aufmerksam zu sein, die versuchen könnten, ihre Passwörter auszunutzen (zum Beispiel, indem Sie einen Mitarbeiter anrufen und nach seinem Passwort fragen, damit der Anrufer „ein Problem beheben“ kann). Alternativ können Entitäten Prozesse implementieren, um zu bestätigen, dass Passwörter die Passwortrichtlinien erfüllen, beispielsweise indem die Passwortauswahl mit einer Liste von nicht akzeptierbaren Passwörtern verglichen wird und Benutzer ein neues Passwort für jedes auswählen, das mit einem in der Liste übereinstimmt. Durch das Anweisen der Benutzer, Passwörter zu ändern, wenn das Passwort möglicherweise nicht mehr sicher ist, können böswillige Benutzer daran gehindert werden, ein legitimes Passwort zu verwenden, um sich nicht autorisierten Zugriff zu verschaffen.
8.3.8 Authentifizierungsrichtlinien und -prozeduren werden dokumentiert und allen Benutzern mitgeteilt, einschließlich: • Anleitungen zur Auswahl von starken Authentifizierungsfaktoren. • Anleitungen, wie Benutzer ihre Authentifizierungsfaktoren schützen sollten. • Anweisungen, zuvor verwendete Passwörter/Passphrasen nicht wiederzuverwenden. • Anweisungen zum Ändern von Passwörtern/Passphrasen bei Verdacht oder Wissen, dass das Passwort/die Passphrasen kompromittiert wurden und wie der Vorfall zu melden ist.	**8.3.8.a** Prozeduren untersuchen und das Personal befragen, um zu verifizieren, dass Authentifizierungsrichtlinien und -prozeduren an alle Benutzer verteilt werden.	
	8.3.8.b Die Authentifizierungsrichtlinien und -prozeduren, die an Benutzer verteilt werden überprüfen, und verifizieren, dass sie die in dieser Anforderung angegebenen Elemente enthalten.	
Zielsetzung des kundenspezifischen Ansatzes	**8.3.8.c** Benutzer befragen, um zu verifizieren, dass sie mit Authentifizierungsrichtlinien und -prozeduren vertraut sind.	
Benutzer kennen sich mit der richtigen Verwendung von Authentifizierungsfaktoren aus und können bei Bedarf auf Hilfe und Anleitungen zugreifen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
8.3.9 Wenn Passwörter/Passphrasen als einziger Authentifizierungsfaktor für den Benutzerzugriff verwendet werden (d. h. in einer Implementierung der Single-Faktor-Authentifizierung), dann entweder: • Passwörter/Passphrasen werden mindestens alle 90 Tage geändert, **ODER** • Die Sicherheitshaltung von Konten wird dynamisch analysiert und der Echtzeitzugriff auf Ressourcen wird entsprechend automatisch bestimmt.	**8.3.9** Wenn Passwörter/Passphrasen als einziger Authentifizierungsfaktor für den Benutzerzugriff verwendet werden, die Systemkonfigurationseinstellungen inspizieren, um zu verifizieren, dass Passwörter/Passphrasen gemäß EINEM der in dieser Anforderung angegebenen Elemente verwaltet werden.	Der Zugriff auf Komponenten im Geltungsbereich, die sich nicht in der CDE befinden, kann unter Verwendung eines einzigen Authentifizierungsfaktors bereitgestellt werden, wie beispielsweise eines Passworts/einer Passphrase, eines Token-Geräts oder einer Smartcard oder eines biometrischen Attributs. Wenn Passwörter/Passphrasen als einziger Authentifizierungsfaktor für einen solchen Zugriff verwendet werden, sind zusätzliche Kontrollen erforderlich, um die Integrität des Passworts/der Passphrase zu schützen.
Zielsetzung des kundenspezifischen Ansatzes		**Gute Praxis**
Ein unentdecktes kompromittiertes Passwort/eine unentdeckte Passphrase kann nicht auf unbestimmte Zeit verwendet werden.		Passwörter/Passphrasen, die lange Zeit ohne Änderung gültig sind, geben böswilligen Personen mehr Zeit, das Passwort/die Passphrase zu knacken. Regelmäßiges Ändern von Passwörtern bietet einer böswilligen Person weniger Zeit, ein Passwort/eine Passphrase zu knacken, und weniger Zeit, ein kompromittiertes Passwort zu verwenden. Die Verwendung eines Passworts/einer Passphrase als einziger Authentifizierungsfaktor stellt bei einer Kompromittierung eine einzelne Fehlerstelle bereit. Daher sind bei diesen Implementierungen Kontrollen erforderlich, um zu minimieren, wie lange böswillige Aktivitäten über ein kompromittiertes Passwort/eine kompromittierte Passphrase auftreten könnten. Die dynamische Analyse des Sicherheitsstatus eines Kontos ist eine weitere Option, die eine schnellere Erkennung und Reaktion auf potenziell kompromittierte Anmeldeinformationen ermöglicht.
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt für im Geltungsbereich enthaltene Systemkomponenten, die nicht in der CDE enthalten sind, da diese Komponenten nicht den MFA-Anforderungen unterliegen. Diese Anforderung soll nicht für Benutzerkonten an Kassenterminals gelten, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs). Diese Anforderung gilt nicht für Kundenkonten von Dienstleistungsanbietern, jedoch für Konten für Personal von Dienstleistungsanbietern.		*(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Eine solche Analyse erfordert eine Reihe von Datenpunkten, die Geräteintegrität, Standort, Zugriffszeiten und die Ressourcen beinhalten können, auf die zugegriffen wird, um in Echtzeit zu bestimmen, ob einem Konto Zugriff auf eine angeforderte Ressource gewährt werden kann. Auf diese Weise kann der Zugriff verweigert und Konten gesperrt werden, wenn der Verdacht besteht, dass Authentifizierungsanmeldeinformationen kompromittiert wurden. **Weitere Informationen** Informationen über die Verwendung der dynamischen Analyse zur Verwaltung des Benutzerzugriffs auf Ressourcen finden Sie unter NIST SP 800-207 Zero Trust Architecture.
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Verwendung eines Passworts/einer Passphrase als einziger Authentifizierungsfaktor stellt bei einer Kompromittierung eine einzelne Fehlerstelle bereit. Daher sind bei diesen Implementierungen Kontrollen erforderlich, um zu minimieren, wie lange böswillige Aktivitäten über ein kompromittiertes Passwort/eine kompromittierte Passphrase auftreten könnten. **Gute Praxis** Passwörter/Passphrasen, die lange Zeit ohne Änderung gültig sind, geben böswilligen Personen mehr Zeit, das Passwort/die Passphrase zu knacken. Regelmäßiges Ändern von Passwörtern bietet einer böswilligen Person weniger Zeit, ein Passwort/eine Passphrase zu knacken, und weniger Zeit, ein kompromittiertes Passwort zu verwenden.
8.3.10 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Wenn Passwörter/Passphrasen als einziger Authentifizierungsfaktor für den Kundenbenutzerzugriff auf Karteninhaberdaten verwendet werden (d. h. bei jeder Implementierung der Einzel-Faktor-Authentifizierung), werden den Kundenbenutzern Anleitungen bereitgestellt, einschließlich: • Anleitungen für Kunden, ihre Benutzerpasswörter/passphrasen regelmäßig zu ändern. • Anleitungen, wann und unter welchen Umständen Passwörter/Passphrasen geändert werden sollen.	**8.3.10** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Wenn Passwörter/Passphrasen als einziger Authentifizierungsfaktor für den Kundenbenutzerzugriff auf Karteninhaberdaten verwendet werden, die den Kundenbenutzern bereitgestellten Anleitungen untersuchen, um zu verifizieren, dass die Anleitungen alle in dieser Anforderung angegebenen Elemente enthalten.	

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes		
Passwörter/Passphrasen für Kunden von Dienstleistungsanbietern können nicht unbegrenzt verwendet werden.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. Diese Anforderung gilt nicht für Konten von Verbraucherbenutzern, die auf ihre eigenen Zahlungskarteninformationen zugreifen. Diese Anforderung für Dienstleistungsanbieter wird mit Inkrafttreten von 8.3.10.1 durch Anforderung 8.3.10.1 ersetzt.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
8.3.10.1 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Wenn Passwörter/Passphrasen als einziger Authentifizierungsfaktor für den Kunden-Benutzerzugriff verwendet werden (d. h. in einer Implementierung der Single-Faktor-Authentifizierung), dann entweder: • Passwörter/Passphrasen werden mindestens alle 90 Tage geändert, **ODER** • Die Sicherheitshaltung von Konten wird dynamisch analysiert und der Echtzeitzugriff auf Ressourcen wird entsprechend automatisch bestimmt.	**8.3.10.1** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Wenn Passwörter/Passphrasen als einziger Authentifizierungsfaktor für den Benutzerzugriff verwendet werden, die Systemkonfigurationseinstellungen inspizieren, um zu verifizieren, dass Passwörter/Passphrasen gemäß EINEM der in dieser Anforderung angegebenen Elemente verwaltet werden.	Die Verwendung eines Passworts/einer Passphrase als einziger Authentifizierungsfaktor stellt bei einer Kompromittierung eine einzelne Fehlerstelle bereit. Daher sind bei diesen Implementierungen Kontrollen erforderlich, um zu minimieren, wie lange böswillige Aktivitäten über ein kompromittiertes Passwort/eine kompromittierte Passphrase auftreten könnten. **Gute Praxis** Passwörter/Passphrasen, die lange Zeit ohne Änderung gültig sind, geben böswilligen Personen mehr Zeit, das Passwort/die Passphrase zu knacken. Regelmäßiges Ändern von Passwörtern bietet einer böswilligen Person weniger Zeit, ein Passwort/eine Passphrase zu knacken, und weniger Zeit, ein kompromittiertes Passwort zu verwenden. Die dynamische Analyse des Sicherheitsstatus eines Kontos ist eine weitere Option, die eine schnellere Erkennung und Reaktion auf potenziell kompromittierte Anmeldedaten ermöglicht. Eine solche Analyse erfordert eine Reihe von Datenpunkten, die Geräteintegrität, Standort, Zugriffszeiten und die Ressourcen beinhalten können, auf die zugegriffen wird, um in Echtzeit zu bestimmen, ob einem Konto Zugriff auf eine angeforderte Ressource gewährt werden kann. Auf diese Weise kann der Zugriff verweigert und Konten gesperrt werden, wenn der Verdacht besteht, dass Kontoanmeldedaten kompromittiert wurden. **Weitere Informationen** Informationen über die Verwendung der dynamischen Analyse zur Verwaltung des Benutzerzugriffs auf Ressourcen finden Sie unter *NIST SP 800-207 Zero Trust Architecture*.
Zielsetzung des kundenspezifischen Ansatzes		
Passwörter/Passphrasen für Kunden von Dienstleistungsanbietern können nicht unbegrenzt verwendet werden.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. Diese Anforderung gilt nicht für Konten von Verbraucherbenutzern, die auf ihre eigenen Zahlungskarteninformationen zugreifen. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.* Bis diese Anforderung am 31. März 2025 in Kraft tritt, können Dienstleistungsanbieter entweder Anforderung 8.3.10 oder 8.3.10.1 erfüllen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn mehrere Benutzer Authentifizierungsfaktoren wie Token, Smartcards und Zertifikate verwenden können, ist es möglicherweise unmöglich, die Person mithilfe des Authentifizierungsmechanismus zu identifizieren. **Gute Praxis** Durch physische und/oder logische Kontrollen (zum Beispiel eine PIN, biometrische Daten oder ein Passwort) zur eindeutigen Authentifizierung des Benutzers des Kontos wird verhindert, dass sich nicht autorisierte Benutzer durch Verwendung eines gemeinsamen Authentifizierungsfaktors Zugriff auf das Benutzerkonto verschaffen.
8.3.11 Wenn Authentifizierungsfaktoren wie physische oder logische Sicherheitstoken, Smartcards oder Zertifikate verwendet werden, dann: • werden Faktoren einem einzelnen Benutzer zugewiesen und nicht von mehreren Benutzern geteilt. • stellen physische und/oder logische Kontrollen sicher, dass nur der beabsichtigte Benutzer diesen Faktor verwenden kann, um Zugriff zu erhalten.	**8.3.11.a** Authentifizierungsrichtlinien und -prozeduren untersuchen, um zu verifizieren, dass Prozeduren zur Verwendung von Authentifizierungsfaktoren wie physische Sicherheitstoken, Smartcards und Zertifikate definiert sind und alle in dieser Anforderung angegebenen Elemente enthalten.	
	8.3.11.b Sicherheitspersonal befragen, um zu verifizieren, dass Authentifizierungsfaktoren einem einzelnen Benutzer zugewiesen werden und nicht von mehreren Benutzern geteilt werden.	
Zielsetzung des kundenspezifischen Ansatzes	**8.3.11.c** Systemkonfigurationseinstellungen, soweit zutreffend, untersuchen, und/oder physische Kontrollen beobachten, um zu verifizieren, dass Kontrollen implementiert sind, um sicherzustellen, dass nur der beabsichtigte Benutzer diesen Faktor verwenden kann, um Zugriff zu erlangen.	
Ein Authentifizierungsfaktor kann nur von dem Benutzer verwendet werden, dem er zugewiesen ist.		

Anforderungen und Testprozeduren		Anleitungen
8.4 Multi-Faktor-Authentifizierung (MFA) Die (MFA) wird implementiert, um den Zugriff auf die CDE zu sichern.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Anforderung von mehr als einem Authentifizierungsfaktor verringert die Wahrscheinlichkeit, dass ein Angreifer Zugriff auf ein System erhält, indem er sich als berechtigter Benutzer ausgibt, da der Angreifer mehrere Authentifizierungsfaktoren kompromittieren müsste. Dies gilt insbesondere in Umgebungen, in denen traditionell der einzige verwendete Authentifizierungsfaktor etwas war, das ein Benutzer kennt, wie beispielsweise ein Passwort oder eine Passphrase. **Definitionen** Die zweimalige Verwendung eines Faktors (zum Beispiel die Verwendung von zwei separaten Passwörtern) gilt nicht als Multi-Faktor-Authentifizierung.
8.4.1 MFA wird für alle Nicht-Konsolen-Zugriffe auf die CDE für Personal mit administrativem Zugriff implementiert.	**8.4.1.a** Netzwerk- und/oder Systemkonfigurationen untersuchen um zu verifizieren, dass MFA für alle Nicht-Konsolen in der CDE für Personal mit administrativem Zugriff erforderlich ist.	
	8.4.1.b Das Administratorpersonal, das sich bei der CDE anmeldet, beobachten und verifizieren, dass MFA erforderlich ist.	
Zielsetzung des kundenspezifischen Ansatzes		
Administrativer Zugriff auf die CDE kann nicht durch die Verwendung eines einzigen Authentifizierungsfaktors erhalten werden.		
Hinweise zur Anwendbarkeit		
Die Anforderung für MFA für den Nicht-Konsolen-Administratorzugriff gilt für jedes Personal mit erhöhten oder gesteigerten Rechten, die über eine Nicht-Konsolen-Verbindung auf die CDE zugreifen, d. h. über einen logischen Zugriff, der über eine Netzwerkschnittstelle statt über eine direkte, physische Verbindung erfolgt. MFA gilt als bewährte Praktik für den nicht konsolenbasierten administrativen Zugriff auf Systemkomponenten im Geltungsbereich, die nicht Teil der CDE sind.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
8.4.2 MFA ist für alle Zugriffe auf die CDE implementiert.	**8.4.2.a** Netzwerk- und/oder Systemkonfigurationen untersuchen, um zu verifizieren, dass MFA für alle Zugriffe auf die CDE implementiert ist.	Die Anforderung von mehr als einem Authentifizierungsfaktor verringert die Wahrscheinlichkeit, dass ein Angreifer Zugriff auf ein System erhält, indem er sich als berechtigter Benutzer ausgibt, da der Angreifer mehrere Authentifizierungsfaktoren kompromittieren müsste. Dies gilt insbesondere in Umgebungen, in denen traditionell der einzige verwendete Authentifizierungsfaktor etwas war, das ein Benutzer kennt, wie beispielsweise ein Passwort oder eine Passphrase.
Zielsetzung des kundenspezifischen Ansatzes	**8.4.2.b** Das Personal, das sich bei der CDE anmeldet, beobachten und Nachweis untersuchen, um zu verifizieren, dass MFA erforderlich ist.	**Definitionen**
Zugriff in bis die CDE kann nicht durch die Verwendung eines einzigen Authentifizierungsfaktors erhalten werden.		Die zweimalige Verwendung eines Faktors (zum Beispiel die Verwendung von zwei separaten Passwörtern) gilt nicht als Multi-Faktor-Authentifizierung.
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nicht für: • Anwendungs- oder Systemkonten, die automatisierte Funktionen durchführen. • Benutzerkonten an Kassenterminals, die gleichzeitig nur auf eine Kartennummer Zugriff haben, um eine einzelne Transaktion zu ermöglichen (wie von Kassierern an Kassenterminals verwendete IDs). MFA ist für beide Zugriffsarten erforderlich, die in den Anforderungen 8.4.2 und 8.4.3 angegeben sind. Daher ersetzt die Anwendung von MFA auf einen Zugriffstyp nicht die Notwendigkeit, eine andere Instanz von MFA auf den anderen Zugriffstyp anzuwenden. Wenn sich eine Person zuerst per Fernzugriff mit dem Netzwerk der Entität verbindet und später eine Verbindung zur CDE aus dem Netzwerk heraus initiiert, würde sich die Person gemäß dieser Anforderung zweimal unter *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Verwendung von MFA authentifizieren, einmal bei der Verbindung über Fernzugriff auf das Netzwerk der Entität und einmal bei der Verbindung über Nicht-Konsolen administrativen Zugriff aus dem Netzwerk der Entität in die CDE. Die MFA-Anforderungen gelten für alle Arten von Systemkomponenten, einschließlich Cloud, gehostete Systeme und lokale Anwendungen, Netzwerksicherheitsgeräte, Arbeitsstationen, Server und Endpunkte und umfassen den direkten Zugriff auf die Netzwerke oder Systeme einer Entität sowie webbasierten Zugriff auf eine Anwendung oder Funktion. MFA für den Fernzugriff auf die CDE kann auf Netzwerk- oder System-/Anwendungsebene implementiert werden; sie muss nicht auf beiden Ebenen angewendet werden. Wenn zum Beispiel MFA verwendet wird, wenn sich ein Benutzer mit dem CDE-Netzwerk verbindet, muss es nicht verwendet werden, wenn sich der Benutzer bei jedem System oder jeder Anwendung innerhalb der CDE anmeldet. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
8.4.3 MFA wird für alle Fern-Netzwerkzugriffe von außerhalb des Netzwerks der Entität, die auf die CDE zugreifen oder diese beeinflussen könnten, wie folgt implementiert: • Sämtlicher Fernzugriff durch jegliches Personal, sowohl Benutzer als auch Administratoren, der von außerhalb des Netzwerks der Entität ausgeht. • Alle Fernzugriffe durch Dritte und Anbieter.	**8.4.3.a** Netzwerk- und/oder Systemkonfigurationen für RAS-Server und -Systeme untersuchen, um zu verifizieren, dass MFA gemäß allen in dieser Anforderung angegebenen Elementen erforderlich ist.	Die Anforderung von mehr als einem Authentifizierungsfaktor verringert die Wahrscheinlichkeit, dass ein Angreifer Zugriff auf ein System erhält, indem er sich als berechtigter Benutzer ausgibt, da der Angreifer mehrere Authentifizierungsfaktoren kompromittieren müsste. Dies gilt insbesondere in Umgebungen, in denen traditionell der einzige verwendete Authentifizierungsfaktor etwas war, das ein Benutzer kennt, wie ein Passwort oder eine Passphrase.
Zielsetzung des kundenspezifischen Ansatzes	**8.4.3.b** Das Personal (zum Beispiel Benutzer und Administratoren), das sich per Fernzugriff mit dem Netzwerk verbindet, beobachten, und verifizieren, dass eine Multi-Faktor-Authentifizierung erforderlich ist.	**Definitionen**
Fernzugriff auf das Netzwerk der Entität kann nicht durch die Verwendung eines einzigen Authentifizierungsfaktors erhalten werden.		Multi-Faktor-Authentifizierung (MFA) erfordert, dass eine Person mindestens zwei der drei in Anforderung 8.3.1 angegebenen Authentifizierungsfaktoren vorlegt, bevor der Zugriff gewährt wird. Die zweimalige Verwendung eines Faktors (zum Beispiel die Verwendung von zwei separaten Passwörtern) gilt nicht als Multi-Faktor-Authentifizierung.
Hinweise zur Anwendbarkeit		
Die Anforderung an MFA für Fernzugriff von außerhalb des Netzwerks der Entität gilt für alle Benutzerkonten, die aus der Ferne auf das Netzwerk zugreifen können, wobei dieser Fernzugriff zu einem Zugriff auf die CDE führt oder führen könnte. Wenn der Fernzugriff auf einen Teil des Netzwerks der Entität erfolgt, das ordnungsgemäß von der CDE segmentiert ist, sodass Fernbenutzer nicht auf die CDE zugreifen oder diese beeinflussen können, ist MFA für den Fernzugriff auf diesen Teil des Netzwerks nicht erforderlich. MFA ist jedoch für jeden Fernzugriff auf Netzwerke mit Zugriff auf die CDE erforderlich und wird für alle Fernzugriffe auf die Netzwerke der Entität empfohlen. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Die MFA-Anforderungen gelten für alle Arten von Systemkomponenten, einschließlich Cloud, gehostete Systeme und lokale Anwendungen, Netzwerksicherheitsgeräte, Arbeitsstationen, Server und Endpunkte und umfassen den direkten Zugriff auf die Netzwerke oder Systeme einer Entität sowie webbasierten Zugriff auf eine Anwendung oder Funktion.		

Anforderungen und Testprozeduren		Anleitungen
8.5 Multi-Faktor-Authentifizierungssysteme (MFA) sind so konfiguriert, dass sie Missbrauch verhindern.		
Definierte Ansatzanforderungen **8.5.1** MFA-Systeme werden wie folgt implementiert: • Das MFA-System ist nicht für Wiederholungsangriffe anfällig. • MFA-Systeme können von Benutzern, einschließlich Administratoren, nicht umgangen werden, es sei denn, dies ist ausdrücklich dokumentiert und ausnahmsweise für einen begrenzten Zeitraum von der Verwaltung autorisiert. • Es werden mindestens zwei verschiedene Arten von Authentifizierungsfaktoren verwendet. • Der Erfolg aller Authentifizierungsfaktoren ist erforderlich, bevor der Zugriff gewährt wird.	**Testprozeduren mit definiertem Ansatz** **8.5.1.a** Anbietersystemdokumentation untersuchen, um zu verifizieren, dass das MFA-System nicht für Wiederholungsangriffe anfällig ist.	**Zweck** Schlecht konfigurierte MFA-Systeme können von Angreifern umgangen werden. Diese Anforderung adressiert daher die Konfiguration von MFA-System(en), die MFA für Benutzer bereitstellen, die auf Systemkomponenten in der CDE zugreifen. **Definitionen** Die zweimalige Verwendung einer Faktorart (zum Beispiel die Verwendung von zwei separaten Passwörtern) gilt nicht als Multi-Faktor-Authentifizierung. **Weitere Informationen** Weitere Informationen zu MFA-Systemen und -Funktionen finden Sie unter Folgendem: PCI SSC's *IInformationsergänzung*: *Anleitungen zur Multi-Faktor-Authentifizierung* PCI SSC's Häufig gestellte Fragen (FAQs) zu diesem Thema.
	8.5.1.b Systemkonfigurationen für die MFA-Implementierung untersuchen, um zu verifizieren, dass sie gemäß allen in dieser Anforderung angegebenen Elementen implementiert sind.	
	8.5.1.c Verantwortliches Personal befragen und Prozesse beobachten, um zu verifizieren, dass alle Anfragen zum Umgehen von MFA von der Verwaltung auf Ausnahmebasis für eine begrenzte Zeitdauer speziell dokumentiert und autorisiert werden.	
	8.5.1.d Personal, das sich an Systemkomponenten in der CDE anmeldet, beobachten, um zu verifizieren, dass der Zugriff erst gewährt wird, nachdem alle Authentifizierungsfaktoren erfolgreich waren.	
Zielsetzung des kundenspezifischen Ansatzes MFA-Systeme sind resistent gegen Angriffe und kontrollieren alle administrativen Überschreibungen streng.	**8.5.1.e** Personal, das sich von außerhalb des Netzwerks der Entität aus der Ferne verbindet, beobachten, um zu verifizieren, dass der Zugriff erst gewährt wird, nachdem alle Authentifizierungsfaktoren erfolgreich waren.	
Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
8.6 Die Verwendung von Anwendungs- und Systemkonten und zugeordneten Authentifizierungsfaktoren ist streng verwaltet.		
Definierte Ansatzanforderungen **8.6.1** Wenn Konten, die von Systemen oder Anwendungen verwendet werden, für die interaktive Anmeldung verwendet werden können, werden diese wie folgt verwaltet: • Interaktive Verwendung wird verhindert, es sei denn, es liegt ein außergewöhnlicher Umstand vor. • Interaktive Verwendung ist auf die für den außergewöhnlichen Umstand erforderliche Zeit beschränkt. • Die geschäftliche Rechtfertigung zur interaktiven Verwendung wird dokumentiert. • Interaktive Verwendung wird ausdrücklich von der Geschäftsleitung genehmigt. • Die individuelle Benutzeridentität wird bestätigt, bevor der Zugriff auf das Konto gewährt wird. • Jede durchgeführte Aktion ist einem einzelnen Benutzer zuzuordnen. **Zielsetzung des kundenspezifischen Ansatzes** Bei interaktiver Nutzung sind alle Aktionen mit Konten, die als System- oder Anwendungskonten gekennzeichnet sind, autorisiert und einer einzelnen Person zurechenbar. **Hinweise zur Anwendbarkeit** *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**Testprozeduren mit definiertem Ansatz** **8.6.1** Anwendungs- und Systemkonten, die interaktiv genutzt werden können, untersuchen, und das Administrationspersonal befragen, um zu verifizieren, dass Anwendungs- und Systemkonten gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Wie individuelle Benutzerkonten erfordern auch System- und Anwendungskonten Rechenschaftspflicht und eine strenge Verwaltung, um sicherzustellen, dass sie nur für den vorgesehenen Zweck verwendet und nicht missbraucht werden. Angreifer kompromittieren häufig System- oder Anwendungskonten, um Zugriff auf Karteninhaberdaten zu erhalten. **Gute Praxis** Wenn möglich, System- und Anwendungskonten so konfigurieren, dass interaktive Anmeldungen nicht zugelassen werden, um zu verhindern, dass sich nicht autorisierte Personen anmelden und das Konto mit den zugehörigen Systemberechtigungen verwenden, und um die Maschinen und Geräte einzuschränken, auf denen das Konto verwendet werden kann. **Definitionen** System- oder Anwendungskonten sind Konten, die Prozesse oder Aufgaben auf einem Computersystem oder einer Anwendung durchführen und sind normalerweise keine Konten, bei denen sich eine Person anmeldet. Diese Konten verfügen normalerweise über erhöhte Berechtigungen, die zum Ausführen spezieller Aufgaben oder Funktionen erforderlich sind. Interaktive Anmeldung ist die Möglichkeit für eine Person, sich bei einem System- oder Anwendungskonto auf die gleiche Weise wie bei einem normalen Benutzerkonto anzumelden. Die Verwendung von System- und Anwendungskonten auf diese Weise bedeutet, dass es keine Verantwortlichkeit und Nachverfolgbarkeit der vom Benutzer durchgeführten Aktionen gibt.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ein nicht ordnungsgemäßer Schutz von Passwörtern/Passphrasen, die von Anwendungs- und Systemkonten verwendet werden, insbesondere wenn diese Konten für die interaktive Anmeldung verwendet werden können, erhöht das Risiko und den Erfolg einer nicht autorisierten Verwendung dieser privilegierten Konten. **Gute Praxis** Das Ändern dieser Werte aufgrund einer vermuteten oder bestätigten Offenlegung kann besonders schwierig zu implementieren sein. Tools können sowohl die Verwaltung als auch die Sicherheit von Authentifizierungsfaktoren für Anwendungs- und Systemkonten erleichtern. Zum Beispiel, Passworttresore oder andere vom System verwaltete Kontrollen in Betracht ziehen.
8.6.2 Passwörter/Passphrasen für alle Anwendungs- und Systemkonten, die für die interaktive Anmeldung verwendet werden können, sind nicht in Skripten, Konfigurations-/Eigenschaftsdateien oder maßgeschneidertem und benutzerdefiniertem Quellcode fest codiert.	**8.6.2.a** Das Personal befragen und die Systementwicklungsverfahren untersuchen, um zu verifizieren, dass Prozesse für Anwendungs- und Systemkonten definiert sind, die für die interaktive Anmeldung verwendet werden können, und festlegen, dass Passwörter/Passphrasen nicht in Skripten, Konfigurations-/Eigenschaftsdateien oder maßgeschneiderten und benutzerdefinierten Quellcodes fest codiert sind.	
	8.6.2.b Skripte, Konfigurations-/Eigenschaftsdateien und maßgeschneiderten und benutzerdefinierten Quellcode für Anwendungs- und Systemkonten, die für die interaktive Anmeldung verwendet werden können, untersuchen, um Passwörter/Passphrasen für diese Konten zu verifizieren, sind nicht vorhanden.	
Zielsetzung des kundenspezifischen Ansatzes		
Passwörter/Passphrasen, die von Anwendungs- und Systemkonten verwendet werden, können nicht von nicht autorisiertem Personal verwendet werden.		
Hinweise zur Anwendbarkeit		
Gespeicherte Passwörter/Passphrasen müssen gemäß PCI DSS-Anforderung 8.3.2 verschlüsselt werden. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** System- und Anwendungskonten stellen ein größeres Sicherheitsrisiko dar als Benutzerkonten, da sie häufig in einem erhöhten Sicherheitskontext ausgeführt werden und Zugriff auf Systemen haben, die Benutzerkonten normalerweise nicht gewährt werden, wie programmgesteuerter Zugriff auf Datenbanken usw. Daher müssen Passwörter/Passphrasen, die für Anwendungs- und Systemkonten verwendet werden, besonders berücksichtigt werden. **Gute Praxis** Entitäten sollten die folgenden Risikofaktoren berücksichtigen, wenn sie bestimmen, wie Anwendungs- und Systempasswörter/Passphrasen gegen Missbrauch geschützt werden: • Wie sicher die Passwörter/Passphrasen gespeichert werden (zum Beispiel ob sie in einem Passwort-Tresor gespeichert sind). • Mitarbeiterfluktuation. • Die Anzahl der Personen mit Zugriff auf den Authentifizierungsfaktor. • Ob das Konto für die interaktive Anmeldung verwendet werden kann. • Ob die Sicherheitshaltung von Konten dynamisch analysiert wird, und der Echtzeitzugriff auf Ressourcen entsprechend automatisch bestimmt wird (siehe Anforderung 8.3.9). Alle diese Elementen wirken sich auf das Risikoniveau für Anwendungs- und Systemkonten aus und können sich auf die Sicherheit von Systemen auswirken, auf die über die System- und Anwendungskonten zugegriffen wird. *(Fortsetzung auf der nächsten Seite)*
8.6.3 Passwörter/Passphrasen für beliebige Anwendungs- und Systemkonten werden wie folgt gegen Missbrauch geschützt: • Passwörter/Passwörter werden regelmäßig geändert (in der Häufigkeit, die in der gezielten Risikoanalyse der Entität festgelegt ist, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird) und bei Verdacht oder Bestätigung einer Kompromittierung. • Passwörter/Passphrasen sind mit ausreichender Komplexität aufgebaut, entsprechend wie häufig die Entität die Passwörter/Passphrasen ändert.	**8.6.3.a** Richtlinien und Verfahren untersuchen, um zu verifizieren, dass Verfahren zum Schutz von Passwörtern/Passphrasen für Anwendungs- oder Systemkonten gegen Missbrauch gemäß allen in dieser Anforderung angegebenen Elementen definiert sind.	
	8.6.3.b Die gezielte Risikoanalyse der Entität zur Änderungshäufigkeit und -komplexität von Passwörtern/Passphrasen, die für die interaktive Anmeldung an Anwendungs- und Systemkonten verwendet werden, untersuchen, um zu verifizieren, dass die Risikoanalyse gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt und adressiert wurde: • Die Häufigkeit, die für regelmäßige Änderungen von Anwendungs- und Systempasswörtern/passphrasen definiert ist. • Die für Passwörter/Passphrasen definierte Komplexität und Angemessenheit der Komplexität im Verhältnis zur Häufigkeit der Änderungen.	
Zielsetzung des kundenspezifischen Ansatzes Passwörter/Passphrasen, die von Anwendungs- und Systemkonten verwendet werden, können nicht unbegrenzt verwendet werden und sind so strukturiert, dass sie Angriffen durch brutale Gewalt und Erratung widerstehen.	**8.6.3.c** Verantwortliches Personal befragen und Einstellungen zur Systemkonfiguration untersuchen, um zu verifizieren, dass Passwörter/Passphrasen für alle Anwendungs- und Systemkonten, die für die interaktive Anmeldung verwendet werden können, gemäß allen in dieser Anforderung angegebenen Elementen gegen Missbrauch geschützt sind.	
Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
		Entitäten sollten ihre gewählte Änderungshäufigkeit für Anwendungs- und Systempasswörter/Passwörter mit ihrer gewählten Komplexität für diese Passwörter/Passphrasen korrelieren – d. h. die Komplexität sollte strenger sein, wenn Passwörter/Passphrasen selten geändert werden und kann weniger streng sein, wenn sie häufiger geändert werden. Eine längere Änderungshäufigkeit ist zum Beispiel gerechtfertigt, wenn die Komplexität von Passwörtern/Passphrasen auf 36 alphanumerische Zeichen mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen eingestellt wird. Bewährte Praktiken sind, Passwortänderungen mindestens einmal im Jahr, eine Passwort-/Passphrase-Länge von mindestens 15 Zeichen und die Komplexität der Passwörter/Passphrase aus alphanumerischen Zeichen mit Groß- und Kleinbuchstaben sowie Sonderzeichen in Betracht zu ziehen. **Weitere Informationen** Informationen zur Variabilität und Gleichwertigkeit der Passwortstärke für Passwörter/Passphrasen unterschiedlicher Formate finden Sie in den Industriestandards (z. B. in der aktuellen Version der *NIST SP 800-63 Digital Identity Guidelines*).

Anforderung 9: Beschränkung des Physischen Zugriffs auf Karteninhaberdaten

Abschnitte	
9.1	Prozesse und Mechanismen zur Einschränkung des physischen Zugriffs auf Karteninhaberdaten werden definiert und verstanden.
9.2	Physische Zugriffskontrollen verwalten den Zutritt zu Einrichtungen und Systemen, die Karteninhaberdaten enthalten.
9.3	Der physische Zugriff für Personal und Besucher wird autorisiert und verwaltet.
9.4	Medien mit Karteninhaberdaten werden sicher gespeichert, darauf zugegriffen, verteilt und vernichtet.
9.5	Interaktionspunkt- (POI)-Geräte sind vor Manipulation und nicht autorisiertem Austausch geschützt.

Übersicht

Jeder physische Zugriff auf Karteninhaberdaten oder Systeme, die Karteninhaberdaten speichern, verarbeiten oder übertragen, bietet Einzelpersonen die Möglichkeit, auf Systeme oder Ausdrucke mit Karteninhaberdaten zuzugreifen und/oder diese zu entfernen; daher sollte der physische Zugriff entsprechend eingeschränkt werden.

In Anforderung 9 werden drei verschiedene Bereiche erwähnt:

1. Anforderungen, die sich speziell auf sensible Bereiche beziehen, sollen nur für diese Bereiche gelten.
2. Anforderungen, die sich speziell auf die Karteninhaberdatenumgebung (CDE) beziehen, sollen für die gesamte CDE gelten, einschließlich aller sensiblen Bereiche innerhalb der CDE.
3. Anforderungen, die sich speziell auf die Einrichtung beziehen, beziehen sich auf die Arten von Kontrollen, die im weiteren Sinne an der physischen Grenze eines Geschäftsgeländes (z. B. eines Gebäudes) verwaltet werden können, in dem sich CDEs und sensible Bereiche befinden. Diese Kontrollen finden oft außerhalb einer CDE oder eines sensiblen Bereichs statt, zum Beispiel ein Wachschalter, der Besucher identifiziert, sie mit Abzeichen versieht und sie protokolliert. Der Begriff „Einrichtung“ wird verwendet, um zu erkennen, dass diese Kontrollen an verschiedenen Stellen innerhalb einer Einrichtung vorhanden sein können, beispielsweise am Gebäudeeingang oder an einem internen Eingang zu einem Rechenzentrum oder Büroraum.

Siehe Anhang G für Definitionen von „Medien“, „Personal“, „sensible Bereiche“ und anderen PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
9.1 Prozesse und Mechanismen zur Einschränkung des physischen Zugriffs auf Karteninhaberdaten werden definiert und verstanden.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
9.1.1 Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 9 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	**9.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 9 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	Bei Anforderung 9.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 9 angegeben sind. Während es wichtig ist, die in Anforderung 9 genannten spezifischen Richtlinien oder Verfahren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Prozeduren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Verfahren und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen. Richtlinien und Prozeduren, einschließlich Aktualisierungen, werden jeglichem betroffenen Personal aktiv mitgeteilt und durch Betriebsprozeduren unterstützt, die beschreiben, wie Aktivitäten durchgeführt werden.
Zielsetzung des kundenspezifischen Ansatzes		
Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 9 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht der Verwaltung.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen sind, ist das Personal sich möglicherweise seiner täglichen Verantwortlichkeiten nicht bewusst und kritische Aktivitäten können nicht stattfinden. **Gute Praxis** Rollen und Verantwortlichkeiten können in Richtlinien und Verfahren dokumentiert oder in separaten Dokumenten gewartet werden. Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen. Ein Verfahren zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).
9.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 9 werden dokumentiert, zugewiesen und verstanden.	**9.1.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 9 dokumentiert und zugewiesen sind.	
	9.1.2.b Personal mit Verantwortlichkeit zur Durchführung von Aktivitäten in Anforderung 9 befragen, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 9 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
9.2 Physische Zugriffskontrollen verwalten den Zutritt zu Einrichtungen und Systemen, die Karteninhaberdaten enthalten.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ohne physische Zugangskontrollen könnten nicht autorisierte Personen möglicherweise Zugriff auf die CDE und sensible Informationen erlangen oder Systemkonfigurationen ändern, Schwachstellen in das Netzwerk einführen oder Geräte vernichten oder stehlen. Der Zweck dieser Anforderung besteht daher darin, dass der physische Zugriff auf die CDE über physische Sicherheitskontrollen wie Abzeichenleser oder andere Mechanismen wie Schloss und Schlüssel kontrolliert wird. **Gute Praxis** Welcher Mechanismus diese Anforderung auch immer erfüllt, es muss für die Organisation ausreichen, um zu verifizieren, dass nur autorisiertem Personal der Zugriff gewährt wird. **Beispiele** Die Zugangskontrollen zu den Einrichtungen umfassen physische Sicherheitskontrollen in jedem Computerraum, Rechenzentrum und anderen physischen Bereichen mit Systemen in der CDE. Es kann auch Abzeichenleser oder andere Geräte umfassen, die physische Zugangskontrollen verwalten, wie beispielsweise Schloss und Schlüssel mit einer aktuellen Liste aller Personen, die die Schlüssel besitzen.
9.2.1 Geeignete Zugangskontrollen für Einrichtungen sind vorhanden, um den physischen Zugriff auf Systeme in der CDE einzuschränken.	**9.2.1** Eintrittskontrollen beobachten und verantwortliches Personal befragen, um zu verifizieren, dass physische Sicherheitskontrollen vorhanden sind, um den Zugriff auf Systeme in der CDE einzuschränken.	
Zielsetzung des kundenspezifischen Ansatzes		
Auf Systemkomponenten in der CDE kann von nicht autorisiertem Personal nicht physisch zugegriffen werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Beibehaltung von Details zu Personen, die sensible Bereiche betreten und verlassen, kann bei Untersuchungen von physischen Verstößen helfen, indem Personen identifiziert werden, die auf die sensiblen Bereiche physisch zugingen, und wann sie diese betreten und verlassen hatten. **Gute Praxis** Welcher Mechanismus diese Anforderung auch immer erfüllt, er sollte alle Ein- und Austrittspunkte in sensible Gebiete wirksam überwachen. Kriminelle, die versuchen, sich physischen Zugriff auf sensible Bereiche zu verschaffen, versuchen häufig, die Überwachungskontrollen zu deaktivieren oder zu umgehen. Um diese Kontrollen vor Manipulation zu schützen, könnten Videokameras so positioniert werden, dass sie außer Reichweite sind und/oder überwacht werden, um Manipulationen zu erkennen. In ähnlicher Weise könnten physische Zugangskontrollmechanismen überwacht werden oder physische Schutzvorrichtungen installiert sein, um zu verhindern, dass sie durch böswillige Personen beschädigt oder deaktiviert werden.
9.2.1.1 Der individuelle physische Zugang zu sensiblen Bereichen innerhalb der CDE wird entweder mit Videokameras oder physischen Zugangskontrollmechanismen (oder beidem) wie folgt überwacht: • Ein- und Austrittspunkte zu/aus sensiblen Bereichen innerhalb der CDE werden überwacht. • Überwachungsgeräte oder -mechanismen sind vor Manipulation oder Deaktivierung geschützt. • Gesammelte Daten werden überprüft und mit anderen Einträgen korreliert. • Gesammelte Daten werden für mindestens drei Monate gespeichert, sofern nicht anders gesetzlich eingeschränkt.	**9.2.1.1.a** Standorte beobachten, wo individuelle physische Zugangspunkte zu sensiblen Bereichen innerhalb der CDE stattfinden, um zu verifizieren, dass entweder Videokameras oder physische Zugangskontrollmechanismen (oder beides) vorhanden sind, um die Ein- und Austrittspunkte zu überwachen. **9.2.1.1.b** Standorte beobachten, wo individuelle physische Zugangspunkte zu sensiblen Bereichen innerhalb der CDE stattfinden, um zu verifizieren, dass entweder Videokameras oder physische Zugangskontrollmechanismen (oder beides) vor Manipulation oder Deaktivierung geschützt sind. **9.2.1.1.c** Die physischen Zugangskontrollmechanismen beobachten und/oder Videokameras untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass: • Gesammelte Daten von Videokameras und/oder physischen Zugangskontrollmechanismen überprüft und mit anderen Einträgen korreliert werden. • Gesammelte Daten für mindestens drei Monate gespeichert werden.	
Zielsetzung des kundenspezifischen Ansatzes Es werden vertrauenswürdige, verifizierbare Aufzeichnungen über das physische Betreten und Verlassen von sensiblen Bereichen geführt.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **9.2.2** Physische und/oder logische Kontrollen werden implementiert, um die Verwendung von öffentlich zugänglichen Netzwerkbuchsen innerhalb der Einrichtung einzuschränken. **Zielsetzung des kundenspezifischen Ansatzes** Nicht autorisierte Geräte können sich aus öffentlichen Bereichen innerhalb der Einrichtung nicht mit dem Netzwerk der Entität verbinden.	**Testprozeduren mit definiertem Ansatz** **9.2.2** Verantwortliches Personal befragen und die Standorte von öffentlich zugänglichen Netzwerkbuchsen beobachten, um zu verifizieren, dass physische und/oder logische Kontrollen vorhanden sind, um den Zugriff auf öffentlich zugängliche Netzwerkbuchsen innerhalb der Einrichtung zu beschränken.	**Zweck** Das Einschränken des Zugriffs auf Netzwerkbuchsen (oder Netzwerkports) verhindert, dass böswillige Personen sich in leicht verfügbare Netzwerkbuchsen einstecken und Zugriff auf die CDE oder auf an die CDE angeschlossene Systeme erhalten. **Gute Praxis** Unabhängig davon, ob logische oder physische Kontrollen oder eine Kombination aus beiden verwendet werden, sollten sie verhindern, dass eine Person oder ein Gerät, das nicht ausdrücklich autorisiert ist, sich mit dem Netzwerk verbinden kann. **Beispiele** Methoden, um diese Anforderung zu erfüllen, beinhalten Netzwerkbuchsen, die sich in öffentlichen Bereichen befinden, und Bereiche, die für Besucher zugänglich sind, könnten deaktiviert und nur aktiviert werden, wenn der Netzwerkzugriff ausdrücklich autorisiert ist. Alternativ könnten Prozesse implementiert werden, die sicherstellen, dass Besucher jederzeit in Bereichen mit aktiven Netzwerkbuchsen eskortiert werden.
Definierte Ansatzanforderungen **9.2.3** Der physische Zugriff auf drahtlose Zugriffspunkten, Gateways, Netzwerk-/Kommunikationshardware und Telekommunikationsleitungen innerhalb der Einrichtung ist eingeschränkt.	**Testprozeduren mit definiertem Ansatz** **9.2.3** Verantwortliches Personal befragen und Standorte von Hardware beobachten, um zu verifizieren, dass der physische Zugriff auf drahtlose Zugriffspunkten, Gateways, Netzwerk-/Kommunikationshardware und Telekommunikationsleitungen innerhalb der Einrichtung eingeschränkt ist.	**Zweck** Ohne angemessene physische Sicherheit beim Zugriff auf drahtlose Komponenten und Geräte sowie Computernetzwerk- und Telekommunikationsgeräte und -leitungen könnten böswillige Benutzer Zugriff auf die Netzwerkressourcen der Entität erlangen. Zusätzlich könnten sie ihre eigenen Geräte mit dem Netzwerk verbinden, um nicht autorisierten Zugriff auf die CDE oder mit der CDE verbundene Systeme zu erhalten. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Physische Netzwerkgeräte sind für nicht autorisiertes Personal nicht zugänglich.		Zusätzlich verhindert die Sicherung der Netzwerk- und Kommunikationshardware, dass böswillige Benutzer den Netzwerkverkehr abfangen oder ihre eigenen Geräte physisch mit kabelgebundenen Netzwerkressourcen verbinden.
Definierte Ansatzanforderungen **9.2.4** Der Zugang zu Konsolen in sensiblen Bereichen ist bei Nichtverwendung durch eine Sperre eingeschränkt. **Zielsetzung des kundenspezifischen Ansatzes** Physische Konsolen in sensiblen Bereichen sind für nicht autorisiertes Personal nicht zugänglich.	**Testprozeduren mit definiertem Ansatz** **9.2.4** Den Versuch eines Systemadministrators, sich in sensiblen Bereichen bei Konsolen anzumelden, beobachten, und verifizieren, dass diese „gesperrt“ sind, um eine nicht autorisierte Verwendung zu verhindern.	**Zweck** Das Sperren von Konsolen-Anmeldebildschirmen verhindert, dass nicht autorisierte Personen Zugriff auf sensible Informationen erhalten, Systemkonfigurationen ändern, Schwachstellen in das Netzwerk einführen oder Aufzeichnungen vernichten.

Anforderungen und Testprozeduren		Anleitungen
9.3 Der physische Zugriff für Personal und Besucher wird autorisiert und verwaltet.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Durch die Etablierung von Verfahren zum Gewähren, Verwalten und Entfernen des Zugriffs, wenn dieser nicht mehr benötigt wird, wird sichergestellt, dass nicht autorisierte Personen keinen Zugriff auf Bereiche mit Karteninhaberdaten erhalten. Darüber hinaus ist es wichtig, den Zugriff auf das eigentliche Abzeichensystem und die Abzeichenmaterialien zu beschränken, um zu verhindern, dass nicht autorisiertes Personal eigene Abzeichen erstellt und/oder eigene Zugriffsregeln aufstellt. **Gute Praxis** Es ist wichtig, das physisch anwesende Personal visuell zu identifizieren und ob es sich um einen Besucher oder einen Mitarbeiter handelt. **Beispiele** Eine Möglichkeit, Personal zu identifizieren, besteht darin, ihnen Abzeichen zuzuweisen.
9.3.1 Es werden Prozeduren zur Autorisierung und Verwaltung des physischen Zugriffs von Personal auf die CDE implementiert, einschließlich: • Identifizierung von Personal. • Verwaltung von Änderungen der physischen Zugriffsanforderungen einer Person. • Widerruf oder Beendigung der Personalidentifizierung. • Beschränkung des Zugriffs auf den Identifizierungsprozess oder -system auf autorisiertes Personal.	**9.3.1.a** Dokumentierte Prozeduren untersuchen, um zu verifizieren, dass Prozeduren für die Autorisierung und Verwaltung des physischen Zugangs von Personal zur CDE gemäß allen in dieser Anforderung angegebenen Elementen definiert sind.	
	9.3.1.b Identifizierungsmethoden, wie ID-Abzeichen beobachten, und Prozesse beobachten, um zu verifizieren, dass das Personal in der CDE eindeutig identifiziert wird.	
Zielsetzung des kundenspezifischen Ansatzes	**9.3.1.c** Prozesse beobachten, um zu verifizieren, der Zugriff auf den Identifizierungsprozess, wie ein Abzeichensystem, auf autorisiertes Personal beschränkt ist.	
Anforderungen für den Zugriff auf die physische CDE werden definiert und durchgesetzt, um Personal zu identifizieren und zu autorisieren.		

<table>
<tr><th colspan="2">Anforderungen und Testprozeduren</th><th>Anleitungen</th></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="5">Zweck
Die Kontrolle des physischen Zugangs auf sensible Bereiche hilft dabei, dass nur autorisiertes Personal mit legitimen geschäftlichen Anforderungen Zugang erhält.
Gute Praxis
Nach Möglichkeit sollten Organisationen über Richtlinien und Prozeduren verfügen, um sicherzustellen, dass alle physischen Zugangsmechanismen vor dem Verlassen der Organisation so schnell wie möglich nach ihrem Abgang zurückgegeben oder deaktiviert werden. Dadurch wird sichergestellt, dass das Personal nach Beendigung des Beschäftigungsverhältnisses keinen physischen Zugang zu sensiblen Bereichen erhält.</td></tr>
<tr><td rowspan="3">9.3.1.1 Der physische Zugang zu sensiblen Bereichen innerhalb des CDE für das Personal wird wie folgt kontrolliert:
• Der Zugang ist autorisiert und basiert auf der individuellen Jobfunktion.
• Der Zugang wird nach Beendigung sofort entzogen.
• Alle physischen Zugangsmechanismen wie Schlüssel, Zugangskarten usw. werden bei Beendigung zurückgegeben oder deaktiviert.</td><td>9.3.1.1.a Personal in sensiblen Bereichen innerhalb der CDE beobachten, verantwortliches Personal befragen und physische Zugangskontrolllisten untersuchen, um zu verifizieren, dass:
• Der Zugang zum sensiblen Bereich autorisiert ist.
• Der Zugang für die berufliche Funktion der Person erforderlich ist.</td></tr>
<tr><td>9.3.1.1.b Prozesse beobachten und Personal befragen, um zu verifizieren, dass der Zugang von allem Personal bei Kündigung sofort entzogen wird.</td></tr>
<tr><td>9.3.1.1.c Bei gekündigtem Personal, physische Zugangskontrolllisten untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass alle physischen Zugangssmechanismen (wie Schlüssel, Zugangskarten usw.) zurückgegeben oder deaktiviert wurden.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes</td><td></td></tr>
<tr><td>Sensible Bereiche sind für nicht autorisiertes Personal nicht zugänglich.</td><td></td></tr>
</table>

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Besucherkontrollen sind wichtig, um die Möglichkeit von nicht autorisierten und böswilligen Personen zu verringern, Zugriff auf Einrichtungen und möglicherweise auf Karteninhaberdaten zu erhalten. Besucherkontrollen stellen sicher, dass Besucher als Besucher identifiziert werden können, damit das Personal ihre Aktivitäten überwachen kann, und dass ihr Zugang nur für die Dauer ihres rechtmäßigen Besuchs beschränkt ist.
9.3.2 Es werden Prozeduren zur Autorisierung und Verwaltung von Besucherzugriffs auf die CDE implementiert, einschließlich: • Besucher werden vor dem Betreten autorisiert. • Besucher werden jederzeit begleitet. • Besucher werden eindeutig identifiziert und erhalten ein Abzeichen oder eine andere Identifizierung, die abläuft. • Besucherabzeichen oder andere Identifizierungsmerkmale unterscheiden Besucher sichtbar vom Personal.	**9.3.2.a** Dokumentierte Prozeduren untersuchen und das Personal befragen, um zu verifizieren, dass Prozeduren für die Autorisierung und Verwaltung des Besucherzugangs zur CDE gemäß allen in dieser Anforderung angegebenen Elementen definiert sind.	
	9.3.2.b Prozesse beobachten, wenn Besucher in der CDE anwesend sind und das Personal befragen, um zu verifizieren, dass Besucher: • Vor dem Betreten der CDE autorisiert sind. • Zu jeder Zeit innerhalb der CDE begleitet werden.	
	9.3.2.c Die Verwendung von Besucherabzeichen oder anderen Identifizierungsmerkmalen beobachten, um zu verifizieren, dass das Abzeichen oder andere Identifizierungen keinen unbegleiteten Zugang zu der CDE ermöglichen.	
	9.3.2.d Besucher in der CDE beobachten, um Folgendes zu verifizieren: • Besucherabzeichen oder andere Identifizierungsmerkmale werden für alle Besucher verwendet. • Besucherabzeichen oder Identifizierungsmerkmale unterscheiden Besucher sichtbar vom Personal.	
Zielsetzung des kundenspezifischen Ansatzes Die Anforderungen für den Besucherzugriff auf CDE werden definiert und durchgesetzt. Besucher dürfen den autorisierten physischen Zugang nicht überschreiten, während sie sich in der CDE befinden.	**9.3.2.e** Besucherabzeichen oder andere Identifizierungen untersuchen und Beweise im Abzeichensystem beobachten, um zu verifizieren, ob Besucherausweise oder andere Identifizierungen ablaufen.	

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **9.3.3** Besucherabzeichen oder -identifizierungen werden vor Verlassen der Anlage oder zum Ablaufdatum abgegeben bzw. deaktiviert. **Zielsetzung des kundenspezifischen Ansatzes** Besucheridentifizierung oder Abzeichen können nach Ablauf nicht wiederverwendet werden.	**Testprozeduren mit definiertem Ansatz** **9.3.3** Besucher, die die Einrichtung verlassen, beobachten und Personal befragen, um zu verifizieren, dass Besucherabzeichen oder andere Identifizierungen vor Verlassen der Einrichtung oder zum Ablaufdatum abgegeben oder deaktiviert werden. bei Abgang oder Ablauf.	**Zweck** Die Sicherstellung der Rückgabe oder Deaktivierung von Besucherabzeichen nach Ablauf oder Abschluss des Besuchs verhindert, dass sich böswillige Personen nach Beendigung des Besuchs mit einem zuvor autorisierten Ausweis physischen Zugang zum Gebäude verschaffen.
Definierte Ansatzanforderungen **9.3.4** Ein Besucherprotokoll wird verwendet, um eine physische Aufzeichnung der Besucheraktivitäten innerhalb der Einrichtung und in sensiblen Bereichen zu führen, einschließlich: • Den Namen des Besuchers und die vertretene Organisation. • Datum und Uhrzeit des Besuchs. • Der Name des Personals, das den physischen Zugang autorisiert. • Aufbewahrung des Protokolls für mindestens drei Monate, sofern nicht anders gesetzlich eingeschränkt. **Zielsetzung des kundenspezifischen Ansatzes** Es werden Aufzeichnungen über Besucherzugriffe geführt, die die Identifizierung von Personen ermöglichen.	**Testprozeduren mit definiertem Ansatz** **9.3.4.a** Das Besucherprotokoll untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass ein Besucherprotokoll verwendet wird, um den physischen Zugang zur Einrichtung und zu sensiblen Bereichen aufzuzeichnen. **9.3.4.b** Das Besucherprotokoll untersuchen und verifizieren, dass das Protokoll Folgendes enthält: • Den Namen des Besuchers und die vertretene Organisation. • Das Personal, das den physischen Zugang autorisiert. • Datum und Zeit des Besuchs. **9.3.4.c** Speicherorte des Besucherprotokolls untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass das Protokoll mindestens drei Monate aufbewahrt wird, soweit gesetzlich nichts anderes eingeschränkt ist.	**Zweck** Ein Besucherprotokoll, das minimale Informationen über den Besucher dokumentiert, kann einfach und kostengünstig gewartet werden. Es hilft bei der Identifizierung des historischen physischen Zugangs zu einem Gebäude oder Raum und des potenziellen Zugriffs auf Karteninhaberdaten. **Gute Praxis** Bei der Protokollierung von Datum und Uhrzeit des Besuchs wird die Einbeziehung sowohl der Eintritts- als auch der Austrittszeiten als bewährte Praktik angesehen, da sie hilfreiche Verfolgungsinformationen liefert und die Gewissheit bietet, dass ein Besucher am Ende des Tages gegangen ist. Es ist auch gut, um zu verifizieren, dass eine Besucher-ID (Führerschein usw.) mit dem Namen übereinstimmt, den er im Besucherprotokoll eingetragen hat.

Anforderungen und Testprozeduren		Anleitungen
9.4 Medien mit Karteninhaberdaten werden sicher gespeichert, darauf zugegriffen, verteilt und vernichtet.		
Definierte Ansatzanforderungen **9.4.1** Alle Medien mit Krateninhaberdaten warden physich gesichert. **Zielsetzung des kundenspezifischen Ansatzes** Auf Medien mit Karteninhaberdaten kann von nicht autorisiertem Personal nicht zugegriffen werden.	**Testprozeduren mit definiertem Ansatz** **9.4.1.** Dokumentation untersuchen, um zu verifizieren, dass die Prozeduren, die zum Schutz der Karteninhaberdaten definiert sind, Kontrollen zum physischen Sichern aller Medien einschließen.	**Zweck** Kontrollen zur physischen Sicherung von Medien sollen verhindern, dass nicht autorisierte Personen Zugriff auf Karteninhaberdaten auf irgendwelchen Medien erhalten. Karteninhaberdaten sind für nicht autorisiertes Ansehen, Kopieren oder Scannen anfällig, wenn sie ungeschützt auf entfernbaren oder tragbaren Medien gespeichert, ausgedruckt oder auf dem Schreibtisch einer anderen Person liegen bleiben.
9.4.1.1 Offline-Medien-Backups mit Karteninhaberdaten werden an einem sicheren Ort gespeichert. **Zielsetzung des kundenspezifischen Ansatzes** Nicht autorisiertes Personal kann nicht auf Offline Backups zugreifen.	**9.4.1.1.a** Dokumentation untersuchen, um zu verifizieren, ob Prozeduren für die physische Sicherung von Offline-Medien-Backups mit Karteninhaberdaten an einem sicheren Ort definiert sind. **9.4.1.1.b** Protokolle oder andere Dokumentation untersuchen und das verantwortliche Personal am Speicherort befragen, um zu verifizieren, dass Offline-Medien-Backups an einem sicheren Ort gespeichert sind.	**Zweck** Wenn sie in einer ungesicherten Einrichtung gespeichert werden, können Backups, die Karteninhaberdaten enthalten, leicht verloren gehen, gestohlen oder aus böswilligen Absichten kopiert werden. **Gute Praxis** Für die sichere Speicherung von Backup-Medien ist es eine gute Praxis, Medien in einer externen Einrichtung zu speichern, wie einem alternativen oder Backup-Standort oder einer kommerziellen Speichereinrichtung.
Definierte Ansatzanforderungen **9.4.1.2** Die Sicherheit des/der Offline-Medien-Backup-Standorte(s) mit Karteninhaberdaten wird mindestens alle 12 Monate überprüft.	**Testprozeduren mit definiertem Ansatz** **9.4.1.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass Prozeduren zur Überprüfung der Sicherheit der Offline-Medien-Backup-Standorte(n) mit Karteninhaberdaten mindestens alle 12 Monate definiert sind. **9.4.1.2.b** Dokumentierte Verfahren, Protokolle oder andere Dokumentation untersuchen und verantwortliches Personal an dem/den Speicherort(en) befragen, um zu verifizieren, dass die Sicherheit des Speicherorts mindestens alle 12 Monate überprüft wird.	**Zweck** Durch die Durchführung regelmäßiger Überprüfungen der Speichereinrichtung kann die Organisation identifizierte Sicherheitsprobleme umgehend adressieren und das potenzielle Risiko minimieren. Es ist wichtig, dass sich die Entität der Sicherheit des Bereichs bewusst ist, in dem Medien gespeichert werden.

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Die Sicherheitskontrollen, die Offline-Backups schützen, werden regelmäßig durch Inspektionen verifiziert.		
Definierte Ansatzanforderungen **9.4.2** Alle Medien mit Karteninhaberdaten werden gemäß der Sensibilität der Daten klassifiziert.	**Testprozeduren mit definiertem Ansatz** **9.4.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass Prozeduren zur Klassifizierung von Medien mit Karteninhaberdaten entsprechend der Sensibilität der Daten definiert sind.	**Zweck** Als vertraulich identifizierte Medien sind möglicherweise nicht angemessen geschützt oder können verloren gehen oder gestohlen werden. **Gute Praxis** Es ist wichtig, dass Medien so identifiziert werden, dass ihr Klassifizierungsstatus ersichtlich ist. Dies bedeutet aber nicht, dass die Medien ein „vertrauliches“ Etikett haben müssen.
	9.4.2.b Medienprotokolle oder andere Dokumentationen untersuchen, um zu verifizieren, dass alle Medien entsprechend der Sensibilität der Daten klassifiziert werden.	
Zielsetzung des kundenspezifischen Ansatzes Medien werden entsprechend klassifiziert und geschützt.		
Definierte Ansatzanforderungen **9.4.3** Außerhalb der Einrichtung versendete Medien mit Karteninhaberdaten werden wie folgt gesichert: • Außerhalb der Einrichtung gesendete Medien werden protokolliert. • Die Medien werden per gesichertem Kurier oder einer anderen Zustellmethode versandt, die genau nachverfolgt werden kann. • Offsite-Verfolgungs-Protokolle enthalten Details zum Medienstandort.	**Testprozeduren mit definiertem Ansatz** **9.4.3.a** Die Dokumentation untersuchen, um zu verifizieren, dass Prozeduren zur Sicherung von Medien definiert sind, die außerhalb der Einrichtung gemäß allen in dieser Anforderung angegebenen Elementen versandt werden.	**Zweck** Medien können verloren gehen oder gestohlen werden, wenn sie auf einem nicht nachverfolgbaren Weg, wie zum Beispiel per Post, versendet werden. Die Verwendung sicherer Kuriere zur Zustellung von Medien, die Karteninhaberdaten enthalten, ermöglicht es Organisationen, ihre Sendungsverfolgungssysteme zu verwenden, um den Bestand und den Standort von Sendungen zu verwalten.
	9.4.3.b Das Personal befragen und die Aufzeichnungen untersuchen, um zu verifizieren, dass alle Medien, die außerhalb der Einrichtung gesendet werden, protokolliert und über einen gesicherten Kurierdienst oder eine andere nachverfolgbare Zustellmethode gesendet werden.	
Zielsetzung des kundenspezifischen Ansatzes Medien werden beim Transport außerhalb der Einrichtung gesichert und verfolgt.	**9.4.3.c** Offsite-Verfolgungs-Protokolle für alle Medien untersuchen, um zu verifizieren, dass die Verfolgungs-Details dokumentiert werden.	

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **9.4.4** Das Management genehmigt alle Medien mit Karteninhaberdaten, die außerhalb der Einrichtung bewegt werden (einschließlich der Verteilung von Medien an Personen). **Zielsetzung des kundenspezifischen Ansatzes** Medien dürfen eine Einrichtung nicht ohne die Zustimmung des verantwortlichen Personals verlassen. **Hinweise zur Anwendbarkeit** Personen, die Medienbewegungen genehmigen, sollten über die entsprechende Verwaltungsautorität verfügen, um diese Genehmigung zu gewähren. Es ist jedoch nicht ausdrücklich erforderlich, dass diese Personen „Verwalter“ als Teil ihres Titels haben.	**Testprozeduren mit definiertem Ansatz** **9.4.4.a** Die Dokumentation untersuchen, um zu verifizieren, dass Verfahren definiert sind, um sicherzustellen, dass Medien, die außerhalb der Einrichtung bewegt werden, von der Verwaltung genehmigt werden. **9.4.4.b** Offsite Medienverfolgungsprotokolle untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass für alle Medien, die außerhalb der Einrichtung bewegt werden (einschließlich Medien, die an Personen verteilt werden), eine ordnungsgemäße Verwaltungsautorisierung eingeholt wurde.	**Zweck** Ohne eine feste Prozedur, um sicherzustellen, dass alle Medienbewegungen genehmigt werden, bevor die Medien aus sicheren Bereichen entfernt werden, würden die Medien nicht verfolgt oder angemessen geschützt, und ihr Standort wäre unbekannt, was zu Verlust oder Diebstahl von Medien führen würde.
Definierte Ansatzanforderungen **9.4.5** Inventurprotokolle aller elektronischen Medien mit Karteninhaberdaten werden geführt. **Zielsetzung des kundenspezifischen Ansatzes** Es werden genaue Inventuren der gespeicherten elektronischen Medien geführt.	**Testprozeduren mit definiertem Ansatz** **9.4.5.a** Dokumentation untersuchen, um zu verifizieren, dass Verfahren definiert sind, um elektronische Medieninventurprotokolle zu führen. **9.4.5.b** Elektronische Medieninventurprotokolle untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass Protokolle geführt werden.	**Zweck** Ohne sorgfältige Inventurmethoden und Speicherkontrollen könnten gestohlene oder fehlende elektronische Medien auf unbestimmte Zeit unbemerkt bleiben.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ohne sorgfältige Inventurmethoden und Speicherkontrollen könnten gestohlene oder fehlende elektronische Medien auf unbestimmte Zeit unbemerkt bleiben.
9.4.5.1 Inventuren elektronischer Medien mit Karteninhaberdaten werden mindestens alle 12 Monate durchgeführt.	**9.4.5.1.a** Die Dokumentation untersuchen, um zu verifizieren, dass Prozeduren definiert sind, um mindestens alle 12 Monate Inventuren elektronischer Medien mit Karteninhaberdaten durchzuführen.	
	9.4.5.1.b Die Inventurprotokolle der elektronischen Medien untersuchen und das Personal befragen, um zu verifizieren, dass Inventuren der elektronischen Medien mindestens alle 12 Monate durchgeführt werden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die Medieninventuren werden regelmäßig verifiziert.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn keine Maßnahmen ergriffen werden, um die auf den gedruckten Medien enthaltenen Informationen vor der Entsorgung zu vernichten, können böswillige Personen Informationen von den entsorgten Medien abrufen, was zu einer Datenkompromittierung führt. Zum Beispiel können böswillige Personen eine als „Dumpster Diving“ bekannte Technik verwenden, bei der sie Mülleimer und Papierkörbe durchsuchen, um nach gedruckten Materialien mit Informationen zu suchen, mit denen sie einen Angriff starten können. Die Sicherung von Speichercontainern für zu vernichtende Materialien verhindert, dass sensible Informationen während der Materialsammlung erfasst werden. **Gute Praxis** Betrachten Sie „zu zerkleinernde“ Container mit einem Schloss, das den Zugang zu seinem Inhalt oder den Zugang zum Inneren des Containers physisch verhindert. **Weitere Informationen** Siehe *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*
9.4.6 Gedruckte Materialien mit Karteninhaberdaten werden, wenn sie aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, wie folgt vernichtet: • Die Materialien werden quergeschnitten, zerkleinert, verbrannt oder eingestampft, sodass Karteninhaberdaten nicht rekonstruiert werden können. • Materialien werden vor der Vernichtung in sicheren Speichercontainern gespeichert.	**9.4.6.a** Die Richtlinie zur regelmäßigen Medienvernichtung untersuchen, um zu verifizieren, dass Prozeduren zur Vernichtung gedruckter Medien mit Karteninhaberdaten definiert sind, die aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, gemäß allen in dieser Anforderung angegebenen Elementen.	
	9.4.6.b Prozesse beobachten und das Personal befragen, um zu verifizieren, dass gedruckte Materialien quergeschnitten, verbrannt oder eingestampft werden, sodass Karteninhaberdaten nicht rekonstruiert werden können.	
	9.4.6.c Speichercontainer, die für Materialien verwendet werden, die zu vernichtende Informationen enthalten, beobachten, um zu verifizieren, dass die Container sicher sind.	
Zielsetzung des kundenspezifischen Ansatzes Karteninhaberdaten können von vernichteten Medien, oder die zur Vernichtung anstehen, nicht wiederhergestellt werden.		
Hinweise zur Anwendbarkeit Diese Anforderungen an die Vernichtung von Medien, wenn diese Medien aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, sind getrennt und unterscheiden sich von PCI DSS-Anforderung 3.2.1, die das sichere Löschen von Karteninhaberdaten betrifft, wenn sie gemäß den Karteninhaberdaten-Aufbewahrungsrichtlinien der Entität nicht mehr benötigt werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn keine Maßnahmen ergriffen werden, um die auf den elektronischen Medien enthaltenen Informationen zu vernichten, wenn sie nicht mehr benötigt werden, können böswillige Personen Informationen von den entsorgten Medien abrufen, was zu einer Datenkompromittierung führt Zum Beispiel können böswillige Personen eine als „Dumpster Diving“ bekannte Technik verwenden, bei der sie Mülleimer und Papierkörbe durchsuchen, um nach Informationen zu suchen, mit denen sie einen Angriff starten können. **Gute Praxis** Die Löschfunktion in den meisten Betriebssystemen ermöglicht Wiederherstellung gelöschter Daten, stattdessen sollte eine dedizierte sichere Löschfunktion oder Anwendung verwendet werden, um Daten nicht wiederherstellbar zu machen. **Beispiele** Methoden zum sicheren Vernichten elektronischer Medien umfassen sicheres Löschen gemäß branchenüblichen Standards für sicheres Löschen, Entmagnetisieren oder physische Vernichtung (wie das Schleifen oder die Zerkleinerung von Festplatten). **Weitere Informationen** Siehe *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization*
9.4.7 Elektronische Medien mit Karteninhaberdaten werden, wenn sie aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, auf eine der folgenden Weisen vernichtet: • Die elektronischen Medien werden vernichtet. • Die Karteninhaberdaten werden unwiederbringlich gemacht, sodass sie nicht rekonstruiert werden können.	**9.4.7.a** Die Richtlinie zur regelmäßigen Medienvernichtung untersuchen, um zu verifizieren, dass Prozeduren zur Vernichtung elektronischer Medien definiert sind, die aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, gemäß allen in dieser Anforderung angegebenen Elementen.	
Zielsetzung des kundenspezifischen Ansatzes Karteninhaberdaten können von gelöschten oder vernichteten Medien nicht wiederhergestellt werden.	**9.4.7.b** Den Medienvernichtungsprozess beobachten und das verantwortliche Personal befragen, um zu verifizieren, dass elektronische Medien mit Karteninhaberdaten mit einer der in dieser Anforderung angegebenen Methoden vernichtet werden.	
Hinweise zur Anwendbarkeit Diese Anforderungen an die Vernichtung von Medien, wenn diese Medien aus geschäftlichen oder rechtlichen Gründen nicht mehr benötigt werden, sind getrennt und unterscheiden sich von PCI DSS-Anforderung 3.2.1, die das sichere Löschen von Karteninhaberdaten betrifft, wenn sie gemäß den Karteninhaberdaten-Aufbewahrungsrichtlinien der Entität nicht mehr benötigt werden.		

Anforderungen und Testprozeduren		Anleitungen
9.5 Interaktionspunkt- (POI)-Geräte sind vor Manipulation und nicht autorisiertem Austausch geschützt.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Kriminelle versuchen, Zahlungskartendaten zu stehlen, indem sie Kartenlesegeräte und Terminals stehlen und/oder manipulieren. Kriminelle werden versuchen, Geräte zu stehlen, um zu lernen, wie man in sie einbricht, und sie versuchen oft, berechtigte Geräte durch betrügerische Geräte zu ersetzen, die ihnen bei jeder Karteneingabe Zahlungskartendaten senden. Sie werden auch versuchen, an der Außenseite von Geräten „Skimming"-Komponenten hinzuzufügen, die Zahlungskartendaten erfassen, bevor sie in das Gerät gelangen – zum Beispiel durch Anbringen eines zusätzlichen Kartenlesers über dem berechtigten Kartenleser, damit die Zahlungskartendaten zweimal erfasst werden: einmal von der Komponente des Kriminellen und dann von der berechtigten Komponente des Geräts. Auf diese Weise können Transaktionen weiterhin ohne Unterbrechung abgeschlossen werden, während der Kriminelle während des Prozesses die Zahlungskartendaten „abschöpft". **Weitere Informationen** Weitere bewährte Praktiken zur Skimming-Verhinderung sind auf der PCI SSC-Webseite verfügbar.
9.5.1 POI-Geräte, die Zahlungskartendaten durch direkte physische Interaktion mit dem Zahlungskartenformfaktor erfassen, sind vor Manipulation und nicht autorisiertem Austausch geschützt, einschließlich der folgenden: • Führen einer Liste von POI-Geräten. • Regelmäßiges Inspizieren von POI-Geräten auf Manipulation oder nicht autorisierten Austausch. • Schulung des Personals, um verdächtiges Verhalten zu erkennen und Manipulationen oder nicht autorisierten Austausch von Geräten zu melden.	**9.5.1** Dokumentierte Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, die alle in dieser Anforderung angegebenen Elemente enthalten.	
Zielsetzung des kundenspezifischen Ansatzes Die Entität hat Prozeduren zum Schutz und zur Verwaltung von Interaktionspunkt-Geräten definiert. Erwartungen, Kontrollen und Aufsicht für die Verwaltung und den Schutz von POI-Geräten werden vom betroffenen Personal definiert und eingehalten.		
Hinweise zur Anwendbarkeit Diese Anforderungen gelten für eingesetzte POI-Geräte, die bei Transaktionen mit vorhandener Karte verwendet werden (d. h. einen Zahlungskartenformfaktor wie eine Karte, die durchgezogen, angetippt oder eingetaucht wird). Diese Anforderung soll nicht für manuelle PAN-Tasteneingabekomponenten wie Computertastaturen gelten. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Diese Anforderung wird für manuelle PAN-Tasteneingabekomponenten wie Computertastaturen empfohlen, ist aber nicht erforderlich. Diese Anforderung gilt nicht für kommerzielle Standardgeräte (zum Beispiel Smartphones oder Tablets), die mobile Geräte im Besitz von Händlern sind, die für den Massenmarkt bestimmt sind.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Führen einer aktuellen Liste von POI-Geräten hilft einer Organisation dabei, zu verfolgen, wo sich Geräte befinden sollen, und schnell zu identifizieren, ob ein Gerät fehlt oder verloren gegangen ist. **Gute Praxis** Das Verfahren zum Führen einer Geräteliste kann automatisiert (zum Beispiel ein Geräteverwaltungssystem) oder manuell (zum Beispiel in elektronischen oder Papieraufzeichnungen dokumentiert) sein. Bei Geräten für unterwegs kann der Standort den Namen des Personals enthalten, dem das Gerät zugewiesen ist. **Beispiele** Methoden zum Warten von Gerätestandorten umfassen das Identifizieren der Adresse des Standorts oder der Einrichtung, an der sich das Gerät befindet.
9.5.1.1 Es wird eine aktuelle Liste von POI-Geräten geführt, einschließlich: • Marke und Modell des Geräts. • Standort des Geräts. • Seriennummer des Geräts oder andere Methoden zur eindeutigen Identifizierung.	**9.5.1.1.a** Die Liste der POI-Geräte untersuchen, um zu verifizieren, dass sie alle in dieser Anforderung angegebenen Elemente enthält.	
	9.5.1.1.b POI-Geräte und Gerätestandorte beobachten und sie mit Geräten in der Liste vergleichen, um zu verifizieren, dass die Liste korrekt und aktuell ist.	
Zielsetzung des kundenspezifischen Ansatzes	**9.5.1.1.c** Personal befragen, um zu verifizieren, dass die Liste der POI-Geräte aktualisiert wird, wenn Geräte hinzugefügt, verlagert, außer Betrieb genommen werden usw.	
Die Identität und der Standort von POI-Geräten werden aufgezeichnet und sind jederzeit bekannt.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Regelmäßige Geräteinspektionen helfen Organisationen, Manipulationen durch externe Beweise – zum Beispiel durch das Hinzufügen eines Kartenskimmers – oder den Ersatz eines Geräts schneller zu erkennen, und minimieren so die potenziellen Auswirkungen der Verwendung betrügerischer Geräte. **Gute Praxis** Methoden zur regelmäßigen Inspektion beinhalten das Überprüfen der Seriennummer oder anderer Gerätemerkmale und das Vergleichen der Informationen mit der Liste der POI-Geräte, um zu verifizieren, dass das Gerät nicht mit einem betrügerischen Gerät ausgetauscht wurde. **Beispiele** Die Art der Inspektion hängt vom Gerät ab. Beispielsweise können Fotos von als sicher bekannten Geräten verwendet werden, um das aktuelle Erscheinungsbild eines Geräts mit seinem ursprünglichen Erscheinungsbild zu vergleichen, um zu sehen, ob es sich geändert hat. Eine andere Möglichkeit besteht darin, einen sicheren Markierungsstift zu verwenden, beispielsweise einen UV-Lichtmarker, um Geräteoberflächen und Geräteöffnungen zu markieren, damit jede Manipulation oder ein Ersatz sichtbar wird. Kriminelle ersetzen oft das äußere Gehäuse eines Geräts, um ihre Manipulation zu verbergen, und diese Methoden können helfen, solche Aktivitäten zu erkennen. Geräteanbieter können auch Sicherheitshinweise und Anleitungen zur Verfügung stellen, um festzustellen, ob das Gerät manipuliert wurde. Anzeichen dafür, dass ein Gerät manipuliert oder ersetzt wurde, sind: *(Fortsetzung auf der nächsten Seite)*
9.5.1.2 Die Oberflächen von POI-Geräten werden regelmäßig inspiziert, um Manipulationen und nicht autorisierten Austausch zu erkennen.	**9.5.1.2.a** Dokumentierte Prozeduren untersuchen, um zu verifizieren, dass Prozesse für die regelmäßige Inspektion von POI-Geräteoberflächen definiert sind, um Manipulationen und nicht autorisierten Austausch zu erkennen.	
	9.5.1.2.b Verantwortliches Personal befragen und Inspektionsprozesse beobachten, um Folgendes zu verifizieren: • Das Personal kennt die Prozeduren zur Inspektion von Geräten. • Alle Geräte werden regelmäßig auf Nachweis von Manipulationen und nicht autorisierten Austausch zu inspiziert.	
Zielsetzung des kundenspezifischen Ansatzes		
Interaktionspunkt-Geräte können ohne rechtzeitige Erkennung nicht manipuliert, ohne Autorisierungnicht ausgetauscht oder mit Skimming-Aufsätzen ausgestattet werden.		

Anforderungen und Testprozeduren		Anleitungen
		• unerwartete Anschlüsse oder Kabel, die an das Gerät angeschlossen wurden, • fehlende oder geänderte Sicherheitsetiketten, • beschädigte oder andersfarbige Gehäuse oder • Änderungen der Seriennummer oder anderer äußerer Markierungen.
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Entitäten sind am besten geeignet, um die Häufigkeit von POI-Geräteinspektionen basierend auf der Umgebung, in der das Gerät betrieben wird, zu bestimmen. **Gute Praxis** Die Häufigkeit der Inspektionen hängt von Faktoren wie dem Standort eines Geräts und davon ab, ob das Gerät beaufsichtigt oder unbeaufsichtigt ist. Zum Beispiel können Geräte, die ohne Aufsicht des Personals der Organisation in öffentlichen Bereichen aufbewahrt werden, häufiger überprüft werden als Geräte, die in sicheren Bereichen aufbewahrt oder beaufsichtigt werden, wenn sie für die Öffentlichkeit zugänglich sind. Darüber hinaus schließen viele POI-Anbieter in ihrer Benutzerdokumentation Anleitungen ein, wie oft und wofür POI-Geräte überprüft werden sollten – Entitäten sollten die Dokumentation ihrer Anbieter konsultieren und diese Empfehlungen in ihre regelmäßigen Inspektionen einbeziehen.
9.5.1.2.1 Die Häufigkeit der regelmäßigen Inspektionen von POI-Geräten und die Art der durchgeführten Inspektionen wird in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird.	**9.5.1.2.1.a** Die gezielte Risikoanalyse der Entität für die Häufigkeit regelmäßiger Inspektionen von POI-Geräten und die Art der durchgeführten Inspektionen untersuchen, um zu verifizieren, dass die Risikoanalyse gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wurde.	
Zielsetzung des kundenspezifischen Ansatzes POI-Geräte werden in einer Häufigkeit überprüft, die das Risiko der Entität adressiert.	**9.5.1.2.1.b** Dokumentierte Ergebnisse der regelmäßigen Geräteinspektionen untersuchen und das Personal befragen, um zu verifizieren, dass die Häufigkeit und Art der durchgeführten POI-Geräteinspektionen mit dem übereinstimmt, was in der für diese Anforderung durchgeführten gezielten Risikoanalyse der Entität definiert ist.	
Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Kriminelle geben sich oft als autorisiertes Wartungspersonal aus, um Zugang zu POI-Geräten zu erhalten. **Gute Praxis** Die Personalschulung sollte beinhalten, jeden, der zur POI-Wartung erscheint, aufmerksam zu machen und zu befragen, um sicherzustellen, dass er autorisiert ist und über einen gültigen Arbeitsauftrag verfügt, einschließlich Vertretern, Wartungs- oder Reparaturpersonal, Technikern, Dienstleistungsanbietern oder anderen Dritten. Alle Dritten, die den Zugriff auf Geräte anfordern, sollten immer verifiziert werden, bevor ihnen der Zugriff bereitgestellt wird – zum Beispiel durch Rücksprache mit der Verwaltung oder telefonische Kontaktaufnahme mit dem POI-Wartungsunternehmen, wie dem Anbieter oder Erwerber, zur Verifizierung. Viele Kriminelle versuchen, das Personal zu täuschen, indem sie sich für die Rolle kleiden (zum Beispiel Werkzeugkästen tragen und Arbeitskleidung tragen) und sie könnten auch über die Standorte von Geräten Bescheid wissen, also sollte das Personal geschult werden, um die Prozeduren immer zu befolgen. Ein weiterer Trick, den Kriminelle anwenden, besteht darin, ein „neues“ POI-Gerät mit Anweisungen zum Austausch gegen ein legitimes Gerät und „Rückgabe“ des legitimen Geräts zu senden. Die Kriminellen können sogar Rückporto an ihre angegebene Adresse senden. Daher sollte sich das Personal immer mit ihrem Vorgesetzten oder Lieferanten vergewissern, dass das Gerät rechtmäßig ist und von einer vertrauenswürdigen Quelle stammt, bevor es installiert oder geschäftlich verwendet wird. *(Fortsetzung auf der nächsten Seite)*
9.5.1.3 Das Personal in POI-Umgebungen wird geschult, um auf Manipulationsversuche oder den Ersatz von POI-Geräten aufmerksam zu machen, und umfasst: • Verifizierung der Identität von Drittpersonen, die sich als Reparatur- oder Wartungspersonal ausgeben, bevor ihnen Zugang zum Modifizieren oder Beheben von Fehlern von Geräten gewährt wird. • Prozeduren, um sicherzustellen, dass Geräte ohne Verifizierung nicht installiert, ersetzt oder zurückgegeben werden. • Sich verdächtigen Verhaltens in der Nähe von Geräten bewusst zu sein. • Melden von verdächtigem Verhalten und Hinweisen auf Gerätemanipulation oder Austausch an das entsprechende Personal.	**9.5.1.3.a** Schulungsmaterialien für Personal in POI-Umgebungen überprüfen, um zu verifizieren, dass sie alle in dieser Anforderung angegebenen Elemente beinhalten.	
	9.5.1.3.b Personal in POI-Umgebungen befragen, um zu verifizieren, dass sie Schulung erhalten haben und die Prozeduren für alle in dieser Anforderung angegebenen Elemente kennen**.**	
Zielsetzung des kundenspezifischen Ansatzes		
Das Personal ist mit den Arten von Angriffen auf POI-Geräte, den technischen und verfahrenstechnischen Gegenmaßnahmen der Entität vertraut und kann bei Bedarf auf Hilfe und Anleitungen zugreifen.		

Anforderungen und Testprozeduren		Anleitungen
		Beispiele Verdächtiges Verhalten, das dem Personal bewusst sein sollte, umfasst Versuche unbekannter Personen, Geräte zu trennen oder zu öffnen. Durch Sicherstellung, dass das Personal über Mechanismen zur Meldung von verdächtigem Verhalten bewusst ist und an wen ein solches Verhalten gemeldet werden soll – zum Beispiel einem Vorgesetzten oder Sicherheitsbeauftragten –, wird die Wahrscheinlichkeit und die potenziellen Auswirkungen einer Manipulation oder eines Austauschs eines Geräts verringert.

Regelmäßige Überwachung und Prüfung der Netzwerke

Anforderung 10: Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten

Abschnitte	
10.1	Prozesse und Mechanismen zur Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten werden definiert und dokumentiert.
10.2	Audit-Protokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten, und die forensische Analyse von Ereignissen zu unterstützen.
10.3	Audit-Protokolle werden vor Vernichtung und nicht autorisierten Änderungen geschützt.
10.4	Audit-Protokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren.
10.5	Der Verlauf des Audit-Protokolls wird gespeichert und steht für Analysen zur Verfügung.
10.6	Zeitsynchronisierungsmechanismen unterstützen konsistente Zeiteinstellungen über alle Systeme hinweg.
10.7	Versagen kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und es wird umgehend auf sie reagiert.

Übersicht

Protokollierungsmechanismen und die Möglichkeit, Benutzeraktivitäten zu verfolgen, sind entscheidend für die Verhinderung, Erkennung oder Minimierung der Auswirkungen einer Datenkompromittierung. Das Vorhandensein von Protokollen auf allen Systemkomponenten und in der Karteninhaberdatenumgebung (CDE) ermöglicht eine gründliche Verfolgung, Warnung und Analyse, wenn etwas schief geht. Die Ermittlung der Ursache einer Kompromittierung ist ohne Systemaktivitätsprotokolle schwierig, wenn nicht sogar unmöglich.

Diese Anforderung gilt für Benutzeraktivitäten, einschließlich derer von Mitarbeitern, Auftragnehmern, Beratern, und internen und externen Anbietern und anderen Dritten (zum Beispiel diejenigen, die Unterstützungs- oder Wartungsdienstleistungen bereitstellen).

Diese Anforderungen gelten nicht für Benutzeraktivitäten von Verbrauchern (Karteninhabern).

Finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
10.1 Prozesse und Mechanismen zur Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten werden definiert und dokumentiert.		
Definierte Ansatzanforderungen **10.1.1** Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 10 identifiziert werden, sind: • Dokumentiert. • Aktuell gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt.	**Testprozeduren mit definiertem Ansatz** **10.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die in Anforderung 10 identifizierten Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Bei Anforderung 10.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 10 angegeben sind. Während es wichtig ist, die in Anforderung 10 genannten spezifischen Richtlinien oder Verfahren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Prozeduren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Verfahren und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen.
Zielsetzung des kundenspezifischen Ansatzes Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 10 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht der Verwaltung.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen werden, ist das Personal sich möglicherweise seiner täglichen Verantwortlichkeiten nicht bewusst und kritische Aktivitäten können nicht stattfinden. **Gute Praxis** Rollen und Verantwortlichkeiten können in Richtlinien und Verfahren dokumentiert oder in separaten Dokumenten gewartet werden. Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen. **Beispiele** Ein Verfahren zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).
10.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 10 werden dokumentiert, zugewiesen und verstanden.	**10.1.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 10 dokumentiert und zugewiesen sind.	
	10.1.2.b Personal mit Verantwortlichkeit zur Durchführung von Aktivitäten in Anforderung 10 befragen, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 10 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
10.2 Audit-Protokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten, und die forensische Analyse von Ereignissen zu unterstützen.		
Definierte Ansatzanforderungen **10.2.1** Audit-Protokolle sind für alle Systemkomponenten und Karteninhaberdaten aktiviert und aktiv.	**Testprozeduren mit definiertem Ansatz** **10.2.1** Den Systemadministrator befragen und Systemkonfigurationen untersuchen, um zu verifizieren, ob Audit-Protokolle für alle Systemkomponenten aktiviert und aktiv sind.	**Zweck** Für alle Systemkomponenten muss ein Protokoll vorhanden sein. Audit-Protokolle alarmieren den Systemadministrator, liefern Daten an andere Überwachungsmechanismen, wie Eindringungserkennungs-Systeme (IDS) und SIEM-Tools (Sicherheitsinformations- und Ereignisüberwachungssysteme), und stellen einen Verlaufsplan für die Untersuchung nach einem Vorfall bereit. Das Protokollieren und Analysieren sicherheitsrelevanter Ereignisse ermöglicht es einer Organisation, potenziell böswillige Aktivitäten zu identifizieren und zu verfolgen. **Gute Praxis** Wenn eine Entität betrachtet, welche Informationen in ihren Protokollen aufgezeichnet werden sollen, ist es wichtig, sich daran zu erinnern, dass die in Audit-Protokollen gespeicherten Informationen sensibel sind und gemäß den Anforderungen in diesem Standard geschützt werden sollten. Es sollte darauf geachtet werden, dass nur wesentliche Informationen in den Audit-Protokollen gespeichert werden, um das Risiko zu minimieren.
Zielsetzung des kundenspezifischen Ansatzes Aufzeichnungen über alle Aktivitäten, die Systemkomponenten und Karteninhaberdaten betreffen, werden erfasst.		
Definierte Ansatzanforderungen **10.2.1.1** Audit-Protokolle erfassen alle individuellen Benutzerzugriffe auf Karteninhaberdaten.	**Testprozeduren mit definiertem Ansatz** **10.2.1.1** Audit-Protokoll-Konfigurationen und Protokolldaten untersuchen, um zu verifizieren, dass alle individuellen Benutzerzugriffe auf Karteninhaberdaten protokolliert werden.	**Zweck** Es ist wichtig, über einen Prozess oder ein System zu verfügen, das den Benutzerzugriff mit den Systemkomponenten verknüpft, auf die zugegriffen wird. Böswillige Personen könnten Kenntnis von einem Benutzerkonto mit Zugriff auf Systeme in der CDE erlangen oder sie könnten ein neues, nicht autorisiertes Konto erstellen, um auf Karteninhaberdaten zuzugreifen. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Aufzeichnungen über alle individuellen Benutzerzugriffe auf Karteninhaberdaten werden erfasst.		**Gute Praxis** Eine Aufzeichnung aller individuellen Zugriffe auf Karteninhaberdaten kann identifizieren, welche Konten möglicherweise kompromittiert oder missbraucht wurden.
Definierte Ansatzanforderungen **10.2.1.2** Audit-Protokolle erfassen alle Aktionen, die von einer Person mit Administratorzugriff ausgeführt werden, einschließlich der interaktiven Verwendung von Anwendungs- oder Systemkonten. **Zielsetzung des kundenspezifischen Ansatzes** Aufzeichnungen aller Aktionen, die von Personen mit erhöhten Rechten ausgeführt werden, werden erfasst.	**Testprozeduren mit definiertem Ansatz** **10.2.1.2** Audit-Protokoll-Konfigurationen und Protokolldaten untersuchen, um zu verifizieren, ob alle Aktionen einer Person mit Administratorzugriff, einschließlich der interaktiven Nutzung von Anwendungs- oder Systemkonten, protokolliert werden.	**Zweck** Konten mit erhöhten Zugriffsprivilegien, wie das „Administrator“- oder „Root“-Konto, können die Sicherheit oder die Betriebsfunktionalität eines Systems erheblich beeinträchtigen. Ohne ein Protokoll der durchgeführten Aktivitäten kann eine Organisation keine Probleme, die aus einem Verwaltungsfehler oder dem Missbrauch von Berechtigungen resultieren, auf die spezifische Aktion und das Konto zurückverfolgen. **Definitionen** Konten mit Administratorzugriff sind diejenigen, denen bestimmte Berechtigungen oder Fähigkeiten für dieses Konto zur Verwaltung von Systemen, Netzwerken und/oder Anwendungen zugewiesen wurden. Die als administrativ betrachteten Funktionen oder Aktivitäten gehen über diejenigen hinaus, die von normalen Benutzern im Rahmen routinemäßiger Geschäftsfunktionen ausgeführt werden.
Definierte Ansatzanforderungen **10.2.1.3** Audit-Protokolle erfassen den gesamten Zugriff auf Audit-Protokolle. **Zielsetzung des kundenspezifischen Ansatzes** Aufzeichnungen über alle Zugriffe auf Audit-Protokolle werden erfasst.	**Testprozeduren mit definiertem Ansatz** **10.2.1.3** Audit-Protokoll-Konfigurationen und Protokolldaten untersuchen, um zu verifizieren, dass der Zugriff auf alle Audit-Protokolle erfasst wird.	**Zweck** Böswillige Benutzer versuchen häufig, Überwachungsprotokolle zu ändern, um ihre Aktionen zu verbergen. Eine Zugriffsaufzeichnung ermöglicht es einer Organisation, Inkonsistenzen oder potenzielle Manipulationen der Protokolle einem einzelnen Konto zuzuordnen. Mit Hilfe von Protokollen, die Änderungen, Hinzufügungen und Löschungen in den Audit-Protokollen aufzeigen, können Schritte von nicht autorisiertem Personal zurückverfolgt werden. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **10.2.1.4** Audit-Protokolle erfassen alle ungültigen logischen Zugriffsversuche. **Zielsetzung des kundenspezifischen Ansatzes** Aufzeichnungen aller ungültigen Zugriffsversuche werden erfasst.	**Testprozeduren mit definiertem Ansatz** **10.2.1.4** Audit-Protokoll-Konfigurationen und Protokolldaten untersuchen, um zu verifizieren, dass ungültige logische Zugriffsversuche erfasst werden.	**Zweck** Böswillige Personen führen häufig mehrere Zugriffsversuche auf Zielsysteme durch. Mehrere ungültige Anmeldeversuche können ein Hinweis auf die Versuche eines nicht autorisierten Benutzers sein, „brutale Gewalt“ zu verwenden oder ein Passwort zu erraten.
Definierte Ansatzanforderungen **10.2.1.5** Audit-Protokolle erfassen alle Änderungen an Identifizierungs- und Authentifizierungsreferenzen einschließlich, aber nicht beschränkt auf: • Erstellung neuer Konten. • Erhöhung der Privilegien. • Alle Änderungen, Ergänzungen oder Löschungen von Konten mit Administratorzugriff. **Zielsetzung des kundenspezifischen Ansatzes** Aufzeichnungen über alle Änderungen der Identifizierungs- und Authentifizierungsreferenzen werden erfasst.	**Testprozeduren mit definiertem Ansatz** **10.2.1.5** Audit-Protokoll-Konfigurationen und Protokolldaten untersuchen, um zu verifizieren, dass Änderungen an Identifizierungs- und Authentifizierungs-Referenzen gemäß allen in dieser Anforderung angegebenen Elementen erfasst werden.	**Zweck** Das Protokollieren von Änderungen an den Authentifizierungsdaten (einschließlich der Erhöhung von Privilegien, Hinzufügen und Löschen von Konten mit Administratorzugriff) liefert Restnachweise für Aktivitäten. Böswillige Benutzer können versuchen, die Authentifizierungsdaten zu manipulieren, um sie zu umgehen oder sich als gültiges Konto auszugeben.
Definierte Ansatzanforderungen **10.2.1.6** Audit-Protokolle erfassen Folgendes: • Alle Initialisierungen neuer Audit-Protokolle, und • Alles Starten, Stoppen oder Pausieren der bestehenden Audit-Protokolle.	**Testprozeduren mit definiertem Ansatz** **10.2.1.6** Audit-Protokoll-Konfigurationen und Protokolldaten untersuchen, um zu verifizieren, dass alle in dieser Anforderung angegebenen Elemente erfasst werden.	**Zweck** Das Abschalten oder Pausieren von Audit-Protokollen vor der Durchführung illegaler Aktivitäten ist gängige Praxis für böswillige Benutzer, die eine Entdeckung vermeiden möchten. Die Initialisierung von Audit-Protokollen

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Aufzeichnungen über alle Änderungen des Aktivitätsstatus des Audit-Protokolls werden erfasst.		könnte darauf hinweisen, dass ein Benutzer die Protokollfunktion deaktiviert hat, um seine Aktionen zu verbergen. *(Fortsetzung auf der nächsten Seite)*
Definierte Ansatzanforderungen **10.2.1.7** Audit-Protokolle erfassen die gesamte Erstellung und Löschung von Objekten auf Systemebene.	**Testprozeduren mit definiertem Ansatz** **10.2.1.7** Audit-Protokoll-Konfigurationen und Protokolldaten untersuchen, um zu verifizieren, dass die Erstellung und Löschung von Objekten auf Systemebene erfasst wird.	**Zweck** Böswillige Software wie Malware erstellt oder ersetzt häufig Objekte auf Systemebene auf dem Zielsystem, um eine bestimmte Funktion oder einen Betrieb auf diesem System zu kontrollieren. Durch die Protokollierung beim Erstellen oder Löschen von Objekten auf Systemebene kann leichter bestimmt werden, ob solche Änderungen autorisiert wurden.
Zielsetzung des kundenspezifischen Ansatzes Aufzeichnungen über Änderungen, die darauf hinweisen, dass ein System von seiner beabsichtigten Funktionalität abgeändert wurde, werden erfasst.		
Definierte Ansatzanforderungen **10.2.2** Audit-Protokolle zeichnen die folgenden Details für jedes auditierbare Ereignis auf: • Benutzeridentifizierung. • Art des Vorkommnisses. • Datum und Uhrzeit. • Erfolgs- und Versagensanzeige. • Entstehung des Vorkommnisses. • Identität oder Name der betroffenen Daten, Systemkomponente, Ressource oder der Dienstleistung (zum Beispiel Name und Protokoll).	**Testprozeduren mit definiertem Ansatz** **10.2.2** Personal befragen und Audit-Protokoll-Konfigurationen und Protokolldaten untersuchen, um zu verifizieren, dass alle in dieser Anforderung angegebenen Elemente in Protokolleinträgen für jedes auditierbare Ereignis (von 10.2.1.1 bis 10.2.1.7) enthalten sind.	**Zweck** Durch das Aufzeichnen dieser Details für die auditierbaren Ereignisse in den Schritten 10.2.1.1 bis 10.2.1.7 kann eine potenzielle Gefährdung schnell identifiziert werden, und zwar mit ausreichenden Details, um die Nachverfolgung verdächtiger Aktivitäten zu erleichtern.

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes		
Ausreichende Daten, um erfolgreiche und fehlgeschlagene Versuche identifizieren zu können und wer, was, wann, wo und wie für jedes in Anforderung 10.2.1 aufgeführte Ereignis erfasst wird.		

Anforderungen und Testprozeduren		Anleitungen
10.3 Audit-Protokolle werden vor Vernichtung und nicht autorisierten Änderungen geschützt.		
Definierte Ansatzanforderungen **10.3.1** Der Lesezugriff auf Audit-Protokoll-Dateien ist auf Personen mit berufsbedingtem Bedarf beschränkt. **Zielsetzung des kundenspezifischen Ansatzes** Nicht autorisiertes Personal kann nicht auf gespeicherte Aktivitätsaufzeichnungen zugreifen.	**Testprozeduren mit definiertem Ansatz** **10.3.1** Systemadministratoren befragen und Systemkonfigurationen und Privilegien untersuchen, um zu verifizieren, dass nur Personen mit einem berufsbezogenen Bedarf Lesezugriff auf Audit-Protokoll-Dateien haben.	**Zweck** Audit-Protokoll-Dateien enthalten sensible Informationen, und der Lesezugriff auf die Protokoll-Dateien darf nur auf Personen mit gültigem Geschäftsbedarf beschränkt werden. Dieser Zugriff beinhaltet Audit-Protokoll-Dateien auf den Ursprungssystemen sowie überall dort, wo sie gespeichert sind. **Gute Praxis** Ein angemessener Schutz der Audit-Protokolle beinhaltet eine starke Zugriffskontrolle, die den Zugriff auf Protokolle auf der Grundlage von „Wissensbedarf“ beschränkt, und die Verwendung von physischer oder Netzwerktrennung, um das Auffinden und Ändern der Protokolle zu erschweren.
Definierte Ansatzanforderungen **10.3.2** Audit-Protokoll-Dateien sind geschützt, um Änderungen durch Personen zu verhindern. **Zielsetzung des kundenspezifischen Ansatzes** Gespeicherte Aktivitätsaufzeichnungen können vom Personal nicht geändert werden.	**Testprozeduren mit definiertem Ansatz** **10.3.2** Systemkonfigurationen und -privilegien untersuchen und Systemadministratoren befragen, um zu verifizieren, dass aktuelle Audit-Protokoll-Dateien durch Zugriffskontrollmechanismen, physische Trennung und/oder Netzwerktrennung vor Änderungen durch Personen geschützt sind.	**Zweck** Eine böswillige Person, die in das Netzwerk eingedrungen ist, wird oft versuchen, die Audit-Protokolle zu bearbeiten, um ihre Aktivität zu verbergen. Ohne einen ausreichenden Schutz der Audit-Protokolle kann deren Vollständigkeit, Richtigkeit und Integrität nicht gewährleistet werden, und die Audit-Protokolle können nach einer Kompromittierung als Untersuchungstool unbrauchbar werden. Daher sollten Audit-Protokolle auf den Ursprungssystemen sowie überall dort, wo sie gespeichert sind, geschützt werden. **Gute Praxis** Entitäten sollten versuchen zu verhindern, dass Protokolle an öffentlich zugänglichen Orten freigelegt werden.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **10.3.3** Audit-Protokoll-Dateien, auch für nach außen gerichtete Technologien, werden zeitnah auf einem sicheren, zentralen, internen Protokollserver oder anderen schwer veränderbaren Medien gesichert. **Zielsetzung des kundenspezifischen Ansatzes** Gespeicherte Aktivitätsaufzeichnungen werden an einem zentralen Ort gesichert und aufbewahrt, um nicht autorisierte Änderungen zu verhindern.	**Testprozeduren mit definiertem Ansatz** **10.3.3** Sicherungskonfigurationen oder Protokolldateien untersuchen, um zu verifizieren, dass aktuelle Audit-Protokoll-Dateien, auch für nach außen gerichtete Technologien, zeitnah auf einem sicheren, zentralen, internen Protokollserver oder anderen schwer veränderbaren Medien gesichert werden.	**Zweck** Eine zeitnahe Sicherung der Protokolle auf einem zentralen Protokollserver oder schwer zu ändernden Medien hält die Protokolle geschützt, selbst wenn das System, das die Protokolle erzeugt, kompromittiert wird. Das Schreiben von Protokollen von nach außen gerichteten Technologien wie drahtlos, Netzwerksicherheitskontrollen, DNS und Mailservern verringert das Risiko, dass diese Protokolle verloren gehen oder verändert werden. **Gute Praxis** Jede Entität bestimmt den besten Weg, Protokolldateien abzusichern, sei es über einen oder mehrere zentrale Protokollserver oder andere sichere Medien. Protokolle können direkt geschrieben, ausgelagert oder von externen Systemen auf das sichere interne System oder Medium kopiert werden.
Definierte Ansatzanforderungen **10.3.4** Dateiintegritätsüberwachung oder Änderungserkennungsmechanismen werden auf Audit-Protokollen verwendet, um sicherzustellen, dass vorhandene Protokolldaten nicht geändert werden können, ohne dass Warnungen generiert werden. **Zielsetzung des kundenspezifischen Ansatzes** Gespeicherte Aktivitätsaufzeichnungen können nicht geändert werden, ohne dass eine Warnung generiert wird.	**Testprozeduren mit definiertem Ansatz** **10.3.4** Systemeinstellungen, überwachte Dateien und Ergebnisse aus Überwachungsaktivitäten untersuchen, um die Verwendung von Software zur Dateiintegritätsüberwachung oder Änderungserkennung auf Audit-Protokollen zu verifizieren.	**Zweck** Datei-Integritätsüberwachungen- oder Änderungserkennungssysteme prüfen auf Änderungen an kritischen Dateien und benachrichtigen, wenn solche Änderungen identifiziert werden. Für Zwecke der Datei-Integritätsüberwachung überwacht eine Entität normalerweise Dateien, die sich nicht regelmäßig ändern, aber bei einer Änderung auf eine mögliche Kompromittierung hinweisen. **Gute Praxis** Software zur Überwachung von Änderungen an Audit-Protokollen sollte so konfiguriert werden, um Warnungen bereitzustellen, wenn vorhandene Protokolldaten oder Dateien geändert oder gelöscht werden. Neue Protokolldaten, die einem Audit-Protokoll hinzugefügt werden, sollten jedoch keine Warnung generieren.

Anforderungen und Testprozeduren		Anleitungen
10.4 Audit-Protokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren.		
Definierte Ansatzanforderungen **10.4.1** Die folgenden Audit-Protokolle werden mindestens einmal täglich überprüft: • Alle Sicherheitsereignisse. • Protokolle aller Systemkomponenten, die CHD und/oder SAD speichern, verarbeiten oder übertragen. • Protokolle aller kritischen Systemkomponenten. • Protokolle aller Server und Systemkomponenten, die Sicherheitsfunktionen durchführen (zum Beispiel Netzwerksicherheitskontrollen, Eindringungs-Erkennungs-Systeme/Eindringungs-Verhinderungs-Systeme (IDS/IPS), Authentifizierungsserver). **Zielsetzung des kundenspezifischen Ansatzes** Potenziell verdächtige oder anomale Aktivitäten werden schnell identifiziert, um die Auswirkungen zu minimieren.	**Testprozeduren mit definiertem Ansatz** **10.4.1.a** Sicherheitsrichtlinien und -verfahren untersuchen, um zu verifizieren, dass Prozesse für die Überprüfung aller in dieser Anforderung angegebenen Elemente mindestens einmal täglich überprüft werden. **10.4.1.b** Prozesse beobachten und Personal befragen, um zu verifizieren, dass alle in dieser Anforderung angegebenen Elemente mindestens einmal täglich überprüft werden	**Zweck** Viele Sicherheitsverletzungen treten Monate auf, bevor sie entdeckt werden. Durch regelmäßige Protokollüberprüfungen können Vorfälle schnell identifiziert und proaktiv adressiert werden. **Gute Praxis** Die tägliche Überprüfung der Protokolle (7 Tage die Woche, 365 Tage im Jahr, einschließlich Feiertage) minimiert den Zeitaufwand und den Aussatz auf potenzielle Sicherheitsverletzungen. Protokoll-Harvesting-, Parsing- und Warntools, zentralisierte Protokollverwaltungssysteme, Ereignisprotokoll-Analysatoren und Sicherheitsinformations- und Ereignisverwaltungslösungen (SIEM) sind Beispiele für automatisierte Tools, die verwendet werden können, um diese Anforderung zu erfüllen. Tägliche Überprüfung von Sicherheitsereignissen – zum Beispiel Benachrichtigungen oder Warnungen, die verdächtige oder anomale Aktivitäten identifizieren – sowie Protokollen von kritischen Systemkomponenten und Protokollen von Systemen, die Sicherheitsfunktionen ausführen, wie Firewalls, IDS/IPS, Dateiintegritätsüberwachungs- (FIM)-Systemen usw. ist erforderlich, um potenzielle Probleme zu identifizieren. Die Bestimmung des „Sicherheitsereignisses“ ist für jede Organisation unterschiedlich und kann die Art der Technologie, den Ort und die Funktion des Geräts berücksichtigen. Organisationen möchten möglicherweise auch eine Basislinie des „normalen“ Verkehrs beibehalten, um anomales Verhalten zu erkennen. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Eine Entität, die dritte Dienstleistungsanbieter verwendet, um Protokollüberprüfungsdienste durchzuführen, ist dafür verantwortlich, den Dienstleistungsanbietern Kontext über die Umgebung der Entität bereitzustellen, damit sie die Umgebung der Entität versteht, eine Basislinie des „normalen“ Datenverkehrs für die Entität hat, und potenzielle Sicherheitsprobleme erkennen kann und genaue Ausnahmen und Anomaliebenachrichtigungen bereitstellen kann.
Definierte Ansatzanforderungen **10.4.1.1** Automatisierte Mechanismen werden verwendet, um Audit-Protokoll-Überprüfungen durchzuführen. **Zielsetzung des kundenspezifischen Ansatzes** Potenziell verdächtige oder anomale Aktivitäten werden über einen wiederholbaren und konsistenten Mechanismus identifiziert. **Hinweise zur Anwendbarkeit** *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**Testprozeduren mit definiertem Ansatz** **10.4.1.1** Protokoll-Überprüfungs-Mechanismen untersuchen und Personal befragen, um zu verifizieren, dass automatisierte Mechanismen verwendet werden, um Protokoll-Überprüfungen durchzuführen.	**Zweck** Manuelle Protokollüberprüfungen sind aufgrund der Menge der generierten Protokolldaten selbst für ein oder zwei Systeme schwierig durchzuführen. Die Verwendung von Protokoll-Harvesting-, Parsing- und Warntools, zentralisierten Protokollverwaltungssystemen, Ereignisprotokoll-Analysatoren und Sicherheitsinformations- und Ereignisverwaltungs-(SIEM)-Lösungen kann jedoch dabei helfen, den Prozess zu vereinfachen, indem Protokollereignisse identifiziert werden, die überprüft werden müssen. **Gute Praxis** Die Entität sollte die Protokollierungstools an alle Änderungen in ihrer Umgebung anpassen, indem sie die Tooleinstellungen regelmäßig überprüft und die Einstellungen aktualisiert, um Änderungen widerzuspiegeln.
Definierte Ansatzanforderungen **10.4.2** Protokolle aller anderen Systemkomponenten (die nicht in Anforderung 10.4.1 angegeben sind) werden regelmäßig überprüft.	**Testprozeduren mit definiertem Ansatz** **10.4.2.a** Sicherheitsrichtlinien und -verfahren untersuchen, um zu verifizieren, dass Prozesse für die regelmäßige Überprüfung der Protokolle aller anderen Systemkomponenten definiert sind.	**Zweck** Die regelmäßige Überprüfung der Protokolle für alle anderen Systemkomponenten (in Anforderung 10.4.1 nicht angegeben) hilft, Hinweise auf potenzielle Probleme oder Versuche

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Potenziell verdächtige oder anomale Aktivitäten für andere Systemkomponenten (nicht in 10.4.1 enthalten) werden gemäß dem identifizierten Risiko der Entität überprüft. **Hinweise zur Anwendbarkeit** Diese Anforderung gilt für alle anderen in den Geltungsbereich fallenden Systemkomponenten, die nicht in Anforderung 10.4.1 enthalten sind.	**10.4.2.b** Dokumentierte Ergebnisse von Protokollüberprüfungen untersuchen und das Personal befragen, um zu verifizieren, dass Protokollüberprüfungen regelmäßig durchgeführt werden.	zu identifizieren, über weniger kritische Systeme auf kritische Systeme zuzugreifen.
Definierte Ansatzanforderungen **10.4.2.1** Die Häufigkeit der regelmäßigen Protokollüberprüfungen für alle anderen Systemkomponenten (nicht in Anforderung 10.4.1 definiert) wird in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird **Zielsetzung des kundenspezifischen Ansatzes** Protokollüberprüfungen für Systemkomponenten mit geringerem Risiko werden in einer Häufigkeit durchgeführt, die dem Risiko der Entität Rechnung trägt. **Hinweise zur Anwendbarkeit** *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**Testprozeduren mit definiertem Ansatz** **10.4.2.1.a** Die gezielte Risikoanalyse der Entität für die Häufigkeit regelmäßiger Protokollüberprüfungen für alle anderen Systemkomponenten (nicht in Anforderung 10.4.1 definiert) untersuchen, um zu verifizieren, dass die Risikoanalyse gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wurde. **10.4.2.1.b** Dokumentierte Ergebnisse der regelmäßigen Protokollüberprüfungen aller anderen Systemkomponenten (nicht definiert in Anforderung 10.4.1) untersuchen und das Personal befragen, um zu verifizieren, dass Protokollüberprüfungen in der Häufigkeit durchgeführt werden, die in der für diese Anforderung durchgeführten gezielten Risikoanalyse der Stelle angegeben ist.	**Zweck** Entitäten können den optimalen Zeitraum bestimmen, um diese Protokolle auf der Grundlage von Kriterien wie der Komplexität der Umgebung jeder Entität, der Anzahl der zu bewertenden Systemtypen und der Funktionen dieser Systeme zu überprüfen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Ausnahmen und Anomalien, die während des Protokollüberprüfungsprozesses identifiziert wurden, nicht untersucht werden, kann es sein, dass die Entität keine Kenntnis von nicht autorisierten und potenziell böswilligen Aktivitäten in ihrem Netzwerk hat. **Gute Praxis** Entitäten sollten bei der Entwicklung ihrer Prozesse zum Definieren und Verwalten von Ausnahmen und Anomalien berücksichtigen, wie sie Folgendes angehen: • Wie Protokollüberprüfungsaktivitäten aufgezeichnet werden, • Wie Ausnahmen und Anomalien eingeordnet und priorisiert werden, • Welche Prozeduren vorhanden sein sollten, um Ausnahmen und Anomalien zu melden und zu eskalieren, und • Wer für die Untersuchung und für etwaige Sanierungsaufgaben verantwortlich ist.
10.4.3 Ausnahmen und Anomalien, die während des Überprüfungsprozesses etabliert wurden, werden adressiert.	**10.4.3.a** Sicherheitsrichtlinien und -prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, um Ausnahmen und Anomalien zu adressieren, die während des Überprüfungsprozesses identifiziert wurden.	
	10.4.3.b Prozesse beobachten und das Personal befragen, um zu verifizieren, dass, wenn Ausnahmen und Anomalien identifiziert werden, diese adressiert werden.	
Zielsetzung des kundenspezifischen Ansatzes		
Verdächtige oder anomale Aktivitäten werden adressiert.		

Anforderungen und Testprozeduren		Anleitungen
10.5 Der Verlauf des Audit-Protokolls wird gespeichert und steht für Analysen zur Verfügung.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Gute Praxis**
10.5.1 Den Audit-Protokoll-Verlauf mindestens 12 Monate aufbewahren, wobei mindestens die letzten drei Monate sofort zur Analyse verfügbar sind.	**10.5.1.a** Die Dokumentation untersuchen, um zu verifizieren, dass Folgendes definiert ist: • Audit-Protokoll-Aufbewahrungsrichtlinien. • Prozeduren zum Aufbewahren des Audit-Protokoll-Verlaufs für mindestens 12 Monate, wobei mindestens die letzten drei Monate sofort online verfügbar sind.	Die Aufbewahrung historischer Audit-Protokolle für mindestens 12 Monate ist notwendig, da Kompromisse oft über bedeutend längere Zeiten unbemerkt bleiben. Durch den zentral gespeicherte Protokollverlauf können Ermittler besser bestimmen, wie lange ein potenzieller Verstoß aufgetreten ist und welche Systeme möglicherweise betroffen sind. Indem Protokolle für drei Monate sofort verfügbar sind, kann eine Entität die Auswirkungen einer Datenschutzverletzung schnell erkennen und minimieren. **Beispiele** Zu den Methoden, mit denen Protokolle sofort verfügbar sind, gehören das Online-Speichern von Protokollen, das Archivieren von Protokollen oder das schnelle Wiederherstellen von Protokollen aus Backups.
	10.5.1.b Konfigurationen des Audit-Protokoll-Verlaufs untersuchen, das Personal befragen und Audit-Protokolle untersuchen, um zu verifizieren, dass der Audit-Protokoll-Verlauf mindestens 12 Monate aufbewahrt wird.	
Zielsetzung des kundenspezifischen Ansatzes	**10.5.1.c** Das Personal befragen und Prozesse beobachten, um zu verifizieren, dass der Audit-Protokoll-Verlauf von mindestens den letzten drei Monaten sofort zur Analyse zur Verfügung stehen.	
Historische Aktivitätsaufzeichnungen sind sofort verfügbar, um die Reaktion auf Vorfälle zu unterstützen, und werden mindestens 12 Monate lang aufbewahrt.		

Anforderungen und Testprozeduren		Anleitungen
10.6 Zeitsynchronisierungsmechanismen unterstützen konsistente Zeiteinstellungen über alle Systeme hinweg.		
Definierte Ansatzanforderungen **10.6.1** Systemuhren und Uhrzeit werden mithilfe der Zeitsynchronisierungstechnologie synchronisiert. **Zielsetzung des kundenspezifischen Ansatzes** Über alle Systeme hinweg wird eine gemeinsame Zeit etabliert. **Hinweise zur Anwendbarkeit** Um die Zeitsynchronisierungstechnologie auf dem neuesten Stand zu halten, schließt Verwalten von Schwachstellen und Patchen der Technologie gemäß den PCI DSS-Anforderungen 6.3.1 und 6.3.3 ein.	**Testprozeduren mit definiertem Ansatz** **10.6.1** Systemkonfigurationseinstellungen untersuchen, um zu verifizieren, dass die Zeitsynchronisierungstechnologie implementiert und auf dem neuesten Stand gehalten wird.	**Zweck** Zeitsynchronisierungstechnologie wird verwendet, um Uhren auf mehreren Systemen zu synchronisieren. Wenn die Uhren nicht richtig synchronisiert sind, kann es schwierig, wenn nicht unmöglich sein, Protokoll-Dateien verschiedener Systeme zu vergleichen und eine genaue Abfolge von Ereignissen zu ermitteln, was für die forensische Analyse nach einer Sicherheitsverletzung entscheidend ist. Für Forensik-Teams nach einem Vorfall sind die Genauigkeit und Konsistenz der Zeit in allen Systemen und der Zeitpunkt jeder Aktivität entscheidend, um festzustellen, wie die Systeme kompromittiert wurden. **Beispiele** Netzwerkzeitprotokoll (NTP) ist ein Beispiel für Zeitsynchronisationstechnologie.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Verwendung seriöser Zeitserver ist eine kritische Komponente des Zeitsynchronisierungsprozesses. Das Akzeptieren von Zeitaktualisierungen von bestimmten, von der Industrie akzeptierten externen Quellen verhindert, dass eine böswillige Person die Zeiteinstellungen auf Systemen ändert. **Gute Praxis** Eine weitere Möglichkeit, die unbefugte Nutzung interner Zeitserver zu verhindern, besteht darin, Aktualisierungen mit einem symmetrischen Schlüssel zu verschlüsseln und Zugriffskontrolllisten zu erstellen, die die IP-Adressen der Client-Rechner angeben, die mit den Zeitaktualisierungen versorgt werden.
10.6.2 Systeme werden wie folgt auf die richtige und konsistente Zeit konfiguriert: • Ein oder mehrere designierte Zeitserver werden verwendet. • Nur der oder die designierten zentralen Zeitserver erhalten die Zeit von externen Quellen. • Die von externen Quellen empfangene Zeit basiert auf der Internationalen Atomzeit oder der koordinierten Weltzeit (UTC). • DEr/die designierten Zeitserver akzeptiert/akzeptieren Zeitaktualisierungen nur von bestimmten, von der Branche akzeptierten externen Quellen. • Wenn es mehr als einen designierten Zeitserver gibt, können die Zeitserver sich einander ansehen, um die genaue Zeit beizubehalten. • Interne Systeme erhalten Zeitinformationen nur von bestimmten zentralen Zeitservern.	**10.6.2** Systemkonfigurationseinstellungen zum Erfassen, Verteilen und Speichern der korrekten Zeit untersuchen, um zu verifizieren, dass die Einstellungen gemäß mit allen in dieser Anforderung angegebenen Elementen konfiguriert werden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die Zeit auf allen Systemen ist genau und konsistent.		

<table>
<tr><th colspan="2">Anforderungen und Testprozeduren</th><th>Anleitungen</th></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="3">Zweck
Angreifer werden versuchen, die Zeitkonfigurationen zu ändern, um ihre Aktivität zu verbergen. Daher verringert die Beschränkung der Fähigkeit, Zeitsynchronisierungskonfigurationen oder die Systemzeit auf Administratoren zu ändern oder zu modifizieren, die Wahrscheinlichkeit, dass ein Angreifer Zeitkonfigurationen erfolgreich ändert.</td></tr>
<tr><td>10.6.3 Die Einstellungen und Daten der Zeitsynchronisierung sind wie folgt geschützt:
Der Zugriff auf Zeitdaten ist auf Personal mit geschäftlichem Bedarf beschränkt.
Alle Änderungen der Zeiteinstellungen auf kritischen Systemen werden protokolliert, überwacht und überprüft.</td><td>10.6.3.a Systemkonfigurationen und Zeitsynchronisierungseinstellungen untersuchen, um zu verifizieren, dass der Zugriff auf Zeitdaten auf Personal mit geschäftlichem Bedarf beschränkt ist.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes

Systemzeiteinstellungen können von nicht autorisiertem Personal nicht geändert werden.</td><td>10.6.3.b Systemkonfigurationen und Zeitsynchronisierungseinstellungen und Protokolle untersuchen, und Prozesse beobachten, um zu verifizieren, dass alle Änderungen an Zeiteinstellungen auf kritischen Systemen protokolliert, überwacht und überprüft werden.</td></tr>
</table>

Anforderungen und Testprozeduren		Anleitungen
10.7 Versagen kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und es wird umgehend auf sie reagiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	
10.7.1 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Versagen von kritischen Sicherheitskontrollsystemen werden sofort erkannt, gewarnt und adressiert, einschließlich, aber nicht beschränkt auf das Versagen der folgenden kritischen Sicherheitskontrollsysteme: • Netzwerksicherheitskontrollen • IDS/IPS • FIM • Anti-Malware-Lösungen • Physische Zugriffskontrollen • Logische Zugriffskontrollen • Audit-Protokollierungsmechanismen • Segmentierungskontrollen (sofern verwendet)	**10.7.1.a** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Die Dokumentation untersuchen, um zu verifizieren, dass Prozesse für die sofortige Erkennung und Adressierung von Versagen von kritischen Sicherheitskontrollsystemen definiert sind, einschließlich, aber nicht beschränkt auf das Versagen aller in dieser Anforderung angegebenen Elemente.	**Zweck** Ohne formelle Prozesse zur Erkennung und Warnung, wenn kritische Sicherheitskontrollen versagen, können Ausfälle für längere Zeit unentdeckt bleiben und Angreifern genügend Zeit bereitstellen, Systemkomponenten zu kompromittieren und Kontodaten von der CDE zu stehlen. **Gute Praxis** Die spezifischen Fehlerarten können je nach Funktion der Gerätesystemkomponente und verwendeter Technologie variieren. Typische Versagen umfassen ein System, das seine Sicherheitsfunktion nicht mehr durchführt oder nicht wie vorgesehen funktioniert, beispielsweise wenn eine Firewall alle ihre Regeln löscht oder offline geht.a
Zielsetzung des kundenspezifischen Ansatzes Versagen in kritischen Sicherheitskontrollsystemen werden umgehend erkannt und adressiert.	**10.7.1.b Zusätzliche Testprozedur nur für Dienstleistungsanbieter-Bewertungen:** Erkennungs- und Warnungsprozesse beobachten und das Personal befragen, um zu verifizieren, dass Versagen kritischer Sicherheitskontrollsysteme erkannt und gemeldet werden und dass das Versagen einer kritischen Sicherheitskontrolle zur Generierung einer Warnung führt.	
Hinweise zur Anwendbarkeit Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. Diese Anforderung wird durch Anforderung 10.7.2 vom 31. März 2025 ersetzt.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ohne formelle Prozesse zur Erkennung und Warnung, wenn kritische Sicherheitskontrollen versagen, können Ausfälle für längere Zeit unentdeckt bleiben und Angreifern genügend Zeit bereitstellen, Systemkomponenten zu kompromittieren und Kontodaten von der CDE zu stehlen. **Gute Praxis** Die spezifischen Fehlerarten können je nach Funktion der Gerätesystemkomponente und verwendeter Technologie variieren. Typische Versagen umfassen ein System, das seine Sicherheitsfunktion nicht mehr durchführt oder nicht wie vorgesehen funktioniert - zum Beispiel wenn eine Firewall alle ihre Regeln löscht oder offline geht.
10.7.2 Versagen von kritischen Sicherheitskontrollsystemen werden sofort erkannt, gewarnt und adressiert, einschließlich, aber nicht beschränkt auf das Versagen der folgenden kritischen Sicherheitskontrollsysteme: • Netzwerksicherheitskontrollen • IDS/IPS • Änderungserkennungsmechanismen • Anti-Malware-Lösungen • Physische Zugriffskontrollen • Logische Zugriffskontrollen • Audit-Protokollierungsmechanismen • Segmentierungskontrollen (sofern verwendet) • Audit-Protokoll-Überprüfungsmechanismen • Automatisierte Sicherheitstesttools (sofern verwendet)	**10.7.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass Prozesse für die sofortige Erkennung und Adressierung von Versagen von kritischen Sicherheitskontrollsystemen definiert sind, einschließlich, aber nicht beschränkt auf das Versagen aller in dieser Anforderung angegebenen Elemente.	
Zielsetzung des kundenspezifischen Ansatzes Versagen in kritischen Sicherheitskontrollsystemen werden umgehend erkannt und adressiert.	**10.7.2.b** Erkennungs- und Warnungsprozesse beobachten und das Personal befragen, um zu verifizieren, dass Versagen kritischer Sicherheitskontrollsysteme erkannt und gemeldet werden und dass das Versagen einer kritischen Sicherheitskontrolle zur Generierung einer Warnung führt.	
Hinweise zur Anwendbarkeit Diese Anforderung gilt für alle Entitäten, einschließlich Dienstleistungsanbieter, und wird Anforderung 10.7.1 ab dem 31. März 2025 ersetzen. Sie beinhaltet zwei zusätzliche kritische Sicherheitskontrollsysteme, die nicht in Anforderung 10.7.1 enthalten sind. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn auf Warnungen bei Versagen von kritischen Sicherheitskontrollsystemen nicht schnell und effektiv reagiert wird, können Angreifer diese Zeit nutzen, um böswillige Software einzuschleusen, die Kontrolle über ein System zu erlangen oder Daten aus der Umgebung der Entität zu stehlen. **Gute Praxis** Dokumentierte Nachweise (zum Beispiel Aufzeichnungen in einem Problemverwaltungssystem) sollten Unterstützung bereitstellen, dass Prozesse und Prozeduren vorhanden sind, um auf Sicherheitsversagen zu reagieren. Darüber hinaus sollte sich das Personal seiner Verantwortung im Fall eines Versagens bewusst sein. Aktionen und Reaktionen auf das Versagen sollten in den dokumentierten Nachweisen festgehalten werden.
10.7.3 Auf Versagen von kritischen Sicherheitskontrollsystemen wird umgehend reagiert, einschließlich, aber nicht beschränkt auf: • Wiederherstellen von Sicherheitsfunktionen. • Identifizieren und Dokumentieren der Dauer (Datum und Uhrzeit von Anfang bis Ende) des Sicherheitsversagens. • Identifizieren und Dokumentieren der Versagensursache(n) und Dokumentieren der erforderlichen Behebung. • Identifizieren und Adressieren von Sicherheitsproblemen, die während des Versagens aufgetreten sind. • Feststellen, ob aufgrund des Sicherheitsversagens weitere Aktionen erforderlich sind. • Implementieren von Kontrollen, um zu verhindern, dass die Versagensursache erneut auftritt. • Wiederaufnehmen der Überwachung der Sicherheitskontrollen.	**10.7.3.a** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass Prozesse definiert und implementiert sind, um auf ein Versagen eines kritischen Sicherheitskontrollsystems zu reagieren und mindestens alle in dieser Anforderung angegebenen Elemente enthalten.	
	10.7.3.b Aufzeichnungen untersuchen, um zu verifizieren, dass Versagen von kritischen Sicherheitskontrollsystemen dokumentiert werden, einschließlich: • Identifizierung der Ursache(n) des Versagens. • Dauer (Datum und Zeit Beginn und Ende) des Sicherheitsversagens. • Details zur erforderlichen Behebung, die erfordert ist, um die Grundursache zu adressieren.	
Zielsetzung des kundenspezifischen Ansatzes Versagen von kritischen Sicherheitskontrollsystemen werden analysiert, eingedämmt und behoben, und Sicherheitskontrollen werden wiederhergestellt, um die Auswirkung zu minimieren. Daraus resultierende Sicherheitsprobleme werden adressiert und Maßnahmen werden ergriffen, um ein erneutes Auftreten zu verhindern.		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit		
Dieses Erfordernis gilt nur, wenn es sich bei der zu beurteilenden Entität um einen Dienstleistungsanbieter handelt, bis zum 31. März 2025, nach dem diese Anforderung für alle Entitäten gelten wird. *Dies ist eine aktuelle v3.2.1-Anforderung, die nur für Dienstleistungsanbieter gilt. Diese Anforderung ist aber bis zum 31. März 2025 eine bewährte Praktik für alle anderen Entitäten, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderung 11: Regelmäßige Prüfung der Sicherheit von Systemen und Netzen

Abschnitte	
11.1	Prozesse und Mechanismen zum regelmäßigen Testen der Sicherheit von Systemen und Netzwerken werden definiert und verstanden.
11.2	Drahtlose Zugangspunkte werden identifiziert und überwacht, und nicht autorisierte drahtlose Zugangspunkte werden adressiert.
11.3	Externe und interne Schwachstellen werden regelmäßig identifiziert, priorisiert und adressiert.
11.4	Externe und interne Penetrationstests werden regelmäßig durchgeführt, und ausnutzbare Schwachstellen und Sicherheitsschwächen werden korrigiert.
11.5	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und es wird darauf reagiert.
11.6	Nicht autorisierte Änderungen auf Zahlungsseiten werden erkannt und es wird darauf reagiert.

Übersicht

Schwachstellen werden ständig von böswilligen Personen und Forschern entdeckt, und durch neue Software eingeführt. Systemkomponenten, Prozesse, und maßgeschneiderte und kundenspezifische Software sollten häufig getestet werden, um sicherzustellen, dass die Sicherheitskontrollen weiterhin eine sich ändernde Umgebung widerspiegeln.

Finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
11.1 Prozesse und Mechanismen zum regelmäßigen Testen der Sicherheit von Systemen und Netzwerken werden definiert und verstanden.		
Definierte Ansatzanforderungen **11.1.1** Alle Sicherheitsrichtlinien und Betriebsprozeduren, die in Anforderung 11 identifiziert werden, sind: • Dokumentiert. • Auf dem neuesten Stand gehalten. • In Verwendung. • Allen betroffenen Parteien bekannt. **Zielsetzung des kundenspezifischen Ansatzes** Erwartungen, Kontrollen und Aufsicht für Besprechungsaktivitäten gemäß Anforderung 11 werden vom betroffenen Personal definiert und eingehalten. Alle unterstützenden Aktivitäten sind wiederholbar, werden konsequent angewendet und entsprechen der Absicht der Verwaltung.	**Testprozeduren mit definiertem Ansatz** **11.1.1** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass Sicherheitsrichtlinien und Betriebsprozeduren gemäß allen in dieser Anforderung angegebenen Elementen verwaltet werden.	**Zweck** Bei Anforderung 11.1.1 geht es um die effektive Verwaltung und Wartung der verschiedenen Richtlinien und Prozeduren, die in Anforderung 11 angegeben sind. Während es wichtig ist, die in Anforderung 11 genannten spezifischen Richtlinien oder Verfahren zu definieren, ist es ebenso wichtig sicherzustellen, dass sie ordnungsgemäß dokumentiert, gewartet und verbreitet werden. **Gute Praxis** Es ist wichtig, Richtlinien und Prozeduren nach Bedarf zu aktualisieren, um Änderungen in Prozessen, Technologien und Geschäftszielsetzungen zu berücksichtigen. Ziehen Sie aus diesem Grund in Erwägung, diese Dokumente so schnell wie möglich nach einer Änderung zu aktualisieren und nicht nur in einem periodischen Zyklus. **Definitionen** Sicherheitsrichtlinien definieren die Sicherheitszielsetzungen und -prinzipien der Entität. Betriebliche Prozeduren beschreiben die Durchführung von Aktivitäten und definieren die Kontrollen, Verfahren und Prozesse, die befolgt werden, um das gewünschte Ergebnis auf konsistente Weise und gemäß den Richtlinien-Zielsetzungen zu erzielen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn Rollen und Verantwortlichkeiten nicht formell zugewiesen sind, ist das Personal sich möglicherweise seiner täglichen Verantwortlichkeiten nicht bewusst und kritische Aktivitäten können nicht stattfinden. **Gute Praxis** Rollen und Verantwortlichkeiten können in Richtlinien und Verfahren dokumentiert oder in separaten Dokumenten gewartet werden. Als Teil der Kommunikation von Rollen und Verantwortlichkeiten können Entitäten erwägen, dass das Personal seine Akzeptanz und ihr Verständnis der ihnen zugewiesenen Rollen und Verantwortlichkeiten anerkennen. **Beispiele** Ein Verfahren zum Dokumentieren von Rollen und Verantwortlichkeiten ist eine Verantwortlichkeits-Zuweisungsmatrix, die beinhaltet, wer verantwortlich, rechenschaftspflichtig, konsultiert und informiert ist (auch RACI-Matrix genannt).
11.1.2 Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 11 werden dokumentiert, zugewiesen und verstanden.	**11.1.2.a** Die Dokumentation untersuchen, um zu verifizieren, dass die Beschreibungen der Rollen und Verantwortlichkeiten für die Durchführung von Aktivitäten in Anforderung 11 dokumentiert und zugewiesen sind.	
	11.1.2.b Personal mit Verantwortlichkeit zur Durchführung von Aktivitäten in Anforderung 11 befragen, um zu verifizieren, ob Rollen und Verantwortlichkeiten wie dokumentiert zugewiesen und verstanden wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten in Anforderung 11 werden zugewiesen. Das Personal ist für die erfolgreiche und kontinuierliche Umsetzung dieser Anforderungen verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
11.2 Drahtlose Zugangspunkte werden identifiziert und überwacht, und nicht autorisierte drahtlose Zugangspunkte werden adressiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
11.2.1 Autorisierte und nicht autorisierte drahtlose Zugangspunkte werden wie folgt verwaltet: • Das Vorhandensein von drahtlosen (Wi-Fi) Zugangspunkten wird getestet für: • Alle autorisierten und nicht autorisierten drahtlosen Zugangspunkte werden erkannt und identifiziert, • Testen, Erkennen und Identifizierung findet mindestens einmal alle drei Monate statt. • Wenn automatisierte Überwachung verwendet wird, dann wird das Personal über generierte Warnungen benachrichtigt.	**11.2.1.a** Richtlinien und Verfahren untersuchen, um zu verifizieren, dass Prozesse für die Verwaltung autorisierter und nicht autorisierter drahtloser Zugangspunkte mit allen in dieser Anforderung angegebenen Elementen definiert sind. **11.2.1.b** Die verwendete(n) Methodik(en) und die daraus resultierende Dokumentation untersuchen, und das Personal befragen, um zu verifizieren, dass Prozesse definiert sind, um autorisierte und nicht autorisierte drahtlose Zugangspunkte gemäß allen in dieser Anforderung angegebenen Elementen zu erkennen und zu identifizieren. **11.2.1.c** Drahtlose Beurteilungsergebnisse untersuchen und das Personal befragen, um zu verifizieren, dass drahtlose Beurteilungen gemäß allen in dieser Anforderung angegebenen Elementen ausgeführt wurden. **11.2.1.d** Wenn eine automatisierte Überwachung verwendet wird, die Konfigurationseinstellungen untersuchen, um zu verifizieren, dass die Konfiguration Warnungen generiert, um das Personal zu benachrichtigen.	Die Implementierung und Ausnutzung von drahtloser Technologie innerhalb eines Netzwerks sind üblicher Wege für böswillige Benutzer, um nicht autorisierten Zugriff auf das Netzwerk und die Karteninhaberdaten zu erhalten. Nicht autorisierte drahtlose Geräte könnten in einem Computer oder einer anderen Systemkomponente versteckt oder daran angeschlossen sein. Diese Geräte könnten auch direkt an einen Netzwerkanschluss, an ein Netzwerkgerät wie einen Schalter oder Router angeschlossen oder als drahtlose Schnittstellenkarte in eine Systemkomponente eingesetzt werden. Wenn ein drahtloses Gerät oder Netzwerk ohne Wissen eines Unternehmens installiert wird, kann es einem Angreifer gestatten, leicht und „unsichtbar“ in das Netzwerk einzudringen. Das Erkennen und Entfernen solcher nicht autorisierter Zugangspunkte verringert die Dauer und die Wahrscheinlichkeit, dass solche Geräte für einen Angriff ausgenutzt werden. **Gute Praxis** Die Größe und Komplexität einer Umgebung werden die geeigneten Tools und Prozesse vorschreiben, die verwendet werden müssen, um ausreichend Gewissheit zu geben, dass kein unerlaubter drahtloser Zugangspunkt in der Umgebung installiert wurde. Zum Beispiel kann die Durchführung einer detaillierten physischen Inspektion eines alleinstehenden Einzelhandelskiosks in einem Einkaufszentrum, *(Fortsetzung auf der nächsten Seite)*
Zielsetzung des kundenspezifischen Ansatzes Nicht autorisierte drahtlose Zugangspunkte werden regelmäßig identifiziert und adressiert.		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Die Anforderung gilt selbst dann, wenn eine Richtlinie existiert, die die Verwendung von drahtloser Technologie verbietet, da Angreifer die Unternehmensrichtlinie nicht lesen und befolgen. Die zur Erfüllung dieser Anforderung verwendeten Methoden müssen ausreichen, um sowohl autorisierte als auch nicht autorisierte Geräte zu erkennen und zu identifizieren, einschließlich nicht autorisierter Geräte, die an Geräten angeschlossen sind, die selbst autorisiert sind.		in dem alle Kommunikationskomponenten in manipulationsresistenten und manipulationssicheren Gehäusen untergebracht sind, ausreichen, um sicherzustellen, dass ein betrügerischer drahtloser Zugangspunkt nicht angebracht oder installiert ist. In einer Umgebung mit mehreren Knoten (wie in einem großen Einzelhandelsgeschäft, Call-Center, Serverraum oder Rechenzentrum) kann jedoch eine detaillierte physische Inspektion schwierig sein. In diesem Fall können mehrere Methoden kombiniert werden, wie beispielsweise das Durchführen von physischen Systeminspektionen in Verbindung mit den Ergebnissen eines drahtlosen Analysators. **Definitionen** Dies wird auch als unerlaubte Zugangspunkt-Erkennung bezeichnet. **Beispiele** Methoden, die verwendet werden können, umfassen, sind aber nicht beschränkt auf drahtlose Netzwerkscans, physische/logische Inspektionen von Systemkomponenten und Infrastruktur, Netzwerkzugriffskontrolle (NAC) oder drahtloses IDS/IPS. NAC und drahtloses IDS/IPS sind Beispiele für automatisierte Überwachungstools.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ein Inventar von autorisierten drahtlosen Zugangspunkten kann Administratoren helfen, schnell zu reagieren, wenn nicht autorisierte drahtlose Zugangspunkte erkannt werden. Dies hilft dabei, die Exposition von CDE gegenüber böswilligen Personen proaktiv zu minimieren. **Gute Praxis** Wenn ein drahtloser Scanners verwendet wird, ist es ebenso wichtig, eine definierte Liste bekannter Zugangspunkte zu haben, die zwar nicht mit dem Unternehmensnetzwerk verbunden sind, aber normalerweise während eines Scans erkannt werden. Diese unternehmensfremden Geräte sind häufig in Gebäuden mit mehreren Mietern oder in nahe beieinander liegenden Unternehmen zu finden. Es ist jedoch wichtig, zu verifizieren, dass diese Geräte nicht mit dem Netzwerkport der Entität oder über ein anderes mit dem Netzwerk verbundenes Gerät verbunden sind und eine SSID erhalten, die einem nahegelegenen Unternehmen ähnelt. Scan-Ergebnisse sollten solche Geräte vermerken und wie erkannt wurde, dass diese Geräte „ignoriert“ werden könnten. Darüber hinaus sollte die Erkennung von nicht autorisierten drahtlosen Zugangspunkten, die als Bedrohung für die CDE erkannt werden, gemäß dem Vorfallreaktionsplan der Entität gemäß Anforderung 12.10.1 verwaltet werden.
11.2.2 Es wird ein Inventar autorisierter drahtloser Zugangspunkte geführt, einschließlich einer dokumentierten geschäftlichen Rechtfertigung.	**11.2.2** Die Dokumentation untersuchen, um zu verifizieren, dass ein Inventar von autorisierten drahtlosen Zugangspunkten geführt wird und eine geschäftliche Rechtfertigung für alle autorisierten drahtlosen Zugangspunkte dokumentiert wird.	
Zielsetzung des kundenspezifischen Ansatzes		
Nicht autorisierte drahtlose Zugangspunkte werden nicht mit autorisierten drahtlosen Zugangspunkten verwechselt.		

Anforderungen und Testprozeduren		Anleitungen
11.3 Externe und interne Schwachstellen werden regelmäßig identifiziert, priorisiert und adressiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
11.3.1 Interne Schwachstellen-Scans werden wie folgt durchgeführt: • Mindestens einmal alle drei Monate. • Risikoreiche und kritische Schwachstellen (gemäß den in Anforderung 6.3.1 definierten Schwachstellenrisiko-Einstufungen der Entität) werden behoben. • Es werden erneute Scans durchgeführt, die bestätigen, dass alle risikoreichen und kritischen Schwachstellen (wie oben erwähnt) behoben wurden. • Das Scan-Tool wird mit den neuesten Schwachstelleninformationen auf dem neuesten Stand gehalten. • Scans werden von qualifiziertem Personal durchgeführt und es besteht organisatorische Unabhängigkeit des Testers.	**11.3.1.a** Interne Scanbericht-Ergebnisse der letzten 12 Monate untersuchen, um zu verifizieren, dass interne Scans in den letzten 12 Monaten mindestens alle drei Monate aufgetreten sind. **11.3.1.b** Interne Scanbericht-Ergebnisse von jedem Scan- und erneutem Scan-Lauf in den letzten 12 Monaten untersuchen, um zu verifizieren, dass alle risikoreichen und kritischen Schwachstellen (identifiziert in PCI DSS-Anforderung 6.3.1) behoben sind. **11.3.1.c** Scan-Tool-Konfigurationen untersuchen und das Personal befragen, um zu verifizieren, dass das Scan-Tool mit den neuesten Schwachstelleninformationen auf dem neuesten Stand ist. **11.3.1.d** Verantwortliches Personal befragen, um zu verifizieren, dass der Scan von einer qualifizierten internen Ressource(n) oder einem qualifizierten externen Dritten durchgeführt wurde und dass die organisatorische Unabhängigkeit des Testers besteht.	Die umgehende Identifizierung und Adressierung von Schwachstellen verringert die Wahrscheinlichkeit, dass eine Schwachstelle ausgenutzt wird und den potenziellen Kompromiss von einer Systemkomponente oder Karteninhaberdaten. Schwachstellen-Scans, die mindestens alle drei Monate ausgeführt werden, stellen diese Erkennung und Identifizierung bereit. **Gute Praxis** Schwachstellen, die das größte Risiko für die Umgebung darstellen (zum Beispiel gemäß Anforderung 6.3.1 als hoch oder kritisch eingestuft) sollten mit höchster Priorität behoben werden. Mehrere Scan-Berichte können für den vierteljährlichen Scan-Prozess kombiniert werden, um zu zeigen, dass alle Systeme gescannt und alle zutreffenden Schwachstellen im Rahmen des dreimonatigen Schwachstellen-Scan-Zyklus behoben wurden. Es kann jedoch eine zusätzliche Dokumentation erforderlich sein, um zu verifizieren, dass nicht behobene Schwachstellen gerade behoben werden. Obwohl Scans mindestens alle drei Monate erforderlich sind, werden häufigere Scans empfohlen, abhängig von der Netzwerkkomplexität, der Häufigkeit der Änderung und den Arten der verwendeten Geräte, Software und Betriebssysteme. **Definitionen** Ein Schwachstellen-Scan ist eine Kombination aus automatisierten Tools, Techniken und/oder Methoden, die auf externen und internen Geräten und Servern ausgeführt werden, um potenzielle Schwachstellen in Anwendungen, *(Fortsetzung auf der nächsten Seite)*
Zielsetzung des kundenspezifischen Ansatzes Die Sicherheitshaltung aller Systemkomponenten wird regelmäßig mit automatisierten Tools verifiziert, die entwickelt wurden, um Schwachstellen innerhalb des Netzwerks zu erkennen. Erkannte Schwachstellen werden basierend auf einem formalen Risikobeurteilungsrahmens bewertet und behoben. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Es ist nicht erforderlich, einen QSA oder ASV zu verwenden, um interne Schwachstellen-Scans auszuführen. Interne Schwachstellen-Scans können von qualifizierten internen Mitarbeitern durchgeführt werden, die einigermaßen unabhängig von der/den zu scannenden Systemkomponente(n) sind (zum Beispiel sollte ein Netzwerkadministrator nicht für das Scannen des Netzwerks verantwortlich sein), oder eine Entität kann sich dafür entscheiden, interne Schwachstellen-Scans von einer auf Schwachstellen-Scans spezialisierten Firma durchführen zu lassen.		Betriebssystemen und Netzwerkgeräten aufzudecken, die von böswilligen Personen gefunden und ausgenutzt werden könnten.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
11.3.1.1 Alle anderen anwendbaren Schwachstellen (die nicht als risikoreich oder kritisch eingestuft werden (gemäß den Schwachstellenrisikoeinstufungen der Entität, die in Anforderung 6.3.1 definiert sind) werden wie folgt verwaltet: • Adressiert basierend auf dem Risiko, das in der gezielten Risikoanalyse der Entität definiert ist, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird. • Erneute Scans werden nach Bedarf ausgeführt.	**11.3.1.1.a** Die gezielte Risikoanalyse der Entität, die das Risiko für die Adressierung aller anderen anwendbaren Schwachstellen definiert (die gemäß den Schwachstellenrisikoeinstufungen der Entität gemäß Anforderung 6.3.1 nicht als risikoreich oder kritisch eingestuft wurden) untersuchen, um zu verifizieren, dass die Risikoanalyse gemäß allen in Anforderung angegebenen 12.3.1 durchgeführt wurde.	Alle Schwachstellen, unabhängig von ihrer Kritikalität, stellen einen potenziellen Angriffsweg bereit und müssen daher regelmäßig adressiert werden, wobei die Schwachstellen, die das größte Risiko darstellen, schneller behoben werden, um das potenzielle Angriffsfenster zu begrenzen.
Zielsetzung des kundenspezifischen Ansatzes	**11.3.1.1.b** Verantwortliches Personal befragen und interne Scan-Berichtergebnisse oder andere Dokumentation untersuchen, um zu verifizieren, dass alle anderen anwendbaren Schwachstellen (die nicht als risikoreich oder kritisch gemäß den Schwachstellenrisiko-Einstufungen der Entität in Anforderung 6.3.1 eingestuft sind) basierend auf dem in der Definition definierten Risiko adressiert werden, und dass der Scan-Prozess bei Bedarf erneute Scans umfasst, um zu bestätigen, dass die Schwachstellen adressiert wurden.	
Schwachstellen niedrigeren Ranges (niedriger als hoch oder kritisch) werden in einer Häufigkeit adressiert, die dem Risiko der Entität entspricht.		
Hinweise zur Anwendbarkeit		
Der Zeitrahmen für die Adressierung von Schwachstellen mit geringerem Risiko hängt von den Ergebnissen einer Risikoanalyse gemäß Anforderung 12.3.1 ab, die (mindestens) die Identifizierung von geschützten Assets, Bedrohungen und der Wahrscheinlichkeit und/oder Auswirkung einer Realisierung einer Bedrohung umfasst. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Authentifiziertes Scannen stellt einen besseren Einblick in die Schwachstellenlandschaft einer Entität bereit, da es Schwachstellen erkennen kann, die nicht authentifizierte Scans nicht erkennen können. Angreifer können Schwachstellen ausnutzen, die einer Entität nicht bekannt sind, da bestimmte Schwachstellen nur durch authentifiziertes Scannen erkannt werden. Authentifiziertes Scannen kann wichtige zusätzliche Informationen über die Schwachstellen einer Organisation liefern. **Gute Praxis** Die für diese Scans verwendeten Berechtigungsnachweise sollten als sehr privilegiert angesehen werden. Sie sollten entsprechend den PCI DSS-Anforderungen 7 und 8 als solche geschützt und kontrolliert werden (mit Ausnahme der Anforderungen für Multi-Faktor-Authentifizierung und Anwendungs- und Systemkonten).
11.3.1.2 Interne Schwachstellen-Scans werden über authentifiziertes Scannen wie folgt durchgeführt: • Systeme, die keine Berechtigungsnachweise für authentifiziertes Scannen akzeptieren können, werden dokumentiert. • Ausreichende Privilegien werden für Systeme verwendet, die Berechtigungsnachweise zum Scannen akzeptieren. • Wenn Konten, die für authentifiziertes Scannen verwendet werden, für die interaktive Anmeldung verwendet werden können, dann werden diese gemäß Anforderung 8.2.2 verwaltet.	**11.3.1.2.a** Scan-Tool-Konfigurationen untersuchen, um zu verifizieren, dass authentifiziertes Scannen für interne Scans mit ausreichenden Privilegien für Systeme verwendet wird, die Berechtigungsnachweise zum Scannen akzeptieren.	
	11.3.1.2.b Scan-Berichtergebnisse untersuchen und das Personal befragen, um zu verifizieren, dass authentifizierte Scans durchgeführt werden.	
	11.3.1.2.c Wenn Konten, die für das authentifizierte Scannen verwendet werden, für die interaktive Anmeldung verwendet werden können, die Konten untersuchen und das Personal befragen, um zu verifizieren, dass die Konten gemäß allen in Anforderung 8.2.2 angegebenen Elementen verwaltet werden.	
Zielsetzung des kundenspezifischen Ansatzes Automatisierte Tools zur Erkennung von Schwachstellen können lokale Schwachstellen jedes Systems erkennen, die aus der Ferne nicht sichtbar sind.	**11.3.1.2.d** Dokumentation untersuchen, um zu verifizieren, dass Systeme, die Referenzen für authentifiziertes Scannen nicht akzeptieren können, definiert sind.	
Hinweise zur Anwendbarkeit Die authentifizierten Scan-Tools können entweder hostbasiert oder netzwerkbasiert sein. „Ausreichende“ Privilegien sind diejenigen, die für den Zugriff auf Systemressourcen erforderlich sind, damit ein gründlicher Scan durchgeführt werden kann, der bekannte Schwachstellen erkennt. Diese Anforderung gilt nicht für Systemkomponenten, die keine Berechtigungsnachweise zum Scannen akzeptieren können. Beispiele für Systeme, die möglicherweise keine Berechtigungsnachweise zum Scannen akzeptieren, umfassen einige Netzwerk- und Sicherheitsanwendungen, Mainframes und Container. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.		
Definierte Ansatzanforderungen **11.3.1.3** Interne Schwachstellen-Scans werden nach jeder bedeutenden Änderung wie folgt durchgeführt: • Risikoreiche und kritische Schwachstellen (gemäß den in Anforderung 6.3.1 definierten Schwachstellenrisiko-Einstufungen der Entität) werden behoben. • Erneute Scans werden nach Bedarf ausgeführt. • Scans werden von qualifiziertem Personal durchgeführt und es besteht organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein). **Zielsetzung des kundenspezifischen Ansatzes** Die Sicherheitshaltung aller Systemkomponenten wird nach wesentlichen Änderungen des Netzwerks oder der Systeme mit automatisierten Tools verifiziert, die entwickelt wurden, um Schwachstellen innerhalb des Netzwerks zu erkennen. Erkannte Schwachstellen werden basierend auf einem formalen Risikobeurteilungsrahmens bewertet und behoben. **Hinweise zur Anwendbarkeit** Ein authentifizierter interner Schwachstellen-Scan gemäß Anforderung 11.3.1.2 ist für Scans, die nach wesentlichen Änderungen durchgeführt werden, nicht erforderlich.	**Testprozeduren mit definiertem Ansatz** **11.3.1.3.a** Änderungsdokumentation und interne Scanberichte untersuchen, um zu verifizieren, dass Systemkomponenten nach bedeutenden Änderungen gescannt wurden. **11.3.1.3.b** Das Personal befragen und interne Scan- und erneute Scan-Berichte untersuchen, um zu verifizieren, dass interne Scans nach bedeutenden Änderungen durchgeführt wurden und dass wie in Anforderung 6.3.1 definierte risikoreiche und kritische Schwachstellen behoben wurden. **11.3.1.3.c** Das Personal befragen, um zu verifizieren, dass interne Scans von einer qualifizierten internen Ressource(n) oder einem qualifizierten externen Dritten durchgeführt wurden und dass die organisatorische Unabhängigkeit des Testers besteht.	**Zweck** Durch das Scannen einer Umgebung nach bedeutenden Änderungen wird sichergestellt, dass die Änderungen ordnungsgemäß abgeschlossen wurden, sodass die Sicherheit der Umgebung durch die Änderung nicht gefährdet wurde. **Gute Praxis** Entitäten sollten Scans nach bedeutenden Änderungen im Rahmen des Änderungsprozesses gemäß Anforderung 6.5.2 durchführen und bevor die Änderung als abgeschlossen betrachtet wird. Alle von der Änderung betroffenen Systemkomponenten müssen gescannt werden.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
11.3.2 Externe Schwachstellen-Scans werden wie folgt durchgeführt: • Mindestens einmal alle drei Monate. • Von einem PCI SSC-zugelassenem Scanning-Anbieter (ASV). • Schwachstellen werden behoben und die Anforderungen des ASV-Programmhandbuchs für einen bestandenen Scan werden erfüllt. • Erneute Scans werden nach Bedarf durchgeführt, um zu bestätigen, dass Schwachstellen gemäß den Anforderungen des ASV-Programmhandbuchs für einen bestandenen Scan behoben wurden.	**11.3.2.a** ASV-Scanberichte der letzten 12 Monate untersuchen, um zu verifizieren, dass externe Schwachstellen-Scans in den letzten 12 Monaten mindestens alle drei Monate aufgetreten sind. **11.3.2.b** Die ASV-Scan-Berichtergebnisse aus jedem Scan- und erneuten Scan-Lauf in den letzten 12 Monaten untersuchen, um zu verifizieren, dass Schwachstellen behoben sind und die Anforderungen des ASV-Programmhandbuchs für einen bestandenen Scan erfüllt sind. **11.3.2.c** ASV-Scanberichte untersuchen, um zu verifizieren, dass die Scans von einem PCI SSC-Zugelassenen Scanning-Anbieter (ASV) durchgeführt wurden.	Angreifer suchen routinemäßig nach ungepatchten oder anfälligen externen Servern, die für einen gezielten Angriff genutzt werden können. Organisationen müssen sicherstellen, dass diese nach außen gerichteten Geräte regelmäßig auf Schwachstellen überprüft werden und dass Schwachstellen gepatcht oder behoben werden, um die Entität zu schützen. Da externe Netzwerke einem größeren Risiko ausgesetzt sind, um kompromittiert zu werden, müssen externe Schwachstellen-Scans mindestens alle drei Monate von einem PCI SSC-Zugelassenen Scanning-Anbieter(ASV) durchgeführt werden.
Zielsetzung des kundenspezifischen Ansatzes		**Gute Praxis**
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		Obwohl Scans mindestens alle drei Monate erforderlich sind, werden häufigere Scans empfohlen, abhängig von der Netzwerkkomplexität, der Häufigkeit der Änderung und den Arten der verwendeten Geräte, Software und Betriebssysteme. Mehrere Scan-Berichte können kombiniert werden, um zu zeigen, dass alle Systeme gescannt und dass alle zutreffenden Schwachstellen im Rahmen des dreimonatigen Schwachstellen-Scan-Zyklus behoben wurden. Es kann jedoch eine zusätzliche Dokumentation erforderlich sein, um zu verifizieren, dass nicht behobene Schwachstellen gerade behoben werden.
Hinweise zur Anwendbarkeit		
Für die anfängliche PCI DSS-Einhaltung ist es nicht erforderlich, dass vier bestandene Scans innerhalb von 12 Monaten abgeschlossen werden, wenn der Beurteiler Folgendes verifiziert: 1) das letzte Scan-Ergebnis war ein bestandener Scan, 2) die Entität hat dokumentierte Richtlinien und Prozeduren, die einen Scan mindestens alle drei Monate erfordern, und 3) in den Scan-Ergebnissen festgestellte Schwachstellen wurden korrigiert, wie in einem oder mehreren erneuten Scans gezeigt. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
In den folgenden r Jahren nach der ersten PCI DSS-Beurteilung müssen jedoch mindestens alle drei Monate bestandene Scans stattgefunden haben. ASV-Scan-Tools können ein breites Spektrum von Netzwerktypen und -topologien scannen. Alle Besonderheiten der Zielumgebung (z. B. Load Balancer, Drittanbieter, ISPs, spezifische Konfigurationen, verwendete Protokolle, Scan-Interferenzen) sollten zwischen dem ASV und dem Scan-Kunden ausgearbeitet werden. Informationen zu den Verantwortlichkeiten des Scan-Kunden, der Scan-Vorbereitung usw. finden Sie im *ASV-Programmhandbuch*, das auf der PCI SSC-Website veröffentlicht ist.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Durch das Scannen einer Umgebung nach bedeutenden Änderungen wird sichergestellt, dass die Änderungen ordnungsgemäß abgeschlossen wurden, sodass die Sicherheit der Umgebung durch die Änderung nicht gefährdet wurde. **Gute Praxis** Entitäten sollten die Notwendigkeit umfassen, Scans nach bedeutenden Änderungen im Rahmen des Änderungsprozesses durchführen und bevor die Änderung als abgeschlossen betrachtet wird. Alle von der Änderung betroffenen Systemkomponenten müssen gescannt werden.
11.3.2.1 Interne Schwachstellen-Scans werden nach jeder bedeutenden Änderung wie folgt durchgeführt: • Schwachstellen, die vom CVSS mit 4.0 oder höher bewertet werden, werden behoben. • Erneute Scans werden nach Bedarf ausgeführt. • Scans werden von qualifiziertem Personal durchgeführt und es besteht organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein).	**11.3.2.1.a** Änderungsdokumentation und externe Scanberichte untersuchen, um zu verifizieren, dass Systemkomponenten nach bedeutenden Änderungen gescannt wurden. **11.3.2.1.b** Das Personal befragen und externe Scan- und erneute Scan-Berichte untersuchen, um zu verifizieren, dass externe Scans nach bedeutenden Änderungen durchgeführt wurden und dass Schwachstellen, die vom CVSS mit 4.0 oder höher bewertet wurden, behoben wurden. **11.3.2.1.c** Das Personal befragen, um zu verifizieren, dass externe Scans von einer qualifizierten internen Ressource(n) oder einem qualifizierten externen Dritten durchgeführt wurden und dass die organisatorische Unabhängigkeit des Testers besteht.	
Zielsetzung des kundenspezifischen Ansatzes		
Die Sicherheitshaltung aller Systemkomponenten wird nach wesentlichen Änderungen des Netzwerks oder der Systeme mit Tools verifiziert, die entwickelt wurden, um Schwachstellen außerhalb des Netzwerks zu erkennen. Erkannte Schwachstellen werden basierend auf einem formalen Risikobeurteilungsrahmens bewertet und behoben.		

Anforderungen und Testprozeduren		Anleitungen
11.4 Externe und interne Penetrationstests werden regelmäßig durchgeführt, und ausnutzbare Schwachstellen und Sicherheitsschwächen werden korrigiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	
11.4.1 Eine Penetrationstest-Methodik wird von der Entität definiert, dokumentiert und implementiert und umfasst: • In der Branche akzeptierte Penetrationstestansätze. • Abdeckung für den gesamten CDE-Umkreis und die kritischen Systeme. • Tests sowohl innerhalb als auch außerhalb des Netzwerks. • Tests, um Segmentierung und Geltungsbereichs-Reduzierungskontrollen zu validieren. • Penetrationstests auf Anwendungsebene, um mindestens die in Anforderung 6.2.4 aufgeführten Schwachstellen zu identifizieren. • Penetrationstests auf Netzwerkebene, die alle Komponenten umfassen, die Netzwerkfunktionen sowie Betriebssysteme unterstützen. • Überprüfung und Berücksichtigung von Bedrohungen und Schwachstellen, die in den letzten 12 Monaten erfahren wurden. • Dokumentierter Ansatz zur Beurteilung und Adressierung des Risikos durch ausnutzbare Schwachstellen und Sicherheitsschwächen, die bei Penetrationstests gefunden werden. • Aufbewahrung der Ergebnisse der Penetrationstests und der Ergebnisse der Behebungsaktivitäten für mindestens 12 Monate.	**11.4.1** Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die von der Entität definierte, dokumentierte und implementierte Penetrationstest-Methodik alle in dieser Anforderung angegebenen Elemente umfasst.	**Zweck** Angreifer verbringen viel Zeit damit, externe und interne Schwachstellen zu finden, um sie auszunutzen, um Zugriff auf Karteninhaberdaten zu erhalten und diese Daten dann zu exfiltrieren. Daher müssen Entitäten ihre Netzwerke gründlich testen, genau wie es ein Angreifer tun würde. Dieses Testen gestattet der Entität, Schwachstellen zu identifizieren und zu beheben, die genutzt werden könnten, um das Netzwerk und die Daten der Entität zu gefährden, und dann geeignete Maßnahmen zu ergreifen, um das Netzwerk und die Systemkomponenten vor solchen Angriffen zu schützen. **Gute Praxis** Penetrationstesttechniken unterscheiden sich je nach Bedarf und Struktur einer Organisation und sollten für die getestete Umgebung geeignet sein – zum Beispiel können Fuzzing-, Injektions- und Fälschungstests angemessen sein. Die Art, Tiefe und Komplexität der Tests hängen von der spezifischen Umgebung und den Bedürfnissen der Organisation ab. **Definitionen** Penetrationstests simulieren eine reale Angriffssituation, um zu identifizieren, wie weit ein Angreifer in eine Umgebung eindringen könnte, wenn dem Tester unterschiedliche Informationen bereitgestellt werden. Dies gestattet einer Entität, ihre potenzielle Exposition besser zu verstehen und eine Strategie zur Abwehr von Angriffen zu entwickeln. Ein Penetrationstest unterscheidet sich von einem Schwachstellen-Scan, da ein Penetrationstest ein aktiver Prozess ist, der in der Regel das Ausnutzen identifizierter Schwachstellen beinhaltet. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Für gründliche technische Tests wird eine formale Methodik definiert, die versucht, Schwachstellen und Sicherheitsschwächen durch simulierte Angriffsmethoden eines kompetenten manuellen Angreifers auszunutzen. **Hinweise zur Anwendbarkeit** Das Testen innerhalb des Netzwerks (oder „internes Penetrationstesten“) bedeutet das Testen sowohl innerhalb der CDE als auch in die CDE von vertrauenswürdigen und nicht vertrauenswürdigen internen Netzwerken. Das Testen von außerhalb des Netzwerks (oder „externes“ Penetrationstesten) bedeutet das Testen des exponierten externen Umkreises von vertrauenswürdigen Netzwerken und kritischen Systemen, die mit öffentlichen Netzwerkinfrastrukturen verbunden sind oder darauf zugänglich sind.		Das alleinige Scannen auf Schwachstellen ist kein Penetrationstest, und ein Penetrationstest ist auch nicht ausreichend, wenn ausschließlich versucht wird, Schwachstellen auszunutzen, die in einem Schwachstellen-Scan gefunden wurden. Die Ausführung eines Schwachstellen-Scans kann einer der ersten Schritte sein, aber es ist nicht der einzige Schritt, den ein Penetrationstester zur Planung der Teststrategie durchführt. Auch wenn ein Schwachstellen-Scan bekannte Schwachstellen nicht erkennt, gewinnt der Penetrationstester oft genug Wissen über das System, um mögliche Sicherheitsschwächen zu erkennen. Penetrationstesten ist ein sehr manueller Prozess. Während einige automatisierte Tools verwendet werden können, nutzt der Tester seine Systemkenntnisse, um Zugriff auf eine Umgebung zu erhalten. Der Tester verkettet häufig mehrere Arten von Ausnutzungen mit dem Ziel, Verteidigungschichten zu durchbrechen. Zum Beispiel wenn der Tester einen Weg findet, Zugriff auf einen Anwendungsserver zu erhalten, dann verwendet der Tester den kompromittierten Server als Ausgangspunkt, um einen neuen Angriff basierend auf den Ressourcen, auf die der Server Zugriff hat, zu inszenieren. Auf diese Weise kann ein Tester die Techniken simulieren, die ein Angreifer verwendet, um potenzielle Schwachstellen in der Umgebung zu identifizieren. Das Testen von Sicherheitsüberwachungs- und -Erkennungsmethoden - zum Beispiel, um die Wirksamkeit von Protokollierungs- und Dateiintegritätsüberwachungsmechanismen zu bestätigen, sollte ebenfalls in Betracht gezogen werden. *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Weitere Informationen Siehe die *Informationsergänzung: Penetrationstestanleitungen* für zusätzliche Anleitungen. In der Branche akzeptierte Penetrationstestansätze beinhalten: *Die Offene-Quelle-Methodik für Sicherheitstests und Handbuch (OSSTMM)* *Open Web Application Security Project (OWASP) Penetrationstestprogramme.*
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
11.4.2 Interne Penetrationstests werden durchgeführt: • Gemäß der definierten Methodik der Entität, • Mindestens alle 12 Monate • Nach jeder bedeutenden Aktualisierung oder jeder Änderung der Infrastruktur oder Anwendung • Durch eine qualifizierte interne Ressource oder einen qualifizierten externen Dritten. • Organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein).	**11.4.2.a** Den Arbeitsumfang und die Ergebnisse des letzten internen Penetrationstests untersuchen, um zu verifizieren, dass Penetrationstesten gemäß allen in dieser Anforderung angegebenen Elementen durchgeführt wird.	Internes Penetrationstesten dient zwei Zwecken. Erstens entdeckt es wie ein externer Penetrationstest Schwachstellen und Fehlkonfigurationen, die von einem Angreifer ausgenutzt werden könnten, der sich einen gewissen Zugriff auf das interne Netzwerk verschafft hat, sei es, weil der Angreifer ein autorisierter Benutzer ist, der nicht autorisierte Aktivitäten ausführt, oder ein externer Angreifer, der es geschafft hatte, in den Umkreis der Entität einzudringen. Zweitens hilft internes Penetrationstesten den Entitäten auch, herauszufinden, wo ihr Änderungskontroll-Prozess gescheitert ist, indem sie bisher unbekannte Systeme erkennen. Zusätzlich überprüft es den Status vieler der Kontrollen, die innerhalb der CDE arbeiten. Ein Penetrationstest ist nicht wirklich ein „Test“, da das Ergebnis eines Penetrationstests nicht als „bestanden“ oder „nicht bestanden“ klassifiziert werden kann. Das beste Ergebnis eines Tests ist ein Katalog von Schwachstellen und Fehlkonfigurationen, von denen eine Entität nichts wusste und die der Penetrationstester gefunden hat, bevor ein Angreifer es konnte.
Zielsetzung des kundenspezifischen Ansatzes	**11.4.2.b** Das Personal befragen, um zu verifizieren, dass der interne Penetrationstest von einer qualifizierten internen Ressource oder einem qualifizierten externen Dritten durchgeführt wurde und dass die organisatorische Unabhängigkeit des Testers besteht (es ist nicht erforderlich, ein QSA oder ASV zu sein).	
Interne Systemverteidigungen werden durch technische Tests gemäß der von der Entität definierten Methodik so oft wie nötig überprüft, um sich entwickelnde und neue Angriffe und Bedrohungen zu adressieren und sicherzustellen, dass wesentliche Änderungen keine unbekannten Schwachstellen einführen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	*(Fortsetzung auf der nächsten Seite)* Ein Penetrationstest, der nichts gefunden hat, ist in der Regel ein Hinweis auf Mängel des Penetrationstesters statt ein positives Spiegelbild der Sicherheitshaltung der Entität. **Gute Praxis** Einige Überlegungen bei der Auswahl einer qualifizierten Ressource, um Penetrationstesten für durchzuführen sind: • Spezifische Penetrationstest-Zertifizierungen, die ein Hinweis auf das Fähigkeitsniveau und die Kompetenz des Testers sein können. • Frühere Erfahrungen mit der Durchführung von Penetrationstests – zum Beispiel die Anzahl der Jahre der Erfahrung sowie Art und Geltungsbereich früherer Engagements können dabei helfen, zu bestätigen, ob die Erfahrung des Testers für die Anforderungen des Engagements geeignet ist. **Weitere Informationen** Siehe die *Informationsergänzung: Penetrationstestanleitungen* auf der PCI SSC-Webseite für zusätzliche Anleitungen.
11.4.3 Externe Penetrationstests werden durchgeführt: • Gemäß der definierten Methodik der Entität, • Mindestens alle 12 Monate • Nach jeder bedeutenden Aktualisierung oder jeder Änderung der Infrastruktur oder Anwendung • Durch eine qualifizierte interne Ressource oder einen qualifizierten externen Dritten. • Organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein).	**11.4.3.a** Den Arbeitsumfang und die Ergebnisse des letzten externen Penetrationstests untersuchen, um zu verifizieren, dass Penetrationstesten gemäß allen in dieser Anforderung angegebenen Elementen durchgeführt wird.	
	11.4.3.b Das Personal befragen, um zu verifizieren, dass der externe Penetrationstest von einer qualifizierten internen Ressource oder einem qualifizierten externen Dritten durchgeführt wurde und dass die organisatorische Unabhängigkeit des Testers besteht (es ist nicht erforderlich, ein QSA oder ASV zu sein).	
Zielsetzung des kundenspezifischen Ansatzes		
Externe Systemverteidigungen werden durch technische Tests gemäß der von der Entität definierten Methodik so oft wie nötig überprüft, um sich entwickelnde und neue Angriffe und Bedrohungen zu adressieren und um sicherzustellen, dass wesentliche Änderungen keine unbekannten Schwachstellen einführen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Ergebnisse eines Penetrationstests sind normalerweise eine priorisierte Liste von Schwachstellen, die bei der Übung entdeckt wurden. Ein Tester wird häufig eine Reihe von Schwachstellen miteinander verkettet haben, um eine Systemkomponente zu kompromittieren. Das Beheben der durch einen Penetrationstest gefundenen Schwachstellen verringert die Wahrscheinlichkeit, dass dieselben Schwachstellen von einem böswilligen Angreifer ausgenutzt werden, deutlich. Die Verwendung des eigenen Schwachstellen-Risikobeurteilungsverfahrens der Entität (siehe Anforderung 6.3.1) stellt sicher, dass die Schwachstellen, die das höchste Risiko für die Entität darstellen, schneller behoben werden. **Gute Praxis** Im Rahmen der Risikobeurteilung der Entität sollten die Entitäten berücksichtigen, wie wahrscheinlich es ist, dass die Schwachstelle ausgenutzt wird und ob in der Umgebung andere Kontrollen vorhanden sind, um das Risiko zu reduzieren. Alle Schwachstellen, die darauf hindeuten, dass die PCI DSS-Anforderungen nicht erfüllt werden, sollten adressiert werden.
11.4.4 Ausnutzbare Schwachstellen und Sicherheitsschwächen, die bei Penetrationstests gefunden wurden, werden wie folgt korrigiert: • Entsprechend der Beurteilung der Entität bezüglich des Risikos durch das Sicherheitsproblem wie in Anforderung 6.3.1 definiert. • Penetrationstests werden wiederholt, um die Korrekturen zu verifizieren.	**11.4.4** Die Ergebnisse von Penetrationstests untersuchen, um zu verifizieren, dass festgestellte ausnutzbare Schwachstellen und Sicherheitsschwächen gemäß allen in dieser Anforderung angegebenen Elementen korrigiert wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Schwachstellen und Sicherheitsschwächen, die bei der Verifizierung der Systemabwehr gefunden wurden, werden gemildert.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn eine Entität Segmentierungskontrollen verwendet, um die CDE von internen nicht vertrauenswürdigen Netzwerken zu isolieren, hängt die Sicherheit der CDE von der Funktion der Segmentierung ab. Bei vielen Angriffen bewegte sich der Angreifer seitlich von einem, was eine Entität als isoliertes Netzwerk betrachtete, in die CDE. Die Verwendung von Penetrationstesttools und -techniken, um zu validieren, dass ein nicht vertrauenswürdiges Netzwerk tatsächlich von der CDE isoliert ist, kann die Entität auf einen Fehler oder eine Fehlkonfiguration der Segmentierungskontrollen aufmerksam machen, die dann behoben werden können. **Gute Praxis** Techniken wie Host-Entdeckung und Port-Scanning können verwendet werden um zu verifizieren, dass Segmente außerhalb der Geltungsbereichs keinen Zugriff auf die CDE haben.
11.4.5 Wenn Segmentierung verwendet wird, um die CDE von anderen Netzwerken zu isolieren, werden Penetrationstests auf den Segmentierungskontrollen wie folgt durchgeführt: • Mindestens einmal alle 12 Monate und nach jeder Änderung der Segmentierungskontrollen/-methoden • Abdeckung aller verwendeten Segmentierungskontrollen/-methoden. • Gemäß der definierten Penetrationstest-Methodik der Entität. • Bestätigung, dass die Segmentierungskontrollen/-methoden betriebsbereit und effektiv sind und die CDE von allen Systemen außerhalb des Geltungsbereichs isolieren. • Bestätigung der Wirksamkeit jeglicher Verwendung von Isolation, um Systeme mit unterschiedlichen Sicherheitsstufen zu trennen (siehe Anforderung 2.2.3). • Durchgeführt von einer qualifizierten internen Ressource oder einem qualifizierten externen Dritten. • Organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein).	**11.4.5.a** Segmentierungskontrollen untersuchen und die Penetrationstestmethodik überprüfen, um zu verifizieren, dass Penetrationstestprozeduren definiert sind, um alle Segmentierungsmethoden gemäß allen in dieser Anforderung angegebenen Elementen zu testen.	
	11.4.5.b Die Ergebnisse des letzten Penetrationstests untersuchen, um zu verifizieren, dass der Penetrationstest alle in dieser Anforderung angegeben Elemente abdeckt und adressiert.	
	11.4.5.c Das Personal befragen, um zu verifizieren, dass der Scan von einer qualifizierten internen Ressource(n) oder einem qualifizierten externen Dritten durchgeführt wurde und dass die organisatorische Unabhängigkeit des Testers besteht (es ist nicht erforderlich, ein QSA oder ASV zu sein).	
Zielsetzung des kundenspezifischen Ansatzes		
Wenn Segmentierung verwendet wird, wird sie regelmäßig durch technische Tests auf ihre kontinuierliche Wirksamkeit, auch nach Änderungen, bei der Isolierung der CDE von allen Systemen außerhalb des Geltungsbereichs verifiziert.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	
11.4.6 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Wenn Segmentierung verwendet wird, um die CDE von anderen Netzwerken zu isolieren, werden Penetrationstests auf den Segmentierungskontrollen wie folgt durchgeführt: • Mindestens einmal alle sechs Monate und nach jeder Änderung der Segmentierungskontrollen/-methoden • Abdeckung aller verwendeten Segmentierungskontrollen/-methoden. • Gemäß der definierten Penetrationstest-Methodik der Entität. • Bestätigung, dass die Segmentierungskontrollen/-methoden betriebsbereit und effektiv sind und die CDE von allen Systemen außerhalb des Geltungsbereichs isolieren. • Bestätigung der Wirksamkeit jeglicher Verwendung von Isolation, um Systeme mit unterschiedlichen Sicherheitsstufen zu trennen (siehe Anforderung 2.2.3). • Durchgeführt von einer qualifizierten internen Ressource oder einem qualifizierten externen Dritten. • Organisatorische Unabhängigkeit des Testers (es ist nicht erforderlich, ein QSA oder ASV zu sein). *(Fortsetzung auf der nächsten Seite)*	**11.4.6.a** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Die Ergebnisse des letzten Penetrationstests untersuchen, um zu verifizieren, dass der Penetrationstest alle in dieser Anforderung angegeben Elemente abdeckt und adressiert hat. **11.4.6.b Zusätzliche Testprozedur nur für Dienstleistungsanbieter-Bewertungen:** Das Personal befragen, um zu verifizieren, dass der Scan von einer qualifizierten internen Ressource(n) oder einem qualifizierten externen Dritten durchgeführt wurde und dass die organisatorische Unabhängigkeit des Testers besteht (es ist nicht erforderlich, ein QSA oder ASV zu sein).	**Zweck** Dienstleistungsanbieter haben typischerweise Zugriff auf größere Mengen an Karteninhaberdaten oder können einen Einstiegspunkt bereitstellen, der ausgenutzt werden kann, um dann mehrere andere Entitäten zu kompromittieren. Dienstleistungsanbieter haben auch typischerweise größere und komplexere Netzwerke, die häufigeren Änderungen unterliegen. Die Wahrscheinlichkeit, dass Segmentierungskontrollen in komplexen und dynamischen Netzwerken versagen, ist in Dienstleistungsanbieter-Umgebungen größer. Durch eine häufigere Validierung von Segmentierungskontrollen werden solche Fehler wahrscheinlich entdeckt, bevor sie von einem Angreifer ausgenutzt werden können, der versucht, seitlich von einem nicht vertrauenswürdigen Netzwerk außerhalb des Geltungsbereichs zur CDE zu wechseln. **Gute Praxis** Obwohl die Anforderung besagt, dass diese Geltungsbereichsvalidierung halbjährlich und nach bedeutenden Änderungen durchgeführt wird, sollte diese Übung so häufig wie möglich durchgeführt werden, um sicherzustellen, dass sie die CDE wirksam von anderen Netzen isoliert.

Anforderungen und Testprozeduren		Anleitungen
Zielsetzung des kundenspezifischen Ansatzes Wenn Segmentierung verwendet wird, wird sie durch technische Tests auf ihre kontinuierliche Wirksamkeit, auch nach Änderungen, bei der Isolierung der CDE von Systemen außerhalb des Geltungsbereichs verifiziert. **Hinweise zur Anwendbarkeit** Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist.		
Definierte Ansatzanforderungen **11.4.7** ***Zusätzliche Anforderungen nur für Multi-Mandanten-Dienstleistungsanbieter:*** Multi-Mandanten-Dienstleistungsanbieter unterstützen ihre Kunden bei externen Penetrationstests gemäß Anforderung 11.4.3 und 11.4.4. **Zielsetzung des kundenspezifischen Ansatzes** Multi-Mandanten Dienstleistungsanbieter unterstützen das Bedürfnis ihrer Kunden nach technischen Tests, indem sie entweder Zugang gewähren oder nachweisen, dass vergleichbare technische Tests durchgeführt wurden. *(Fortsetzung auf der nächsten Seite)*	**Testprozeduren mit definiertem Ansatz** **11.4.7** ***Zusätzliche Testprozedur nur für Multi-Mandanten-Dienstleistungsanbieter:*** Nachweise untersuchen, um zu verifizieren, dass Multi-Mandanten- Dienstleistungsanbieter ihre Kunden bei externen Penetrationstests gemäß Anforderung 11.4.3 und 11.4.4 unterstützen.	**Zweck** Entitäten müssen Penetrationstests gemäß PCI DSS ausführen, um das Verhalten von Angreifern zu simulieren und Schwachstellen in ihrer Umgebung aufzudecken. In geteilten und Cloud-Umgebungen kann der Multi-Mandant-Dienstleistungsanbieter besorgt sein, dass die Aktivitäten eines Penetrationstesters die Systeme anderer Kunden beeinträchtigen. Multi-Mandanten-Dienstleistungsanbieter können Penetrationstests nicht verbieten, weil dadurch die Systeme ihrer Kunden ausgenutzt werden könnten. Daher müssen Multi-Mandanten-Dienstleistungsanbieter Kundenanfragen zur Ausführung von Penetrationstests oder zu Penetrationstestergebnissen unterstützen.

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Diese Anforderung gilt nur, wenn die die bewertete Entität ein Multi-Mandanten-Dienstleistungsanbieter ist. Um diese Anforderung zu erfüllen, kann ein Multi-Mandanten-Dienstleistungsanbieter entweder: • Ihren Kunden den Nachweis erbringen, dass Penetrationstests gemäß den Anforderungen 11.4.3 und 11.4.4 an der abonnierten Infrastruktur des Kunden durchgeführt wurden, oder • Jedem ihrer Kunden sofortigen Zugriff bereitstellen, damit Kunden ihre eigenen Penetrationstests durchführen können. Den Kunden vorgelegte Nachweise können geschwärzte Penetrationstestergebnisse umfassen, sie müssen jedoch ausreichende Informationen enthalten, um zu beweisen, dass alle Elemente der Anforderungen 11.4.3 und 11.4.4 im Namen des Kunden erfüllt wurden. Beziehen Sie sich auch auf Anhang A1: Zusätzliche PCI DSS-Anforderungen für Multi-Mandanten-Diensleistungsanbieter. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
11.5 Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und es wird darauf reagiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Eindringungs-Erkennungs- und/oder Eindringungs-Verhinderungs-Techniken (wie IDS/IPS) vergleichen den in das Netzwerk eingehenden „Verkehr mit bekannten „Signaturen" und/oder Verhaltensweisen von Tausenden von Kompromittierungsarten (Hacker-Tools, Trojaner und andere Malware) und senden dann Warnmeldungen und/oder stoppen den Versuch, sobald er stattfindet. Ohne einen proaktiven Ansatz, um nicht autorisierte Aktivitäten zu erkennen, könnten Angriffe auf (oder der Missbrauch) von Computerressourcen für lange Zeit unbemerkt bleiben. Die Auswirkung eines Eindringens in die CDE hängt in vielerlei Hinsicht von der Zeit ab, die ein Angreifer in der Umgebung hat, bevor er entdeckt wird. **Gute Praxis** Durch diese Techniken generierte Sicherheitswarnungen sollten kontinuierlich überwacht werden, damit die versuchten oder tatsächlichen Eindringungsversuche gestoppt und potenzielle Schäden begrenzt werden können. **Definitionen** Kritische Stellen könnten Netzsicherheitskontrollen zwischen Netzwerksegmenten (zum Beispiel zwischen einer DMZ und einem internen Netzwerk oder zwischen einem Netzwerk im Geltungsbereich und einem Netzwerk außerhalb des Geltungsbereichs) und Punkte zum Schutz von Verbindungen zwischen einer weniger vertrauenswürdigen und einer vertrauenswürdigeren Systemkomponente umfassen, sind aber nicht darauf beschränkt.
11.5.1 Eindringungs-Erkennungs- und/oder Eindringungs-Verhinderungs-Techniken werden verwendet, um Eindringungen in das Netzwerk wie folgt zu erkennen und/oder zu verhindern: • Der gesamte Verkehr wird im Umkreis der CDE überwacht. • Der gesamte Verkehr wird an kritischen Stellen in der CDE überwacht. • Das Personal wird vor vermuteten Kompromittierungen gewarnt. • Alle Engines, Baselines und Signaturen für Eindringungs-Erkennung und -Verhinderung werden auf dem neuesten Stand gehalten.	**11.5.1.a** Systemkonfigurationen und Netzwerkdiagramme untersuchen, um zu verifizieren, dass Techniken zur Erkennung und/oder zur Verhinderung von Eindringlingen zur Überwachung des gesamten Verkehrs vorhanden sind: • An dem Umkreis der CDE. • An kritischen Stellen in der CDE.	
	11.5.1.b Systemkonfigurationen untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass Eindringungs-Erkennungs- und/oder Eindringungs-Verhinderungs-Techniken das Personal vor mutmaßlichen Kompromittierungen warnt.	
Zielsetzung des kundenspezifischen Ansatzes	**11.5.1.c** Systemkonfigurationen und Herstellerdokumentation untersuchen, um zu verifizieren, dass Eindringungs-Erkennungs- und/oder Eindringungs-Verhinderungs-Techniken so konfiguriert sind, um alle Engines, Baselines und Signaturen auf dem neuesten Stand zu halten.	
Es werden Mechanismen implementiert, um verdächtigen oder anormalen Netzwerkverkehr in Echtzeit zu erkennen, der auf Aktivitäten von Bedrohungsakteuren hinweisen kann. Auf diese Mechanismen erzeugte Warnungen werden durch das Personal oder durch automatisierte Mittel reagiert, die sicherstellen, dass Systemkomponenten aufgrund der erkannten Aktivität nicht kompromittiert werden können.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Erkennen von verdeckten Malware-Kommunikationsversuchen (z. B. DNS-Tunneling) kann dazu beitragen, die seitliche Verbreitung von Malware innerhalb eines Netzwerks und die Exfiltration von Daten zu blockieren. Bei der Entscheidung, wo diese Kontrolle platziert werden soll, sollten Entitäten kritische Orte im Netzwerk und wahrscheinliche Routen für verdeckte Kanäle berücksichtigen. Wenn Malware in einer infizierten Umgebung Fuß fasst, versucht sie häufig, einen Kommunikationskanal zu einem Befehls- und Kontroll-Server (C&C) aufzubauen. Über den C&C-Server kommuniziert und kontrolliert der Angreifer Malware auf kompromittierten Systemen, um böswillige Nutzlasten oder Anweisungen zu liefern oder Datenexfiltration einzuleiten. In vielen Fällen wird die Malware indirekt über Botnets mit dem C&C-Server kommunizieren, die Überwachung umgehen, Kontrollen sperren und diese Methoden unwirksam machen, um die verdeckten Kanäle zu erkennen. **Gute Praxis** Zu den Methoden, die beim Erkennen und Behandeln von Malware-Kommunikationskanälen helfen können, gehören Echtzeit-Endpunkt-Scans, Filterung des ausgehenden Verkehrs, eine „Zulassungs“liste, Tools zur Verhinderung von Datenverlust und Tools zur Überwachung der Netzwerksicherheit wie IDS/IPS. Zusätzlich sind DNS-Abfragen und -Antworten eine wichtige Datenquelle, die von Netzwerkverteidigern verwendet wird, *(Fortsetzung auf der nächsten Seite)*
11.5.1.1 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Eindringungs-Erkennungs- und/oder Eindringungs-Verhinderungs-Techniken erkennen, warnen/verhindern und adressieren verdeckte Malware-Kommunikationskanäle.	**11.5.1.1.a** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Dokumentations- und Konfigurationseinstellungen untersuchen, um zu verifizieren, dass Methoden zum Erkennen und Warnen/Verhindern von verdeckten Malware-Kommunikationskanälen vorhanden sind und funktionieren.	
	11.5.1.1.b ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Den Vorfalls-Reaktionsplan der Entität (Anforderung 12.10.1) untersuchen, um zu verifizieren, dass er eine Reaktion für den Fall erfordert und definiert, dass verdeckte Malware-Kommunikationskanäle entdeckt werden.	
Zielsetzung des kundenspezifischen Ansatzes	**11.5.1.1.c** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Verantwortliches Personal befragen und Prozesse beobachten, um zu verifizieren, dass das Personal über Kenntnisse über verdeckte Malware-Kommunikations- und Kontrolltechniken verfügt und weiß, wie es bei Verdacht auf Malware reagiert.	
Mechanismen sind vorhanden, um verdeckte Kommunikationen mit Befehls- und Kontrollsystemen zu erkennen und zu warnen/zu verhindern. Auf diese Mechanismen generierte Warnungen werden vom Personal oder durch automatisierte Mittel reagiert, um sicherzustellen, dass solche Kommunikationen blockiert werden. *(Fortsetzung auf der nächsten Seite)*		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		um die Reaktion auf Vorfälle sowie die Entdeckung von Eindringlingen zu unterstützen. Wenn diese Transaktionen für die Verarbeitung und Analyse gesammelt werden, können sie eine Reihe wertvoller Sicherheitsanalyseszenarien ermöglichen. Es ist wichtig, dass Organisationen über die Betriebsmodi von Malware auf dem neuesten Stand sind, da deren Abschwächung dazu beitragen kann, die Auswirkungen von Malware in der Umgebung zu erkennen und zu begrenzen.
Definierte Ansatzanforderungen **11.5.2** Ein Mechanismus zur Erkennung von Änderungen (zum Beispiel Tools zur Überwachung der Dateiintegrität) wird wie folgt eingesetzt: • Um das Personal auf nicht autorisierte Änderungen (einschließlich Änderungen, Ergänzungen und Löschungen) kritischer Dateien aufmerksam zu machen, • Um kritische Dateivergleiche mindestens einmal wöchentlich durchzuführen. **Zielsetzung des kundenspezifischen Ansatzes** Kritische Dateien können von nicht autorisiertem Personal nicht geändert werden, ohne dass eine Warnung generiert wird.	**Testprozeduren mit definiertem Ansatz** **11.5.2.a** Systemeinstellungen, überwachte Dateien und Ergebnisse aus Überwachungsaktivitäten untersuchen, um die Verwendung eines Änderungs- Erkennungsmechanismus zu verifizieren. **11.5.2.b** Einstellungen für den Änderungs-Erkennungsmechanismus untersuchen, um zu verifizieren, dass er gemäß allen in dieser Anforderung angegebenen Elementen implementiert ist.	**Zweck** Änderungen an kritischen System-, Konfigurations- oder Inhaltsdateien können ein Hinweis darauf sein, dass ein Angreifer auf das System eines Unternehmens zugegriffen hat. Solche Änderungen können es einem Angreifer gestatten, zusätzliche böswillige Aktionen durchzuführen, auf Karteninhaberdaten zuzugreifen und/oder Aktivitäten durchzuführen, ohne entdeckt oder aufgezeichnet zu werden. Ein Änderungserkennungsmechanismus erkennt und bewertet solche Änderungen an kritischen Dateien und generiert Warnungen, auf die nach definierten Prozessen reagiert werden kann, damit das Personal geeignete Maßnahmen ergreifen kann. Wenn die Lösung zur Erkennung von Veränderungen nicht ordnungsgemäß umgesetzt

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Für Zwecke der Änderungserkennung sind kritische Dateien in der Regel Dateien, die sich nicht regelmäßig ändern, deren Änderung jedoch auf eine Systemkompromittierung oder das Risiko einer Kompromittierung hinweisen könnte. Änderungserkennungsmechanismen wie Produkte zur Überwachung der Dateiintegrität werden normalerweise mit kritischen Dateien für das zugehörige Betriebssystem vorkonfiguriert. Andere kritische Dateien, wie für benutzerdefinierte Anwendungen, müssen von der Entität (d.h. dem Händler oder Dienstleistungsanbieter) bewertet und definiert werden.		und ihre Ausgabe überwacht werden, könnte eine böswillige Person Inhalte von Konfigurationsdateien, Betriebssystemprogrammen oder ausführbaren Anwendungen hinzufügen, entfernen oder verändern. Nicht autorisierte Änderungen können, wenn sie nicht erkannt werden, bestehende Sicherheitskontrollen unwirksam machen und/oder dazu führen, dass Karteninhaberdaten ohne erkennbare Auswirkungen auf die normale Verarbeitung gestohlen werden. **Gute Praxis** Beispiele für Dateiarten, die überwacht werden sollten, umfassen, sind aber nicht beschränkt auf: • Ausführbare Systemdateien • Ausführbare Anwendungsdateien. • Konfigurations- und Parameterdateien. • Zentral gespeicherte, historische oder archivierte Audit-Protokolle. • Zusätzliche kritische Dateien, die von Entität bestimmt werden (zum Beispiel durch Risikobeurteilung oder auf andere Weise). **Beispiele** Änderungserkennungslösungen wie Überwachung der Dateiintegrität (FIM)-Tools prüfen auf Änderungen, Hinzufügungen und Löschungen an kritischen Dateien und benachrichtigen, wenn solche Änderungen erkannt werden.

Anforderungen und Testprozeduren		Anleitungen
11.6 Nicht autorisierte Änderungen auf Zahlungsseiten werden erkannt und es wird darauf reagiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
11.6.1 Ein Änderungs- und Manipulationserkennungsmechanismus wird wie folgt eingesetzt: • Um das Personal über nicht autorisierte Änderungen (einschließlich Anzeichen für Kompromittierung, Änderungen, Ergänzungen und Löschungen) der HTTP-Kopfzeile und des Inhalts von Zahlungsseiten, wie sie vom Verbraucherbrowser empfangen werden, zu warnen. • Der Mechanismus ist so konfiguriert, dass er die empfangene HTTP-Kopfzeile und die Zahlungsseite bewertet. • Die Mechanismusfunktionen werden wie folgt durchgeführt: – Mindestens einmal alle sieben Tage. **ODER** – Regelmäßig (in der Häufigkeit, die in der gezielten Risikoanalyse der Entität definiert ist, die gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wird.	**11.6.1.a** Systemeinstellungen, überwachte Zahlungsseiten und Ergebnisse aus Überwachungsaktivitäten untersuchen, um die Verwendung eines Änderungs- und Manipulationserkennungsmechanismus zu verifizieren. **11.6.1.b** Konfigurationseinstellungen untersuchen, um zu verifizieren, dass der Mechanismus gemäß allen in dieser Anforderung angegebenen Elementen konfiguriert ist. **11.6.1.c** Wenn die Mechanismusfunktionen mit einer von der Entität definierten Häufigkeit durchgeführt werden, die gezielte Risikoanalyse der Entität untersuchen, um die Häufigkeit zu bestimmen, um zu verifizieren, dass die Risikoanalyse gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wurde. **11.6.1.d** Konfigurationseinstellungen untersuchen und Personal befragen, um verifizieren, dass die Funktionen entweder: • Mindestens einmal alle sieben Tage durchgeführt werden **ODER** • In der Häufigkeit, die in der gezielten Risikoanalyse der Entität für diese Anforderung definiert wurde.	Viele Webseiten verlassen sich jetzt auf das Zusammensetzen von Objekten, einschließlich aktiver Inhalte (hauptsächlich JavaScript), von mehreren Internet-Standorten. Zusätzlich wird der Inhalt vieler Webseiten mithilfe von Inhaltsverwaltungs- und Tag-Verwaltungssystemen definiert, die mit herkömmlichen Änderungserkennungsmechanismen möglicherweise nicht überwacht werden können. Daher ist der einzige Ort, um Änderungen oder Anzeichen für böswillige Aktivitäten zu erkennen, der Verbraucherbrowser, während die Seite erstellt und das gesamte JavaScript interpretiert wird. Durch den Vergleich der aktuellen Version der HTTP-Kopfzeile und des aktiven Inhalts von Zahlungsseiten, wie sie mit früheren oder bekannten Versionen vom Verbraucherbrowser empfangen werden, ist es möglich, nicht autorisierte Änderungen zu erkennen, die auf einen Skimming-Angriff hinweisen können. Zusätzlich können durch die Suche nach bekannten Indikatoren für Kompromittierung und Skriptelementen oder Verhaltensweisen, die für Skimmer typisch sind, verdächtige Warnungen ausgegeben werden. *(Fortsetzung auf der nächsten Seite)*
Zielsetzung des kundenspezifischen Ansatzes		
E-Commerce-Skimming-Code oder -Techniken können nicht zu Zahlungsseiten hinzugefügt werden, die vom Verbraucherbrowser empfangen werden, ohne dass eine rechtzeitige Warnung generiert wird. Anti-Skimming-Maßnahmen können nicht von Zahlungsseiten entfernt werden, ohne dass eine sofortige Warnung generiert wird.		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit Die Absicht dieser Anforderung besteht nicht darin, dass eine Entität Software in den Systemen oder Browsern ihrer Verbraucher installiert, sondern dass die Entität Techniken wie die in den obigen Beispielen in der Anleitungsspalte beschriebenen verwendet, um unerwartete Skriptaktivitäten zu verhindern und zu erkennen. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		**Beispiele** Mechanismen, die Änderungen der Kopfzeilen und des Inhalts der Zahlungsseite erkennen und melden, umfassen, sind aber nicht beschränkt auf: • Verstöße gegen die Inhaltssicherheitsrichtlinie (CSP) können der Entität über die *report-to*- oder *report-uri*-CSP-Direktive gemeldet werden. • Änderungen am CSP selbst können auf Manipulationen hinweisen • Die externe Überwachung durch Systeme, die die empfangenen Webseiten anfordern und analysieren (auch als synthetische Benutzerüberwachung bekannt), kann Änderungen an JavaScript in Zahlungsseiten erkennen und Personal warnen • Das Einbetten eines manipulationssicheren Manipulationserkennungs-Skripts in die Zahlungsseite kann warnen und sperren, wenn böswilliges Skriptverhalten erkannt wird. • Reverse Proxies und Inhaltslieferungsnetzwerke können Änderungen in Skripten erkennen und das Personal warnen Diese Mechanismen sind häufig Abonnement- oder Cloud-basiert, können aber auch auf kundenspezifischen und maßgeschneiderten Lösungen basieren.

Beibehaltung einer Informationssicherheitspolitik

Anforderung 12: Unterstützung der Informationssicherheit durch Organisatorische Richtlinien und Programme

Abschnitte	
12.1	Eine umfassende Informationssicherheitsrichtlinie, die den Schutz des Informationsvermögens der Entität regelt und vorgibt, ist bekannt und aktuell.
12.2	Richtlinien zur akzeptablen Verwendung für Endbenutzertechnologien werden definiert und implementiert.
12.3	Risiken für die Karteninhaberdatenumgebung werden formell identifiziert, bewertet und verwaltet.
12.4	PCI DSS-Einhaltung wird verwaltet.
12.5	Der PCI DSS-Geltungsbereich wird dokumentiert und validiert.
12.6	Die Aufklärung über das Sicherheitsbewusstsein ist eine fortlaufende Aktivität.
12.7	Das Personal wird überprüft, um Risiken durch Insider-Bedrohungen zu reduzieren.
12.8	Das Risiko für Informationsassets im Zusammenhang mit den Beziehungen zu dritten Dienstleistungsanbietern (TPSP) wird verwaltet.
12.9	Dritte Dienstleistungsanbieter (TPSPs) unterstützen die PCI DSS-Einhaltung ihrer Kunden.
12.10	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf die CDE auswirken könnten, wird umgehend reagiert.

Übersicht

Die allgemeine Informationssicherheitspolitik der Organisation gibt den Ton für die gesamte Entität vor und informiert das Personal, was von ihm erwartet wird. Das gesamte Personal sollte sich der Sensibilität von Karteninhaberdaten und seiner Verantwortung für deren Schutz bewusst sein.

Im Sinne von Anforderung 12 bezieht sich „Personal“ auf Vollzeit- und Teilzeitbeschäftigte, Zeitarbeitskräfte, Auftragnehmer und Berater mit Sicherheitsverantwortungen für den Schutz von Kontodaten oder die die Sicherheit von Kontodaten beeinträchtigen können.

Finden Sie in Anhang G Definitionen von PCI DSS-Begriffen.

Anforderungen und Testprozeduren		Anleitungen
12.1 Eine umfassende Informationssicherheitsrichtlinie, die den Schutz des Informationsvermögens der Entität regelt und vorgibt, ist bekannt und aktuell.		
Definierte Ansatzanforderungen **12.1.1** Eine gesamte Richtlinie zur Informationssicherheit ist: • Etabliert. • Veröffentlicht. • Gewartet. • Weitergabe an das gesamte relevante Personal sowie an relevante Anbieter und Geschäftspartner.	**Testprozeduren mit definiertem Ansatz** **12.1.1** Die Informationssicherheitsrichtlinie untersuchen und das Personal befragen, um zu verifizieren, dass die gesamte Informationssicherheitsrichtlinie gemäß allen in dieser Anforderung angegebenen Elementen verwaltet wird.	**Zweck** Die allgemeine Informationssicherheitsrichtlinie einer Organisation ist mit allen anderen Richtlinien und Verfahren verbunden, die den Schutz von Karteninhaberdaten definieren, und regelt diese. Die Informationssicherheitsrichtlinie kommuniziert die Absichten und Ziele der Verwaltung in Bezug auf den Schutz seiner wertvollsten Assets, einschließlich der Karteninhaberdaten. Ohne eine Informationssicherheitsrichtlinie treffen Personen ihre eigenen Wertentscheidungen über die Kontrollen, die innerhalb der Organisation erforderlich sind, was dazu führen kann, dass die Organisation weder ihre gesetzlichen, behördlichen und vertraglichen Verpflichtungen erfüllt noch in der Lage ist, ihre Assets in konsistenter Weise angemessen zu schützen Um sicherzustellen, dass die Richtlinie implementiert wird, ist es wichtig, dass das gesamte relevante Personal innerhalb der Organisation sowie relevante Dritte, Anbieter und Geschäftspartner sich der Informationssicherheitsrichtlinie der Organisation und ihrer Verantwortung für den Schutz von Informationsressourcen bewusst sind. *(Fortsetzung auf der nächsten Seite)*
Zielsetzung des kundenspezifischen Ansatzes Die strategischen Zielsetzungen und Prinzipien der Informationssicherheit sind definiert, verabschiedet und dem gesamten Personal bekannt.		

Anforderungen und Testprozeduren		Anleitungen
		Gute Praxis Die Sicherheitsrichtlinie für die Organisation identifiziert den Zweck, den Umfang, die Verantwortlichkeit und die Informationen, die die Position der Organisation in Bezug auf die Informationssicherheit klar definiert. Die allgemeine Informationssicherheitsrichtlinie unterscheidet sich von einzelnen Sicherheitsrichtlinien, die bestimmte Technologien oder Sicherheitsdisziplinen adressieren. Diese Richtlinie legt die Direktiven für die gesamte Organisation fest, während individuelle Sicherheitsrichtlinien die allgemeine Sicherheitsrichtlinie ausrichten und unterstützen und spezifische Zielsetzungen für Technologie- oder Sicherheitsdisziplinen kommunizieren. Es ist wichtig, dass das gesamte relevante Personal innerhalb der Organisation sowie relevante Dritte, Anbieter und Geschäftspartner sich der Informationssicherheitsrichtlinie der Organisation und ihrer Verantwortung für den Schutz von Informationsressourcen bewusst sind. **Definitionen** „Relevant“ für diese Anforderung bedeutet, dass die Informationssicherheitsrichtlinie an diejenigen weitergegeben wird, deren Rollen für einige oder alle Themen der Richtlinie gelten, entweder innerhalb des Unternehmens oder aufgrund von Dienstleistungen/Funktionen, die von einem Anbieter oder Dritten erbracht werden.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.1.2 Die Informationssicherheitsrichtlinie wird: • Mindestens alle 12 Monate überprüft. • Bei Bedarf aktualisiert, um Änderungen der Geschäftszielsetzungen oder Risiken für die Umwelt widerzuspiegeln.	**12.1.2** Die Dokumentation untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass die Richtlinie gemäß allen in dieser Anforderung angegebenen Elementen verwaltet wird.	Sicherheitsbedrohungen und zugehörige Schutzmethoden entwickeln sich schnell weiter. Ohne die Aktualisierung der Informationssicherheitsrichtlinie, um relevante Änderungen widerzuspiegeln, werden möglicherweise keine neuen Maßnahmen zur Abwehr dieser Bedrohungen ergriffen.
Zielsetzung des kundenspezifischen Ansatzes		
Die Informationssicherheitsrichtlinie spiegelt weiterhin die strategischen Ziele und Prinzipien der Organisation wider.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.1.3 Die Sicherheitsrichtlinie definiert die Rollen und Verantwortlichkeiten für die Informationssicherheit für das gesamte Personal eindeutig, und das gesamte Personal ist sind sich seiner Verantwortung für die Informationssicherheit bewusst und erkennt diese an.	**12.1.3.a** Die Informationssicherheitsrichtlinie untersuchen, um zu verifizieren, dass sie die Rollen und Verantwortlichkeiten der Informationssicherheit für das gesamte Personal klar definieren.	Ohne klar definierte Zuweisung von Sicherheitsrollen und Verantwortlichkeiten kann es zu einem Missbrauch der Informationsressourcen der Organisation oder zu einer inkonsistenten Interaktion mit dem Informationssicherheitspersonal kommen, was zu einer unsicheren Implementierung von Technologien oder der Verwendung veralteter oder unsicherer Technologien führt.
	12.1.3.b Das Personal in verschiedenen Rollen befragen, um zu verifizieren, dass es seine Verantwortungen für die Informationssicherheit versteht.	
	12.1.3.c Dokumentierte Beweise untersuchen, um zu verifizieren, dass das Personal seine Verantwortungen für die Informationssicherheit anerkennt.	
Zielsetzung des kundenspezifischen Ansatzes		
Das Personal versteht seine Rolle beim Schutz der Karteninhaberdaten der Entität.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Um sicherzustellen, dass jemand mit ausreichender Autorität und Verantwortung das Informationssicherheitsprogramm der Organisation aktiv verwaltet und vertritt, muss die Rechenschaftspflicht und Verantwortung für die Informationssicherheit auf der Führungsebene innerhalb einer Organisation übertragen werden. Zu den gängigen Geschäftsleitungen für diese Rolle gehören der Beauftragte für Informationssicherheit (CISO) und der Sicherheitsbeauftragte (CSO – um diese Anforderung zu erfüllen, muss die CSO-Rolle für die Informationssicherheit verantwortlich sein). Diese Positionen befinden sich häufig auf der höchsten Führungsebene und sind Teil der Führungsebene oder C-Ebene, die in der Regel dem geschäftsführenden Direktor oder dem Vorstand untersteht. **Gute Praxis** Entitäten sollten auch Übergangs- und/oder Nachfolgepläne für dieses Schlüsselpersonal in Betracht ziehen, um potenzielle Lücken bei kritischen Sicherheitsaktivitäten zu vermeiden.
12.1.4 Die Verantwortung für die Informationssicherheit wird einem Beauftragten für Informationssicherheit oder einem anderen im Bereich Informationssicherheit sachkundigen Mitglied der Geschäftsleitung formell zugewiesen.	**12.1.4** Die Informationssicherheitsrichtlinie untersuchen, um zu verifizieren, dass die informationssicherheit einem Beauftragten für Informationssicherheit oder einem anderen im Bereich Informationssicherheit sachkundigen Mitglied der Geschäftsleitung formell zugewiesen ist.	
Zielsetzung des kundenspezifischen Ansatzes		
Ein designiertes Mitglied der Geschäftsleitung ist für die Informationssicherheit verantwortlich.		

Anforderungen und Testprozeduren		Anleitungen
12.2 Richtlinien zur akzeptablen Verwendung für Endbenutzertechnologien werden definiert und implementiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.2.1 Richtlinien zur akzeptablen Verwendung für Endbenutzertechnologien werden dokumentiert und implementiert, einschließlich: • Ausdrückliche Genehmigung durch autorisierte Parteien. • Akzeptable Verwendungen der Technologie. • Liste der Produkte, die vom Unternehmen für die Verwendung durch Mitarbeiter freigegeben wurden, einschließlich Hardware und Software.	**12.2.1** Die Richtlinien zur akzeptablen Verwendung von Endbenutzertechnologien untersuchen verantwortliches Personal befragen, um zu verifizieren, dass Prozesse gemäß allen in dieser Anforderung angegebenen Elementen dokumentiert und implementiert werden.	Endbenutzertechnologien sind eine bedeutende Investition und können ein bedeutendes Risiko für eine Organisation darstellen, wenn sie nicht ordnungsgemäß verwaltet werden. Die Richtlinien zur akzeptablen Nutzung beschreiben das erwartete Verhalten des Personals bei der Verwendung der Informationstechnologie der Organisation und spiegeln die Risikotoleranz der Organisation wider Diese Richtlinien unterweisen das Personal, was es mit Unternehmensgeräten tun darf und was nicht, und unterweisen das Personal in richtigen und falschen Verwendungen der Internet- und E-Mail-Ressourcen des Unternehmens. Solche Richtlinien können eine Organisation rechtlich schützen und es ihr ermöglichen, zu handeln, wenn die Richtlinien verletzt werden. **Gute Praxis** Es ist wichtig, dass Nutzungsrichtlinien durch technische Kontrollen unterstützt werden, um die Durchsetzung der Richtlinien zu verwalten. Die Strukturierung von Richtlinien als einfache „tun“- und „nicht tun“-Anforderungen, die mit einem Zweck verknüpft sind, kann dabei helfen, Mehrdeutigkeiten zu beseitigen und dem Personal den Kontext für die Anforderung bereitzustellen.
Zielsetzung des kundenspezifischen Ansatzes Die Verwendung von Endbenutzertechnologien wird definiert und verwaltet, um eine autorisierte Nutzung sicherzustellen.		
Hinweise zur Anwendbarkeit Beispiele für Endbenutzertechnologien, für die akzeptable Verwendungsrichtlinien erwartet werden,schließen ein, sind jedoch nicht darauf beschränkt: Fernzugriff und drahtlose Technologien, Laptops, Tablets, Mobiltelefone und entfernbare elektronische Medien, E-Mail- und Internetverwendung.		

Anforderungen und Testprozeduren		Anleitungen
12.3 Risiken für die Karteninhaberdatenumgebung werden formell identifiziert, bewertet und verwaltet.		
Definierte Ansatzanforderungen **12.3.1** Jede PCI DSS-Anforderung, die Flexibilität für die Häufigkeit ihrer Durchführung bereitstellt (zum Beispiel Anforderungen, die regelmäßig durchgeführt werden müssen), wird durch eine gezielte Risikoanalyse unterstützt, die dokumentiert wird und Folgendes umfasst: • Identifizierung der zu schützenden Assets. • Identifizierung der Bedrohung(en), gegen die die Anforderung schützt. • Identifizierung von Faktoren, die zur Wahrscheinlichkeit und/oder Auswirkung beitragen, dass eine Bedrohung realisiert wird. • Ergebnisanalyse, die bestimmt und begründet, wie oft die Anforderung durchgeführt werden muss, um die Wahrscheinlichkeit zu minimieren, dass die Bedrohung realisiert wird. • Überprüfung jeder gezielten Risikoanalyse mindestens alle 12 Monate, um zu bestimmen, ob die Ergebnisse noch gültig sind oder ob eine aktualisierte Risikoanalyse erforderlich ist. • Durchführung von aktualisierten Risikoanalysen bei Bedarf, wie von der jährlichen Überprüfung bestimmt ist. **Zielsetzung des kundenspezifischen Ansatzes** Aktuelle Kenntnisse und Beurteilungen der Risiken für die CDE werden aufrechterhalten. **Hinweise zur Anwendbarkeit** *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**Testprozeduren mit definiertem Ansatz** **12.3.1** Dokumentierte Richtlinien und Verfahren untersuchen, um zu verifizieren, dass ein Prozess zur Durchführung gezielter Risikoanalysen für jede PCI DSS-Anforderung definiert ist, die Flexibilität für die Häufigkeit der Durchführung der Anforderung bereitstellt, und dass der Prozess alle in dieser Anforderung angegebenen Elemente umfasst.	**Zweck** Einige PCI DSS-Anforderungen gestatten es einer Entität zu definieren, wie oft eine Aktivität basierend auf dem Risiko für die Umgebung durchgeführt wird. Die Durchführung dieser Risikoanalyse gemäß einer Methodik stellt die Gültigkeit und Konsistenz mit Richtlinien und Verfahren sicher. Diese gezielte Risikoanalyse (im Gegensatz zu einer traditionellen unternehmensweiten Risikobeurteilung) konzentriert sich auf diejenigen PCI DSS-Anforderungen, die einer Entität Flexibilität gestatten, wie oft eine Entität eine bestimmte Kontrolle durchführt. Für diese Risikoanalyse bewertet die Entität jede PCI DSS-Anforderung, die diese Flexibilität bereitstellt, sorgfältig und bestimmt die Häufigkeit, die eine angemessene Sicherheit für die Entität unterstützt, und das Risikoniveau, das die Entität zu akzeptieren bereit ist. Die Risikoanalyse identifiziert die spezifischen Assets, wie die Systemkomponenten und Daten - zum Beispiel Protokolldateien oder Anmeldeinformationen - die durch die Anforderung geschützt werden sollen, sowie die Bedrohung(en) oder Ergebnisse, von denen die Anforderung die Assets schützt von – zum Beispiel Malware, ein unentdeckter Eindringling oder der Missbrauch von Anmeldeinformationen. Beispiele für Faktoren, die zur Wahrscheinlichkeit oder Auswirkung beitragen könnten, umfassen solche, die die Anfälligkeit eines Assets gegenüber einer Bedrohung erhöhen könnten – zum Beispiel die Exposition gegenüber nicht vertrauenswürdigen Netzwerken. die Komplexität der Umgebung oder eine hohe *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
		Personalfluktuation – sowie die Kritikalität der Systemkomponenten, oder das Volumen und die Sensibilität der zu schützenden Daten. Die Überprüfung der Ergebnisse dieser gezielten Risikoanalysen mindestens alle 12 Monate und bei Änderungen, die sich auf das Risiko für die Umwelt auswirken könnten, gestattet der Organisation, sicherzustellen, dass die Ergebnisse der Risikoanalyse mit organisatorischen Veränderungen und sich entwickelnden Bedrohungen, Trends und Technologien auf dem neuesten Stand bleiben und dass die ausgewählten Häufigkeiten das Risiko der Entität noch angemessen abdecken. **Gute Praxis** Eine unternehmensweite Risikobeurteilung, bei der es sich um eine punktuelle Aktivität handelt, die es Entitäten ermöglicht, Bedrohungen und damit verbundene Schwachstellen zu identifizieren, wird empfohlen, ist jedoch nicht erforderlich, damit Entitäten umfassendere und neu auftretende Bedrohungen ermitteln und verstehen, die das Potenzial haben, sich negativ auf ihr Geschäft auszuwirken. Diese unternehmensweite Risikobeurteilung könnte als Teil eines übergreifenden Risikoverwaltungsprogramms erstellt werden, das als eine Eingabe für die jährliche Überprüfung der gesamten Informationssicherheitspolitik einer Organisation verwendet wird (siehe Anforderung 12.1.1). Beispiele für Risikobeurteilungsmethodiken für unternehmensweite Risikobeurteilungen umfassen, sind aber nicht beschränkt auf ISO 27005 und NIST SP 800-30.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **12.3.2** Für jede PCI DSS-Anforderung, die die Entität mit dem kundenspezifischen Ansatz erfüllt, wird eine gezielte Risikoanalyse durchgeführt, die Folgendes umfasst: • Dokumentierter Nachweis, der jedes in Anhang D aufgeführte Element detailliert beschreibt: Kundenspezifischer Ansatz (einschließlich mindestens einer Kontrollmatrix und einer Risikoanalyse). • Genehmigung dokumentierter Nachweise durch die Geschäftsleitung. • Durchführung der gezielten Risikoanalyse mindestens alle 12 Monate. **Zielsetzung des kundenspezifischen Ansatzes** Diese Anforderung ist Teil des kundenspezifischen Ansatzes und muss von denjenigen erfüllt werden, die den kundenspezifischen Ansatz verwenden. **Hinweise zur Anwendbarkeit** Diese Anforderung gilt nur für Entitäten, die einen kundenspezifischen Ansatz verwenden.	**Testprozeduren mit definiertem Ansatz** **12.3.2** Die dokumentierte gezielte Risikoanalyse für jede PCI DSS-Anforderung, die die Entität mit dem kundenspezifischen Ansatz erfüllt, untersuchen, um zu verifizieren, dass die Dokumentation für jede Anforderung vorhanden ist und allen in dieser Anforderung angegebenen Elementen entspricht.	**Zweck** Eine Risikoanalyse nach einer wiederholbaren und robusten Methodik ermöglicht es einer Entität, die kundenspezifische Ansatzzielsetzung zu erreichen. **Definitionen** Der kundenspezifische Ansatz zur Erfüllung einer PCI DSS-Anforderung gestattet es Entitäten, die verwendeten Kontrollen zu definieren, um die angegebene kundenspezifische Ansatzzielsetzung einer bestimmten Anforderung auf eine Art und Weise zu erfüllen, die sich nicht streng an die definierte Anforderung hält.. Von diesen Kontrollen wird erwartet, dass sie die durch die definierte Anforderung gebotene Sicherheit mindestens erfüllen oder übertreffen und eine umfangreiche Dokumentation durch die Entität mit dem kundenspezifischen Ansatz erfordern. **Weitere Informationen** Siehe Anhang D Kundenspezifischer Ansatz für Anweisungen zur Dokumentation der erforderlichen Nachweise für den kundenspezifischen Ansatz. Siehe Anhang E Beispielvorlagen zur Unterstützung eines kundenspezifischen Ansatzes für Vorlagen, die Entitäten verwenden können, um ihre kundenspezifischen Kontrollen zu dokumentieren. Beachten, dass die Verwendung der Vorlagen zwar optional ist, die in jeder Vorlage angegebenen Informationen jedoch dokumentiert und jedem Bewerter der Entität zur Verfügung gestellt werden müssen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.3.3 Die verwendeten kryptografischen Chiffrensammlungen und Protokolle werden mindestens alle 12 Monate dokumentiert und überprüft, einschließlich mindestens der folgenden: • Ein aktuelles Inventar aller verwendeten kryptografischen Chiffrensammlungen und Protokolle, einschließlich Zweck und wo sie verwendet werden. • Aktive Überwachung von Branchentrends in Bezug auf die dauerhafte Funktionsfähigkeit aller verwendeten kryptografischen Chiffrensammlungen und Protokolle. • Eine dokumentierte Strategie, um auf erwartete Änderungen bei kryptografischen Schwachstellen zu reagieren.	**12.3.3** Die Dokumentation für verwendete kryptografische Suiten und Protokolle untersuchen und das Personal befragen, um zu verifizieren, dass die Dokumentation und die Überprüfung allen in dieser Anforderung angegebenen Elementen entspricht.	Protokolle und Verschlüsselungsstärken können sich aufgrund der Identifizierung von Schwachstellen oder Designfehlern schnell ändern oder veraltet sein. Um aktuelle und zukünftige Anforderungen an die Datensicherheit zu erfüllen, müssen Entitäten wissen, wo Kryptografie verwendet wird, und verstehen, wie sie schnell auf Änderungen reagieren können, die sich auf die Stärke ihrer kryptografischen Implementierungen auswirken. **Gute Praxis** Kryptografische Agilität ist wichtig, um sicherzustellen, dass eine Alternative zum ursprünglichen Verschlüsselungsverfahren oder kryptografischen Primitiv verfügbar ist, mit Plänen, auf die Alternative ohne bedeutende Änderungen an der Systeminfrastruktur zu aktualisieren. Zum Beispiel, wenn die Entität weiß, wann Protokolle oder Algorithmen von Standardisierungsgremien veraltet sind, kann sie proaktiv Pläne für eine Aufrüstung erstellen, bevor die Abwertung Auswirkungen auf den Betrieb hat. **Definitionen** „Kryptografische Agilität“ bezieht sich auf die Fähigkeit, die in einer Organisation eingesetzten Verschlüsselungs- und zugehörigen Verifizierungstechnologien zu überwachen und zu verwalten. **Weitere Informationen** Siehe *NIST SP 800-131a, Umstellung der Verwendung kryptografischer Algorithmen und Schlüssellängen*.
Zielsetzung des kundenspezifischen Ansatzes		
Die Entität kann schnell auf Schwachstellen in kryptografischen Protokollen oder Algorithmen reagieren, wenn diese Schwachstellen den Schutz der Karteninhaberdaten beeinträchtigen.		
Hinweise zur Anwendbarkeit		
Die Anforderung gilt für alle kryptografischen Suiten und Protokolle, die zur Erfüllung der PCI DSS-Anforderungen verwendet werden. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Hardware- und Softwaretechnologien entwickeln sich ständig weiter, und Organisationen müssen sich der Änderungen der von ihnen verwendeten Technologien sowie der sich entwickelnden Bedrohungen dieser Technologien bewusst sein, um sicherzustellen, dass sie sich auf Schwachstellen in Hardware und Software vorbereiten und diese verwalten können, die nicht vom Anbieter oder Entwickler behoben werden. **Gute Praxis** Unternehmen sollten Firmware-Versionen überprüfen, um sicherzustellen, dass sie aktuell bleiben und von den Anbietern unterstützt werden. Organisationen müssen sich auch der von Technologieanbietern an ihren Produkten oder Prozessen vorgenommenen Änderungen bewusst sein, um zu verstehen, wie sich diese Änderungen auf die Nutzung der Technologie durch die Organisation auswirken können. Regelmäßige Überprüfungen von Technologien, die sich auf PCI DSS-Kontrollen auswirken oder sie beeinflussen, können bei Kauf-, Nutzungs- und Bereitstellungsstrategien helfen und sicherstellen, dass Kontrollen, die auf diesen Technologien beruhen, wirksam bleiben. Diese Überprüfungen umfassen, sind aber nicht beschränkt auf die Überprüfung von Technologien, die vom Anbieter nicht mehr unterstützt werden und/oder die Sicherheitsanforderungen der Organisation nicht mehr erfüllen.
12.3.4 Die verwendeten Hardware- und Softwaretechnologien werden mindestens alle 12 Monate überprüft, einschließlich mindestens der folgenden: • Analyse, dass die Technologien weiterhin umgehend Sicherheitsfehlerbehebungen von Anbietern erhalten. • Analyse, dass die Technologien die PCI DSS-Einhaltung der Entität weiterhin unterstützen (und nicht ausschließen). • Dokumentation aller Branchenankündigungen oder Trends im Zusammenhang mit einer Technologie, wie wenn ein Anbieter Pläne für das „Ende des Lebenszyklus“ einer Technologie angekündigt hat. • Dokumentation eines von der Geschäftsleitung genehmigten Plans zur Behebung veralteter Technologien, einschließlich derer, für die Anbieter Pläne zum „Ende des Lebenszyklus“ angekündigt haben.	**12.3.4** Dokumentation für die Überprüfung der verwendeten Hard- und Softwaretechnologien untersuchen und das Personal befragen, um zu verifizieren, dass die Überprüfung allen in dieser Anforderung angegebenen Elementen entspricht.	
Zielsetzung des kundenspezifischen Ansatzes		
Die Hardware- und Softwaretechnologien der Entität sind auf dem neuesten Stand und werden vom Anbieter unterstützt. Pläne zum Entfernen oder Ersetzen aller nicht unterstützten Systemkomponenten werden regelmäßig überprüft.		
Hinweise zur Anwendbarkeit		
Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.		

Anforderungen und Testprozeduren		Anleitungen
12.4 PCI DSS-Einhaltung wird verwaltet.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.4.1 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Die Geschäftsleitung trägt die Verantwortung für den Schutz der Karteninhaberdaten und ein PCI-DSS-Einhaltungs-Programm, das Folgendes umfasst: • Gesamtverantwortlichkeit für die Wartung der PCI DSS-Einhaltung. • Definition einer Charta für ein PCI DSS-Einhaltungs-Programm und Kommunikation mit der Geschäftsleitung.	**12.4.1** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Die Dokumentation untersuchen, um zu verifizieren, dass die Geschäftsleitung die Verantwortung für den Schutz der Karteninhaberdaten und ein PCI DSS-Einhaltungs-Programm gemäß allen in dieser Anforderung angegebenen Elementen etabliert hat.	Die Zuweisung von PCI DSS-Einhaltungs-Verantwortlichkeiten durch die Geschäftsleitung gewährleistet die Transparenz des PCI DSS-Einhaltungs-Programms auf Führungsebene und bietet die Möglichkeit, geeignete Fragen zu stellen, um die Wirksamkeit des Programms zu bestimmen und strategische Prioritäten zu beeinflussen.
Zielsetzung des kundenspezifischen Ansatzes		
Führungskräfte sind für die Sicherheit der Karteninhaberdaten verantwortlich und rechenschaftspflichtig.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. Die Geschäftsleitung kann C-Stufen-Positionen, Vorstände oder Ähnliches umfassen. Die spezifischen Titel hängen von der jeweiligen Organisationsstruktur ab. Die Verantwortung für das PCI DSS-Einhaltungs-Programm kann einzelnen Rollen und/oder Geschäftseinheiten innerhalb der Organisation zugewiesen werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die regelmäßige Bestätigung, dass Sicherheitsrichtlinien und -verfahren befolgt werden, stellt sicher, dass die erwarteten Kontrollen aktiv sind und wie beabsichtigt funktionieren. Diese Anforderung unterscheidet sich von anderen Anforderungen, die eine durchzuführende Aufgabe spezifizieren. Die Zielsetzung dieser Überprüfungen besteht nicht darin, andere PCI DSS-Anforderungen wieder durchzuführen, sondern zu bestätigen, dass Sicherheitsaktivitäten fortlaufend durchgeführt werden. **Gute Praxis** Diese Überprüfungen können auch verwendet werden, um zu verifizieren, dass geeignete Beweise geführt werden – zum Beispiel Audit-Protokolle, Schwachstellen-Scan-Berichte, Überprüfungen von Regelsätzen für die Netzwerksicherheitskontrolle –, um die Entität bei der Vorbereitung ihrer nächsten PCI DSS-Beurteilung zu unterstützen. **Beispiele** Betrachtet man Anforderung 1.2.7 als ein Beispiel, so wird Anforderung 12.4.2 dadurch erfüllt, dass mindestens alle drei Monate bestätigt wird, dass die Überprüfungen der Konfigurationen der Netzwerksicherheitskontrollen in der erforderlichen Häufigkeit stattgefunden haben. Andererseits wird Anforderung 1.2.7 erfüllt, indem diese Konfigurationen wie in der Anforderung angegeben überprüft werden.
12.4.2 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Überprüfungen werden mindestens alle drei Monate, um zu bestätigen, dass das Personal seine Aufgaben gemäß allen Sicherheitsrichtlinien und allen Betriebsverfahren erfüllt. Überprüfungen werden von Personal durchgeführt, das anders als diejenigen ist, die zum Durchführen der gegebenen Aufgaben verantwortlich sind, sind aber nicht beschränkt auf die folgenden Aufgaben: • Tägliche Protokollüberprüfungen. • Konfigurationsüberprüfungen für Netzwerksicherheitskontrollen. • Anwenden von Konfigurationsstandards auf neue Systeme. • Reagieren auf Sicherheitswarnungen. • Änderungsverwaltungsprozesse.	**12.4.2.a** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse für die Ausführung von Überprüfungen definiert sind, um zu bestätigen, dass das Personal seine Aufgaben gemäß allen Sicherheitsrichtlinien und allen betrieblichen Prozeduren durchführt, einschließlich, aber nicht beschränkt auf die in dieser Anforderung angegebenen Aufgaben.	
Zielsetzung des kundenspezifischen Ansatzes Die betriebliche Wirksamkeit kritischer PCI DSS-Kontrollen wird regelmäßig durch manuelle Überprüfung der Aufzeichnungen überprüft.	**12.4.2.b** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Verantwortliches Personal befragen und Aufzeichnungen von Überprüfungen untersuchen, um zu verifizieren, dass Überprüfungen durchgeführt werden: • Mindestens einmal alle drei Monate. • Durch Personal, das nicht für die Durchführung der jeweiligen Aufgabe zuständig ist.	
Hinweise zur Anwendbarkeit Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.4.2.1 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Überprüfungen, die gemäß Anforderung 12.4.2 ausgeführt werden, sind so dokumentiert, dass sie Folgendes umfassen: • Ergebnisse der Überprüfungen. • Dokumentierte Behebungsaktionen, die für alle Aufgaben ergriffen wurden, die nicht gemäß Anforderung 12.4.2 durchgeführt wurden. • Überprüfung und Abnahme der Ergebnisse durch Personal, das für das PCI DSS-Einhaltungsprogramm verantwortlich ist.	**12.4.2.1** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Dokumentation aus den Überprüfungen, die gemäß PCI DSS-Anforderung 12.4.2 durchgeführt wurden untersuchen, um zu verifizieren, dass die Dokumentation alle in dieser Anforderung angegebenen Elemente enthält.	Die Absicht dieser unabhängigen Überprüfungen besteht darin, zu bestätigen, ob Sicherheitsaktivitäten kontinuierlich durchgeführt werden. Diese Überprüfungen können auch verwendet werden, um zu verifizieren, dass geeignete Beweise geführt werden – zum Beispiel Audit-Protokolle, Schwachstellen-Scan-Berichte, Überprüfungen von Regelsätzen für die Netzwerksicherheitskontrolle –, um die Entität bei der Vorbereitung ihrer nächsten PCI DSS-Beurteilung zu unterstützen.
Zielsetzung des kundenspezifischen Ansatzes		
Erkenntnisse aus betrieblichen Wirksamkeitsprüfungen werden von der Verwaltung ausgewertet; entsprechende Sanierungsmaßnahmen werden implementiert.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur, wenn die Entität, die bewertet wird, ein Dienstleistungsanbieter ist. Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist.		

Anforderungen und Testprozeduren		Anleitungen
12.5 Der PCI DSS-Geltungsbereich wird dokumentiert und validiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Führen einer aktuellen Liste aller Systemkomponenten ermöglicht es einer Organisation, den Geltungsbereich ihrer Umgebung zu definieren und die PCI DSS-Anforderungen genau und effizient zu implementieren. Ohne ein Inventar könnten einige Systemkomponenten übersehen und versehentlich von den Konfigurationsstandards der Organisation ausgeschlossen werden. **Gute Praxis** Wenn eine Entität ein Inventar aller Assets führt, sollten diese Systemkomponenten im Geltungsbereich von PCI DSS unter den anderen Assets eindeutig identifizierbar sein. Inventare sollten Container oder Bilder enthalten, die instanziiert werden können. Das Zuweisen eines Eigentümers zum Inventar hilft dabei, um sicherzustellen, dass das Inventar aktuell bleibt. **Beispiele** Zu den Methoden zum Warten eines Inventars gehören eine Datenbank, eine Reihe von Dateien oder ein Inventarverwaltungstool.
12.5.1 Ein Inventar der Systemkomponenten, die für PCI DSS gelten, einschließlich einer Beschreibung der Funktion/Verwendung, wird geführt und auf dem neuesten Stand gehalten.	**12.5.1.a** Das Inventar untersuchen, um zu verifizieren, dass es alle im Lieferumfang enthaltenen Systemkomponenten und eine Beschreibung der Funktion/Verwendung für jede enthält.	
	12.5.1.b Das Personal befragen, um zu verifizieren, dass das Inventar auf dem neuesten Stand ist.	
Zielsetzung des kundenspezifischen Ansatzes		
Alle Systemkomponenten im Geltungsbereich von PCI DSS werden identifiziert und sind bekannt.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	
12.5.2 Der PCI DSS-Geltungsbereich wird dokumentiert und von der Entität mindestens einmal alle 12 Monate und bei bedeutenden Änderungen an der Umgebung innerhalb des Geltungsbereichs bestätigt. Die Scoping-Validierung beinhaltet mindestens: • Identifizieren aller Datenflüsse für die verschiedenen Zahlungsphasen (zum Beispiel Autorisierung, Erfassung der Abrechnung, Rückbuchungen und Rückerstattungen) und Akzeptanzkanäle (zum Beispiel Karte vorhanden, Karte nicht vorhanden und E-Commerce). • Aktualisierung aller Datenflussdiagramme gemäß Anforderung 1.2.4. • Identifizieren aller Standorte, an denen Kontendaten gespeichert, verarbeitet und übermittelt werden, einschließlich, aber nicht beschränkt auf: 1) alle Standorte außerhalb der derzeit definierten CDE, 2) Anwendungen, die CHD verarbeiten, 3) Übertragungen zwischen Systemen und Netzwerken, und 4) Datei-Backups. • Identifizierung aller Systemkomponenten in der CDE, die mit der CDE verbunden sind oder die die Sicherheit der CDE beeinträchtigen könnten. • Identifizierung aller verwendeten Segmentierungskontrollen und der Umgebung(en), aus denen die CDE segmentiert wird, einschließlich der Begründung für Umgebungen, die außerhalb des Geltungsbereichs liegen. • Identifizieren aller Verbindungen von dritten Entitäten mit Zugriff auf die CDE. *(Fortsetzung auf der nächsten Seite)*	**12.5.2.a** Dokumentierte Ergebnisse von Protokollüberprüfungen untersuchen und das Personal befragen, um zu verifizieren, dass die wie folgt durchgeführt werden. • Mindestens einmal alle 12 Monate. • Nach erheblichen Änderungen an der Umgebung im Geltungsbereich. **12.5.2.b** Dokumentierte Ergebnisse von Geltungsbereichs-Überprüfungen, die von der Entität durchgeführt wurden, um zu verifizieren, dass die PCI DSS-Scoping-Bestätigungsaktivität alle in dieser Anforderung angegebenen Elemente enthält.	**Zweck** Eine häufige Validierung des PCI DSS-Geltungsbereichs hilft dabei, sicherzustellen, dass der PCI DSS-Geltungsbereich auf dem neuesten Stand bleibt und an sich ändernde Geschäftszielsetzungen angepasst ist, und dass daher Sicherheitskontrollen alle geeigneten Systemkomponenten schützen. **Gute Praxis** Genaues Scoping beinhaltet die kritische Bewertung der CDE und aller angeschlossenen Systemkomponenten, um die erforderliche Abdeckung für die PCI DSS-Anforderungen zu bestimmen. Scoping-Aktivitäten, einschließlich sorgfältiger Analyse und fortlaufender Überwachung, tragen dazu bei, sicherzustellen, dass die Systeme im Geltungsbereich angemessen abgesichert sind. Beim Dokumentieren von Kontodatenspeicherorten kann die Entität erwägen, eine Tabelle oder Tabellenkalkulation zu erstellen, die die folgenden Informationen enthält: • Datenspeicher (Datenbanken, Dateien, Cloud usw.), einschließlich des Zwecks der Datenspeicherung und der Aufbewahrungsfrist, • Welche CHD-Elemente gespeichert werden (PAN, Ablaufdatum, Name des Karteninhabers und/oder alle Elemente von SAD vor Abschluss der Autorisierung), • Wie die Daten gesichert werden (Art der Verschlüsselung und Stärke, Hashierungs-Algorithmus und -stärke, Abschneiden, Tokenisierung), *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
• Bestätigung, dass alle identifizierten Datenflüsse, Kontodaten, Systemkomponenten, Segmentierungskontrollen und Verbindungen von Dritten mit Zugriff auf die CDE im Geltungsbereich enthalten sind.		• Wie der Zugriff auf Datenspeicher protokolliert wird, einschließlich einer Beschreibung des/der verwendeten Protokollierungsmechanismus/Protokollierungsmechanismen (Unternehmenslösung, Anwendungsebene, Betriebssystemebene usw.). Zusätzlich zu internen Systemen und Netzwerken müssen alle Verbindungen von dritten Entitäten – beispielsweise Geschäftspartnern, Entitäten, die Fernunterstützungs-Dienstleistungen anbieten, und anderen Dienstanbietern – identifiziert werden, um die Aufnahme in den PCI DSS-Geltungsbereich zu bestimmen. Sobald die Verbindungen im Geltungsbereich identifiziert wurden, können die anwendbaren PCI DSS-Kontrollen implementiert werden, um das Risiko zu verringern, dass eine Verbindung von Dritten verwendet wird, um die CDE einer Entität zu gefährden. Ein Daten-Entdeckungs-Tool oder eine Methodik kann verwendet werden, um die Identifizierung aller Quellen und Standorte von PAN zu erleichtern und nach PAN zu suchen, die sich auf Systemen und Netzwerken außerhalb der aktuell definierten CDE oder an unerwarteten Stellen innerhalb der definierten CDE befindet – zum Beispiel bei einem Fehlerprotokoll oder Speicher-Dumpdatei. Dieser Ansatz kann dazu beitragen, dass zuvor unbekannte PAN-Standorte erkannt und die PAN entweder beseitigt oder ordnungsgemäß gesichert wird. **Weitere Informationen** Für zusätzliche Anleitungen siehe *Informationsergänzung: Anleitungen für PCI DSS-Scoping und Netzwerksegmentierung*.
Zielsetzung des kundenspezifischen Ansatzes Der PCI DSS-Geltungsbereich wird regelmäßig und nach bedeutenden Änderungen durch umfassende Analysen und geeignete technische Maßnahmen verifiziert.		
Hinweise zur Anwendbarkeit Diese jährliche Bestätigung des PCI DSS-Geltungsbereichs ist eine Aktivität, die voraussichtlich von der zu bewertenden Entität durchgeführt wird, und ist nicht identisch mit der Scoping-Bestätigung, die vom Bewerter der Entität während der jährlichen Bewertung durchgeführt wird, noch soll sie durch diese ersetzt werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.5.2.1 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Der PCI DSS-Geltungsbereich wird dokumentiert und von der Entität mindestens einmal alle sechs Monate und bei bedeutenden Änderungen an der Umgebung innerhalb des Geltungsbereichs bestätigt. Die Scoping-Validierung umfasst mindestens alle Elemente, die in Anforderung 12.5.2 angegeben sind.	**12.5.2.1.a** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Dokumentierte Ergebnisse von Geltungsbereichsüberprüfungen untersuchen und das Personal befragen, um zu verifizieren, dass Überprüfungen gemäß Anforderung 12.5.2 durchgeführt werden: • Mindestens einmal alle sechs Monate, und • Nach bedeutenden Änderungen	Dienstleistungsanbieter haben typischerweise Zugriff auf größere Mengen an Karteninhaberdaten als Händler, oder können einen Einstiegspunkt bereitstellen, der ausgenutzt werden kann, um dann mehrere andere Entitäten zu kompromittieren. Dienstleistungsanbieter haben auch typischerweise größere und komplexere Netzwerke, die häufigeren Änderungen unterliegen. Die Wahrscheinlichkeit von übersehenen Änderungen des Geltungsbereichs in komplexen und dynamischen Netzwerken ist in Dienstleistungsanbieter-Umgebungen größer. Durch eine häufigere Validierung des PCI DSS-Geltungsbereichs werden solche übersehenen Änderungen wahrscheinlich entdeckt, bevor sie von einem Angreifer ausgenutzt werden können.
Zielsetzung des kundenspezifischen Ansatzes Die Genauigkeit des PCI DSS-Geltungsbereichs wird durch umfassende Analysen und geeignete technische Maßnahmen auf kontinuierliche Genauigkeit verifiziert.	**12.5.2.1.b** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Dokumentierte Ergebnisse von Geltungsbereichs-Überprüfungen untersuchen, um zu verifizieren, dass die Scoping-Validierung alle in Anforderung 12.5.2 spezifizierten Elemente enthält.	
Hinweise zur Anwendbarkeit *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Struktur und die Verwaltung einer Organisation definieren die Anforderungen und das Protokoll für effektive und sichere Betriebe. Änderungen an dieser Struktur könnten negative Auswirkungen auf bestehende Kontrollen und Rahmenwerke haben, indem Ressourcen, die früher PCI DSS-Kontrollen unterstützten, neu zugewiesen oder entfernt werden oder neue Verantwortlichkeiten übernommen werden, die möglicherweise keine etablierten Kontrollen eingerichtet haben. Daher ist es wichtig, den Geltungsbereich und die Kontrollen des PCI DSS zu überarbeiten, wenn es Änderungen an der Struktur und der Verwaltung einer Organisation gibt, um sicherzustellen, dass Kontrollen vorhanden und aktiv sind. **Beispiele** Änderungen an der Organisationsstruktur umfassen, sind aber nicht beschränkt auf Unternehmensfusionen oder -übernahmen und bedeutenden Änderungen oder Neuzuweisungen von Personal, das für Sicherheitskontrollen verantwortlich ist.
12.5.3 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** Bedeutende Änderungen an der Organisationsstruktur führen zu einer formellen (internen) Überprüfung der Auswirkungen auf den PCI DSS-Geltungsbereich und die Anwendbarkeit von Kontrollen, wobei die Ergebnisse der Geschäftsleitung mitgeteilt werden.	**12.5.3.a** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, sodass eine bedeutende Änderung der Organisationsstruktur zu einer dokumentierten Überprüfung der Auswirkungen auf den PCI DSS-Geltungsbereich und die Anwendbarkeit von Kontrollen führt.	
Zielsetzung des kundenspezifischen Ansatzes Der PCI DSS-Geltungsbereich wird nach bedeutenden organisatorischen Änderungen bestätigt.	**12.5.3.b** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Dokumentation (zum Beispiel Besprechungsprotokolle) untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass bedeutende Änderungen an der Organisationsstruktur zu dokumentierten Überprüfungen führten, die alle in dieser Anforderung angegebenen Elemente enthielten, wobei die Ergebnisse der Geschäftsleitung mitgeteilt wurden.	
Hinweise zur Anwendbarkeit Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
12.6 Die Aufklärung über das Sicherheitsbewusstsein ist eine fortlaufende Aktivität.		
Definierte Ansatzanforderungen **12.6.1** Ein formales Sicherheitsbewusstseinsprogramm wird implementiert, um das gesamte Personal auf die Informationssicherheitsrichtlinien und -prozeduren der Entität und seine Rolle beim Schutz der Karteninhaberdaten aufmerksam zu machen. **Zielsetzung des kundenspezifischen Ansatzes** Das Personal ist über die Bedrohungslandschaft und seine Verantwortung für den Betrieb relevanter Sicherheitskontrollen informiert und kann bei Bedarf auf Unterstützung und Anleitungen zugreifen.	**Testprozeduren mit definiertem Ansatz** **12.6.1** Das Sicherheitsbewusstseinsprogramm untersuchen, um zu verifizieren, dass es dem gesamten Personal Bewusstsein über die Informationssicherheitsrichtlinie und -prozeduren der Entität und die Rolle des Personals beim Schutz der Karteninhaberdaten bereitstellt.	**Zweck** Wenn das Personal nicht über die Informationssicherheitsrichtlinien und -prozeduren ihres Unternehmens und ihre eigenen Sicherheitsverantwortlichkeiten unterrichtet sind, können implementierte Sicherheitsvorkehrungen und -prozesse durch unbeabsichtigte Fehler oder vorsätzliche Aktionen unwirksam werden.
Definierte Ansatzanforderungen **12.6.2** Das Sicherheitsbewusstseinsprogramm ist: • Mindestens einmal alle 12 Monate überprüft und • Nach Bedarf aktualisiert, um neue Bedrohungen und Schwachstellen zu adressieren, die sich auf die Sicherheit der CDE der Entität oder auf die dem Personal bereitgestellten Informationen über ihre Rolle beim Schutz von Karteninhaberdaten auswirken können. **Zielsetzung des kundenspezifischen Ansatzes** Der Inhalt des Sicherheitsbewusstseinsmaterials wird regelmäßig überprüft und aktualisiert. **Hinweise zur Anwendbarkeit** *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**Testprozeduren mit definiertem Ansatz** **12.6.2** Den Inhalt des Sicherheitsbewusstseinsprogramms, Überprüfungsnachweise untersuchen, und das Personal befragen, um zu verifizieren, dass das Sicherheitsbewusstseinsprogramm mit allen in dieser Anforderung angegebenen Elementen übereinstimmt.	**Zweck** Die Bedrohungsumgebung und die Verteidigungen einer Entität sind nicht statisch. Daher müssen die Materialien des Sicherheitsbewusstseinsprogramms so oft wie nötig aktualisiert werden, um sicherzustellen, dass die von dem Personal empfangenen Bildung auf dem neuesten Stand ist und die aktuelle Bedrohungsumgebung widerspiegelt.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Schulung des Personals stellt sicher, dass es die Informationen über die Wichtigkeit der Informationssicherheit erhält und dass es seine Rolle beim Schutz der Organisation versteht. Das Anfordern einer Bestätigung durch das Personal hilft dabei, sicherzustellen, dass es die Sicherheitsrichtlinien und -prozeduren gelesen und verstanden hat und dass es sich zur Einhaltung dieser Richtlinien verpflichtet hat und dies auch weiterhin tun wird. **Gute Praxis** Entitäten können Schulungen für neue Mitarbeiter als Teil des Personaleinarbeitungsprozesses integrieren. Die Schulung sollte die sicherheitsbezogenen „tun“ und „nicht tun“ skizzieren. Regelmäßige Auffrischungsschulungen stärken wichtige Sicherheitsprozesse und -prozeduren, die vergessen oder umgangen werden können. Entitäten sollten erwägen, Sicherheitsbewusstseinsschulungen zu verlangen, wenn Personal in Rollen wechselt, in denen es sich auf die Sicherheit von Kontodaten auswirken kann, von Rollen, in denen sie diese Auswirkungen nicht hatten. Methoden und Schulungsinhalte können je nach der Personalrolle variieren. **Beispiele** Verschiedene Methoden, die verwendet werden können, um Sicherheitsbewusstsein und Aufklärung zu bereitzustellen, umfassen Poster, Briefe, webbasierte Schulungen, persönliche Schulungen, Teambesprechungen und Anreize. Personalbestätigungen können schriftlich oder elektronisch aufgezeichnet werden.
12.6.3 Das Personal erhält folgende Sicherheitsbewusstseinsschulungen: • Bei Einstellung und mindestens einmal alle 12 Monate. • Es werden mehrere Kommunikationsmethoden verwendet. • Das Personal bestätigt mindestens einmal alle 12 Monate, dass es die Informationssicherheitsrichtlinie und -prozeduren gelesen und verstanden hat.	**12.6.3.a** Aufzeichnungen des Sicherheitsbewusstseinsprogramms untersuchen, um zu verifizieren, dass das Personal bei der Einstellung und mindestens einmal alle 12 Monate an einer Sicherheitsbewusstseinsschulung teilnimmt.	
	12.6.3.b Sicherheitsbewusstseins-Programm-Materialien untersuchen, um zu verifizieren, dass das Programm mehrere Methoden umfasst, um Bewusstsein zu vermitteln und das Personal zu schulen.	
	12.6.3.c Das Personal befragen, um zu verifizieren, dass es eine Bewusstseinsschulung vervollständigt hat und sich ihrer Rolle beim Schutz von Karteninhaberdaten bewusst ist.	
Zielsetzung des kundenspezifischen Ansatzes Das Personal bleibt über die Bedrohungslandschaft und seine Verantwortung für den Betrieb relevanter Sicherheitskontrollen informiert und kann bei Bedarf auf Unterstützung und Anleitungen zugreifen.	**12.6.3.d** Sicherheitsbewusstseins-Programm-Materialien und Bestätigungen des Personals untersuchen, um zu verifizieren, dass das Personal mindestens einmal alle 12 Monate bestätigt, dass es die Richtlinien und Prozeduren zur Informationssicherheit gelesen und verstanden hat.	

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu minimieren, ist es wichtig, dass das Personal darin geschult wird, wie es potenzielle Phishing- und verwandte Angriffe und Social-Engineering-Versuche erkennt, darauf reagiert und melden kann. **Gute Praxis** Ein wirksames Sicherheitsbewusstseinsprogramm sollte Beispiele für Phishing-E-Mails und regelmäßige Tests umfassen, um zu bestimmen, wie häufig Mitarbeiter solche Angriffe melden. Die Schulungsmaterialien, die eine Entität zu diesem Thema in Betracht ziehen kann, beinhalten: • Wie Phishing- und andere Social-Engineering-Angriffe identifiziert werden. • Wie auf mutmaßliches Phishing und Social Engineering reagiert wird. • Wo und wie mutmaßliche Phishing- und Social-Engineering-Aktivitäten gemeldet werden. Eine Betonung der Berichterstattung gestattet es der Organisation, positives Verhalten zu belohnen, technische Abwehrmaßnahmen zu optimieren (siehe Anforderung 5.4.1) und sofort Maßnahmen zu ergreifen, um ähnliche Phishing-E-Mails, die technische Abwehrmaßnahmen umgangen haben, aus den Posteingängen der Empfänger zu entfernen.
12.6.3.1 Die Sicherheitsbewusstseinsschulung umfasst das Bewusstsein für Bedrohungen und Schwachstellen, die sich auf die Sicherheit des CDE auswirken könnten, einschließlich, aber nicht beschränkt auf: • Phishing und verwandte Angriffe. • Social Engineering.	**12.6.3.1** Den Inhalt der Sicherheitsbewusstseinsschulung untersuchen, um zu verifizieren, dass sie alle in dieser Anforderung angegebenen Elemente enthält.	
Zielsetzung des kundenspezifischen Ansatzes Das Personal kennt seine eigenen menschlichen Schwachstellen und weiß, wie Angreifer versuchen werden, solche Schwachstellen auszunutzen. Das Personal kann bei Bedarf auf Hilfe und Anleitungen zugreifen.		
Hinweise zur Anwendbarkeit Siehe Anforderung 5.4.1 für Anleitungen zum Unterschied zwischen technischen und automatisierten Kontrollen, um Phishing-Angriffe zu erkennen und Benutzer vor ihnen zu schützen, und diese Anforderung für die Bereitstellung von Sicherheitsbewusstseins-Schulungen der Benutzer betreffs Phishing und Social Engineering. Dies sind zwei getrennte und unterschiedliche Anforderungen, und eine wird nicht erfüllt, indem Kontrollen implementiert werden, die von der anderen gefordert werden. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.6.3.2 Die Sicherheitsbewusstseinsschulung umfasst das Bewusstsein für die akzeptable Verwendung von Endbenutzertechnologien gemäß Anforderung 12.2.1.	**12.6.3.2** DenSicherheitsbewusstseinsschulungsinhalt untersuchen, um zu verifizieren, dass er Bewusstsein für die akzeptable Verwendung von Endbenutzertechnologien gemäß Anforderung 12.2.1 umfasst.	Durch die Einbeziehung der wichtigsten Punkte der Richtlinie zur akzeptablen Verwendung in regelmäßige Schulungen und den damit verwandten Zusammenhang wird das Personal seine Verantwortlichkeiten verstehen und wie sich diese auf die Sicherheit der Systeme einer Organisation auswirken.
Zielsetzung des kundenspezifischen Ansatzes		
Das Personal bleibt über seine Verantwortung für die Sicherheit und den Betrieb von Endbenutzertechnologien informiert und kann bei Bedarf auf Unterstützung und Anleitungen zugreifen.		
Hinweise zur Anwendbarkeit		
Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.		

Anforderungen und Testprozeduren		Anleitungen
12.7 Das Personal wird überprüft, um Risiken durch Insider-Bedrohungen zu reduzieren.		
Definierte Ansatzanforderungen **12.7.1** Potentielles Personal, das Zugriff auf die CDE haben wird, wird vor der Einstellung im Rahmen der örtlichen Gesetze überprüft, um das Risiko von Angriffen aus internen Quellen zu minimieren. **Zielsetzung des kundenspezifischen Ansatzes** Das Risiko, das damit verbunden ist, neuen Mitarbeitern Zugang zur CDE zu gewähren, wird verstanden und verwaltet. **Hinweise zur Anwendbarkeit** Für potenzielles Personal, das für Positionen wie Ladenkassierer eingestellt werden soll, die beim Ermöglichen einer Transaktion nur Zugriff auf jeweils eine Kartennummer haben, ist diese Anforderung nur eine Empfehlung.	**Testprozeduren mit definiertem Ansatz** **12.7.1** Die verantwortliche Verwaltung der Personalabteilung befragen, um zu verifizieren, dass vor der Einstellung von potenziellem Personal, das Zugriff auf die CDE hat, im Rahmen der örtlichen Gesetze eine Überprüfung ausgeführt wird.	**Zweck** Die Durchführung einer gründlichen Überprüfung vor der Einstellung von potenziellem Personal, von dem erwartet wird, dass es Zugriff auf die CDE erhält, erhalten, stellt den Entitäten die Informationen bereit, die erforderlich sind, um informierte Risikoentscheidungen in Bezug auf das von ihnen eingestellte Personal zu treffen, das Zugriff auf die CDE haben wird. Weitere Vorteile der Überprüfung von potenziellem Personal umfassen die Unterstützung bei der Sicherstellung der Sicherheit am Arbeitsplatz und die Bestätigung der Angaben potenzieller Mitarbeiter in ihren Lebensläufen. **Gute Praxis** Entitäten sollten eine Überprüfung des vorhandenen Personals in Erwägung ziehen, wenn dieses in eine Rolle wechselt, in der es Zugriff auf die CDE, von einer Rolle aus, in der es diesen Zugriff noch nicht hatte. Um effektiv zu sein, sollte das Screening-Niveau für die Position angemessen sein. Zum Beispiel können Positionen, die eine größere Verantwortung erfordern oder die Administratorzugriff auf kritische Daten oder Systeme haben, eine detailliertere oder häufigere Überprüfung rechtfertigen als Positionen mit weniger Verantwortung und Zugriff. **Beispiele** Screening-Optionen können, je nach Region der Entität, frühere Beschäftigungsgeschichte, Überprüfung öffentlicher Informationen/Ressourcen sozialer Medien, Vorstrafenregister, Kredithistorie und Referenzprüfungen umfassen.

Anforderungen und Testprozeduren		Anleitungen
12.8 Das Risiko für Informationsassets im Zusammenhang mit den Beziehungen zu dritten Dienstleistungsanbietern (TPSP) wird verwaltet.		
Definierte Ansatzanforderungen **12.8.1** Eine Liste aller dritten Dienstleistungsanbieter, (TPSPs), mit denen Kontodaten geteilt werden oder die die Sicherheit von Kontodaten beeinträchtigen könnten, wird geführt, einschließlich einer Beschreibung für jeden der bereitgestellten Dienstleistungen.	**Testprozeduren mit definiertem Ansatz** **12.8.1.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, um eine Liste von TPSPs zu führen, einschließlich einer Beschreibung für jeden der bereitgestellten Dienstleistungen, für alle TPSPs, mit denen Kontodaten geteilt werden oder die die Sicherheit von Kontodaten beeinträchtigen könnten.	**Zweck** Die Pflege einer Liste aller TPSPs identifiziert, wo sich potenzielle Risiken außerhalb der Organisation erstrecken, und definiert die erweiterte Angriffsfläche der Organisation. **Beispiele** Verschiedene Arten von TPSPs beinhalten solche, die: • Kontodaten im Auftrag der Entität speichern, verarbeiten oder übertragen (wie Zahlungs-Gateways, Zahlungsabwickler, Zahlungsdienstleistungsanbieter (PSPs) und externe Speicheranbieter). • Systemkomponenten, die in der PCI DSS-Beurteilung der Entität enthalten sind, verwalten (wie Anbieter von Netzwerksicherheitskontrolldienstleistungen, Anti-Malware-Dienstleistungen und Verwaltung von Sicherheitsvorfällen und Ereignissen (SIEM); Kontakt- und Callcenter; Webhosting-Unternehmen; und IaaS, PaaS, SaaS- und FaaS-Cloud-Anbieter). • Die Sicherheit der CDE der Entität beeinträchtigen könnten (wie Anbieter, die Unterstützung per Fernzugriff bereitstellen, und Entwickler von maßgeschneiderter Software).
Zielsetzung des kundenspezifischen Ansatzes Es werden Aufzeichnungen über TPSPs und die bereitgestellten Dienstleistungen geführt.	**12.8.1.b** Die Dokumentation untersuchen, um zu verifizieren, dass eine Liste aller TPSPs geführt wird, die eine Beschreibung der bereitgestellten Dienstleistungen enthält.	
Hinweise zur Anwendbarkeit Die Verwendung eines PCI DSS-konformen TPSP macht eine Entität nicht PCI DSS-konform und enthebt sie auch nicht der Verantwortung für ihre eigene PCI DSS-Einhaltung.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die schriftliche Bestätigung von einem TPSP demonstriert seine Verpflichtung für die Aufrechterhaltung der angemessenen Sicherheit der Kontodaten, die er von seinen Kunden erhält, und dass der TPSP sich der Assets, die während der Bereitstellung der TPSP-Dienstleistung betroffen sein könnten, voll bewusst ist. Inwieweit ein bestimmter TPSP für die Sicherheit von Kontodaten verantwortlich ist, hängt von der bereitgestellten Dienstleistung und der Vereinbarung zwischen dem Anbieter und der bewerteten Entität (dem Kunden) ab. In Verbindung mit Anforderung 12.9.1 soll diese Anforderung ein einheitliches Maß an Verständnis zwischen Parteien über ihre anwendbaren PCI DSS-Verantwortlichkeiten fördern. Zum Beispiel kann die Vereinbarung die anwendbaren PCI DSS-Anforderungen enthalten, die als Teil der bereitgestellten Dienstleistung aufrechterhalten werden müssen. **Gute Praxis** Die Entität kann auch erwägen, in ihre schriftliche Vereinbarung mit einem TPSP aufzunehmen, dass der TPSP die Anfrage nach Informationen von der Entität gemäß Anforderung 12.9.2 unterstützen wird. Entitäten werden auch verstehen wollen, ob irgendwelche TPSPs „verschachtelte“ Beziehungen mit anderen TPSPs haben, was bedeutet, dass der primäre TPSP Verträge mit anderen TPSPs zum Zwecke der Bereitstellung einer Dienstleistung abschließt. *(Fortsetzung auf der nächsten Seite)*
12.8.2 Schriftliche Vereinbarungen mit TPSPs werden wie folgt gewartet: • Mit allen TPSPs, mit denen Kontodaten geteilt werden oder die die Sicherheit der CDE beeinträchtigen könnten, werden schriftliche Vereinbarungen aufrechterhalten. • Schriftliche Vereinbarungen beinhalten Bestätigungen von TPSPs, dass sie für die Sicherheit von Kontodaten verantwortlich sind, die die TPSPs besitzen oder anderweitig im Namen der Entität speichern, verarbeiten oder übertragen, oder in dem Umfang, in dem sie die Sicherheit der CDE der Entität beeinträchtigen könnten.	**12.8.2.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, um schriftliche Vereinbarungen mit allen TPSPs gemäß allen in dieser Anforderung angegebenen Elementen aufrechtzuerhalten.	
Zielsetzung des kundenspezifischen Ansatzes	**12.8.2.b** Schriftliche Vereinbarungen mit TPSPs untersuchen, um zu verifizieren, dass sie gemäß allen in dieser Anforderung angegebenen Elementen aufrechterhalten werden.	
Es werden Aufzeichnungen darüber geführt, dass jeder TPSP seine Verantwortung für den Schutz von Kontodaten bestätigt.		
Hinweise zur Anwendbarkeit		
Der genaue Wortlaut einer Bestätigung hängt von der Vereinbarung zwischen den beiden Parteien, den Details der bereitgestellten Dienstleistung und den jeder Partei zugewiesenen Verantwortlichkeiten ab. Die Bestätigung muss nicht den genauen Wortlaut enthalten, der in dieser Anforderung bereitgestellt ist. Der Nachweis, dass ein TPSP die PCI DSS-Anforderungen erfüllt (zum Beispiel eine PCIDSS-Bescheinigung der Einhaltung (AOC) oder eine Erklärung auf der Website eines Unternehmens), ist nicht dasselbe wie eine in dieser Anforderung angegebenen schriftliche Vereinbarung.		

Anforderungen und Testprozeduren		Anleitungen
		Es ist wichtig zu verstehen, ob sich der primäre TPSP auf den/die sekundären TPSP(s) verlässt, um die gesamte Einhaltung einer Dienstleistung zu erreichen, und welche Arten von schriftlichen Vereinbarungen der primäre TPSP mit den sekundären TPSPs getroffen hat. Entitäten können erwägen, in ihre schriftliche Vereinbarung eine Abdeckung für alle „verschachtelten" TPSPs aufzunehmen, die ein primärer TPSP verwenden kann. **Weitere Informationen** Siehe die *„Informationsergänzung: Sicherheitsgarantie von Drittanbietern* für weitere Anleitungen.
Definierte Ansatzanforderungen **12.8.3** Für die Beauftragung von TPSPs wird ein etablierter Prozess implementiert, einschließlich einer ordnungsgemäßen Sorgfaltspflicht vor der Beauftragung.	**Testprozeduren mit definiertem Ansatz** **12.8.3.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse für zum Beauftragen von TPSPs definiert sind, einschließlich einer angemessenen Sorgfaltspflicht vor der Beauftragung.	**Zweck** Ein gründliches Verfahren zur Beauftragung von TPSPs, einschließlich Details für die Auswahl und Überprüfung vor der Beauftragung, hilft dabei, dass ein TPSP vor dem Aufbau einer formellen Beziehung intern von einer Entität überprüft wird und dass das mit der Beauftragung des TPSP verbundene Risiko für Karteninhaberdaten verstanden wird. **Gute Praxis** Spezifische Sorgfaltspflicht-Prozesse und -Ziele sind für jede Organisation unterschiedlich. Elemente, die berücksichtigt werden sollten, umfassen die Meldepraktiken des Anbieters, die Prozeduren zur Benachrichtigung bei Verstößen und Vorfallsreaktions-Prozeduren, Details, wie die PCI DSS-Verantwortlichkeiten zwischen den einzelnen Parteien zugewiesen werden, wie der TPSP seine PCI DSS-Einhaltung validiert und welche Nachweise er bereitstellt.
Zielsetzung des kundenspezifischen Ansatzes Die Fähigkeit, Absicht und Ressourcen eines voraussichtlichen TPSP, um Kontodaten angemessen zu schützen, werden bewertet, bevor der TPSP beauftragt wird.	**12.8.3.b** Nachweise untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass die für die Beauftragung von TPSPs eine ordnungsgemäße Sorgfaltspflicht vor der Beauftragung umfasst.	

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Kenntnis des PCI DSS-Einhaltungsstatus aller beauftragten TPSPs stellt Gewissheit und Bewusstsein dafür bereit, ob sie die Anforderungen einhalten, die für die Dienstleistungen gelten, die sie der Organisation anbieten. **Gute Praxis** Wenn der TPSP eine Vielzahl von Dienstleistungen anbietet, sollte der Einhaltung-Status, den die Entität überwacht, spezifisch für die an die Entität gelieferten Dienstleistungen und die Dienstleistungen sein, die für die PCI DSS-Bewertung der Entität in Frage kommen. Wenn ein TPSP über eine PCI DSS-Einhaltungsbescheinigung verfügt, (AOC), wird erwartet, dass der TPSP diese den Kunden auf Anfrage bereitstellen sollte, um seinen PCI DSS-Einhaltungsstatus nachzuweisen Wenn der TPSP keiner PCI DSS-Bewertung unterzogen wurde, kann er möglicherweise andere ausreichende Nachweise erbringen, um zu demonstrieren, dass er die geltenden Anforderungen erfüllt hat, ohne sich einer formellen Einhaltungsvalidierung zu unterziehen. Zum Beispiel kann der TPSP dem Gutachter der Entität spezifische Nachweise vorlegen, damit der Gutachter bestätigen kann, dass die geltenden Anforderungen erfüllt sind. Alternativ kann sich der TPSP für mehrere Beurteilungen auf Abruf durch jeden der Gutachter seiner Kunden entscheiden, wobei jede Beurteilung darauf abzielt, zu bestätigen, dass die geltenden Anforderungen erfüllt sind. *(Fortsetzung auf der nächsten Seite)*
12.8.4 Es wird ein Programm implementiert, um den PCI DSS-Einhaltungsstatus der TPSPs mindestens einmal alle 12 Monate zu überwachen.	**12.8.4.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, um den PCI DSS-Einhaltungsstatus von TPSPs mindestens einmal alle 12 Monate zu überwachen.	
	12.8.4.b Die Dokumentation untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass der PCI DSS-Einhaltungsstatus von jedem TPSP mindestens einmal alle 12 Monate überwacht wird.	
Zielsetzung des kundenspezifischen Ansatzes		
Der PCI DSS-Einhaltungsstatus von TPSPs wird regelmäßig verifiziert.		
Hinweise zur Anwendbarkeit		
Wenn eine Entität eine Vereinbarung mit einem TPSP zur Erfüllung der PCI DSS-Anforderungen im Namen der Entität hat (zum Beispiel über eine Firewall-Dienstleistung), muss die Entität mit dem TPSP zusammenarbeiten, um sicherzustellen, dass die anwendbaren PCI DSS-Anforderungen erfüllt werden. Wenn der TPSP diese anwendbaren PCI DSS-Anforderungen nicht erfüllt, dann sind diese Anforderungen auch für die Entität „nicht vorhanden“.		

Anforderungen und Testprozeduren		Anleitungen
		Weitere Informationen Weitere Informationen zu Drittanbietern von Dienstleistungen finden Sie unter: • PCI DSS-Abschnitt: *Verwendung von Drittanbietern von Dienstleistungen*. • *Informationsergänzung: Sicherheitsgarantie von Drittanbietern*.
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Es ist wichtig, dass die Entität versteht, welche PCI DSS-Anforderungen und Unteranforderungen seine TPSPs erfüllen, welche Anforderungen zwischen dem TPSP und der Entität gemeinsam genutzt werden und für diejenigen, die gemeinsam genutzt werden, Angaben darüber machen, wie die Anforderungen gemeinsam genutzt werden und welche Entität für die Erfüllung jeder Unteranforderung verantwortlich ist. Ohne dieses gemeinsame Verständnis ist es unvermeidlich, dass die Entität und der TPSP davon ausgehen, dass eine bestimmte PCI DSS-Unteranforderung in der Verantwortung der anderen Partei liegt, und diese Unteranforderung daher möglicherweise überhaupt nicht adressiert wird. Die spezifischen Informationen, die eine Entität wartet, wird von der jeweiligen Vereinbarung mit ihren Anbietern, der Art der Dienstleistung usw. abhängen. TPSPs können ihre PCI DSS-Verantwortlichkeiten so definieren, dass sie für alle ihre Kunden gleich sind; andernfalls sollte diese Verantwortung zwischen der Entität und TPSP vereinbart werden. *(Fortsetzung auf der nächsten Seite)*
12.8.5 Es werden Informationen darüber verwaltet, welche PCI DSS-Anforderungen von jedem TPSP verwaltet werden, welche von der Entität verwaltet werden und welche zwischen dem TPSP und der Entität geteilt werden.	**12.8.5.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, um Informationen darüber aufrechtzuerhalten, welche PCI DSS-Anforderungen von jedem TPSP verwaltet werden, welche von der Entität verwaltet werden und welche zwischen dem TPSP und der Entität geteilt werden.	
Zielsetzung des kundenspezifischen Ansatzes	**12.8.5.b** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass die Entität Informationen darüber aufrechterhält, welche PCI DSS-Anforderungen von jedem TPSP verwaltet werden, welche von der Entität verwaltet werden und irgendwelche, die von beiden Entitäten gemeinsam genutzt werden.	
Aufzeichnungen über die PCI DSS-Anforderungen und verwandte Systemkomponenten, für die jeder TPSPs allein oder gemeinsam verantwortlich ist, werden aufrechterhalten und regelmäßig überprüft.		

Anforderungen und Testprozeduren		Anleitungen
		Gute Praxis Entitäten können diese Verantwortlichkeiten über eine Matrix dokumentieren, die alle anwendbaren PCI DSS-Anforderungen identifiziert und für jede Anforderung angibt, ob die Entität oder TPSP für die Erfüllung dieser Anforderung verantwortlich ist oder ob es sich um eine gemeinsame Verantwortung handelt. Diese Art von Dokument wird oft als *Verantwortungsmatrix* bezeichnet. Für Entitäten ist es auch wichtig zu verstehen, ob irgendwelche TPSPs „verschachtelte" Beziehungen mit anderen TPSPs haben, was bedeutet, dass der primäre TPSP Verträge mit anderen TPSPs zum Zwecke der Bereitstellung einer Dienstleistung abschließt. Es ist wichtig zu verstehen, ob sich der primäre TPSP auf den/die sekundären TPSP(s) verlässt, um die gesamte Einhaltung einer Dienstleistung zu erreichen, und wie der primäre TPSP die Leistung der Dienstleistung und den PCI DSS-Einhaltungs-Status des/der sekundären TPSP(s) überwacht. Beachten Sie, dass der primäre TPSP dafür verantwortlich ist, alle sekundären TPSPs zu verwalten und zu überwachen. **Weitere Informationen** Siehe *„Informationsergänzung: Sicherheitsgarantie von Drittanbietern* für eine Muster-Verantwortungsmatrix-Vorlage.

Anforderungen und Testprozeduren		Anleitungen
12.9 Dritte Dienstleistungsanbieter (TPSPs) unterstützen die PCI DSS-Einhaltung ihrer Kunden.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.9.1 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** TPSPs erkennen gegenüber Kunden schriftlich an, dass sie für die Sicherheit von Kontodaten, verantwortlich sind, die der TPSP besitzt oder anderweitig im Auftrag des Kunden speichert, verarbeitet oder übermittelt, oder in dem Umfang, in dem sie die Sicherheit der CDE des Kunden beeinträchtigen könnten.	**12.9.1** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** TPSP-Richtlinien, -Verfahren und -Vorlagen, die für schriftliche Vereinbarungen verwendet werden, untersuchen, um zu verifizieren, dass Prozesse für den TPSP definiert werden, um Kunden schriftliche Bestätigungen gemäß allen in dieser Anforderung angegebenen Elementen bereitzustellen.	In Verbindung mit Anforderung 12.8.2 soll diese Anforderung ein einheitliches Maß an Verständnis zwischen TPSPs und ihren Kunden über ihre anwendbaren PCI DSS-Verantwortlichkeiten fördern. Die Anerkennung der TPSPs beweist ihr Engagement für die Aufrechterhaltung der angemessenen Sicherheit der Kontodaten, die sie von ihren Kunden erhalten. Die Methode, mit der der TPSP eine schriftliche Bestätigung bereitstellt, sollte zwischen dem Anbieter und seinen Kunden vereinbart werden.
Zielsetzung des kundenspezifischen Ansatzes		
TPSPs erkennen ihre Sicherheitsverantwortung gegenüber ihren Kunden formell an.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist. Der genaue Wortlaut einer Bestätigung hängt von der Vereinbarung zwischen den beiden Parteien, den Details der bereitgestellten Dienstleistung und den jeder Partei zugewiesenen Verantwortlichkeiten ab. Die Bestätigung muss nicht den genauen Wortlaut enthalten, der in dieser Anforderung bereitgestellt ist.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.9.2 ***Zusätzliche Anforderungen nur für Dienstleistungsanbieter:*** TPSPs unterstützen die Informationsanfragen ihrer Kunden, um die Anforderungen 12.8.4 und 12.8.5 zu erfüllen, indem sie auf Kundenanfrage Folgendes bereitstellen: • PCI DSS-Einhaltungs-Statusinformationen für alle Dienstleistungen, die der TPSP im Auftrag von Kunden durchführt (Anforderung 12.8.4). • Informationen darüber, welche PCI DSS-Anforderungen in der Verantwortung des TPSP und welche in der Verantwortung des Kunden liegen, einschließlich etwaiger gemeinsamer Verantwortlichkeiten (Anforderung 12.8.5).	**12.9.2.** ***Zusätzliche Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse für den TPSP definiert sind, um Kundenanfragen betreffs Informationen zu unterstützen, um die Anforderungen 12.8.4 und 12.8.5 in gemäß allen in dieser Anforderung angegebenen Elementen zu erfüllen.	Wenn ein TPSP nicht die erforderlichen Informationen bereitstellt, damit seine Kunden ihre Sicherheits- und Einhaltungsanforderungen erfüllen können, können die Kunden weder Karteninhaberdaten schützen noch ihre eigenen vertraglichen Verpflichtungen erfüllen. **Gute Praxis** Wenn ein TPSP über eine PCI DSS-Einhaltungsbescheinigung verfügt, (AOC), wird erwartet, dass der TPSP diese den Kunden auf Anfrage bereitstellen sollte, um seinen PCI DSS-Einhaltungsstatus nachzuweisen Wenn der TPSP keiner PCI DSS-Bewertung unterzogen wurde, können sie möglicherweise andere ausreichende Nachweise erbringen, um zu demonstrieren, dass er die geltenden Anforderungen erfüllt hat, ohne sich einer formellen Einhaltungsvalidierung zu unterziehen. Zum Beispiel kann der TPSP dem Gutachter der Entität spezifische Nachweise vorlegen, damit der Gutachter bestätigen kann, dass die geltenden Anforderungen erfüllt sind. Alternativ kann sich der TPSP für mehrere Beurteilungen auf Abruf durch jeden der Gutachter seiner Kunden entscheiden, wobei jede Beurteilung darauf abzielt, zu bestätigen, dass die geltenden Anforderungen erfüllt sind. TPSPs sollten ihren Kunden ausreichende Nachweise vorlegen, um zu verifizieren, dass der Geltungsbereich der PCI-DSS-Bewertung des TPSP die für den Kunden geltenden Dienstleistungen umfasst und dass die relevanten PCI-DSS-Anforderungen untersucht wurden und festgestellt wurde, dass sie vorhanden sind. *(Fortsetzung auf der nächsten Seite)*
Zielsetzung des kundenspezifischen Ansatzes		
TPSPs stellen bei Bedarf Informationen bereit, um die Bemühungen ihrer Kunden zur PCI DSS-Einhaltung zu unterstützen.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist.		

Anforderungen und Testprozeduren		Anleitungen
		TPSPs können ihre PCI DSS-Verantwortlichkeiten so definieren, dass sie für alle ihre Kunden gleich sind; andernfalls sollte diese Verantwortung zwischen dem Kunden und TPSP vereinbart werden. Es ist wichtig, dass der Kunde versteht, welche PCI DSS-Anforderungen und Unteranforderungen seine TPSPs erfüllen, welche Anforderungen zwischen dem TPSP und dem Kunden gemeinsam genutzt werden und für diejenigen, die gemeinsam genutzt werden, Angaben darüber machen, wie die Anforderungen gemeinsam genutzt werden und welche Entität für die Erfüllung jeder Unteranforderung verantwortlich ist. Ein Beispiel für die Dokumentation dieser Verantwortlichkeiten ist eine Matrix, die alle anwendbaren PCI DSS-Anforderungen identifiziert und angibt, ob der Kunde oder TPSP für die Erfüllung dieser Anforderung verantwortlich ist oder ob es sich um eine gemeinsame Verantwortung handelt. **Weitere Informationen** Weitere Anleitungen finden Sie unter: • PCI DSS-Abschnitt: Verwendung von Drittanbietern von Dienstleistungen. • Informationsergänzung: Sicherheitsgarantie von Drittanbietern (schließt eine Muster-Verantwortungsmatrix-Vorlage ein.

Anforderungen und Testprozeduren		Anleitungen
12.10 Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf die CDE auswirken könnten, wird umgehend reagiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ohne einen umfassenden Vorfallsreaktionsplan, der ordnungsgemäß verbreitet, gelesen und von den verantwortlichen Parteien verstanden wird, könnten Verwirrung und das Fehlen einer einheitlichen Reaktion zu weiteren Ausfallzeiten für das Unternehmen, unnötiger öffentlicher Medienpräsenz sowie finanziellen und/oder Reputationsverlust und gesetzliche Haftung führen. **Gute Praxis** Der Vorfallsreaktionsplan sollte gründlich sein und alle wichtigen Elemente für die Beteiligten (zum Beispiel Recht, Kommunikation) enthalten, damit die Entität im Falle einer Verletzung, die sich auf Kontodaten auswirken könnte, effektiv reagieren kann. Es ist wichtig, den Plan mit den aktuellen Kontaktinformationen aller Personen auf dem neuesten Stand zu halten, die für die Reaktion auf Vorfälle zuständig sind. Weitere relevante Parteien für Benachrichtigungen können Kunden, Finanzinstitute (Erwerber and Herausgeber), und Geschäftspartner sein. Entitäten sollten überlegen, wie sie in ihren Vorfallsreaktionsplänen alle Datenkompromittierungen innerhalb der ZDE adressieren, einschließlich Kontodaten, drahtlose Verschlüsselungsschlüssel, Verschlüsselungsschlüssel, die für die Übertragung und Speicherung von Kontodaten oder Karteninhaberdaten verwendet werden, usw. **Beispiele** Gesetzliche Anforderungen für die Meldung von Kompromittierungen beinhalten diejenigen in den meisten US-Bundesstaaten, *(Fortsetzung auf der nächsten Seite)*
12.10.1 Ein Vorfallreaktionsplan ist vorhanden und kann im Falle eines vermuteten oder bestätigten Sicherheitsvorfalls aktiviert werden. Der Plan umfasst, ist aber nicht beschränkt, Folgendes: • Rollen, Verantwortlichkeiten, und Kommunikations- und Kontaktstrategien im Falle eines vermuteten oder bestätigten Sicherheitsvorfalls, mindestens einschließlich der Benachrichtigung von Zahlungsmarken und Erwerbern. • Vorfallreaktionsprozeduren mit spezifischen Eindämmungs- und Minderungsaktivitäten für verschiedene Arten von Vorfällen. • Prozeduren zur Wiederherstellung und Kontinuität des Geschäftsbetriebs. • Daten-Backup-Prozesse. • Analyse der gesetzlichen Anforderungen zur Meldung von Kompromittierungen. • Abdeckungen und Reaktionen aller kritischen Systemkomponenten. • Referenz auf oder Einschluss von Vorfallreaktionsprozeduren von den Zahlungsmarken.	**12.10.1.a** Den Vorfallreaktionsplan untersuchen, um zu verifizieren, dass der Plan existiert und mindestens die in dieser Anforderung angegebenen Elemente enthält.	
	12.10.1.b Das Personal befragen und die Dokumentation von zuvor gemeldeten Vorfällen oder Warnungen untersuchen, um zu verifizieren, dass der dokumentierte Vorfallsreaktionsplan und die Prozeduren befolgt wurden.	
Zielsetzung des kundenspezifischen Ansatzes		
Ein umfassender Plan zur Reaktion auf Vorfälle wird gepflegt, der den Erwartungen der Kartenmarke entspricht.		

Anforderungen und Testprozeduren		Anleitungen
		die EU-Datenschutz-Grundverordnung (DSGVO) und das Gesetz zum Schutz personenbezogener Daten (Singapur). **Weitere Informationen** Weitere Informationen finden Sie unter *NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide*.
Definierte Ansatzanforderungen **12.10.2** Mindestens einmal alle 12 Monate wird der Reaktionsplan für Sicherheitsvorfälle: • Überprüft und der Inhalt wird bei Bedarf aktualisiert. • Getestet, einschließlich aller in Anforderung 12.10.1 aufgeführten Elemente. **Zielsetzung des kundenspezifischen Ansatzes** Der Vorfallsreaktionsplan wird regelmäßig aktualisiert und getestet.	**Testprozeduren mit definiertem Ansatz** **12.10.2** Das Personal befragen und die Dokumentation überprüfen, um zu verifizieren, dass der Sicherheits-Vorfallsreaktionsplan einmal alle 12 Monate: • Überprüft und nach Bedarf aktualisiert wird. • Getestet, einschließlich aller in Anforderung 12.10.1 aufgeführten Elemente.	**Zweck** Durch ordnungsgemäßes Testen des Sicherheits-Vorfallsreaktionsplans können fehlerhafte Geschäftsprozesse identifiziert werden und es kann sichergestellt werden, dass wichtige Schritte nicht ausgelassen werden, was zu einer erhöhten Exposition während eines Vorfalls führen könnte. Das regelmäßige Testen des Plans stellt sicher, dass die Prozesse funktionsfähig bleiben, und stellt auch sicher, dass das gesamte Personal in der Organisation mit dem Plan vertraut ist. **Gute Praxis** Der Test des Vorfallsreaktionsplans kann simulierte Vorfälle und die entsprechenden Reaktionen in Form einer „Tischtop-Übung“ umfassen, die die Teilnahme von relevantem Personal einschließt. Eine Überprüfung des Vorfalls und der Qualität der Reaktion kann Entitäten die Gewissheit geben, dass alle erforderlichen Elemente im Plan enthalten sind.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ein Vorfall könnte jederzeit auftreten, wenn daher eine Person, die in der Vorfallreaktion geschult und mit dem Plan der Entität vertraut ist, zur Verfügung steht, wenn ein Vorfall erkannt wird, erhöht sich die Fähigkeit der Entität, korrekt auf die Vorfälle zu reagieren. **Gute Praxis** Häufig wird bestimmtes Personal als Teil eines Sicherheits-Vorfallsreaktionsteams bestimmt, wobei das Team die Gesamtverantwortung für die Reaktion auf Vorfälle (möglicherweise nach einem rotierenden Zeitplan) und die Verwaltung dieser Vorfälle gemäß dem Plan trägt. Das Vorfallsreaktionsteam kann aus fest zugewiesenen Kernmitgliedern oder „auf Anfrage“-Personal bestehen, das je nach Fachwissen und den Besonderheiten des Vorfalls bei Bedarf hinzugezogen werden kann. Die Verfügbarkeit von Ressourcen für eine schnelle Reaktion auf Vorfälle minimiert die Unterbrechung des Unternehmens. Beispiele für Arten von Aktivitäten, auf die das Team oder Einzelpersonen reagieren sollten, umfassen alle Beweise für nicht autorisierte Aktivität, die Erkennung nicht autorisierter drahtloser Zugriffspunkte, kritische IDS-Warnungen und Berichte über nicht autorisierte Änderungen an kritischen Systemen oder Inhaltsdateien.
12.10.3 Bestimmtes Personal steht rund um die Uhr zur Verfügung, um auf vermutete oder bestätigte Sicherheitsvorfälle zu reagieren.	**12.10.3** Die Dokumentation untersuchen und verantwortliches Personal, das bestimmte Rollen einnimmt, befragen, um zu verifizieren, dass bestimmtes Personal rund um die Uhr verfügbar ist, um auf Sicherheitsvorfälle zu reagieren.	
Zielsetzung des kundenspezifischen Ansatzes		
Auf Vorfälle wird gegebenenfalls sofort reagiert.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen **12.10.4** Das Personal, das für die Reaktion auf vermutete und bestätigte Sicherheitsvorfälle verantwortlich ist, wird angemessen und regelmäßig in ihren Verantwortlichkeiten für Vorfallsreaktion geschult. **Zielsetzung des kundenspezifischen Ansatzes** Das Personal kennt seine Rolle und Verantwortlichkeiten bei der Vorfallsreaktion und kann bei Bedarf auf Unterstützung und Anleitungen zugreifen.	**Testprozeduren mit definiertem Ansatz** **12.10.4** Schulungsdokumentation untersuchen und das Vorfall-Reaktionspersonal befragen, um zu verifizieren, dass das Personal angemessen und regelmäßig in seinen Verantwortlichkeiten für die Vorfallsreaktion geschult wird.	**Zweck** Ohne ein geschultes und schnell verfügbares Vorfallsreaktionsteam könnten ausgedehnte Schäden am Netzwerk auftreten und kritische Daten und Systeme können durch unsachgemäßen Umgang mit den Zielsystemen „verseucht“ werden. Dies kann den Erfolg einer Untersuchung nach dem Vorfall behindern. **Gute Praxis** Es ist wichtig, dass alle an der Vorfallsreaktion beteiligten Personen in der Verwaltung von Beweismaterial für Forensik und Untersuchungen ind und sich damit auskennen.
Definierte Ansatzanforderungen **12.10.4.1** Die Häufigkeit der regelmäßigen Schulungen für das Personal zur Vorfallsreaktion ist in der gezielten Risikoanalyse der Entität definiert, die gemäß allen in Anforderung 12.3,1 angegebenen Elementen durchgeführt wird. **Zielsetzung des kundenspezifischen Ansatzes** Das Vorfallsreaktionspersonal wird in einer Häufigkeit geschult, die das Risiko der Entität adressiert. **Hinweise zur Anwendbarkeit** *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**Testprozeduren mit definiertem Ansatz** **12.10.4.1.a** Die gezielte Risikoanalyse der Entität auf die Häufigkeit von Schulungen für Vorfallsreaktionspersonal untersuchen, um zu verifizieren, dass die Risikoanalyse gemäß allen in Anforderung 12.3.1 angegebenen Elementen durchgeführt wurde. **12.10.4.1.b** Dokumentierte Ergebnisse der regelmäßigen Schulungen von Vorfallsreaktionspersonal untersuchen und das Personal befragen, um zu verifizieren, dass Schulungen in der Häufigkeit durchgeführt werden, die in der für diese Anforderung durchgeführten gezielten Risikoanalyse der Entität angegeben ist.	**Zweck** Die Umgebung und der Vorfallsreaktionsplan jeder Entität sind unterschiedlich und der Ansatz hängt von einer Reihe von Faktoren ab, einschließlich der Größe und Komplexität der Entität, dem Grad der Änderung der Umgebung, der Größe des Vorfallsreaktionsteams und der Personalfluktuation Die Durchführung einer Risikoanalyse wird es der Entität gestatten, die optimale Häufigkeit für die Schulung von Personal mit Verantwortlichkeiten für die Vorfallsreaktion zu bestimmen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
12.10.5 Der Sicherheits-Vorfallsreaktionsplan umfasst die Überwachung und Reaktion auf Warnungen von Sicherheitsüberwachungssystemen, einschließlich, aber nicht beschränkt auf: • Eindringungs-Erkennungs- und Eindringungs-Verhinderungs-Systeme. • Netzwerksicherheitskontrollen • Änderungserkennungsmechanismen für kritische Dateien. • Den Änderungs- und Manipulationserkennungsmechanismus für Zahlungsseiten. *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens eine bewährte Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.* • Erkennung von nicht autorisierten drahtlosen Zugriffspunkte.	**12.10.5** Die Dokumentation untersuchen und Vorfallsreaktionsprozesse beobachten, um zu verifizieren, dass die Überwachung und Reaktion auf Warnungen von Sicherheitsüberwachungssystemen im Sicherheits-Vorfallreaktionsplan abgedeckt sind, einschließlich, aber nicht beschränkt auf die in dieser Anforderung angegebenen Systeme.	Die Reaktion auf Warnungen, die von Sicherheitsüberwachungssystemen generiert werden, die ausdrücklich darauf ausgelegt sind, sich auf potenzielle Risiken für Daten zu konzentrieren, ist kritisch, um einen Verstoß zu verhindern, und muss daher in die Vorfallsreaktionsprozesse aufgenommen werden.
Zielsetzung des kundenspezifischen Ansatzes		
Auf Warnungen, die von Überwachungs- und Erkennungstechnologien generiert werden, wird strukturiert und wiederholbar reagiert.		
Hinweise zur Anwendbarkeit		
Der obige Aufzählungspunkt (für die Überwachung und Reaktion auf Warnungen von einem Änderungs- und Manipulationserkennungsmechanismus für Zahlungsseiten) ist eine bewährte Praktik bis zum 31. März 2025, danach ist er als Teil von Anforderung 12.10.5 erforderlich und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Einbeziehung von gewonnenen Erkenntnissen in den Vorfallsreaktionsplan nach Auftreten eines Vorfalls und die Berücksichtigung von Branchenentwicklungen hilft dabei, den Plan auf dem neuesten Stand zu halten und auf aufkommende Bedrohungen und Sicherheitstrends reagieren zu können. **Gute Praxis** Die gewonnene Erkenntnisse-Übung sollte alle Ebenen des Personals einbeziehen. Obwohl sie oft Teil der Überprüfung des gesamten Vorfalls ist, sollte sie sich darauf konzentrieren, wie die Reaktion der Entität auf den Vorfall verbessert werden könnte. Es ist wichtig, nicht nur Elemente der Reaktion zu berücksichtigen, die nicht die geplanten Ergebnisse hatten, sondern auch zu verstehen, was gut funktioniert hat und ob Erkenntnisse aus diesen Elementen, die gut funktioniert haben, auf Bereiche des Plans angewendet werden können, die dies nicht getan haben. Eine weitere Möglichkeit zur Optimierung des Vorfallsreaktionsplans einer Entität besteht darin, die Angriffe auf andere Organisationen zu verstehen und diese Informationen zur Feinabstimmung der Erkennungs-, Eindämmungs-, Minderungs- oder Wiederherstellungsverfahren der Entität zu verwenden.
12.10.6 Der Sicherheits-Vorfallsreaktionsplan wird gemäß den gewonnenen Erkenntnissen und zur Einbeziehung von Branchenentwicklungen geändert und weiterentwickelt.	**12.10.6.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, um den Reaktionsplan für Sicherheitsvorfälle gemäß den gewonnenen Erkenntnissen zu ändern und weiterzuentwickeln und Branchenentwicklungen einzubeziehen.	
	12.10.6.b Den Sicherheits-Vorfallsreaktionsplan untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass der Sicherheits-Vorfallsreaktionsplan gemäß den gewonnenen Erkenntnissen und zur Einbeziehung von Branchenentwicklungen geändert und weiterentwickelt wird.	
Zielsetzung des kundenspezifischen Ansatzes		
Die Wirksamkeit und Genauigkeit des Vorfallsreaktionsplans wird nach jedem Aufruf überprüft und aktualisiert.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Dokumentieren von Vorfällen-Reaktionsverfahren, die befolgt werden, falls gespeichertes PAN irgendwo gefunden wird, wo es nicht erwartet wird, hilft dabei, die notwendigen Behebungsaktionen zu identifizieren und zukünftige Lecks zu verhindern. **Gute Praxis** Wenn PAN außerhalb der CDE gefunden wurde, sollte eine Analyse durchgeführt werden, um 1) festzustellen, ob es unabhängig von anderen Daten oder mit sensiblen Authentifizierungsdaten gespeichert wurde, 2) die Quelle der Daten zu identifizieren und 3) die Kontrolllücken zu identifizieren, die dazu führten, dass die Daten außerhalb der CDE lagen. Entitäten sollten betrachten, ob Faktoren wie Geschäftsprozesse, Benutzerverhalten, falsche Systemkonfigurationen usw. dazu beigetragen haben, dass die PAN an einem unerwarteten Ort gespeichert wurde. Wenn solche beitragenden Faktoren vorhanden sind, sollten sie gemäß dieser Anforderung adressiert werden, um ein erneutes Auftreten zu verhindern.
12.10.7 Es sind Vorfallsreaktionsprozeduren vorhanden, die beim Nachweis von gespeicherter PAN an einem Ort eingeleitet werden, an dem dies nicht zu erwarten ist, und umfassen: • Bestimmen, was zu tun ist, wenn PAN außerhalb der CDE entdeckt wird, einschließlich ihres Abrufs, sicheren Löschens und/oder Migration in die aktuell definierte CDE, soweit zutreffend. • Identifizieren, ob sensible Authentifizierungsdaten mit PAN gespeichert sind. • Bestimmen, woher die Kontodaten stammten und wie sie dort gelandet sind, wo es nicht erwartet wurde. • Beheben von Datenlecks oder Prozesslücken, die dazu führten, dass die Kontodaten dort waren, wo es nicht erwartet wurde.	**12.10.7.a** Dokumentierte Vorfallsreaktionsprozeduren untersuchen, um zu verifizieren, dass Prozeduren für die Reaktion auf die Erkennung gespeicherter PAN an Orten, an denen nicht erwartet wird, dass sie vorhanden sind, bereit sind, eingeleitet zu werden, und alle in dieser Anforderung angegebenen Elemente enthalten.	
Zielsetzung des kundenspezifischen Ansatzes	**12.10.7.b** Personal befragen und Aufzeichnungen von Reaktionsaktionen untersuchen, um zu verifizieren, dass Vorfallsreaktionsprozeduren durchgeführt werden, wenn gespeicherte PAN überall dort entdeckt werden, wo es nicht zu erwarten ist.	
Es sind Prozesse vorhanden, um auf Situationen schnell zu reagieren, sie zu analysieren und sie zu adressieren, falls Klartext-PANs erkannt werden, wo dies nicht erwartet wird.		
Hinweise zur Anwendbarkeit		
Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.		

Anhang A Zusätzliche PCI DSS-Anforderungen

Diese Anhang enthält zusätzliche PCI DSS-Anforderungen für verschiedene Arten von Entitäten Die Abschnitte in diesem Anhang beinhalten:

- Anhang A1: Zusätzliche PCI DSS-Anforderungen für Multi-Mandanten-Dienstleistungsanbieter
- Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Entitäten, die SSL/Early TLS für Karte anwesend POS-POI-Terminalverbindungen verwenden.
- Anhang A3: Ergänzende Validierung für bestimmte Entitäten (DESV)

Anleitungen und Anwendbarkeitsinformationen werden in jedem Abschnitt bereitgestellt.

Anhang A1: Zusätzliche PCI DSS-Anforderungen für Multi-Mandanten-Dienstleistungsanbieter

Abschnitte
A1.1 Multi-Mandanten-Dienstleistungsanbieter schützen und trennen alle Kundenumgebungen und Daten.
A1.2 Multi-Mandanten-Dienstleistungsanbieter erleichtern die Protokollierung und die Vorfallsreaktion für alle Kunden.

Übersicht

Alle Dienstleistungsanbieter sind dafür verantwortlich, die PCI DSS-Anforderungen für ihre eigenen Umgebungen zu erfüllen, die für die ihren Kunden angebotenen Dienstleistungen gelten. Darüber hinaus müssen Multi-Mandanten-Dienstleistungsanbieter die Anforderungen in diesem Anhang erfüllen.

Multi-Mandanten-Dienstleistungsanbieter sind eine Art von Dienstleistungsanbietern, die stellen Händlern und anderen Dienstleistungsanbietern verschiedene gemeinsam genutzte Dienstleistungen bereit, wo Kunden Systemressourcen teilen (wie physische oder virtuelle Server), Infrastruktur, Anwendungen (einschließlich Software als eine Dienstleistung (SaaS)), und/oder Datenbanken. Die Dienstleistungen können das Hosten mehrerer Entitäten auf einem einzigen gemeinsam genutzten Server, das Bereitstellen von E-Commerce- und/oder „Einkaufswagen"-Dienstleistungen, webbasierten Hosting-Dienstleistungen, Zahlungsanwendungen, verschiedenen Cloud-Anwendungen und -Dienstleistungen sowie Verbindungen zu Zahlungsgateways und –prozessoren einschließen, sind aber nicht beschränkt darauf.

Dienstleistungsanbieter, die nur gemeinsam genutzte Rechenzentrumsdienstleistungen anbieten (häufig als Co-Standort- oder „Co-Lo"-Anbieter bezeichnet), bei denen Ausrüstung, Platz und Bandbreite auf Mietbasis verfügbar sind, gelten in diesem Sinne dieses Anhangs nicht als Multi-Mandanten-Dienstleistungsanbieter.

Hinweis: Auch wenn ein Multi-Mandanten-Dienstleistungsanbieter diese Anforderungen erfüllen kann, ist jeder Kunde dennoch dafür verantwortlich, die für seine Umgebung geltenden PCI DSS-Anforderungen einzuhalten und die Einhaltung gegebenenfalls zu validieren. Häufig gibt es PCI DSS-Anforderungen, für die der Anbieter und der Kunde (für vielleicht verschiedene Aspekte der Umgebung) die Verantwortung teilen. Die Anforderungen 12.8 und 12.9 beschreiben spezifische Anforderungen an die Beziehungen zwischen allen dritten Dienstleistungsanbieter (TPSPs) und ihren Kunden sowie die Verantwortlichkeiten beider. Dieses beinhaltet die Definition der spezifischen Dienstleistungen, die der Kunde erhält, zusammen mit den PCI DSS-Anforderungen, für deren Erfüllung der Kunde verantwortlich ist, welche in der Verantwortung des TPSP liegen und welche Anforderungen zwischen dem Kunden und dem TPSP geteilt werden.

Anforderungen und Testprozeduren		Anleitungen
A1.1 Multi-Mandanten-Dienstleistungsanbieter schützen und trennen alle Kundenumgebungen und Daten.		
Definierte Ansatzanforderungen **A1.1.1** Die logische Trennung wird wie folgt implementiert: • Der Anbieter kann ohne Autorisierung nicht auf die Umgebungen seiner Kunden zugreifen. • Kunden können ohne Autorisierung nicht auf die Umgebung des Anbieters zugreifen. **Zielsetzung des kundenspezifischen Ansatzes** Kunden können nicht auf die Umgebung des Anbieters zugreifen. Der Anbieter kann ohne Autorisierung nicht auf die Umgebungen seiner Kunden zugreifen. **Hinweise zur Anwendbarkeit** *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*	**Testprozeduren mit definiertem Ansatz** **A1.1.1** Die Dokumentation und System- und Netzwerkkonfigurationen untersuchen und das Personal befragen, um zu verifizieren, dass die logische Trennung gemäß allen in dieser Anforderung angegebenen Elementen implementiert wird.	**Zweck** Ohne Kontrollen zwischen der Anbieterumgebung und der Kundenumgebung könnte ein böswilliger Akteur innerhalb der Umgebung des Anbieters die Umgebung des Kunden kompromittieren, und ähnlich könnte ein böswilliger Akteur in einer Kundenumgebung den Anbieter und möglicherweise andere Kunden des Anbieters kompromittieren. Multi-Mandanten-Umgebungen sollten voneinander und von der Infrastruktur des Anbieters isoliert sein, sodass sie separat verwaltete Entitäten ohne Konnektivität zwischen ihnen sein können. **Gute Praxis** Anbieter sollten eine starke Trennung zwischen den Umgebungen sicherstellen, die für den Kundenzugriff konzipiert sind, zum Beispiel Konfigurations- und Abrechnungsportale, und der privaten Umgebung des Anbieters, auf die nur autorisiertes Personal des Anbieters zugreifen sollte. Der Zugriff des Dienstleistungsanbieters auf Kundenumgebungen wird gemäß Anforderung 8.2.3 durchgeführt. **Weitere Informationen** Siehe die *Informationsergänzung: PCI SSC Cloud-Berechnungs-Richtlinien* für weitere Anleitungen zu Cloud-Umgebungen.

<table>
<tr><th colspan="2">Anforderungen und Testprozeduren</th><th>Anleitungen</th></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="3">Zweck
Es ist wichtig, dass ein Multi-Mandanten-Dienstleistungsanbieter Kontrollen definiert, damit jeder Kunde nur auf seine eigene Umgebung und CDE zugreifen kann, um nicht autorisierten Zugriff von der Umgebung eines Kunden auf eine andere zu verhindern.
Beispiele
In einer Cloud-basierten Infrastruktur, wie ein Infrastruktur als Dienstleistung m (IaaS)-Angebot, kann die CDE des Kunden virtuelle Netzwerkgeräte und virtuelle Server enthalten, die von den Kunden konfiguriert und verwaltet werden, einschließlich Betriebssysteme, Dateien, Speicher usw.</td></tr>
<tr><td rowspan="2">A1.1.2 Kontrollen werden implementiert, sodass jeder Kunde nur die Erlaubnis hat, auf seine eigenen Karteninhaberdaten und CDE zuzugreifen.</td><td>A1.1.2.a Die Dokumentation untersuchen, um zu verifizieren, dass Kontrollen definiert werden, sodass jeder Kunde nur die Erlaubnis hat, auf seine eigenen Karteninhaberdaten und CDE zuzugreifen.</td></tr>
<tr><td>A1.1.2.b Systemkonfigurationen untersuchen, um zu verifizieren, dass Kunden Privilegien haben, die etabliert sind, um nur auf ihre eigenen Kontodaten und CDE zuzugreifen.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes
Kunden können nicht auf die Umgebungen anderer Kunden zugreifen.</td><td></td><td></td></tr>
<tr><td>Definierte Ansatzanforderungen</td><td>Testprozeduren mit definiertem Ansatz</td><td rowspan="3">Zweck
Um unbeabsichtigte oder absichtliche Auswirkungen auf die Umgebungen oder Kontodaten anderer Kunden zu verhindern, ist es wichtig, dass jeder Kunde nur auf die ihm zugeordneten Ressourcen zugreifen kann.</td></tr>
<tr><td>A1.1.3 Kontrollen werden implementiert, sodass jeder Kunde nur auf Ressourcen zugreifen kann, die ihm zugeordnet sind.</td><td>A1.1.3 Kundenprivilegien untersuchen, um zu verifizieren, dass jeder Kunde nur auf die ihm zugeordneten Ressourcen zugreifen kann.</td></tr>
<tr><td>Zielsetzung des kundenspezifischen Ansatzes
Kunden können Ressourcen, die anderen Kunden zugeordnet sind, nicht beeinflussen.</td><td></td></tr>
</table>

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
A1.1.4 Die Wirksamkeit von logischen Trennungskontrollen, die zur Trennung von Kundenumgebungen verwendet werden, wird mindestens einmal alle sechs Monate durch Penetrationstesten bestätigt.	**A1.1.4** Die Ergebnisse der jüngsten Penetrationstests untersuchen, um zu verifizieren, dass Testen die Wirksamkeit der logischen Trennungskontrollen bestätigt haben, die zur Trennung von Kundenumgebungen verwendet werden.	Multi-Mandanten-Dienstleistungsanbieter sind für die Verwaltung der Segmentierung zwischen ihren Kunden verantwortlich. Ohne technische Zusicherung, dass die Segmentierungskontrollen wirksam sind, ist es möglich, dass Änderungen an der Technologie des Dienstleistungsanbieters unbeabsichtigt eine Schwachstelle erstellen, die von allen Kunden des Dienstleistungsanbieters ausgenutzt werden könnte.
Zielsetzung des kundenspezifischen Ansatzes		**Gute Praxis**
Die Segmentierung von Kundenumgebungen aus anderen Umgebungen wird regelmäßig auf ihre Wirksamkeit validiert.		Die Wirksamkeit von Trennungstechniken kann bestätigt werden, indem von Dienstleistungsanbietern erstellte vorübergehende (Mock-up-)Umgebungen verwendet werden, die Kundenumgebungen darstellen, und versucht wird, 1) von einer anderen Umgebung auf eine vorübergehende Umgebung zuzugreifen und 2) über das Internet auf eine vorübergehende Umgebung zuzugreifen.
Hinweise zur Anwendbarkeit		
Das Testen einer angemessenen Trennung zwischen Kunden in einer Dienstleistungsanbieterumgebung mit mehreren Mandanten erfolgt zusätzlich zu den Penetrationstests, die in Anforderung 11.4.6 angegeben sind. *Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.*		

Anforderungen und Testprozeduren		Anleitungen
A1.2 Multi-Mandanten-Dienstleistungsanbieter erleichtern die Protokollierung und die Vorfallreaktion für alle Kunden.		
Definierte Ansatzanforderungen **A1.2.1** Audit-Protokoll-Fähigkeit wird für die Umgebung jedes Kunden aktiviert, die mit PCC DSS-Anforderung 10 konsistent ist, einschließlich: • Protokolle sind für gängige Anwendungen von Drittanbietern aktiviert. • Protokolle sind standardmäßig aktiv. • Protokolle sind nur für die Überprüfung durch den besitzenden Kunden verfügbar. • Protokollstandorte werden dem besitzenden Kunden klar kommuniziert. • Protokolldaten und -verfügbarkeit sind mit der PCI-DSS-Anforderung 10 konsistent. **Zielsetzung des kundenspezifischen Ansatzes** Die Protokollfähigkeit steht allen Kunden zur Verfügung, ohne dass die Vertraulichkeit anderer Kunden beeinträchtigt wird.	**Testprozeduren mit definiertem Ansatz** **A1.2.1** Die Dokumentation und Systemkonfigurationseinstellungen untersuchen, um zu verifizieren, dass der Anbieter die Audit-Protokollfähigkeit für jede Kundenumgebung gemäß allen in dieser Anforderung angegebenen Elementen aktiviert hat.	**Zweck** Protokollinformationen sind nützlich, um Sicherheitsvorfälle zu erkennen und zu beheben, und sind für forensische Untersuchungen von unschätzbarem Wert. Kunden müssen daher Zugriff auf diese Protokolle haben. Protokollinformationen können jedoch auch von einem Angreifer zur Aufklärung verwendet werden, sodass die Protokollinformationen eines Kunden nur für den Kunden zugänglich sein dürfen, auf den sich das Protokoll bezieht.
Definierte Ansatzanforderungen **A1.2.2** Prozesse oder Mechanismen werden implementiert, um sofortige forensische Untersuchungen im Falle eines vermuteten oder bestätigten Sicherheitsvorfalls für einen Kunden zu unterstützen und/oder zu erleichtern. **Zielsetzung des kundenspezifischen Ansatzes** Im Falle eines vermuteten oder bestätigten Sicherheitsvorfalls steht allen Kunden eine forensische Untersuchung zur Verfügung.	**Testprozeduren mit definiertem Ansatz** **A1.2.2** Dokumentierte Prozeduren untersuchen, um zu verifizieren, dass der Anbieter über Prozesse oder Mechanismen verfügt, um eine sofortige forensische Untersuchung zugehöriger Server im Falle eines vermuteten oder bestätigten Sicherheitsvorfalls für einen Kunden zu unterstützen und/oder zu erleichtern.	**Zweck** Im Falle einer vermuteten oder bestätigten Verletzung der Vertraulichkeit von Karteninhaberdaten versucht der forensische Ermittler eines Kunden, die Ursache der Verletzung zu finden, den Angreifer aus der Umgebung auszuschließen und sicherzustellen, dass alle nicht autorisierten Zugriffe entfernt werden. Schnelle und effiziente Antworten auf Anfragen forensischer Ermittler können die Zeit, die der Ermittler benötigt, um die Umgebung des Kunden zu sichern, erheblich verkürzen.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
A1.2.3 Prozesse oder Mechanismen sind implementiert, um vermutete oder bestätigte Sicherheitsvorfälle und Schwachstellen zu melden und zu adressieren, einschließlich: • Kunden können Sicherheitsvorfälle und Schwachstellen an den Anbieter sicher melden. • Der Anbieter adressiert und behebt vermutete oder bestätigte Sicherheitsvorfälle und Schwachstellen gemäß Anforderung 6.3.1.	**A1.2.3** Dokumentierte Prozeduren untersuchen und das Personal befragen, um zu verifizieren, dass der Anbieter über einen Mechanismus zum Melden und Adressieren vermuteter oder bestätigter Sicherheitsvorfälle und Schwachstellen gemäß allen in dieser Anforderung angegebenen Elementen verfügt.	Sicherheitsschwachstellen in den bereitgestellten Dienstleistungen können die Sicherheit aller Kunden des Dienstleistungsanbieters beeinträchtigen und müssen daher gemäß den etablierten Prozessen des Dienstleistungsanbieters verwaltet werden, wobei der Behebung von Schwachstellen mit der höchsten Wahrscheinlichkeit eines Kompromisses Priorität eingeräumt wird. Kunden werden bei der Verwendung der Dienstleistung wahrscheinlich Schwachstellen und Sicherheitsfehlkonfigurationen bemerken. Die Implementierung sicherer Methoden für Kunden, um von Sicherheitsvorfälle und Schwachstellen zu melden, ermutigt Kunden, potenzielle Probleme zu melden, und versetzt den Anbieter in die Lage, potenzielle Probleme in ihrer Umgebung schnell zu erkennen und zu beheben.
Zielsetzung des kundenspezifischen Ansatzes		
Vermutete oder bestätigte Sicherheitsvorfälle oder Schwachstellen werden entdeckt und adressiert. Kunden werden gegebenenfalls informiert.		
Hinweise zur Anwendbarkeit		
Diese Anforderung ist bis zum 31. März 2025 eine bewährte Praktik, danach wird sie benötigt und muss bei einer PCI DSS-Bewertung vollständig berücksichtigt werden.		

Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Entitäten, die SSL/Early TLS für Karte Anwesend POS-POI-Terminalverbindungen Verwenden

Abschnitte
A2.1 POI-Terminals, die SSL und/oder frühe Versionen von TLS verwenden, sind bestätigt, für bekannte SSL/TLS-Ausnutzungen nicht anfällig zu sein.

Übersicht

Dieser Anhang gilt nur für Entitäten, die SSL/frühes TLS als Sicherheitskontrolle zum Schutz von POS-POI-Terminals verwenden, einschließlich Dienstleistungsanbietern, die Verbindungen zu POS-POI-Terminals bereitstellen.

Entitäten, die SSL und frühes TLS für POS-POI-Terminalverbindungen verwenden, müssen so schnell wie möglich auf eine Aktualisierung auf ein starkes kryptografisches Protokoll hinarbeiten. Zusätzlich dürfen SSL und/oder frühes TLS nicht in Umgebungen eingeführt werden, in denen diese Protokolle nicht bereits vorhanden sind. Zum Zeitpunkt der Veröffentlichung ist es schwierig, die bekannten Sicherheitsschwachstellen in POS-POI-Zahlungsterminals auszunutzen. Es können jedoch jederzeit neue Schwachstellen auftauchen, und es liegt an der Organisation, sich über Schwachstellentrends auf dem Laufenden zu halten und festzustellen, ob sie gegenüber bekannte Ausnutzungen anfällig sind.

Die direkt betroffenen PCI DSS-Anforderungen sind:

- **Anforderung 2.2.5**: Wenn irgendwelche unsicheren Dienstleistungen, Protokolle oder Dämonen vorhanden sind, wird die geschäftliche Rechtfertigung wird dokumentiert, und zusätzliche Sicherheitsfunktionen werden dokumentiert und implementiert, die das Risiko der Verwendung von unsicheren Dienstleistungen, Protokollen oder Dämonen reduzieren.
- **Anforderung 2.2.7**: Alle administrativen Nicht-Konsolen-Zugriffe werden mit Verwendung von starker Kryptographie verschlüsselt.
- **Anforderung 4.2.1**: Starke Kryptographie- und Sicherheitsprotokolle werden implementiert, um PAN während der Übertragung über offene, öffentliche Netzwerke zu schützen:

SSL und frühe TLS dürfen nicht als Sicherheitskontrolle verwendet werden, um diese Anforderungen zu erfüllen, außer im Fall von POS-POI-Terminalverbindungen, wie in diesem Anhang detailliert. Um Entitäten zu unterstützen, die an der Migration von SSL/frühen TLS auf POS-POI-Terminals arbeiten, sind die folgenden Bestimmungen enthalten:

- Neue Implementierungen von POS-POI-Terminals dürfen kein SSL oder frühes TLS als Sicherheitskontrolle verwenden.
- Alle Anbieter von POS-POI-Terminaldienstleistungen müssen ein sicheres Dienstleistungsangebot bereitstellen.
- Dienstleistungsanbieter, die bestehende Implementierungen von POS-POI-Terminals unterstützen, die SSL und/oder frühe Versionen von TLS verwenden, müssen über einen formalen Risikominderungs- und Migrationsplan verfügen.
- POS-POI-Terminals in Umgebungen mit vorhandener Karte, die nachweislich nicht anfällig für bekannte Ausnutzungen von SSL und frühes TLS sind, **und die SSL/TLS-Terminalpunkte, mit denen sie verbunden sind**, können SSL/frühes TLS weiterhin als Sicherheitskontrolle verwenden.

Anforderungen in diesem Anhang sind für den kundenspezifischen Ansatz nicht geeignet.

Anforderungen und Testprozeduren		Anleitungen
A2.1 POI-Terminals, die SSL und/oder frühe Versionen von TLS verwenden, sind bestätigt, für bekannte SSL/TLS-Ausnutzungen nicht anfällig zu sein.		
Definierte Ansatzanforderungen **A2.1.1** Wenn POS-POI-Terminals am Händler- oder Zahlungsakzeptanzstandort SSL und/oder frühes TLS verwenden, bestätigt die Entität, dass die Geräte für bekannte Ausnutzung für diese Protokolle nicht anfällig sind. **Zielsetzung des kundenspezifischen Ansatzes** Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet. **Hinweise zur Anwendbarkeit** Diese Anforderung soll für die Entität mit dem POS-POI-Terminal gelten, wie einen Händler. Diese Anforderung gilt nicht für Dienstleistungsanbieter, die als Terminierungs- oder Verbindungspunkt zu diesen POS-POI-Terminals dienen. Die Anforderungen A2.1.2 und A2.1.3 gelten für POS-POI-Dienstleistungsanbieter. Die Zulassung von POS-POI-Terminals, die derzeit nicht gegenüber Ausnutzungen anfällig sind, basiert auf den derzeit bekannten Risiken. Wenn neue Ausnutzungen eingeführt werden, für die POS-POI-Terminals anfällig sind, müssen die POS-POI-Terminals sofort aktualisiert werden.	**Testprozeduren mit definiertem Ansatz** **A2.1.1** Für POS-POI-Terminals, die SSL und/oder frühes TLS verwenden, bestätigen, dass die Entität über eine Dokumentation verfügt (zum Beispiel Anbieterdokumentation, System-/Netzwerkkonfigurationsdetails), die verifiziert, dass die Geräte gegenüber bekannten Ausnutzungen für SSL/frühes TLS nicht anfällig sind.	**Zweck** POS-POI-Terminals, die in Umgebungen mit vorhandener Karte verwendet werden, können weiterhin SSL/frühes TLS verwenden, wenn gezeigt werden kann, dass das POS-POI-Terminal für die derzeit bekannten Ausnutzungen nicht anfällig ist. **Gute Praxis** SSL ist jedoch eine veraltete Technologie und könnte in Zukunft gegenüber zusätzlichen Sicherheitsschwachstellen anfällig sein; es wird daher dringend empfohlen, POS-POI-Terminals so schnell wie möglich auf ein sicheres Protokoll zu aktualisieren. Wenn SSL/frühes TLS in der Umgebung nicht benötigt wird, sollten die Verwendung und der Rückfall auf diese Versionen deaktiviert werden. **Weitere Informationen** Weitere Anleitungen finden Sie in den aktuellen PCI SSC-Informationsergänzungen zu SSL/frühes TLS.

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** POS-POI-Terminierungspunkte, einschließlich, aber nicht beschränkt auf Dienstleistungsanbieter wie Erwerber oder Erwerber-Prozessoren, können weiterhin SSL/frühes TLS verwenden, wenn gezeigt werden kann, dass der Dienstleistungsanbieter über Kontrollen verfügt, die das Risiko der Unterstützung dieser Verbindungen für die Umgebung des Dienstleistungsanbieters mindern. **Gute Praxis** Dienstleistungsanbieter sollten alle Kunden, die SSL/frühes TLS verwenden, über die mit seiner Verwendung verbundenen Risiken und die Notwendigkeit der Migration auf ein sicheres Protokoll informieren. **Definitionen** Der Risikominderungs- und Migrationsplan ist ein von der Entität erstelltes Dokument, das ihre Pläne für die Migration zu einem sicheren Protokoll beschreibt und die Kontrollen beschreibt, die die Entität eingerichtet hat, um das mit SSL/frühen TLS verbundene Risiko zu reduzieren, bis die Migration abgeschlossen ist. **Weitere Informationen** Weitere Anleitungen zu Risikominderungs- und Migrationsplänen finden Sie in den aktuellen PCI SSC-Informationsergänzungen zu SSL/frühe TLS.
A2.1.2 Zusätzliche *Anforderung nur für Dienstleistungsanbieter:* Alle Dienstleistungsanbieter mit bestehenden Verbindungspunkten zu POS-POI-Terminals, die SSL und/oder frühes TLS verwenden, wie in A2.1 definiert, verfügen über einen formellen Risikominderungs- und Migrationsplan, der Folgendes umfasst: • Beschreibung der Nutzung, einschließlich welche Daten übertragenden werden, Arten und Anzahl der Systeme, die SSL/frühes TLS verwenden und/oder unterstützen, und Art der Umgebung. • Ergebnisse der Risikobeurteilung und Kontrollen zur Risikominderung sind vorhanden. • Beschreibung der Prozesse, um neue Schwachstellen im Zusammenhang mit SSL/frühen TLS zu überwachen. • Beschreibung der Änderungskontrollprozesse, die implementiert werden, um sicherzustellen, dass SSL/frühes TLS nicht in neuen Umgebungen implementiert wird. • Übersicht über den Migrationsprojektplan, um SSL/frühes TLS zu einem späteren Zeitpunkt zu ersetzen.	**A2.1.2 Zusätzliche*Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Den dokumentierten Risikominderungs- und Migrationsplan überprüfen, um zu verifizieren, dass er alle in dieser Anforderung angegebenen Elemente enthält.	
Zielsetzung des kundenspezifischen Ansatzes Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		
Hinweise zur Anwendbarkeit Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Kunden müssen in der Lage sein, ihre POIs zu aktualisieren, um die Schwachstelle bei der Verwendung von SSL und frühen TLS zu beseitigen. In vielen Fällen müssen Kunden einen schrittweisen oder allmählichen Ansatz verfolgen, um ihren POS-POI-Bestand vom unsicheren Protokoll auf ein sicheres Protokoll zu migrieren, und verlangen daher vom Dienstleistungsanbieter, dass er ein sicheres Angebot unterstützt. **Weitere Informationen** Weitere Anleitungen finden Sie in den aktuellen PCI SSC-Informationsergänzungen zu SSL/frühes TLS.
A2.1.3 Zusätzliche *Anforderung* nur für Dienstleistungsanbieter: Alle Dienstleistungsanbieter stellen ein sicheres Dienstleistungsangebot bereit.	**A2.1.3 Zusätzliche *Testprozedur nur für Bewertungen von Dienstleistungsanbietern:*** Systemkonfigurationen und Begleitdokumentation untersuchen, um zu verifizieren, dass der Dienstleistungsanbieter eine sichere Protokolloption für seine Dienstleistung anbietet.	
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		
Hinweise zur Anwendbarkeit		
Diese Anforderung gilt nur, wenn die zu bewertende Entität ein Dienstleistungsanbieter ist.		

Anhang A3: Ergänzende Validierung für Bestimmte Entitäten (DESV)

Abschnitte
A3.1 Ein PCI DSS-Einhaltungsprogramm wird implementiert.
A3.2 Der PCI DSS-Geltungsbereich wird dokumentiert und validiert.
A3.3 PCI DSS ist in Geschäft wie gewohnt (BAU)PCI DSS (BAU)--Aktivitäten integriert.
A3.4 Der logische Zugriff auf die Karteninhaberdatenumgebung wird kontrolliert und verwaltet.
A3.5 Verdächtige Ereignisse werden identifiziert und es wird darauf reagiert.

Übersicht

Dieser Anhang gilt nur für Entitäten, die von Zahlungsmarke(n) oder Erwerbern als Erfordern einer zusätzlichen Validierung bestehender PCI-DSS-Anforderungen bezeichnet werden. Eine Entität muss sich NUR auf Anweisung eines Erwerbers oder einer Zahlungsmarke einer Bewertung gemäß diesem Anhang unterziehen. Beispiele von Entitäten, für die dieser Anhang gelten könnte, umfassen:

- Diejenigen, die große Mengen von Kontodaten speichern, verarbeiten und/oder übertragen,
- Diejenigen, die Aggregationspunkte für Kontodaten bereitstellen, oder
- Diejenigen, die erhebliche oder wiederholte Verletzungen von Kontodaten erlitten haben.

Zusätzlich können andere PCI-Standards auf die Vervollständigung dieses Anhangs verweisen.

Diese zusätzlichen Validierungsschritte sollen eine größere Sicherheit dafür bieten, dass die PCI DSS-Kontrollen effektiv und kontinuierlich aufrechterhalten werden, indem die Geschäft wie gewohnt-Prozesse (BAU) validiert und die Validierung und Scoping-Überlegungen verstärkt werden.

Hinweis: *Einige Anforderungen haben definierte Zeitrahmen (zum Beispiel mindestens einmal alle drei Monate oder mindestens einmal alle sechs Monate), innerhalb derer bestimmte Aktivitäten durchgeführt werden müssen. Für die anfängliche Bewertung dieses Dokuments ist es nicht erforderlich, dass für jeden dieser Zeitrahmen im Vorjahr eine Aktivität durchgeführt wurde, wenn der Bewerter Folgendes überprüft:*

- *Die Aktivität wurde gemäß den geltenden Anforderungen innerhalb des letzten Zeitrahmens (zum Beispiel der letzten Dreimonats- oder Sechsmonatsperiode) durchgeführt und*
- *Die Entität hat Richtlinien und Prozeduren für die Fortführung der Aktivität innerhalb des festgelegten Zeitrahmens dokumentiert.*

Für die folgenden Jahre nach der anfänglichen Bewertung muss innerhalb jedes erforderlichen Zeitrahmens eine Aktivität durchgeführt worden sein (zum Beispiel muss eine alle drei Monate erforderliche Aktivität mindestens viermal im Vorjahr in einem Abstand von nicht mehr als 90 Tagen durchgeführt worden sein).

Nicht alle Anforderungen in PCI DSS gelten für alle Entitäten, die einer PCI DSS-Bewertung unterzogen werden können. Aus diesem Grund werden einige PCI DSS-Anforderungen in diesem Anhang dupliziert. Alle Fragen zu diesem Anhang sollten an Erwerber oder Zahlungsmarken adressiert werden.

Anforderungen und Testprozeduren		Anleitungen
A3.1 Ein PCI DSS-Einhaltungsprogramm wird implementiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Zuweisung von PCI DSS-Einhaltungs-Verantwortlichkeiten durch die Geschäftsleitung gewährleistet die Transparenz des PCI DSS-Einhaltungs-Programms auf Führungsebene und bietet die Möglichkeit, geeignete Fragen zu stellen, um die Wirksamkeit des Programms zu bestimmen und strategische Prioritäten zu beeinflussen. **Gute Praxis** Die Geschäftsleitung kann C-Stufen-Positionen, Vorstände oder Ähnliches umfassen. Die spezifischen Titel hängen von der jeweiligen Organisationsstruktur ab. Die Verantwortung für das PCI DSS-Einhaltungs-Programm kann einzelnen Rollen und/oder Geschäftseinheiten innerhalb der Organisation zugewiesen werden.
A3.1.1 Die Geschäftsleitung trägt die Verantwortung für den Schutz der Kontendaten und ein PCI DSS-Einhaltungsprogramm, das Folgendes umfasst: • Gesamtverantwortlichkeit für die Wartung der PCI DSS-Einhaltung. • Definieren einer Charta für ein PCI DSS-Einhaltungs-Programm. • Bereitstellung von Aktualisierungen für die Geschäftsführung und den Vorstand über PCI DSS-Einhaltungs-Initiativen und -Probleme, einschließlich Abhilfemaßnahmen mindestens einmal alle 12 Monate. **PCI DSS-Referenz**: *Anforderung 12*	**A3.1.1.a** Die Dokumentation untersuchen, um zu verifizieren, dass die Geschäftsleitung Gesamtverantwortung für die Aufrechterhaltung der PCI DSS-Einhaltung der Entität zugewiesen hat. **A3.1.1.b** Die PCI DSS-Charta des Unternehmens untersuchen, um zu verifizieren, dass sie die Bedingungen, unter denen das PCI DSS-Einhaltungs-Programm organisiert wird, umreißt. **A3.1.1.c** Protokolle von Sitzungen der Geschäftsleitung und des Verwaltungsrats und/oder Präsentationen untersuchen, um zu verifizieren, dass PCI DSS-Einhaltungs-Initiativen und Behebungsmaßnahmen mindestens einmal alle 12 Monate kommuniziert werden.	
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ein formelles Einhaltungsprogramm ermöglicht es einer Organisation, die Gesundheit ihrer Sicherheitskontrollen zu überwachen, proaktiv zu handeln, wenn eine Kontrolle fehlschlägt, und Aktivitäten und den Einhaltungs-Status in der gesamten Organisation effektiv zu kommunizieren. **Gute Praxis** Das PCI DSS-Einhaltungs-Programm kann ein dediziertes Programm oder Teil eines übergreifenden Einhaltungs- und/oder Führungsprogramms sein und sollte eine klar definierte Methodik beinhalten, die eine konsistente und effektive Bewertung demonstriert. Strategische Geschäftsentscheidungen, die auf potenzielle PCI DSS-Auswirkungen analysiert werden sollten, können Fusionen und Übernahmen, neue Technologiekäufe oder neue Zahlungsakzeptanzkanäle umfassen. **Definitionen** Die Aufrechterhaltung und Überwachung der gesamten PCI DSS-Einhaltung einer Organisation umfasst die Identifizierung von Aktivitäten, die täglich, wöchentlich, monatlich, alle drei Monate oder jährlich durchgeführt werden sollen, und die Sicherstellung, dass diese Aktivitäten entsprechend durchgeführt werden (zum Beispiel unter Verwendung einer Sicherheitsselbstbewertung oder einer PDCA-Methodik). **Beispiele** Methodiken, die die Verwaltung von Einhaltungsprogrammen unterstützen, umfassen Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC und Six Sigma.
A3.1.2 Ein formelles PCI DSS-Einhaltungsprogramm ist vorhanden, das Folgendes umfasst: • Definition von Aktivitäten zur Aufrechterhaltung und Überwachung der allgemeinen PCI DSS-Einhaltung, einschließlich normale Geschäftsaktivitäten. • Jährliche PCI DSS-Beurteilungsprozesse. • Prozesse für die kontinuierliche Validierung der PCI DSS-Anforderungen (zum Beispiel täglich, wöchentlich, alle drei Monate, anwendbar je nach Anforderung). • Ein Prozess zur Durchführung von Business-Impact-Analysen, um potenzielle PCI DSS-Auswirkungen für strategische Geschäftsentscheidungen zu bestimmen. **PCI DSS-Referenz**: *Anforderungen 1-12*	**A3.1.2.a** Informations-Sicherheitsrichtlinien und -prozeduren untersuchen, um zu verifizieren, dass Prozesse für ein formelles PCI DSS-Einhaltungsprogramm definiert sind, die alle in dieser Anforderung angegebenen Elemente umfassen. **A3.1.2.b** Personal befragen und Einhaltungs-Aktivitäten beobachten, um zu verifizieren, dass ein formelles PCI DSS-Einhaltungsprogramm gemäß allen in dieser Anforderung angegebenen Elementen implementiert wird.	
Zielsetzung des kundenspezifischen Ansatzes Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die formale Definition spezifischer PCI DSS-Einhaltungsrollen und -Verantwortlichkeiten hilft dabei, die Rechenschaftspflicht und Überwachung laufender PCI DSS-Einhaltungs-Bemühungen sicherzustellen. **Gute Praxis** Das Eigentum sollte Personen zugewiesen werden, die Autorität haben, um risikobasierte Entscheidungen zu treffen, und denen die Verantwortung für die jeweilige Funktion obliegt. Pflichten sollten formal definiert werden, und Eigentümer sollten in der Lage sein, ein Verständnis für diese Verantwortlichkeiten und Rechenschaftspflicht aufzuweisen. Einhaltungsrollen können einem einzelnen Eigentümer oder mehreren Eigentümern für verschiedene Anforderungselemente zugewiesen werden.
A3.1.3 PCI DSS-Einhaltungsrollen und -Verantwortlichkeiten sind speziell definiert und einem oder mehreren Personal formell zugewiesen, einschließlich: • Verwalten von PCI DSS-Geschäft wie gewohnt-Aktivitäten. • Verwalten von jährlichen PCI DSS-Beurteilungen. • Verwalten von kontinuierlicher Validierung der PCI DSS-Anforderungen (zum Beispiel täglich, wöchentlich, alle drei Monate, anwendbar je nach Anforderung). • Verwalten von Business-Impact-Analysen, um potenzielle PCI DSS-Auswirkungen für strategische Geschäftsentscheidungen zu bestimmen. **PCI DSS-Referenz**: *Anforderung 12*	**A3.1.3.a** Informationssicherheitsrichtlinien und -prozeduren untersuchen und das Personal befragen, um zu verifizieren, dass die PCI DSS-Einhaltungs-Rollen und -Verantwortlichkeiten speziell definiert und einem oder mehreren Personal gemäß allen Elementen dieser Anforderung formell zugewiesen sind.	
	A3.1.3.b Verantwortliches Personal befragen und verifizieren, dass es mit seinem zugewiesenen PCI DSS-Einhaltungs-Verantwortlichkeiten ist sind und diese erfüllt.	
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Personal, das für PCI DSS-Einhaltung verantwortlich ist, hat einen spezifischen Schulungsbedarf, der über das hinausgeht, was normalerweise durch allgemeine Sicherheitsbewusstseinsschulungen bereitgestellt wird, um es ihm zu ermöglichen, seine Rolle zu erfüllen. **Gute Praxis** Personen mit PCI DSS-Einhaltungs-Verantwortlichkeiten sollten spezielle Schulungen erhalten, die sich zusätzlich zu einem allgemeinen Bewusstsein für Informationssicherheit auf bestimmte Sicherheitsthemen, Fähigkeiten, Prozesse oder Methodiken konzentrieren, die befolgt werden müssen, damit diese Personen ihre Einhaltungs-Verantwortlichkeiten effektiv erfüllen können. Schulungen können von Dritten wie PCI SSC (zum Beispiel PCI-Bewusstsein, PCIP und ISA), Zahlungsmarken und Erwerbern angeboten werden, oder Schulungen können intern sein. Die Schulungsinhalte sollten für die berufliche Funktion der Person anwendbar sein, aktuell sein und die neuesten Sicherheitsbedrohungen und/oder Versionen von PCI DSS enthalten. **Weitere Informationen** Für zusätzliche Anleitungen siehe *Informationsergänzung: Bewährte Praktiken für die Implementierung eines Sicherheitsbewusstsein-Programms*.
A3.1.4 Eine aktuelle PCI DSS- und/oder Informationssicherheitsschulung wird mindestens einmal alle 12 Monate für Personal mit Verantwortlichkeiten für PCI-DSS Einhaltung (wie in A3.1.3 identifiziert) bereitgestellt. **PCI DSS-Referenz**: *Anforderung 12*	**A3.1.4.a** Informationssicherheitsrichtlinien und -prozeduren untersuchen, um zu verifizieren, dass PCI-DSS- und/oder Informationssicherheitsschulung mindestens einmal alle 12 Monate für jede Rolle mit PCI DSS-Einhaltungs-Verantwortlichkeiten erforderlich ist.	
Zielsetzung des kundenspezifischen Ansatzes	**A3.1.4.b** Personal befragen und Teilnahmebescheinigungen oder andere Aufzeichnungen untersuchen, um zu verifizieren, dass Personal mit PCI DSS-Einhaltungs-Verantwortlichkeit mindestens einmal alle 12 Monate aktuelle PCI DSS- und/oder ähnliche Informationssicherheitsschulungen erhält.	
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
A3.2 Der PCI DSS-Geltungsbereich wird dokumentiert und validiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	
A3.2.1 Der PCI DSS-Geltungsbereich wird dokumentiert und auf Genauigkeit mindestens einmal alle drei Monate und bei bedeutenden Änderungen an der Umgebung innerhalb des Geltungsbereichs bestätigt. Die Scoping-Validierung beinhaltet mindestens: • Identifizieren aller Datenflüsse für die verschiedenen Zahlungsphasen (zum Beispiel Autorisierung, Erfassung der Abrechnung, Rückbuchungen und Rückerstattungen) und Akzeptanzkanäle (zum Beispiel Karte vorhanden, Karte nicht vorhanden und E-Commerce, .). • Aktualisierung aller Datenflussdiagramme gemäß Anforderung 1.2.4. • Identifizieren aller Standorte, an denen Kontodaten gespeichert, verarbeitet und übertragen werden, einschließlich, aber nicht beschränkt auf 1) alle Standorte außerhalb der derzeit definierten CDE, 2) Anwendungen, die CHD verarbeiten, 3) Übertragungen zwischen Systemen und Netzwerken und 4) Datei-Backups. • Alle Kontodaten, die außerhalb der aktuell definierten CDE gefunden werden, entweder 1) sicher löschen, 2) in die aktuell definierte CDE migrieren oder 3) die aktuell definierte CDE erweitern, um sie aufzunehmen. • Identifizierung aller Systemkomponenten in der CDE, die mit der CDE verbunden sind oder die die Sicherheit der CDE beeinträchtigen könnten.	**A3.2.1.a** Dokumentierte Ergebnisse von Protokollüberprüfungen untersuchen und das Personal befragen, um zu verifizieren, dass die wie folgt durchgeführt werden. • Mindestens einmal alle drei Monate. • Nach erheblichen Änderungen an der Umgebung im Geltungsbereich. **A3.2.1.b** Dokumentierte Ergebnisse von Geltungsbereichs-Überprüfungen untersuchen, die mindestens einmal alle drei Monate stattfinden, um zu verifizieren, dass die PCI DSS-Scoping-Validierung alle in dieser Anforderung angegebenen Elemente enthält.	**Zweck** Eine häufige Validierung des PCI DSS-Geltungsbereichs hilft dabei, sicherzustellen, dass der PCI DSS-Geltungsbereich auf dem neuesten Stand bleibt und an sich ändernde Geschäftszielsetzungen angepasst ist, und dass deswegen Sicherheitskontrollen alle geeigneten Systemkomponenten schützen. **Gute Praxis** Genaues Scoping beinhaltet die kritische Bewertung der CDE und aller angeschlossenen Systemkomponenten, um die erforderliche Abdeckung für die PCI DSS-Anforderungen zu bestimmen. Scoping-Aktivitäten, einschließlich sorgfältiger Analyse und fortlaufender Überwachung, tragen dazu bei, sicherzustellen, dass die Systeme im Geltungsbereich angemessen abgesichert sind. Beim Dokumentieren von Kontodatenspeicherorten kann die Entität erwägen, eine Tabelle oder Tabellenkalkulation zu erstellen, die die folgenden Informationen enthält: • Datenspeicher (Datenbanken, Dateien, Cloud usw.), einschließlich den Zweck der Datenspeicherung und der Aufbewahrungsfrist, • Welche CHD-Elemente gespeichert werden (PAN, Ablaufdatum, Name des Karteninhabers und/oder alle Elemente von SAD vor Abschluss der Autorisierung), • Wie die Daten gesichert werden (Art der Verschlüsselung und Stärke, Hashierungs-Algorithmus und -stärke, Abschneiden, Tokenisierung), • Wie der Zugriff auf Datenspeicher protokolliert wird, einschließlich einer Beschreibung des/der verwendeten Protokollierungsmechanismus/Protokollierungsmechanismen (Unternehmenslösung, Anwendungsebene, Betriebssystemebene usw.). *(Fortsetzung auf der nächsten Seite)*

Anforderungen und Testprozeduren		Anleitungen
• Identifizierung aller verwendeten Segmentierungskontrollen und der Umgebung(en), aus denen die CDE segmentiert wird, einschließlich der Begründung für Umgebungen, die außerhalb des Geltungsbereichs liegen. • Identifizieren aller Verbindungen zu dritten Entitäten mit Zugriff auf die CDE. • Bestätigung, dass alle identifizierten Datenflüsse, Kontodaten, Systemkomponenten, Segmentierungskontrollen und Verbindungen von Dritten mit Zugriff auf die CDE im Geltungsbereich enthalten sind. **PCI DSS-Referenz**: *Geltungsbereich der PCI-DSS-Anforderungen; Anforderung 12.*		Zusätzlich zu internen Systemen und Netzwerken müssen alle Verbindungen von dritten Entitäten – beispielsweise Geschäftspartnern, Entitäten, die Fernunterstützungs-Dienstleistungen anbieten, und anderen Dienstanbietern – identifiziert werden, um die Aufnahme in den PCI DSS-Geltungsbereich zu bestimmen. Sobald die Verbindungen im Geltungsbereich identifiziert wurden, können die anwendbaren PCI DSS-Kontrollen implementiert werden, um das Risiko zu verringern, dass eine Verbindung von Dritten verwendet wird, um die CDE einer Entität zu gefährden. Ein Daten-Entdeckungs-Tool oder eine Methodik kann verwendet werden, um die Identifizierung aller Quellen und Standorte von PAN zu erleichtern und nach PAN zu suchen, die sich auf Systemen und Netzwerken außerhalb der aktuell definierten CDE oder an unerwarteten Stellen innerhalb der definierten CDE befindet – zum Beispiel bei einem Fehlerprotokoll oder Speicher-Dumpdatei. Dieser Ansatz kann dazu beitragen, dass zuvor unbekannte PAN-Standorte erkannt und die PAN entweder beseitigt oder ordnungsgemäß gesichert wird. **Weitere Informationen** Siehe *„Informationsergänzung: Anleitungen für PCI DSS-Scoping und Netzwerksegmentierung* für zusätzliche Anleitungen.
Zielsetzung des kundenspezifischen Ansatzes Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Änderungen an Systemen oder Netzwerken können bedeutende Auswirkungen auf den PCI DSS-Geltungsbereich haben. Beispielsweise können Änderungen an Regelsätzen für die Netzwerksicherheit ganze Netzwerksegmente in den Geltungsbereich bringen, oder neue Systeme können der CDE hinzugefügt werden, die angemessen geschützt werden müssen. Eine formelle Auswirkungsbewertung, die vor einer Änderung durchgeführt wird, gibt der Einrichtung die Gewissheit, dass die Änderung die Sicherheit der CDE nicht negativ beeinträchtigt. **Gute Praxis** Prozesse, um die potenziellen Auswirkungen zu bestimmen, die Änderungen an Systemen und Netzwerken auf den PCI DSS-Geltungsbereich einer Entität haben können, können als Teil eines dedizierten PCI DSS-Einhaltungsprogramms durchgeführt werden oder unter das übergreifende Einhaltungs- und/oder Kontroll-Programm einer Entität fallen.
A3.2.2 Die Auswirkungen des PCI DSS-Geltungsbereichs für alle Änderungen an Systemen oder Netzwerken werden bestimmt, einschließlich Hinzufügungen neuer Systeme und neuer Netzwerkverbindungen. Die Prozesse umfassen: • Durchführen einer formellen PCI-DSS-Auswirkungsbewertung. • Identifizieren anwendbarer PCI DSS-Anforderungen für das System oder Netzwerk. • Aktualisieren des PCI-DSS-Geltungsbereich wenn angemessen. • Dokumentierte Abnahme der Ergebnisse der Auswirkungsbewertung durch verantwortliches Personal (wie in A3.1.3 definiert). **PCI DSS-Referenz**: *Geltungsbereich der PCI DSS-Anforderungen; Anforderung 1-12*	**A3.2.2** Die Änderungsdokumentation untersuchen und das Personal befragen, um zu verifizieren, dass für jede Änderung an Systemen oder Netzwerken die Auswirkungen des PCI DSS-Geltungsbereichs bestimmt werden und alle in dieser Anforderung angegebenen Elemente enthalten.	
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Es ist wichtig, über Prozesse zur Analyse aller an Systemen oder Netzwerken vorgenommenen Änderungen zu verfügen, um sicherzustellen, dass alle geeigneten PCI DSS-Kontrollen auf alle Systeme oder Netzwerke angewendet werden, die aufgrund einer Änderung zur Umgebung innerhalb des Geltungsbereichs hinzugefügt werden. Der Einbau dieser Validierung in Veränderungsmanagementprozesse hilft dabei, sicherzustellen, dass Geräteinventare und Konfigurationsstandards auf dem neuesten Stand gehalten werden und Sicherheitskontrollen bei Bedarf angewendet werden. **Gute Praxis** Ein Änderungsmanagement-Prozess sollte unterstützende Nachweise enthalten, dass die PCI DSS-Anforderungen durch einen iterativen Prozess implementiert oder beibehalten werden. **Beispiele** PCI DSS-Anforderungen, die verifiziert werden sollten, umfassen, sind aber nicht beschränkt auf: • Netzwerkdiagramme werden aktualisiert, um Änderungen widerzuspiegeln. • Systeme werden gemäß Konfigurationsstandards konfiguriert, wobei alle Standardpasswörter geändert und unnötige Dienste deaktiviert werden. • Systeme werden mit den erforderlichen Kontrollen geschützt – zum Beispiel durch Überwachung der Dateiintegrität, Anti-Malware, Patches und Audit-Protokollierung. • Sensible Authentifizierungsdaten werden nicht gespeichert, und die gesamte Kontodatenspeicherungwird dokumentiert und in die Richtlinien und Prozeduren zur Datenaufbewahrung aufgenommen. • Neue Systeme werden in den vierteljährlichen Schwachstellen-Scan-Prozess aufgenommen.
A3.2.2.1 Nach Abschluss einer Änderung wird bestätigt, dass alle relevanten PCI DSS-Anforderungen auf allen neuen oder geänderten Systemen und Netzwerken implementiert sind, und die Dokumentation wird gegebenenfalls aktualisiert. **PCI DSS-Referenz**: *Geltungsbereich der PCI-DSS-Anforderungen; Anforderung 1-12*	**A3.2.2.1** Änderungsaufzeichnungen und die betroffenen Systeme/Netzwerke untersuchen, und das Personal befragen, um zu verifizieren, dass alle relevanten PCI DSS-Anforderungen als implementiert bestätigt wurden und die Dokumentation als Teil der Änderung aktualisiert wurde.	
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Struktur und die Verwaltung einer Organisation definieren die Anforderungen und das Protokoll für effektive und sichere Betriebe. Änderungen an dieser Struktur könnten negative Auswirkungen auf bestehende Kontrollen und Rahmenwerke haben, indem Ressourcen, die früher PCI DSS-Kontrollen unterstützten, neu zugewiesen oder entfernt werden oder neue Verantwortlichkeiten übernommen werden, die möglicherweise keine etablierten Kontrollen eingerichtet haben. Daher ist es wichtig, den Geltungsbereich und die Kontrollen des PCI DSS zu überarbeiten, wenn es Änderungen an der Struktur und der Verwaltung einer Organisation gibt, um sicherzustellen, dass Kontrollen vorhanden und aktiv sind. **Beispiele** Änderungen an der Organisationsstruktur umfassen, sind aber nicht beschränkt auf Unternehmensfusionen oder -übernahmen und bedeutenden Änderungen oder Neuzuweisungen von Personal, das für Sicherheitskontrolle verantwortlich ist.
A3.2.3 Änderungen an der Organisationsstruktur führen zu einer formellen (internen) Überprüfung der Auswirkungen auf den PCI DSS-Geltungsbereich und die Anwendbarkeit von Kontrollen. **PCI DSS-Referenz**: *Anforderung 12*	**A3.2.3** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass eine Änderung der Organisationsstruktur zu einer formellen Überprüfung der Auswirkungen auf den PCI DSS-Geltungsbereich und die Anwendbarkeit von Kontrollen führt.	
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** PCI DSS erfordert normalerweise, dass Segmentierungskontrollen alle zwölf Monate durch Penetrationstests verifiziert werden. Durch eine häufigere Validierung von Segmentierungskontrollen werden solche Fehler in der Segmentierung wahrscheinlich entdeckt, bevor sie von einem Angreifer ausgenutzt werden können, der versucht, seitlich von einem nicht vertrauenswürdigen Netzwerk außerhalb des Geltungsbereichs zur CDE zu wechseln. **Gute Praxis** Obwohl die Anforderung besagt, dass diese Geltungsbereichsvalidierung mindestens einmal alle sechs Monate und nach einer bedeutenden Änderung durchgeführt wird, sollte diese Übung so häufig wie möglich durchgeführt werden, um sicherzustellen, dass sie die CDE wirksam von anderen Netzen isoliert. **Weitere Informationen** Siehe *„Informationsergänzung: Penetrationstestanleitungen* für zusätzliche Anleitungen.
A3.2.4 Wenn Segmentierung verwendet wird, wird der PCI DSS-Geltungsbereich wie folgt bestätigt: • Gemäß der in Anforderung 11.4.1 definierten Methodik der Entität. • Penetrationstests werden an Segmentierungskontrollen mindestens einmal alle sechs Monate und nach jeder Änderung der Segmentierungskontrollen/-methoden durchgeführt. • Der Penetrationstest umfasst alle verwendeten Segmentierungskontrollen/-methoden. • Der Penetrationstest verifiziert, dass die Segmentierungskontrollen/-methoden betriebsbereit und effektiv sind und die CDE von allen Systemen außerhalb des Geltungsbereichs isolieren. **PCI DSS-Referenz**: *Anforderung 11*	**A3.2.4** Die Ergebnisse des letzten Penetrationstests untersuchen, um zu verifizieren, dass der Test gemäß allen in dieser Anforderung angegebenen Elementen ausgeführt wurde.	
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** PCI DSS erfordert, dass bewertete Entitäten im Rahmen der Scoping-Übung das Vorhandensein aller Klartext-PANs in ihren Umgebungen identifizieren und dokumentieren müssen. Implementieren einer Datenentdeckung-Methodik, die alle Quellen und Standorte von Klartext-PANs identifiziert und nach Klartext-PANs auf Systemen und Netzwerken außerhalb der aktuell definierten CDE oder an unerwarteten Stellen innerhalb der definierten CDE sucht – zum Beispiel in einem Fehlerprotokoll oder einer Speicherdumpdatei – hilft dabei, sicherzustellen, dass zuvor unbekannte Standorte von Klartext-PAN erkannt und ordnungsgemäß gesichert werden. **Beispiele** Ein Datenentdeckungsprozess kann über eine Vielzahl von Methoden durchgeführt werden, einschließlich, aber nicht beschränkt auf 1) kommerziell erhältliche Datenentdeckungssoftware, 2) ein intern entwickeltes Datenentdeckungsprogramm oder 3) eine manuelle Suche. Bei Bedarf kann auch eine Kombination von Methoden verwendet werden. Unabhängig von der verwendeten Methode besteht das Ziel der Bemühungen darin, alle Quellen und Speicherorte von Klartext-PAN zu finden (nicht nur in der definierten CDE).
A3.2.5 Es wird eine Datenentdeckungs-Methodik implementiert, die: • Den PCI DSS-Geltungsbereich bestätigt. • Findet alle Quellen und Speicherorte von Klartext-PAN mindestens einmal alle drei Monate und bei bedeutenden Änderungen an der CDE oder den Prozessen. • Das Potenzial für Klartext-PAN adressiert, sich auf Systemen und Netzwerken außerhalb der derzeit definierten CDE zu befinden. **PCI DSS-Referenz**: *Geltungsbereich der PCI-DSS-Anforderungen*	**A3.2.5.a** Die dokumentierte Datenentdeckungsmethodik untersuchen, um zu verifizieren, dass sie alle in dieser Anforderung angegebenen Elemente enthält.	
Zielsetzung des kundenspezifischen Ansatzes	**A3.2.5.b** Ergebnisse aus jüngsten Datenentdeckungsbemühungen untersuchen, und verantwortliches Personal befragen, um zu verifizieren, die Datenentdeckung mindestens einmal alle drei Monate und bei bedeutenden Änderungen an der CDE oder den Prozessen durchgeführt wird.	
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ein Prozess zum Testen der Wirksamkeit der Methoden zur Datenentdeckung stellt die Vollständigkeit und Genauigkeit von Kontodaten sicher. **Gute Praxis** Der Vollständigkeit halber sollten Systemkomponenten in den Netzwerken im Geltungsbereich, und Systeme in Netzwerken außerhalb des Geltungsbereichs in den Datenentdeckungsprozess einbezogen werden. Der Datenentdeckungsprozess soll auf allen verwendeten Betriebssystemen und Plattformen wirksam sein. Die Genauigkeit kann getestet werden, indem Test-PANs auf Systemkomponenten und verwendeten Dateiformaten platziert werden und bestätigt wird, dass die Datenentdeckungsmethode die Test-PANs erkannt hat.
A3.2.5.1 Datenentdeckungsmethoden werden wie folgt bestätigt: • Die Wirksamkeit der Methoden wird getestet. • Methoden sind in der Lage, Klartext-PAN auf allen Arten von Systemkomponenten und verwendeten Dateiformaten zu entdecken. • Die Wirksamkeit von Datenentdeckungsmethoden wird mindestens einmal alle 12 Monate bestätigt. **PCI DSS-Referenz**: *Geltungsbereich der PCI-DSS-Anforderungen*	**A3.2.5.1.a** Das Personal befragen und die Dokumentation überprüfen, um Folgendes zu verifizieren: • Die Entität verfügt über einen Prozess zum Testen der Wirksamkeit von Methoden, die zur Datenentdeckung verwendet werden. • Der Prozess umfasst, zu verifizieren, dass die Methoden in der Lage sind, Klartext-PAN auf allen Arten von Systemkomponenten und verwendeten Dateiformaten zu entdecken.	
Zielsetzung des kundenspezifischen Ansatzes	**A3.2.5.1.b** Die Ergebnisse der Wirksamkeitstests untersuchen, um zu verifizieren, dass die Wirksamkeit von Datenentdeckungsmethoden mindestens einmal alle 12 Monate bestätigt wird.	
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Das Dokumentieren von Reaktionsprozeduren, die befolgt werden, falls Klartext-PAN außerhalb der CDE gefunden wird, hilft dabei, die notwendigen Behebungsaktionen zu identifizieren und zukünftige Lecks zu verhindern. **Gute Praxis** Wenn PAN außerhalb der CDE gefunden wurde, sollte eine Analyse durchgeführt werden, um 1) festzustellen, ob es unabhängig von anderen Daten oder mit sensiblen Authentifizierungsdaten gespeichert wurde, 2) die Quelle der Daten zu identifizieren und 3) die Kontrolllücken zu identifizieren, die dazu führten, dass die Daten außerhalb der CDE lagen. Entitäten sollten betrachten, ob Faktoren wie Geschäftsprozesse, Benutzerverhalten, falsche Systemkonfigurationen usw. dazu beigetragen haben, dass die PAN an einem unerwarteten Ort gespeichert wurde. Wenn solche beitragenden Faktoren vorhanden sind, sollten sie gemäß dieser Anforderung adressiert werden, um ein erneutes Auftreten zu verhindern.
A3.2.5.2 Es sind Reaktionsprozeduren implementiert, die bei Erkennung einer Klartext-PAN außerhalb der CDE eingeleitet werden, um Folgendes einzuschließen: • Bestimmen, was zu tun ist, wenn Klartext-PAN außerhalb der CDE entdeckt wird, einschließlich ihres Abrufs, sicheren Löschens und/oder Migration in die aktuell definierte CDE, soweit zutreffend. • Bestimmen, wie die Daten außerhalb der CDE gelandet sind. • Beheben von Datenlecks oder Prozesslücken, die dazu führten, dass die Daten außerhalb der CDE sind. • Identifizieren der Quelle der Daten. • Identifizieren, ob irgendwelche Verfolgungsdaten mit den PANs gespeichert sind.	**A3.2.5.2.a** Dokumentierte Reaktionsprozeduren untersuchen, um zu verifizieren, dass Prozeduren für die Reaktion auf die Erkennung von Klartext-PANs außerhalb der CDE definiert sind und alle in dieser Anforderung angegebenen Elemente enthalten.	
Zielsetzung des kundenspezifischen Ansatzes	**A3.2.5.2.b** Das Personal befragen und Aufzeichnungen von Reaktionsaktionen untersuchen, um zu verifizieren, dass Behebungsaktivitäten durchgeführt werden, wenn Klartext-PAN außerhalb der CDE erkannt wird.	
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die Verwendung von Mechanismen zum Erkennen und Verhindern, dass nicht autorisierte PANs die CDE verlassen, gestattet es einer Organisation, Situationen zu erkennen und zu verhindern, die zu Datenverlust führen können. **Gute Praxis** Die Abdeckung der Mechanismen sollte E-Mails, Downloads auf entfernbaren Medien und die Ausgabe auf Druckern umfassen, ist aber nicht darauf beschränkt. **Beispiele** Mechanismen zum Erkennen und Verhindern des nicht autorisierten Verlusts von Klartext-PANs können die Verwendung geeigneter Tools wie Datenverlustverhinderungs (DLP)-Lösungen sowie manuelle Prozesse und Verfahren umfassen.
A3.2.6 Es werden Mechanismen implementiert, um zu erkennen und zu verhindern, dass Klartext-PANs die CDE über einen nicht autorisierten Kanal, eine Methode oder einen Prozess verlassen, einschließlich Mechanismen, die: • Aktiv laufen. • Konfiguriert sind, um zu erkennen und zu verhindern, dass Klartext-PAN die CDE über einen nicht autorisierten Kanal, eine nicht autorisierte Methode oder einen nicht autorisierten Prozess verlässt. • Generierung von Audit-Protokollen und Warnungen bei Erkennung von Klartext-PAN, die die CDE über einen nicht autorisierten Kanal, eine nicht autorisierte Methode oder einen nicht autorisierten Prozess verlässt. **PCI DSS-Referenz**: *Geltungsbereich der PCI-DSS-Anforderungen; Anforderung 12*	**A3.2.6.a** Die Dokumentation untersuchen und implementierte Mechanismen beobachten, um zu verifizieren, dass die Mechanismen mit allen in dieser Anforderung angegebenen Elementen übereinstimmen. **A3.2.6.b** Audit-Protokolle und Warnungen untersuchen und verantwortliches Personal befragen, um zu verifizieren, dass Warnungen untersucht werden.	
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Versuche, Klartext-PAN über einen nicht autorisierten Kanal, eine nicht autorisierte Methode oder einen nicht autorisierten Prozess zu entfernen, können auf die böswillige Absicht hindeuten, Daten zu stehlen, oder können die Aktionen eines autorisierten Mitarbeiters sein, der die richtigen Methoden nicht kennt oder einfach nicht befolgt. Eine umgehende Untersuchung dieser Vorkommnisse kann identifizieren, wo Behebungen erforderlich sind, und liefert wertvolle Informationen, um zu verstehen, woher die Bedrohungen kommen.
A3.2.6.1 Reaktionsprozeduren werden implementiert, um eingeleitet zu werden, wenn Versuche erkannt werden, Klartext-PAN über einen nicht autorisierten Kanal, eine nicht autorisierte Methode oder einen nicht autorisierten Prozess aus der CDE zu entfernen. Reaktionsprozeduren umfassen: • Prozeduren zur sofortigen Untersuchung von Warnungen durch verantwortliches Personal. • Prozeduren zur Behebung von Datenlecks oder Prozesslücken, falls erforderlich, um Datenverlust zu vermeiden. **PCI DSS-Referenz**: *Anforderung 12*	**A3.2.6.1.a** Dokumentierte Reaktionsprozeduren untersuchen, um zu verifizieren, dass Prozeduren für die Reaktion auf versuchte Entfernung von Klartext-PANs von der CDE über einen nicht autorisierten Kanal, eine nicht autorisierte Methode oder einen nicht autorisierten Prozess alle in dieser Anforderung angegebenen Elemente enthalten: • Prozeduren zur sofortigen Untersuchung von Warnungen durch verantwortliches Personal. • Prozeduren zur Behebung von Datenlecks oder Prozesslücken, falls erforderlich, um Datenverlust zu vermeiden.	
Zielsetzung des kundenspezifischen Ansatzes Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.	**A3.2.6.1.b** Das Personal befragen und Aufzeichnungen über ergriffene Aktionen untersuchen, wenn erkannt wird, dass Klartext-PANs die CDE über einen nicht autorisierten Kanal, eine nicht autorisierte Methode oder einen nicht autorisierten Prozess verlassen, und verifizieren, dass Behebungsaktivitäten durchgeführt wurden.	

Anforderungen und Testprozeduren		Anleitungen
A3.3 PCI DSS ist in Geschäft wie gewohnt (BAU)-Aktivitäten integriert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Ohne formelle Prozesse für die sofortige (so bald wie möglich) Erkennung, Warnung und Adressierung kritischer Sicherheitskontrollfehler können Versagen unentdeckt bleiben oder für längere Zeit ungelöst bleiben. Darüber hinaus haben Angreifer ohne formalisierte zeitgebundene Prozesse ausreichend Zeit, um Systeme zu kompromittieren und Kontodaten von der CDE zu stehlen. **Gute Praxis** Die spezifischen Fehlerarten können je nach Funktion der Gerätesystemkomponente und verwendeter Technologie variieren. Typische Versagen umfassen ein System, das seine Sicherheitsfunktion nicht mehr durchführt oder nicht wie vorgesehen funktioniert, beispielsweise wenn eine Firewall alle ihre Regeln löscht oder offline geht. *(Fortsetzung auf der nächsten Seite)*
A3.3.1 Versagen von kritischen Sicherheitskontrollsystemen werden sofort erkannt, gewarnt und adressiert, einschließlich, aber nicht beschränkt auf das Versagen von: • Netzwerksicherheitskontrollen • IDS/IPS • FIM • Anti-Malware-Lösungen • Physische Zugriffskontrollen • Logische Zugriffskontrollen • Audit-Protokollierungsmechanismen • Segmentierungskontrollen (sofern verwendet) • Automatisierte Audit-Protokoll-Überprüfungsmechanismen *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens einer bewährten Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.* • Automatisierte Code-Überprüfungs-Tools (falls verwendet). *Dieser Aufzählungspunkt ist bis zum Datum des Inkrafttretens einer bewährten Praktik, weitere Informationen finden Sie in den Anwendbarkeitshinweisen unten.* **PCI DSS-Referenz**: *Anforderungen 1-12*	**A3.3.1.a** Dokumentierte Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse definiert sind, um kritische Sicherheitskontrollversagen gemäß allen in dieser Anforderung angegebenen Elemente sofort zu erkennen, auf sie zu warnen und sie zu adressieren.	
Zielsetzung des kundenspezifischen Ansatzes	**A3.3.1.b** Erkennungs- und Warnungsprozesse untersuchen und das Personal befragen, um zu verifizieren, dass Prozesse für alle kritischen Sicherheitskontrollen, die in dieser Anforderung angegeben sind, implementiert werden und dass jedes Versagen einer kritischen Sicherheitskontrolle zur Generierung einer Warnung führt.	
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Hinweise zur Anwendbarkeit		
Die obigen Aufzählungspunkte (für automatisierte Protokollüberprüfungsmechanismen und automatisierte Codeüberprüfungstools (falls verwendet)) sind bewährte Praktiken bis zum 31. März 2025, danach sind sie als Teil von Anforderung A3.3.1 erforderlich und müssen berücksichtigt werden		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Wenn auf Warnungen bei Versagen von kritischen Sicherheitskontrollsystemen nicht schnell und effektiv reagiert wird, können Angreifer diese Zeit nutzen, um böswillige Software einzuschleusen, die Kontrolle über ein System zu erlangen oder Daten aus der Umgebung der Entität zu stehlen. **Gute Praxis** Dokumentierte Nachweise (zum Beispiel Aufzeichnungen in einem Problemverwaltungssystem) sollten vorhandene Prozesse und Prozeduren unterstützen, die auf Sicherheitsversagen reagieren. Darüber hinaus sollte sich das Personal seiner Verantwortung im Fall eines Versagens bewusst sein. Aktionen und Reaktionen auf das Versagen sollten in den dokumentierten Nachweisen festgehalten werden.
A3.3.1.2 Auf Versagen irgendwelcher kritischer Sicherheitskontrollsysteme wird umgehend reagiert. Prozesse zur Reaktion auf Versagen in Sicherheitskontrollsystemen umfassen: • Wiederherstellen von Sicherheitsfunktionen. • Identifizieren und Dokumentieren der Dauer (Datum und Uhrzeit von Anfang bis Ende) des Sicherheitsversagens. • Identifizieren und Dokumentieren der Ursache(n) des Versagens, einschließlich der Grundursache, und Dokumentieren der Behebung, die zum Adressieren der Grundursache erforderlich ist. • Identifizierung und Behebung von Sicherheitsproblemen, die während des Versagens aufgetreten sind. • Feststellen, ob aufgrund des Sicherheitsversagens weitere Aktionen erforderlich sind. • Implementieren von Kontrollen, um zu verhindern, dass die Versagensursache erneut auftritt. • Wiederaufnehmen der Überwachung der Sicherheitskontrollen. **PCI DSS-Referenz**: *Anforderungen 1-12*	**A3.3.1.2.a** Dokumentierte Richtlinien und Prozeduren untersuchen und das Personal befragen, um zu verifizieren, dass Prozesse definiert und implementiert sind, um umgehend auf ein Sicherheitskontrollversagen gemäß allen in dieser Anforderung angegebenen Elemente zu reagieren. **A3.3.1.2.b** Aufzeichnungen untersuchen, um zu verifizieren, dass Sicherheitskontrollversagen dokumentiert werden, einschließlich: • Identifizierung der Ursache(n) des Versagens, einschließlich Grundursache. • Dauer (Datum und Zeit Beginn und Ende) des Sicherheitsversagens. • Details zur erforderlichen Behebung, die erfordert ist, um die Grundursache zu adressieren.	
Zielsetzung des kundenspezifischen Ansatzes Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Hardware- und Softwaretechnologien entwickeln sich ständig weiter, und Organisationen müssen sich der Änderungen an den von ihnen verwendeten Technologien sowie der sich entwickelnden Bedrohungen für diese Technologien bewusst sein. Die Ausführung angemessener Überprüfungen dieser Technologien stellt sicher, dass sie sich auf Schwachstellen in Hardware und Software vorbereiten und diese verwalten können, die nicht vom Anbieter oder Entwickler behoben werden. **Gute Praxis** Organisationen sollten auch in Betracht ziehen, Firmware-Versionen zu überprüfen, um sicherzustellen, dass sie aktuell bleiben und von den Anbietern unterstützt werden. Organisationen müssen sich auch der von Technologieanbietern an ihren Produkten oder Prozessen vorgenommenen Änderungen bewusst sein, um zu verstehen, wie sich diese Änderungen auf die Nutzung der Technologie durch die Organisation auswirken können. Regelmäßige Überprüfungen von Technologien, die sich auf PCI DSS-Kontrollen auswirken oder sie beeinflussen, können bei Kauf-, Nutzungs- und Bereitstellungsstrategien helfen und sicherstellen, dass Kontrollen, die auf diesen Technologien beruhen, wirksam bleiben. Diese Überprüfungen umfassen, sind aber nicht beschränkt auf die Überprüfung von Technologien, die vom Anbieter nicht mehr unterstützt werden und/oder die Sicherheitsanforderungen der Organisation nicht mehr erfüllen.
A3.3.2 Hardware- und Softwaretechnologien werden mindestens einmal alle 12 Monate überprüft, um zu bestätigen, ob sie weiterhin die PCC DSS-Anforderungen der Organisation erfüllen. **PCI DSS-Referenz**: *Anforderungen 2, 6, 12.*	**A3.3.2.a** Dokumentierte Richtlinien und Prozeduren untersuchen und Personal befragen, um zu verifizieren, dass Prozesse definiert und implementiert sind, um Hardware- und Softwaretechnologien zu überprüfen, um zu bestätigen, ob sie weiterhin die PCI DSS-Anforderungen der Organisation erfüllen.	
	A3.3.2.b Die Ergebnisse der letzten Überprüfungen von Hardware- und Softwaretechnologien überprüfen, um zu verifizieren, dass Überprüfungen mindestens einmal alle 12 Monate durchgeführt werden.	
Zielsetzung des kundenspezifischen Ansatzes Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.	**A3.3.2.c** Die Dokumentation untersuchen, um zu verifizieren, dass für alle Technologien, bei denen festgestellt wurde, dass sie die PCI DSS-Anforderungen der Organisation nicht mehr erfüllen, ein Plan zur Behebung der Technologie vorhanden ist.	
Hinweise zur Anwendbarkeit Der Prozess umfasst einen Plan für die Behebung von Technologien, die die PCI DSS-Anforderungen der Organisation nicht mehr erfüllen, bis hin zum Ersatz der Technologie, wie angemessen.		

Anforderungen und Testprozeduren		Anleitungen
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck** Die regelmäßige Bestätigung, dass Sicherheitsrichtlinien und -verfahren befolgt werden, stellt sicher, dass die erwarteten Kontrollen aktiv sind und wie beabsichtigt funktionieren. Die Zielsetzung dieser Überprüfungen besteht nicht darin, andere PCI DSS-Anforderungen wieder durchzuführen, sondern zu bestätigen, dass Sicherheitsaktivitäten fortlaufend durchgeführt werden. **Gute Praxis** Diese Überprüfungen können auch verwendet werden, um zu verifizieren, dass geeignete Beweise geführt werden – zum Beispiel Audit-Protokolle, Schwachstellen-Scan-Berichte, Überprüfungen von Regelsätzen für die Netzwerksicherheitskontrolle –, um die Entität bei der Vorbereitung ihrer nächsten PCI DSS-Beurteilung zu unterstützen. **Beispiele** Betrachtet man Anforderung 1.2.7 als ein Beispiel, so wird Anforderung A3.3.3 dadurch erfüllt, dass mindestens alle drei Monate bestätigt wird, dass die Überprüfungen der Konfigurationen der Netzwerksicherheitskontrollen in der erforderlichen Häufigkeit stattgefunden haben. Andererseits wird Anforderung 1.2.7 erfüllt, indem diese Konfigurationen wie in der Anforderung angegeben überprüft werden.
A3.3.3 Überprüfungen werden mindestens einmal alle drei Monate durchgeführt, um zu verifizieren, dass die BAU-Aktivitäten befolgt werden. Überprüfungen werden von Personal durchgeführt, das dem PCI DSS-Einhaltungsprogramm zugewiesen ist (wie in A3.1.3 angegeben), und umfassen: • Bestätigung, dass alle BAU-Aktivitäten, einschließlich A3.2.2, A3.2.6 und A3.3.1, durchgeführt werden. • Bestätigung, dass das Personal Sicherheitsrichtlinien und Betriebsverfahren befolgt (zum Beispiel tägliche Protokollüberprüfungen, Regelsatzüberprüfungen für Netzwerksicherheitskontrollen, Konfigurationsstandards für neue Systeme). • Dokumentieren, wie die Überprüfungen abgeschlossen wurden, einschließlich wie alle BAU-Aktivitäten als vorhanden verifiziert wurden. • Sammlung dokumentierter Nachweise, wie für die jährliche PCI DSS-Bewertung erforderlich. • Überprüfung und Abnahme der Ergebnisse durch Personal, das für das PCI DSS-Einhaltungsprogramm verantwortlich ist, wie in A3.1.3 identifiziert ist. • Aufbewahrung von Aufzeichnungen und Dokumentationen für mindestens 12 Monate, die alle BAU-Aktivitäten abdecken. **PCI DSS-Referenz**: *Anforderungen 1-12*	**A3.3.3.a** Richtlinien und Prozeduren untersuchen, um zu verifizieren, dass Prozesse zum Überprüfen und Verifizieren von BAU-Aktivitäten gemäß allen in dieser Anforderung angegebenen Elementen definiert sind. **A3.3.3.b** Verantwortliches Personal befragen und Aufzeichnungen von Überprüfungen untersuchen, um zu verifizieren, dass • Überprüfungen werden von Personal durchgeführt, das dem PCI DSS-Einhaltungsprogramm zugewiesen ist. • Überprüfungen werden mindestens einmal alle drei Monate durchgeführt.	
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
A3.4 Der logische Zugriff auf die Karteninhaberdatenumgebung wird kontrolliert und verwaltet.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
A3.4.1 Benutzerkonten und Zugriffsprivilegien auf Systemkomponenten innerhalb des Geltungsbereichs werden mindestens einmal alle sechs Monate überprüft, um sicherzustellen, dass Benutzerkonten und Zugriffsprivilegien basierend auf der Jobfunktion angemessen bleiben und dass der gesamte Zugriff autorisiert ist. **PCI DSS-Referenz**: *Anforderung 7*	**A3.4.1** Verantwortliches Personal befragen und unterstützende Dokumentation untersuchen, um zu verifizieren, dass: • Benutzerkonten und Zugriffsrechte mindestens alle sechs Monate überprüft werden. • Überprüfungen bestätigen, dass der Zugriff basierend auf der Jobfunktion angemessen ist und dass jeder Zugriff autorisiert ist.	Die regelmäßige Überprüfung der Zugriffsrechte hilft, übermäßige Zugriffsrechte zu erkennen, die verbleiben, nachdem sich die Jobverantwortlichkeiten der Benutzer geändert haben, Systemfunktionen sich geändert haben oder andere Änderungen. Wenn übermäßige Benutzerrechte nicht zeitgerecht widerrufen werden, können sie von böswilligen Benutzern für nicht autorisierten Zugriff verwendet werden. Diese Überprüfung stellt eine weitere Gelegenheit bereit, um sicherzustellen, dass Konten für alle gekündigten Benutzer entfernt wurden (falls zum Zeitpunkt der Kündigung welche übersehen wurden), sowie um sicherzustellen, dass der Zugriff von Dritten, die keinen Zugriff mehr benötigen, beendet wurde.
Zielsetzung des kundenspezifischen Ansatzes		
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anforderungen und Testprozeduren		Anleitungen
A3.5 Verdächtige Ereignisse werden identifiziert und es wird darauf reagiert.		
Definierte Ansatzanforderungen	**Testprozeduren mit definiertem Ansatz**	**Zweck**
A3.5.1 Es wird eine Methodik zur sofortigen Identifizierung von Angriffsmustern und unerwünschtem Verhalten systemübergreifend implementiert, die Folgendes umfasst: • Identifizierung von Anomalien oder verdächtigen Aktivitäten, sobald sie auftreten. • Ausgabe von sofortigen Warnungen an verantwortliches Personal bei Erkennung verdächtiger Aktivitäten oder Anomalien. • Reaktion auf Warnungen gemäß dokumentierten Reaktionsprozeduren. **PCI DSS-Referenz**: *Anforderungen 10, 12*	**A3.5.1.a** Die Dokumentation untersuchen und das Personal befragen, um zu verifizieren, dass eine Methodik definiert und implementiert ist, um Angriffsmuster und unerwünschtes Verhalten systemübergreifend schnell zu erkennen, und die alle in dieser Anforderung angegebenen Elemente enthält.	Die Fähigkeit, Angriffsmuster und unerwünschtes Verhalten systemübergreifend zu identifizieren – beispielsweise mithilfe zentral verwalteter oder automatisierter Protokollkorrelationstools – ist entscheidend, um die Auswirkungen einer Datenkompromittierung zu verhindern, zu erkennen oder zu minimieren. Das Vorhandensein von Protokollen in allen Umgebungen erlaubt eine gründliche Verfolgung, Warnung und Analyse, wenn etwas schief geht. Die Bestimmung der Ursache einer Kompromittierung ist sehr schwierig, wenn nicht sogar unmöglich, ohne einen Prozess zur Bestätigung von Informationen von kritischen Systemkomponenten und Systemen, die Sicherheitsfunktionen durchführen, wie zum Beispiel Netzwerksicherheitskontrollen, IDS/IPS und Systeme zur Dateiintegritätsüberwachung (FIM). Daher müssen Protokolle für alle kritischen Systemkomponenten und Systeme, die Sicherheitsfunktionen durchführen, gesammelt, korreliert und aufrechterhalten werden. Dies könnte die Verwendung von Softwareprodukten und Dienstleistungsmethodiken zur Bereitstellung von Echtzeitanalysen, Warnmeldungen und Berichten umfassen, zum Beispiel Sicherheitsinformationen und Ereignisverwaltung (SIEM), FIM oder Änderungserkennung.
Zielsetzung des kundenspezifischen Ansatzes	**A3.5.1.b** Vorfallsreaktionsprozeduren untersuchen und verantwortliches Personal befragen, um Folgendes zu verifizieren: • Bereitschaftspersonal wird umgehend benachrichtigt. • Auf Warnungen wird nach dokumentierten Reaktionsprozeduren reagiert.	
Diese Anforderung ist für den kundenspezifischen Ansatz nicht geeignet.		

Anhang B Kompensierende Kontrollen

Kompensierende Kontrollen können in Betracht gezogen werden, wenn eine Entität eine PCI DSS-Anforderung aufgrund einer legitimen und dokumentierten technischen oder geschäftlichen Einschränkung nicht explizit erfüllen kann, aber das mit der Anforderung verbundene Risiko durch Implementierung anderer oder kompensierender Kontrollen ausreichend gemindert hat.

Kompensierende Kontrollen müssen folgende Kriterien erfüllen:

1. Die Absicht und Strenge der ursprünglichen PCI DSS-Anforderung erfüllen.
2. Ein ähnliches Verteidigungsniveau wie die ursprüngliche PCI DSS-Anforderung bereitstellen, sodass die kompensierende Kontrolle das Risiko, gegen das die ursprüngliche PCI DSS-Anforderung schützen sollte, ausreichend ausgleicht. Um die Absicht einer Anforderung zu verstehen, siehe *die Zielsetzung des kundenspezifischen Ansatzes* für die meisten PCI DSS-Anforderungen. Wenn eine Anforderung nicht für den kundenspezifischen Ansatz geeignet ist und daher keine Zielsetzung des kundenspezifischen Ansatzes hat, Beziehung auf den **Zweck** in der Spalte „Anleitungen“ für diese Anforderung.
3. Sie müssen über die anderen Anforderungen des PCI DSS „hinausgehen“. (Die einfache Einhaltung anderer PCI DSS-Anforderungen ist keine kompensierende Kontrolle.)
4. Bei der Bewertung der "darüber hinausgehenden" kompensierenden Kontrollen ist Folgendes zu beachten:

Hinweis: *Alle kompensierenden Kontrollen müssen von dem Bewerter, der die PCI-DSS-Bewertung durchführt, überprüft und auf Angemessenheit validiert werden. Die Wirksamkeit einer kompensierenden Kontrolle hängt von den Besonderheiten der Umgebung ab, in der die Kontrolle implementiert wird, den umgebenden Sicherheitskontrollen und der Konfiguration der Kontrolle. Entitäten sollten sich bewusst sein, dass eine gegebene kompensierende Kontrolle nicht in allen Umgebungen effektiv ist.*

   a. Bestehende PCI DSS-Anforderungen KÖNNEN NICHT als kompensierende Kontrollen betrachtet werden, wenn sie bereits für das zu überprüfende Element erforderlich sind. Zum Beispiel müssen Passwörter für den Administratorzugriff ohne Konsole verschlüsselt gesendet werden, um das Risiko des Abfangens von Administratorpasswörtern im Klartext zu mindern. Eine Entität kann keine anderen PCI-DSS-Kennwortanforderungen (Eindringlingssperre, komplexe Passwörter usw.) verwenden, um das Fehlen verschlüsselter Passwörter zu kompensieren, da diese anderen Passwortanforderungen das Risiko des Abfangens von Klartextpasswörtern nicht mindern. Die anderen Passwortkontrollen sind auch bereits PCI DSS-Anforderungen für das zu prüfende Element (Passwörter).
   b. Bestehende PCI DSS-Anforderungen KÖNNEN als kompensierende Kontrollen betrachtet werden, wenn sie für einen anderen Bereich erforderlich sind aber nicht für das zu überprüfende Element erforderlich sind.

c. Bestehende PCI DSS-Anforderungen können mit neuen Kontrollen kombiniert werden, um zu einer kompensierenden Kontrolle zu werden. Zum Beispiel, wenn ein Unternehmen nicht in der Lage ist, eine Schwachstelle zu adressieren, die über eine Netzwerkschnittstelle ausgenutzt werden kann, weil noch keine Sicherheitsaktualisierung von einem Anbieter verfügbar ist, könnte eine kompensierende Kontrolle aus Kontrollen bestehen, die Folgendes umfassen: 1) interne Netzwerksegmentierung, 2) Beschränkung des Netzwerkzugriffs auf die anfällige Schnittstelle auf nur erforderliche Geräte (IP-Adress- oder MAC-Adressfilterung) und 3) IDS/IPS-Überwachung des gesamten Verkehrs, der an die anfällige Schnittstelle gerichtet ist.

5. Das zusätzliche Risiko adressieren, das durch die Nichteinhaltung der PCI DSS-Anforderung entsteht.
6. Die Anforderung derzeit und in Zukunft adressieren. Eine kompensierende Kontrolle kann keine Anforderung adressieren, die in der Vergangenheit versäumt wurde (zum Beispiel, wenn die Durchführung einer Aufgabe vor zwei Quartalen erforderlich war, diese Aufgabe jedoch nicht durchgeführt wurde).

Der Bewerter muss die kompensierenden Kontrollen während jeder jährlichen PCI DSS-Bewertung gründlich bewerten, um zu bestätigen, dass jede kompensierende Kontrolle das Risiko, dass die ursprüngliche PCI DSS-Anforderung gemäß den obigen Punkten 1-6 adressieren sollte, angemessen adressiert.

Um die Einhaltung aufrechtzuerhalten, müssen Prozesse und Kontrollen vorhanden sein, um sicherzustellen, dass die kompensierenden Kontrollen nach Abschluss der Bewertung wirksam bleiben. Darüber hinaus müssen die Ergebnisse der kompensierenden Kontrolle im zutreffenden Bericht für die Bewertung (zum Beispiel ein Einhaltungsbericht oder ein Fragebogen zur Selbstbewertung) im entsprechenden PCI DSS-Anforderungsabschnitt dokumentiert werden, und bei der Übermittlung des zutreffenden Berichts an die anfordernde Organisation eingeschlossen werden.

Anhang C Arbeitsblatt für Kompensierende Kontrollen

Die Entität muss dieses Arbeitsblatt verwenden, um kompensierende Kontrollen für alle Anforderungen zu definieren, bei denen kompensierende Kontrollen verwendet werden, um eine PCI DSS-Anforderung zu erfüllen. Beachten Sie, dass kompensierende Kontrollen auch gemäß den Anweisungen im Einhaltungsbericht im entsprechenden Abschnitt zu den PCI DSS-Anforderungen dokumentiert werden sollten.

Hinweis: *Nur Entitäten, die eine Risikoanalyse durchgeführt haben und legitime und dokumentierte technologische oder geschäftliche Einschränkungen haben, können die Verwendung von kompensierenden Kontrollen in Betracht ziehen, um die Einhaltung zu erreichen.*

Anforderungsnummer und -definition:

	Erforderte Informationen	Erklärung
1. Einschränkungen	Die legitimen technischen oder geschäftlichen Einschränkungen dokumentieren, die die Einhaltung der ursprünglichen Anforderung verhindern.	
2. Definition von kompensierenden Kontrollen	Die kompensierenden Kontrollen definieren; erklären, wie sie die Ziele der ursprünglichen Kontrolle und das erhöhte Risiko, falls vorhanden, adressieren.	
3. Zielsetzung	Die Zielsetzung der ursprünglichen Kontrolle (zum Beispiel die Zielsetzung des kundenspezifischen Ansatzes) definieren.	
	Die Zielsetzung, die durch die kompensierende Kontrolle erfüllt wird *(Hinweis: Dies kann, muss aber nicht, die Zielsetzung des kundenspezifischen Ansatzes für die PCI-DSS-Anforderung sein).*	
4. Identifiziertes Risiko	Jedes zusätzliche Risiko identifizieren, das durch das Fehlen der ursprünglichen Kontrolle entsteht.	
5. Validierung von kompensierenden Kontrollen	Definieren, wie die kompensierenden Kontrollen validiert und getestet wurden.	
6. Aufrechterhaltung	Prozess(e) und Kontrollen definieren, um kompensierende Kontrollen aufrechtzuerhalten.	

Anhang D Kundenspezifischer Ansatz

Dieser Ansatz ist für Entitäten gedacht, die sich dazu entschließen, die in einer PCI DSS-Anforderung Zielsetzung des kundenspezifischen Ansatzes auf eine Weise zu erfüllen, die sich nicht streng an die definierte Anforderung hält. Der kundenspezifische Ansatz gestattet es einer Entität, einen strategischen Ansatz zur Erfüllung der Zielsetzung des kundenspezifischen Ansatzes einer Anforderung zu verfolgen, sodass sie die Sicherheitskontrollen bestimmen und entwerfen kann, die erforderlich sind, um die Zielsetzung auf eine für diese Organisation einzigartige Weise zu erfüllen.

Die Entität, die einen kundenspezifischen Ansatz implementiert, muss folgende Kriterien erfüllen:

- Nachweise über jede kundenspezifische Kontrolle dokumentieren und aufrechterhalten, einschließlich aller Informationen, die in der Kontrollmatrixvorlage in Anhang E1 angegeben sind.
- Eine gezielte Risikoanalyse (PCI DSS-Anforderung 12.3.2) für jede kundenspezifische Kontrolle durchführen und dokumentieren, einschließlich aller Informationen, die in der Vorlage für gezielte Risikoanalysen in Anhang E2 angegeben sind.
- Tests für jede kundenspezifische Kontrolle durchführen, um die Wirksamkeit zu beweisen, und die durchgeführten Tests, die verwendeten Methoden, was getestet wurde, wann die Tests durchgeführt wurden, und die Ergebnisse der Tests in der Kontrollmatrix dokumentieren.
- Nachweise über die Wirksamkeit jeder kundenspezifischen Kontrolle überwachen und aufrechterhalten.
- Abgeschlossene Kontrollmatrix(en), gezielte Risikoanalysen, Testnachweise und Nachweise der kundenspezifischen Wirksamkeit der Kontrollen an seinen Bewerter bereitstellen.

Der Bewerter, der eine Bewertung von kundenspezifischen Kontrollen durchführt, muss die folgenden Kriterien erfüllen:

- Die Kontrollmatrix(en) der Entität, die gezielte Risikoanalyse und den Nachweis der Wirksamkeit der Kontrollen überprüfen, um die kundenspezifische(n) Kontrolle(n) vollständig zu verstehen und um zu verifizieren, dass die Entität alle Dokumentations- und Nachweisanforderungen des kundenspezifischen Ansatzes erfüllt.
- Die geeigneten Testprozeduren, die erforderlich sind, um gründliche Tests jeder kundenspezifischen Kontrolle durchzuführen, ableiten und dokumentieren.
- Jede kundenspezifische Kontrolle testen, um zu bestimmen, ob die Implementierung der Entität 1) die Zielsetzung des kundenspezifischen Ansatzes der Anforderung erfüllt und 2) zu einer Feststellung „an Ort und Stelle“ für die Anforderung führt.
- QSAs halten jederzeit die in den QSA-Qualifikationsanforderungen definierten Unabhängigkeitsanforderungen aufrecht. Das bedeutet, dass ein QSA, der an der Entwicklung oder Implementierung einer kundenspezifischen Kontrolle beteiligt ist, nicht auch Testverfahren für diese kundenspezifische Kontrolle ableitet, bewertet oder bei der Bewertung dieser kundenspezifischen Kontrolle hilft.

Von der Entität und ihrem Assessor wird erwartet, dass sie zusammenarbeiten, um sicherzustellen, dass 1) sie sich einig sind, dass die kundenspezifischen Kontrolle(n) die Zielsetzung des kundenspezifischen Ansatzes vollständig erfüllen, 2) der Bewerter die kundenspezifische Kontrolle vollständig versteht und 3) die Entität die abgeleiteten Tests versteht, die der Bewerter durchführen wird.

Die Verwendung des kundenspezifischen Ansatzes muss von einem QSA oder ISA abgeschlossen und gemäß den Anweisungen in der Vorlage für den Bericht zur Einhaltung (ROC) und den Anweisungen in den *FAQs zur Verwendung mit der ROC-Vorlage für PCI DSS v4.0* dokumentiert werden, die auf der PCI SSC-Website verfügbar sind.

Entitäten, die einen Selbstbewertungsfragebogen ausfüllen, sind nicht berechtigt, einen kundenspezifischen Ansatz zu verwenden; diese Entitäten können sich jedoch dafür entscheiden, dass ein QSA oder ISA ihre Bewertung durchführt und sie in einer ROC-Vorlage dokumentiert.

Die Verwendung des kundenspezifischen Ansatzes kann von Organisationen reguliert werden, die Einhaltungsprogramme verwalten (zum Beispiel Zahlungsmarken und Erwerber). Daher müssen Fragen zur Verwendung eines kundenspezifischen Ansatzes an diese Organisationen weitergeleitet werden, einschließlich zum Beispiel, ob eine Entität verpflichtet ist, einen QSA zu verwenden, oder eine ISA verwenden darf, um eine Bewertung unter Verwendung des kundenspezifischen Ansatzes zu vervollständigen.

Hinweis: *Kompensierende Kontrollen sind beim kundenspezifischen Ansatz keine Option. Da der kundenspezifische Ansatz es einer Entität gestattet, die Kontrollen die zur Erfüllung der Zielsetzung des kundenspezifischen Ansatzes einer Anforderung erforderlich sind, zu bestimmen und zu entwerfen, wird von der Einheit erwartet, dass sie die Kontrollen, die sie für diese Anforderung entworfen hat, effektiv implementiert, ohne dass sie auch alternative, kompensierende Kontrollen implementieren muss.*

Anhang E Beispielvorlagen zur Unterstützung eines Kundenspezifischen Ansatzes

Dieser Anhang enthält Beispielvorlagen für die Kontrollmatrix und eine gezielte Risikoanalyse, die von der Entität als Teil des kundenspezifischen Ansatzes zu dokumentieren sind. Diese Vorlagen sind Beispiele für Formate, die verwendet werden könnten. *Obwohl es nicht erforderlich ist, dass Entitäten die in diesem Anhang bereitgestellten spezifischen Formate befolgen, müssen die Kontrollmatrix und die gezielte Risikoanalyse der Entität alle in diesen Vorlagen definierten Informationen enthalten.*

E1 Beispielhafte Kontrollmatrixvorlage

Das Folgende ist eine beispielhafte Kontrollmatrixvorlage, die eine Entität zum Dokumentieren ihrer kundenspezifischen Implementierung verwenden kann.

Wie in *Anhang D* beschrieben: *Kundenspezifischer Ansatz*, Entitäten, die den kundenspezifischen Ansatz verwenden, müssen eine Kontrollmatrix ausfüllen, um Details für jede implementierte Kontrolle bereitzustellen, die erklären, was implementiert ist, wie die Entität bestimmt hat, dass die Kontrollen die erklärte Zielsetzung einer PCI DSS-Anforderung erfüllen, wie die Kontrolle mindestens das gleiche Niveau des Schutzes bereitstellt, wie er durch die Erfüllung der definierten Anforderung erreicht würde, und wie die Entität Gewissheit über die Wirksamkeit der Kontrolle auf laufender Basis hat.

Der Bewerter verwendet die Informationen in jeder Kontrollmatrix, um die Bewertung zu planen und vorzubereiten.

Diese beispielhafte Kontrollmatrixvorlage enthält die Mindestinformationen, die von der Entität dokumentiert und dem Bewerter für eine kundenspezifische Validierung zur Verfügung gestellt werden müssen. Obwohl es nicht erforderlich ist, diese spezielle Vorlage zu verwenden, ist es erforderlich, dass die kundenspezifische Ansatzdokumentation der Entität alle in dieser Vorlage definierten Informationen enthält und dass die Entität diese genauen Informationen ihrem Bewerter bereitstellt.

Die Kontrollmatrix ersetzt nicht die Notwendigkeit für den Bewerter, unabhängig geeignete Testverfahren zur Validierung der implementierten Kontrollen zu entwickeln. Der Bewerter muss dennoch die erforderlichen Tests durchführen, um zu verifizieren, dass die Kontrollen die Zielsetzung der Anforderung erfüllen, wirksam sind und ordnungsgemäß gewartet werden. Die Kontrollmatrix ersetzt auch nicht die Berichtsanforderungen für kundenspezifische Validierungen, wie in der ROC-Vorlage angegeben.

Die Kontrollmatrix muss mindestens die Informationen in der folgenden Tabelle enthalten.

Beispielhafte Kontrollmatrixvorlage für PCI DSS-Anforderungen, die über den kundenspezifischen Ansatz erfüllt werden **Von der zu beurteilenden Entität auszufüllen**		
Kundenspezifischer Kontrollname/Identifizierer	<Die Entität definiert, wie sie sich auf diese Kontrolle beziehen möchte>	
Anzahl der PCI DSS-Anforderung(en) und Zielsetzung(en), die mit dieser(n) Kontrolle(n) erfüllt werden	Anforderung #: Anforderung #:	Zielsetzung: Zielsetzung:
Details der Kontrolle(n)		
Was ist(sind) die implementierte(n) Kontrolle(n)?	<Die Entität beschreibt, was die Kontrolle ist und was sie tut>	
Wo wird(werden) die Kontrolle(n) implementiert?	<Die Entität identifiziert Standorte von Einrichtungen und Systemkomponenten, an denen die Kontrolle implementiert und verwaltet wird>	
Wann ist(werden) die Kontrolle(n) durchgeführt?	<Die Entität detailliert, wie häufig die Kontrolle durchgeführt wird – zum Beispiel kontinuierlich in Echtzeit ausgeführt wird oder planmäßig zu NN-Zeiten und in XX Intervallen ausgeführt wird>	
Wer hat die Gesamtverantwortung und Rechenschaftspflicht für die Kontrolle(n)?	<Die Entität enthält Angaben zu individuellem Personal/Rollen mit Verantwortung und Rechenschaftspflicht für diese Kontrolle>	
Wer ist an der Verwaltung, Wartung und Überwachung der Kontrolle(n) beteiligt?	<Die Entität umfasst Details zu individuellem Persona/Rollen und/oder Teams, soweit zutreffend, die die Kontrolle verwalten, aufrechterhalten und überwachen>	
Für jede **PCI-DSS-Anforderung, für die die Kontrolle(n) verwendet wird(werden), stellt die Entität Einzelheiten zu Folgendem bereit:**		
Die Entität beschreibt, wie die implementierte(n) Kontrolle(n) die angegebene ***kundenspezifische Ansatz-Zielsetzung*** der PCI DSS-Anforderung erfüllt(erfüllen).	<Die Entität beschreibt, wie die Kontrolle die angegebene kundenspezifische Ansatzzielsetzung der PCI DSS-Anforderung erfüllt, und fasst die verwandten Ergebnisse zusammen>	

Beispielhafte Kontrollmatrixvorlage für PCI DSS-Anforderungen, die über den kundenspezifischen Ansatz erfüllt werden Von der zu beurteilenden Entität auszufüllen	
Die Entität beschreibt die **von ihr durchgeführten Tests** und die Ergebnisse dieser Tests, die zeigen, dass die Kontrolle(n) das Ziel der anwendbaren Anforderung erfüllt(erfüllen).	<Die Entität beschreibt die von ihr durchgeführten Tests, um zu beweisen, dass Kontrolle die angegebene Zielsetzung der PCI DSS-Anforderung erfüllt, und fasst die verwandten Ergebnisse zusammen>
Die Entität beschreibt kurz die Ergebnisse der getrennten gezielten Risikoanalyse, **die sie durchgeführt hat,** die die implementierte(n) Kontrolle(n) erklärt und beschreibt, wie die Ergebnisse verifizieren, dass die Kontrolle(n) mindestens ein gleichwertiges Schutzniveau wie der definierte Ansatz für die anwendbare PCI DSS-Anforderung bereitstellt. *Siehe die getrennte gezielte Risikoanalysevorlage für Details, wie diese Risikoanalyse dokumentiert wird*.	<Die Entität beschreibt kurz die Ergebnisse ihrer Risikoanalyse für diese Kontrolle, die getrennt in der gezielten Risikoanalyse detailliert ist>
Die Entität beschreibt die Maßnahmen, **die sie implementiert hat**, um sicherzustellen, dass die Kontrolle(n) aufrechterhalten und ihre Wirksamkeit kontinuierlich sichergestellt wird. *Zum Beispiel, wie die Entität auf Kontrollen-Wirksamkeit überwacht, wie Kontrollversagen erkannt und darauf reagiert wird und welche Maßnahmen ergriffen werden.*	<Die Entität beschreibt, wie sie sicherstellt, dass die Kontrolle aufrechterhalten wird und wie die Wirksamkeit der Kontrolle sichergestellt wird.>

E2 Beispielhafte gezielte Risikoanalysevorlage

Das Folgende ist ein Beispiel für eine gezielte Risikoanalysevorlage, die eine Entität für ihre kundenspezifische Implementierung verwenden kann. *Obwohl es nicht erforderlich ist, dass eine Entität diesem spezifischen Format folgt, muss ihre kundenspezifische Ansatzdokumentation alle in dieser Vorlage definierten Informationen enthalten.*

Wie in *Anhang D* beschrieben: *Kundenspezifischer Ansatz* und gemäß der PCI DSS-Anforderung 12.3.2 muss eine Entität, die den kundenspezifischen Ansatz verwendet, eine detaillierte gezielte Risikoanalyse für jede Anforderung bereitstellen, die die Entität mit dem kundenspezifischen Ansatz erfüllt. Die Risikoanalyse definiert das Risiko, bewertet die Auswirkungen auf die Sicherheit, wenn die definierte Anforderung nicht erfüllt wird, und beschreibt, wie die Entität festgestellt hat, dass die Kontrollen mindestens ein gleichwertiges Schutzniveau bieten, wie es von der definierten PCI DSS-Anforderung bereitgestellt wird.

Der Bewerter verwendet die Informationen in der gezielten Risikoanalyse, um die Bewertung zu planen und vorzubereiten.

Bei der Vervollständigung einer gezielten Risikoanalyse für einen kundenspezifischen Ansatz, ist es wichtig, an Folgendes zu denken:

- Das Asset, das geschützt wird sind die Karteninhaberdaten, die von der Entität gespeichert, verarbeitet oder übertragen werden.
- Der Bedrohungsakteur ist hochmotiviert und fähig. Die Motivation und Fähigkeiten von Bedrohungsakteuren nehmen tendenziell in Bezug auf die Menge an Karteninhaberdaten zu, die bei einem erfolgreichen Angriff realisiert werden.
- Die Wahrscheinlichkeit, dass eine Entität von Bedrohungsakteuren anvisiert wird, steigt, wenn die Entität größere Mengen an Karteninhaberdaten speichert, verarbeitet oder überträgt.
- Das Unheil steht in direktem Zusammenhang mit der Zielsetzung. Zum Beispiel, wenn die Zielsetzung lautet: „böswillige Software kann nicht ausgeführt werden", dann ist das Unheil, dass böswillige Software ausgeführt wird; wenn die Zielsetzung lautet: „die täglichen Verantwortlichkeiten für die Durchführung aller Aktivitäten werden zugeordnet", dann ist das Unheil, dass die Verantwortlichkeiten nicht zugeordnet werden.

Hinweis: *Der Begriff „Unheil", wie er in dieser gezielten Risikoanalyse verwendet wird (zum Beispiel in 1.3 in der nachstehenden Tabelle), bezieht sich auf ein Vorkommen oder ein Ereignis, das sich negativ auf die Sicherheitshaltung der Entität auswirkt. Beispiele hierfür sind das Fehlen einer Richtlinie, das Versagen, einen Schwachstellenscan auszuführen, oder dass Malware in der Umgebung der Entität ausgeführt wird.*

Diese beispielhafte gezielte Risikoanalysevorlage enthält die Mindestinformationen, die von der Entität dokumentiert und dem Bewerter für eine kundenspezifische Validierung zur Verfügung gestellt werden müssen. Obwohl es nicht erforderlich ist, diese spezielle Vorlage zu verwenden, ist es erforderlich, dass die kundenspezifische Ansatzdokumentation der Entität alle in dieser Vorlage definierten Informationen enthält und dass die Entität diese genauen Informationen ihrem Bewerter bereitstellt.

Die gezielte Risikoanalyse muss mindestens die Informationen in der folgenden Tabelle enthalten.

Beispielhafte gezielte Risikoanalyse für PCI DSS-Anforderungen, die über den kundenspezifischen Ansatz erfüllt werden **Von der zu beurteilenden Entität auszufüllen**	
Punkt	**Details**
1. Die Anforderung identifizieren	
1.1 Die PCI-DSS-Anforderung wie geschrieben identifizieren.	<Die Entität identifiziert die Anforderung>
1.2 Die Zielsetzung der PCI DSS-Anforderung wie geschrieben identifizieren.	<Die Entität identifiziert die Zielsetzung der Anforderung>

Beispielhafte gezielte Risikoanalyse für PCI DSS-Anforderungen, die über den kundenspezifischen Ansatz erfüllt werden Von der zu beurteilenden Entität auszufüllen	
Punkt	**Details**
1.3 Das Unheil beschreiben, das die Anforderung verhindern sollte	<Die Entity beschreibt das Unheil> <Die Entität beschreibt den Effekt auf ihre Sicherheit, wenn das Ziel von der Entität nicht erfolgreich erfüllt wird.> <Die Entität beschreibt, welche Sicherheitsgrundlagen nicht vorhanden wären oder was ein Bedrohungsakteur möglicherweise tun kann, wenn die Zielsetzung von der Entität nicht erfolgreich erfüllt wird.>
2. Die vorgeschlagene Lösung beschreiben	
2.1 Kundenspezifischer Kontrollname/Identifizierer	<Die Entität identifiziert die kundenspezifische Kontrolle wie in der Kontrollmatrix dokumentiert.>
2.2 Welche Teile der geschriebenen Anforderung werden sich in der vorgeschlagenen Lösung ändern?	<Die Entität identifiziert, welche Elemente der Anforderung durch den definierten Ansatz nicht erfüllt werden und daher durch den kundenspezifischen Ansatz abgedeckt werden. Dies kann so klein sein wie die Änderung der Periodizität einer Anforderung oder die Implementierung eines völlig anderen Satzes von Kontrollen, um die Zielsetzung zu erfüllen.>
2.3 Wie wird die vorgeschlagene Lösung das Unheil verhindern?	<Die Entität beschreibt, wie die in der Kontrollmatrix detaillierten Kontrollen das in 1.3 identifizierte Unheil verhindern.>

Beispielhafte gezielte Risikoanalyse für PCI DSS-Anforderungen, die über den kundenspezifischen Ansatz erfüllt werden Von der zu beurteilenden Entität auszufüllen						
Punkt	**Details**					
3. Alle Änderungen der WAHRSCHEINLICHKEIT des Vorkommens von Unheil analysieren, das zu einer Verletzung der Vertraulichkeit von Karteninhaberdaten führt						
3.1 Die in der Kontrollmatrix detaillierten Faktoren, die die Wahrscheinlichkeit beeinflussen, dass das Unheil auftritt, beschreiben.	Die Entität beschreibt: • Wie erfolgreich die Kontrollen bei der Verhinderung des Unheils sein werden • Wie die in der Kontrollmatrix detaillierten Kontrollen die Wahrscheinlichkeit reduzieren, dass das Unheil auftritt					
3.2 Die Gründe beschreiben, warum das Unheil auch nach der Anwendung der kundenspezifischen Kontrolle auftreten kann.	Die Entität beschreibt: • Die typischen Gründe für das Scheitern der Kontrolle, die Wahrscheinlichkeit dafür und wie es verhindert werden könnte • Wie belastbar sind die Prozesse und Systeme der Entität, um zu erkennen, dass die Kontrolle(n) nicht normal funktionieren? • Wie könnte ein Bedrohungsakteur diese Kontrolle umgehen – welche Schritte müsste er unternehmen, wie schwer ist es, würde der Bedrohungsakteur erkannt werden, bevor die Kontrolle fehlschlägt? Wie wurde dies bestimmt?					
3.3 Inwieweit stellen die im kundenspezifischen Ansatz beschriebenen Kontrollen eine Änderung der Wahrscheinlichkeit dar, dass das Unheil auftritt, verglichen mit der Anforderung des definierten Ansatzes?	Unheil mehr wird wahrscheinlich stattfinden	☐	Keine Änderung	☐	Unheil weniger wird wahrscheinlich stattfinden	☐
3.4 Die Argumentation für Ihre Bewertung der Änderung der Wahrscheinlichkeit, dass das Unheil auftritt, bereitstellen, sobald die kundenspezifischen Kontrollen vorhanden sind.	Die Entität stellt bereit: • Die Begründung für die unter 3.3. dokumentierte Bewertung. • Die Kriterien und Werte, die für die Bewertung verwendet wurden, sind unter 3.3 dokumentiert.					

Beispielhafte gezielte Risikoanalyse für PCI DSS-Anforderungen, die über den kundenspezifischen Ansatz erfüllt werden Von der zu beurteilenden Entität auszufüllen				
Punkt	**Details**			
4. Alle Änderungen an den AUSWIRKUNGEN des nicht autorisierten Zugriffs auf Kontodaten analysieren				
4.1 Für den Geltungsbereich der Systemkomponenten, die diese Lösung abdeckt, welche Menge an Kontodaten wäre einem nicht autorisierten Zugriff ausgesetzt, wenn die Lösung ausfallen würde?	**4.1.1** Anzahl der gespeicherten PANs	*Maximal zu einem beliebigen Zeitpunkt*	**4.1.2** Anzahl der über einen Zeitraum von 12 Monaten verarbeiteten oder übertragenen PANs	*Gesamt*
4.2 Beschreibung, wie die kundenspezifischen Kontrollelemente direkt: • Die Anzahl der kompromittierten individuellen PANs reduzieren, wenn ein Bedrohungsakteur erfolgreich ist, und/oder • Eine schnellere Benachrichtigung der Kartenmarken über die kompromittierten PANs gestatten.	Die Auswirkungen auf das Zahlungsökosystem hängen direkt mit der Anzahl der kompromittierten Konten zusammen und wie schnell kompromittierte PANs vom Kartenaussteller gesperrt werden können Die Entität beschreibt, wie die kundenspezifischen Kontrollen Folgendes erreichen, wenn eine der kundenspezifischen Kontrollen: • Die Menge an Karteninhaberdaten reduziert, die gespeichert, verarbeitet oder übertragen werden, und daher das reduziert, was einem erfolgreichen Angreifer zur Verfügung steht, und/oder • Die Zeit bis zur Erkennung, Benachrichtigung über kompromittierte Konten, und Eindämmung des Bedrohungsakteurs verringert.			
5. Risikofreigabe und -überprüfung				
5.1 Ich habe die obige Risikoanalyse überprüft und stimme zu, dass die Verwendung des vorgeschlagenen kundenspezifischen Ansatzes, wie detailliert beschrieben, mindestens ein gleichwertiges Schutzniveau bietet wie der definierte Ansatz für die anwendbare PCI DSS-Anforderung.	Ein Mitglied der Geschäftsleitung muss den vorgeschlagenen individuellen Ansatz überprüfen und ihm zustimmen. <Das Mitglied der Geschäftsleitung der Entität unterzeichnet, dass es den hierin dokumentierten kundenspezifischer Ansatz überprüft und ihm zugestimmt hat.>			
5.2 Diese Risikoanalyse muss spätestens bis zu überprüft und zu aktualisiert werden:	Die Risikoanalyse sollte mindestens alle zwölf Monate und häufiger überprüft werden, wenn der kundenspezifische Ansatz selbst zeitlich begrenzt ist (zum Beispiel, weil ein Technologiewechsel geplant ist) oder wenn andere Faktoren eine notwendige Veränderung diktieren. Geben Sie im Falle einer außerplanmäßigen Risikoüberprüfung den Grund für die Überprüfung an. <Die Entität gibt das Datum an, an dem die gezielte Risikoanalyse überprüft und aktualisiert wurde.>			

Anhang F Einsatz des PCI Software Security Framework zur Unterstützung von Anforderung 6

PCI-DSS-Anforderung 6 definiert Anforderungen für die Entwicklung und Wartung sicherer Systeme und Software. Da der PCI SSC Sichere Software Standard und der Sichere SLC Standard (zusammen das Software Sicherheits-Rahmenwerk) strenge Softwaresicherheitsanforderungen enthalten, kann die Verwendung von maßgeschneiderter und kundenspezifischer Software, die gemäß einem der beiden Standards entwickelt und aufrechterhalten wird, der Entität helfen, mehrere Anforderungen in PCI DSS-Anforderung 6 zu erfüllen, ohne dass zusätzliche detaillierte Tests durchgeführt werden müssen, und kann auch die Verwendung des kundenspezifischen Ansatzes für andere Anforderungen unterstützen. Details siehe Tabelle 7.

Hinweis: *Diese Unterstützung zur Erfüllung von Anforderung 6 gilt nur für Software, die speziell gemäß dem Sicheren Softwarestandard oder dem Sicheren SLC Standard entwickelt und aufrechterhalten wird; sie erstreckt sich nicht auf andere Software- oder Systemkomponenten im Geltungsbereich von Anforderung 6.*

Tabelle 7. Einsatz des PCI Software Security Framework zur Unterstützung von Anforderung 6

PCI DSS-Anforderungen	Wie PCI DSS-Anforderungen auf Software angewandt wird, die gemäß dem Sicheren Softwarestandard entwickelt und gewartet wird	Wie PCI DSS-Anforderungen auf Software angewandt wird, die gemäß dem Sicheren SLC-Standard entwickelt und gewartet wird
6.1 Prozesse und Mechanismen zur Durchführung von Aktivitäten in Anforderung 6 sind definiert und verstanden.	PCI DSS-Anforderungen/Zielsetzungen gelten wie gewohnt.	
6.2 Maßgeschneiderte und kundenspezifische Software wird sicher entwickelt.	Die PCI-DSS-Anforderung 6.2.4 kann für Software, die gemäß dem Sicheren Software-Standard entwickelt und gewartet wird, als vorhanden betrachtet werden.	Die PCI-DSS-Anforderung 6.2 kann für Software, die gemäß dem Sicheren Software-Standard entwickelt und gewartet wird, als vorhanden betrachtet werden.
6.3 Sicherheitsschwachstellen werden identifiziert und sofort adressiert.	PCI DSS-Anforderungen/Zielsetzungen gelten wie gewohnt. Software, die gemäß dem Sicheren SLC-Standard entwickelt und gewartet wird, kann den kundenspezifischen Ansatz für die Zielsetzungen von Anforderung 6.3 unterstützen. Während die Verwendung von Software, die gemäß dem Sicheren SLC-Standard entwickelt und gewartet wird, die Gewissheit bereitstellt, dass der Anbieter Sicherheitspatches und Softwareaktualisierungen zeitnah zur Verfügung stellt, **behält die Entität die Verantwortung** dafür, sicherzustellen, dass Patches und Aktualisierungen gemäß den PCI DSS-Anforderungen installiert werden.	

PCI DSS-Anforderungen	Wie PCI DSS-Anforderungen auf Software angewandt wird, die gemäß dem Sicheren Softwarestandard entwickelt und gewartet wird	Wie PCI DSS-Anforderungen auf Software angewandt wird, die gemäß dem Sicheren SLC-Standard entwickelt und gewartet wird
6.4 Öffentlich zugängliche Webanwendungen sind gegen Angriffe geschützt.	PCI DSS-Anforderungen/Zielsetzungen gelten wie gewohnt.	
6.5 Änderungen an allen Systemkomponenten werden sicher verwaltet.	PCI DSS-Anforderungen/Zielsetzungen gelten wie gewohnt. Software, die gemäß dem Sicheren SLC-Standard entwickelt und gewartet wird, kann den kundenspezifischen Ansatz für die Zielsetzungen von Anforderung 6.5 unterstützen. Während die Verwendung von Software, die gemäß dem Sicheren SLC-Standard entwickelt und aufrechterhalten wird, die Gewissheit bereitstellt, dass der Anbieter Änderungsverwaltungsprozeduren während der Entwicklung von Software und verwandten Aktualisierungen befolgt, **behält die Entität die Verantwortung** dafür, sicherzustellen, dass Software und andere Änderungen an Systemkomponenten gemäß den PCI DSS-Anforderungen in die Produktionsumgebung implementiert werden.	

Verwendung von maßgeschneiderter und kundenspezifischer Software, die von einem sicheren SLC-qualifizierten Anbieter entwickelt und gewartet wird

Bei der Validierung der Verwendung von Software, die von einem qualifizierten Anbieter für Sicheres SLC entwickelt und gewartet wird, um die PCI DSS-Anforderung 6.2 zu erfüllen und den kundenspezifischen Ansatz für Anforderungen 6.3 und 6.5 zu unterstützen, muss der Bewerter bestätigen, dass Folgendes erfüllt ist:

- Der Softwareanbieter ist aktuell in der PCI SSC Liste der für Sicheren SLC qualifizierten Anbieter aufgeführt, d. h. die Validierung ist nicht abgelaufen.
- Die Software wurde unter Verwendung von Softwarelebenszyklus-Verwaltungspraktiken entwickelt und gewartet, die als Teil der Validierung des Softwareanbieters bewertet wurden.
- Die Entität folgt den Implementierungsanleitungen, die vom Qualifizierter Anbieter von Sicherer SLC bereitgestellt werden.

Verwendung von maßgeschneiderter und benutzerdefinierter Software, die gemäß dem Sicheren SLC-Standard entwickelt wurde

Entitäten, die intern Software ausschließlich für ihre Verwendung entwickeln oder die Software für die Verwendung durch eine einzelne Entität entwickeln, können sich dafür entscheiden, einen Sicheren SLC-Bewerter zu beauftragen, um ihre Softwarelebenszyklus-Verwaltungspraktiken anhand des Sicheren SLC-Standards zu bewerten. Der Sichere SLC-Bewerter dokumentiert die Ergebnisse der Bewertung in einem Sicheren SLC_einhaltungsbericht (ROC) und einer Sicheren SLC-Einhaltungsbescheinigung (AOC).

Software, die gemäß Softwarelebenszyklus-Verwaltungspraktiken entwickelt und aufrechterhalten wird, stellt die gleiche Unterstützung für PCI DSS-Anforderung 6 bereit wie Software, die von einem Sicheren SLC-qualifizierten Anbieter entwickelt und aufrechterhalten wird, wenn diese Praktiken von einem Sicheren SLC-Bewerter bewertet und bestätigt wurden, dass sie die Sicheren SLC-Standard-Anforderungen erfüllen Anforderungen, wobei die Ergebnisse in einem sicheren SLC ROC und AOC dokumentiert werden.

Validierung der Verwendung des Sicheren SLC-Standards

Bei der Validierung der Verwendung von Software, die gemäß dem Sicheren SLC Standard entwickelt und aufrechterhalten wurde, um die PCI DSS-Anforderung 6.2 zu erfüllen und den kundenspezifischen Ansatz für die Anforderungen 6.3 und 6.5 zu unterstützen, muss der Bewerter bestätigen, dass Folgendes erfüllt ist:

- Die Softwarelebenszyklus-Verwaltungspraktiken wurden von einem Sicheren SLC-Bewerter bewertet und bestätigt, dass sie alle Anforderungen des Sicheren SLC-Standards erfüllen, wobei die Ergebnisse in einem Sicheren SLC-Bericht über die Einhaltung (ROC) und einer Sicheren SLC-Bescheinigung der Einhaltung (AOC) dokumentiert sind.
- Die Software wurde unter Verwendung der Softwarelebenszyklus-Verwaltungspraktiken entwickelt und aufrechterhalten, die von der Sicheren SLC-Bewertung abgedeckt werden.
- Eine vollständige Sichere SLC-Bewertung der Softwarelebenszyklus-Verwaltungspraktiken wurde innerhalb der letzten 36 Monate durchgeführt. Zusätzlich, wenn die letzte vollständige Sichere SLC-Bewertung vor mehr als 12 Monaten stattgefunden hat, wurde vom Entwickler/Anbieter innerhalb der letzten 12 Monate eine jährliche Bescheinigung bereitgestellt, die die fortgesetzte Einhaltung des Sicheren SLC-Standards für die verwendeten Softwarelebenszyklus-Verwaltungspraktiken bestätigt.

Validierung der Verwendung des Sicheren Software-Standards

Bei der Validierung der Verwendung von Software, die gemäß dem Sicheren Software Standard entwickelt und aufrechterhalten wurde, um die PCI DSS-Anforderung 6.2.4 zu erfüllen und den kundenspezifischen Ansatz für die Anforderungen 6.3 und 6.5 zu unterstützen, muss der Bewerter bestätigen, dass Folgendes erfüllt ist:

- Die Sichere Software-Bewertung wurde von einem Sicheren Software-Bewerter durchgeführt und bestätigte, dass sie alle Anforderungen des Sicheren Software Standards erfüllt, wobei die Ergebnisse in einem Sicheren Software-Validierungsbericht (ROV) und einer Sicheren Software Bescheinigung der Validierung (AOV) dokumentiert werden.
- Die Software wurde unter Verwendung der Softwarelebenszyklus-Verwaltungspraktiken entwickelt und aufrechterhalten, die von der Sicheren Software Bewertung abgedeckt werden.
- Innerhalb der letzten 36 Monate wurde eine vollständige Sichere Software Bewertung durchgeführt. Zusätzlich, wenn die letzte vollständige Sichere Software Bewertung vor mehr als 12 Monaten stattgefunden hat, wurde vom Entwickler/Anbieter innerhalb der letzten 12 Monate eine jährliche Bescheinigung bereitgestellt, die die fortgesetzte Einhaltung des Sicheren Software Standards bestätigt.

Anhang G PCI-DSS-Glossar von Begriffen, Abkürzungen und Akronymen

Begriff	Definition
Abschneiden	Methode zum Unlesbarmachen einer vollständigen PAN durch Entfernen eines Segments von PAN-Daten. Das Abschneiden bezieht sich auf den Schutz der PAN, wenn sie elektronisch gespeichert, verarbeitet oder übertragen wird. Siehe Maskierung zum Schutz der PAN bei Anzeige auf Bildschirmen, Papierbelegen usw.
Administratorzugriff	Erhöhte oder erweiterte Privilegien, die einem Konto für dieses Konto gewährt werden, um Systeme, Netzwerke und/oder Anwendungen zu verwalten. Der Administratorzugriff kann dem Konto einer Person oder einem integrierten Systemkonto zugewiesen werden. Konten mit Administratorzugriff werden je nach Betriebssystem und Organisationsstruktur häufig als „Superbenutzer“, „Root“, „Administrator“, „Admin“, „Sysadmin“ oder „Aufsichtsbehörden-Staat“ bezeichnet.
AES	Akronym für „Erweiterter Verschlüsselungsstandard.” Siehe Starke Kryptographie.
Änderungskontrolle	Prozesse und Prozeduren, um Änderungen an Systemen und Software auf Auswirkungen vor der Implementierung zu überprüfen, zu testen und zu genehmigen.
ANSI	Akronym für „American National Standards Institute.”
Anti-Malware	Software, die entwickelt wurde, um verschiedene Formen böswilliger Software zu erkennen, zu entfernen, zu blockieren oder einzudämmen.
Anwendung	Umfasst alle gekauften, kundenspezifischen und maßgeschneiderten Softwareprogramme oder Programmgruppen, einschließlich sowohl interner als auch externer (zum Beispiel Web-)Anwendungen.
Anwendungs- und Systemkonten	Auch als „Dienstleistungskonten“ bezeichnet. Kontendie Prozesse ausführen oder Aufgaben auf einem Computersystem oder in einer Anwendung durchführen. Diese Konten verfügen normalerweise über erhöhte Berechtigungen, die zum Durchführen spezieller Aufgaben oder Funktionen erforderlich sind und sind normalerweise keine Konten, die von einer Person verwendet werden.
AOC	Akronym für „Einhaltungsbescheinigung“. Die AOC ist das offizielle PCI SSC-Formular für Händler und Dienstleistungsanbieter, um die Ergebnisse einer PCI DSS-Bewertung zu bescheinigen, wie sie in einem Selbstbewertungsfragebogen (SAQ) oder Einhaltungsbericht (ROC) dokumentiert sind.
ASV	Akronym für „Zugelassenem Scanning-Anbieter.” Vom PCI SSC zugelassenes Unternehmen zur Ausführung externer Schwachstellen-Scanning-Dienstleistungen.

Begriff	Definition
Audit-Protokoll	Auch als „Audit-Pfad“ bezeichnet. Chronologische Aufzeichnung von Systemaktivitäten. Stellt einen unabhängig verifizierbaren Pfad bereit, der ausreicht, um die Rekonstruktion, Überprüfung und Untersuchung der Abfolge von Umgebungen und Aktivitäten zu erlauben, die den Betrieb, die Prozedur oder das Ereignis in einer Transaktion vom Beginn bis zum Endergebnis umgeben oder dazu führen.
Ausstellende Dienstleistungen	Beispiele für ausstellende Dienstleistungen umfassen und Autorisierung und Kartenpersonalisierung, sind aber nicht darauf beschränkt.
Aussteller	Auch als „ausstellende Bank“ oder „ausstellendes Finanzinstitut“ bezeichnet. Entität, die Zahlungskarten ausstellt oder Ausstellungsdienstleistungen durchführt, erleichtert oder unterstützt, einschließlich, aber nicht beschränkt auf ausstellende Banken und ausstellende Verarbeiter.
Authentifizierung	Prozess zur Verifizierung der Identität einer Person, eines Geräts oder eines Prozesses. Die Authentifizierung erfolgt typischerweise mit einem oder mehreren Authentifizierungsfaktoren. Siehe Konto, Authentifizierungs-Anmeldeinformationen, und Authentifizierungsfaktor.
Authentifizierungs-Anmeldeinformationen	Kombination aus der Benutzer-ID oder Konto-ID plus dem/den Authentifizierungsfaktor(en), der/die zum Authentifizieren einer Person, eines Geräts oder eines Prozesses verwendet wird/werden. Siehe Konto und Authentifizierungsfaktor.
Authentifizierungsfaktor	Das Element, das verwendet wird, um die Identität einer Person oder eines Prozesses auf einem Computersystem nachzuweisen oder zu verifizieren. Authentifizierung erfolgt typischerweise mit einem oder mehreren Authentifizierungsfaktoren: • Eine Information wie ein Passwort oder eine Passphrase • Ein Besitz wie ein Token-Gerät oder eine Smartcard • Etwas Persönliches, wie ein biometrisches Element. Die ID (oder Konto) und Authentifizierungsfaktor werden zusammen als Authentifizierungsnachweise betrachtet.” Siehe Konto und Authentifizierungs-Anmeldeinformationen.
Autorisierung	Im Zusammenhang mit der Zugriffskontrolle ist die Autorisierung die Gewährung von Zugriffs- oder anderen Rechten für einen Benutzer, ein Programm oder einen Prozess. Die Autorisierung definiert, was eine Person oder ein Programm nach erfolgreicher Authentifizierung tun kann. Im Zusammenhang mit einer Zahlungskartentransaktion bezieht sich die Autorisierung auf den Autorisierungsprozess, der abgeschlossen wird, wenn ein Händler eine Transaktionsantwort erhält (zum Beispiel eine Genehmigung oder Ablehnung).
BAU	Akronym für „Geschäft wie gewohnt."

Begriff	Definition
CDE	Akronym für „Karteninhaberdatenumgebung.“ Die CDE besteht aus: • Die Systemkomponenten, Personen und Prozesse, die Karteninhaberdaten und/oder sensible Authentifizierungsdaten speichern, verarbeiten und übertragen, und/oder • Systemkomponenten, die keine CHD/SAD speichern, verarbeiten oder übertragen dürfen, aber uneingeschränkt mit Systemkomponenten verbunden sind, die CHD/SAD speichern, verarbeiten oder übertragen.
CERT	Akronym für "Computer-Notfallreaktionsteam".
CIS	Akronym für „Zentrum für Internetsicherheit“
CVSS	Akronym für „Gemeinsames Bewertungssystem für Schwachstellen“. Weitere Informationen finden Sie im ASV-Programmleitfaden.
Datenflussdiagramm	Ein Diagramm, das zeigt, wie Daten durch eine Anwendung, ein System oder ein Netzwerk fließen.
Definierter Ansatz	Siehe „Ansätze zur Implementierung und Validierung von PCI DSS“ in PCI DSS Anforderungen und Sicherheitsbewertungsprozeduren.
Dienstleistungsanbieter	Geschäftsentität, die keine Zahlungsmarke ist und direkt an der Verarbeitung, Speicherung oder Übertragung von Karteninhaberdaten im Auftrag einer anderen Entität beteiligt ist. Dieses umfasst Zahlungs-Gateways, Zahlungs-Dienstleistungsanbieter (PSPs) und unabhängige Vertriebsorganisationen (ISOs). Dies umfasst auch Unternehmen, die Dienstleistungen anbieten, die die Sicherheit von Karteninhaberdaten kontrollieren oder sich auf sie auswirken könnten. Beispiele umfassen verwaltete Dienstleistungsanbieter, die verwaltete Firewalls, IDS und andere Dienstleistungen bereitstellen, sowie Hosting-Anbieter und andere Entitäten. Wenn eine Entität eine Dienstleistung bereitstellt, die nur die Bereitstellung eines öffentlichen Netzwerkzugriffs einbezieht – wie ein Telekommunikationsunternehmen, das nur die Kommunikationsverbindung bereitstellt –, würde die Entität nicht als Dienstleistungsanbieter für diese Dienstleistung betrachtet (obwohl sie als Dienstleistungsanbieter für andere Dienstleistungen angesehen werden kann). Siehe Multi-Mandantenanbieter und Dritter Dienstleistungsanbieter. Drei- oder vierstelliger Wert im Magnetstreifen, der auf das Ablaufdatum der Zahlungskarte auf den Verfolgungsdaten folgt. Es wird für verschiedene Dinge verwendet, wie zum Definieren von Dienstleistungsattributen, zum Unterscheiden zwischen internationalem und nationalem Austausch oder zum Identifizieren von Nutzungsbeschränkungen.
DMZ	Abkürzung für „entmilitarisierte Zone“. Physisches oder logisches Unternetzwerk, das dem internen privaten Netzwerk einer Organisation eine zusätzliche Sicherheitsebene bietet.
DNS	Akronym für „Domänennamensystem".

Begriff	Definition
Doppelte Kontrolle	Prozess der Verwendung von zwei oder mehr separaten Entitäten (normalerweise Personen), die zusammenarbeiten, um sensible Funktionen oder Informationen zu schützen. Beide Einheiten sind gleichermaßen für den physischen Schutz von Materialien verantwortlich, die an anfälligen Transaktionen beteiligt sind. Es ist keiner einzelnen Person gestattet, auf die Materialien (zum Beispiel den kryptografischen Schlüssel) zuzugreifen oder diese zu verwenden. Für die manuelle Schlüsselerzeugung, -beförderung, -ladung, -speicherung und -wiedergewinnung erfordert doppelte Kontrolle die Aufteilung der Kenntnis des Schlüssels unter den Entitäten. Siehe Gespaltenes Wissen.
Drittanbieter von Dienstleistungen (TPSP)	Jeder Dritte, der als Dienstleistungsanbieter im Namen einer Entität handelt. Siehe Multi-Mandantenanbieter und Dienstleistungsanbieter.
ECC	Akronym für „Elliptische-Kurven-Kryptographie." Siehe Starke Kryptographie.
E-Commerce (web) Umleitungsserver	Ein Server, der einen Kundenbrowser von der Website eines Händlers an einen anderen Ort zur Zahlungsabwicklung während einer E-Commerce-Transaktion umleitet.
Entfernbare elektronische Medien	Medien, die digitalisierte Daten speichern, die leicht entfernt und/oder von einem Computersystem zu einem anderen transportiert werden können. Beispiele für entfernbare elektronische Medien umfassen CD-ROM, DVD-ROM, USB-Flash-Laufwerke und externe/tragbare Festplatten. In diesem Zusammenhang umfassen entfernbare elektronische Medien keine Hot-Swap-fähigen Laufwerke, Bandlaufwerke, die für Massen-Backups verwendet werden, oder andere Medien, die normalerweise nicht zum Transport von Daten von einem Standort zur Verwendung an einem anderen verwendet werden.
Entität	Begriff, der verwendet wird, um das Unternehmen, die Organisation oder das Geschäft, zu vertreten, das einer PCI DSS-Bewertung unterzogen wird.
Erwerber	Auch als „Handelsbank“, „erwerbende Bank“ oder „erwerbendes Finanzinstitut“ bezeichnet. Entität, in der Regel ein Finanzinstitut, das Zahlungskartentransaktionen für Händler verarbeitet und von einer Zahlungsmarke als Erwerber definiert wird. Erwerber unterliegen den Regeln und Prozeduren für Zahlungsmarken bezüglich der Händler-Einhaltung. Siehe Zahlungsverarbeiter.
Fernzugriff	Zugriff auf das Netzwerk einer Entität von einem Standort außerhalb dieses Netzwerks. Ein Beispiel für eine Technologie für den Fernzugriff ist ein VPN.
Festplattenverschlüsselung	Technik oder Technologie (entweder Software oder Hardware) zum Verschlüsseln aller gespeicherten Daten auf einem Gerät (zum Beispiel einer Festplatte oder einem Flash-Laufwerk). Alternativ wird Verschlüsselung auf Dateiebene oder Datenbankverschlüsselung auf Spaltenebene verwendet, um Inhalte bestimmter Dateien oder Spalten zu verschlüsseln.
Firewall	Hardware- und/oder Softwaretechnologie, die Netzwerkressourcen vor nicht autorisiertem Zugriff schützt. Eine Firewall erlaubt oder verweigert Computerverkehr zwischen Netzwerken mit unterschiedlichen Sicherheitsstufen basierend auf einer Reihe von Regeln und anderen Kriterien.

Begriff	Definition
Forensik	Auch als „Computerforensik“ bezeichnet. Da sie sich auf Informationssicherheit bezieht, die Anwendung von Untersuchungstools und Analysetechniken, um Beweise aus Computerressourcen zu sammeln, um die Ursache von Datenkompromittierungen zu bestimmen. Untersuchungen zur Kompromittierung von Zahlungsdaten werden in der Regel von einem PCI Forensischen Ermittler (PFI) durchgeführt.
FTP	Akronym für „Dateiübertragungsprotokoll.“ Netzwerkprotokoll zur Übertragung von Daten von einem Computer zu einem anderen über ein öffentliches Netzwerk wie das Internet. FTP wird weitgehend als unsicheres Protokoll angesehen, da Passwörter und Dateiinhalte ungeschützt und im Klartext gesendet werden. FTP kann sicher über SSH oder andere Technologien implementiert werden.
Generierung des kryptografischen Schlüssels	Die Schlüsselgenerierung ist eine der Funktionen innerhalb der Schlüsselverwaltung. Die folgenden Dokumente stellen anerkannte Anleitungen zur ordnungsgemäßen Schlüsselgenerierung bereit: • *NIST Special Publication 800-133: Empfehlung für die Generierung kryptografischer Schlüssel* • *ISO 11568-2 Finanzdienstleistungen – Schlüsselverwaltung (Einzelhandel) — Teil 2: Symmetrische Chiffren, ihre Schlüsselverwaltung und ihr Lebenszyklus* – 4.3 Schlüsselgenerierung • *ISO 11568-4 Finanzdienstleistungen – Schlüsselverwaltung (Einzelhandel) — Teil 4: Asymmetrische Kryptosysteme – Schlüsselverwaltung und Lebenszyklus* – 6.2 Schlüssel-Lebenszyklusphasen - Generierung • *European Payments Council EPC 342-08 Richtlinien zur Verwendung von Algorithmen und zur Schlüsselverwaltung* – 4.1.1 Schlüsselgenerierung [für symmetrische Algorithmen] – 4.2.1 Schlüsselgenerierung [für asymmetrische Algorithmen]
Geringste Privilegien	Das Mindestmaß an Privilegien, das erforderlich ist, um die Rollen und Verantwortlichkeiten der Jobfunktion durchzuführen.
Gespaltenes Wissen	Eine Methode, bei der zwei oder mehr Entitäten getrennt Schlüsselkomponenten oder Schlüsselanteile haben, die einzeln keine Kenntnis des resultierenden kryptografischen Schlüssels vermitteln.
Gezielte Risikoanalyse	Für PCI DSS-Zwecke eine Risikoanalyse, die sich auf eine oder mehrere bestimmte PCI DSS-Anforderung(en) von Interesse konzentriert, entweder weil die Anforderung Flexibilität erlaubt (zum Beispiel in Bezug auf die Häufigkeit) oder, für den kundenspezifischen Ansatz, um zu erklären, wie die Entität das Risiko bewertet hat und bestimmt hat, dass die kundenspezifische Kontrolle die Zielsetzung einer PCI-DSS-Anforderung erfüllt.

Begriff	Definition
Händler	Für die Zwecke des PCI DSS wird ein Händler als jede Entität definiert, die Zahlungskarten mit den Logos einer am PCI SSC teilnehmenden Zahlungsmarke als Zahlung für Waren und/oder Dienstleistungen akzeptiert. Ein Händler, der Zahlungskarten als Zahlungsmittel für Waren und/oder Dienstleistungen akzeptiert, kann auch ein Dienstleistungsanbieter sein, wenn die verkauften Dienstleistungen dazu führen, dass Karteninhaberdaten im Auftrag anderer Händler oder Dienstleistungsanbieter gespeichert, verarbeitet oder übertragen werden. Zum Beispiel ist ein ISP ein Händler, der Zahlungskarten für die monatliche Abrechnung akzeptiert, aber auch ein Dienstleistungsanbieter, wenn er Händler als Kunden hostet.
Hashing	Eine Methode zum Schützen von Daten, die Daten in einen Nachrichtenauszug mit fester Länge konvertiert. Hashing ist eine einseitige (mathematische) Funktion, bei der ein nicht geheimer Algorithmus eine Nachricht beliebiger Länge als Eingabe nimmt und eine Ausgabe fester Länge erzeugt (normalerweise als „Hash-Code“ oder „Meldungsübersicht“ bezeichnet). Hash-Funktionen müssen die folgenden Eigenschaften haben: • Es ist rechnerisch nicht möglich, die ursprüngliche Eingabe nur anhand des Hash-Codes zu bestimmen. • Es ist rechnerisch nicht möglich, zwei Eingaben zu finden, die denselben Hash-Code angeben.
HSM	Akronym für „Hardware-Sicherheitsmodul“ oder „Host-Sicherheitsmodul“. Ein physisch und logisch geschütztes Hardwaregerät, das einen sicheren Satz kryptografischer Dienstleistungen bereitstellt, die für kryptografische Schlüsselverwaltungsfunktionen und/oder die Entschlüsselung von Kontodaten verwendet werden.
IDS	Akronym für „Eindringungs-Erkennungs-System.“
Interaktive Anmeldung	Der Prozess von einer Person, die Authentifizierungs-Anmeldeinformationen bereitstellt, um sich direkt bei einem Anwendungs- oder Systemkonto anzumelden.
IPS	Akronym für „Eindringungs-Verhinderungs-System.“
ISO	Akronym für „International Organization for Standardization.”
Karteninhaber	Kunde, für den eine Zahlungskarte ausgestellt wurde, oder jede Person, die zur Verwendung der Zahlungskarte autorisiert ist.
Karteninhaberdaten (CHD)	Karteninhaberdaten bestehen mindestens aus der vollständigen PAN. Karteninhaberdaten können auch in Form der vollständigen PAN plus Folgendes erscheinen: Name des Karteninhabers, Ablaufdatum und/oder Dienstleistungscode. Siehe Sensible Authentifizierungsdaten für zusätzliche Datenelemente, die möglicherweise im Rahmen einer Zahlungstransaktion übertragen oder verarbeitet (aber nicht gespeichert) werden.
Karten-Skimmer	Ein physisches Gerät, das häufig an ein legitimes Kartenlesegerät angeschlossen ist und dazu dient, die Informationen einer Zahlungskarte unrechtmäßig zu erfassen und/oder zu speichern.

Begriff	Definition
Kartenverifizierungscode	Wird auch als Kartenvalidierungscode oder -wert oder Kartensicherheitscode bezeichnet. Für PCI-DSS-Zwecke ist er der drei- oder vierstellige Wert, der auf der Vorder- oder Rückseite einer Zahlungskarte aufgedruckt ist. Kann entsprechend den individuellen teilnehmenden Zahlungsmarken als CAV2, CVC2, CVN2, CVV2 oder CID bezeichnet werden. Wenden Sie sich für weitere Informationen an die teilnehmenden Zahlungsmarken.
Klartextdaten	Unverschlüsselte Daten.
Kommerziell von der Stange (COTS)	Beschreibung von Produkten, die Lagerartikel sind, die nicht speziell für einen bestimmten Kunden oder Benutzer angepasst oder entwickelt wurden und zur Verwendung sofort verfügbar sind.
Kompensierende Kontrollen	Siehe PCI DSS Anhänge B und C
Kompromittierung	Auch als „Datenkompromittierung“ oder „Datenverletzung“ bezeichnet. Eindringen in ein Computersystem, bei dem der Verdacht besteht, dass nicht autorisierte Offenlegung/Diebstahl, Änderung oder Zerstörung von Karteninhaberdaten vorliegt.
Konsole	Direkt angeschlossener Bildschirm und/oder Tastatur, die den Zugriff auf und die Kontrolle eines Servers, Mainframe-Computers oder eines anderen Systemtyps erlaubt. Siehe Zugriff ohne Konsole.
Konto	Wird auch als „Benutzer-ID“, „Konto-ID“ oder „Anwendungs-ID“ bezeichnet. Wird verwendet, um eine Person oder einen Prozess auf einem Computersystem zu identifizieren. Siehe Authentifizierungs-Anmeldeinformationen und Authentifizierungsfaktor.
Kontodaten	Kontodaten bestehen aus Karteninhaberdaten und/oder sensiblen Authentifizierungsdaten Siehe Karteninhaberdaten und Sensible Authentifizierungsdaten.
Kritische Systeme	Ein System oder eine Technologie, die von der Entität als besonders wichtig erachtet wird. Zum Beispiel kann ein kritisches System für die Durchführung eines Geschäftsbetriebs oder für die Aufrechterhaltung einer Sicherheitsfunktion wesentlich sein. Beispiele für kritische Systeme umfassen häufig Sicherheitssysteme, öffentlich zugängliche Geräte und Systeme, Datenbanken und Systeme, die Karteninhaberdaten speichern, verarbeiten oder übertragen.
Kryptografischer Schlüssel	Ein Parameter, der in Verbindung mit einem kryptografischen Algorithmus verwendet wird, der für Betriebe wie die folgenden verwendet wird: • Umwandlung von Klartextdaten in Chiffretextdaten, • Umwandlung von Chiffretextdaten in Klartextdaten, • Eine aus Daten berechnete digitale Unterschrift, • Verifizierung einer aus Daten berechneten digitalen Unterschrift, • Ein aus Daten berechneter Authentifizierungscode, oder • Eine Vereinbarung zum Austausch eines gemeinsamen Geheimnisses. Siehe *Starke Kryptographie.*

Begriff	Definition
Kryptographischer Algorithmus	Auch als „Verschlüsselungsalgorithmus“ bezeichnet. Ein klar spezifizierter umkehrbarer mathematischer Prozess, der zum Umwandeln von Klartextdaten in verschlüsselte Daten und umgekehrt verwendet wird. Siehe Starke Kryptographie.
Kryptoperiode	Die Zeitspanne, in der ein kryptografischer Schlüssel für seinen definierten Zweck verwendet werden kann. Wird häufig in Bezug auf den Zeitraum definiert, für den der Schlüssel aktiv ist, und/oder die Menge an Chiffretext, die vom Schlüssel erzeugt wurde, und gemäß bewährten Praktiken und Richtlinien der Branche (zum Beispiel NIST Special Publication 800-57).
Kundenspezifischer Ansatz	Siehe „PCI DSS-Abschnitt: 8Ansätze zur Implementierung und Validierung von PCI DSS“.
LAN	Akronym für „lokales Netzwerk."
LDAP	Akronym für „Leichtes Verzeichniszugriffsprotokoll.”
Logische Zugriffskontrolle	Mechanismen, die die Verfügbarkeit von Informationen oder informationsverarbeitenden Ressourcen nur auf autorisierte Personen oder Anwendungen beschränken... Siehe Physische Zugriffskontrolle.
MAC	In Kryptografie, ein Akronym für „Authentifizierungscode der Nachricht“. Siehe Starke Kryptographie.
Magnetstreifendaten	Siehe Nachverfolgungsdaten.
Maskierung	Methode zum Verbergen eines PAN-Segments, wenn es angezeigt oder gedruckt wird. Die Maskierung wird verwendet, wenn keine geschäftliche Notwendigkeit besteht, die gesamte PAN anzuzeigen. Maskierung bezieht sich auf den Schutz der PAN bei Anzeige auf Bildschirmen, Papierbelegen, Ausdrucken usw.
Maskierung	Siehe Abschneiden für den Schutz der PAN, wenn sie elektronisch gespeichert, verarbeitet oder übertragen wird.
Maßgeschneiderte und kundenspezifische Software	Maßgeschneiderte Software wird für die Entität von einem Dritten im Namen der Entität und gemäß den Spezifikationen der Entität entwickelt. Kundenspezifische Software wird von der Entität für den eigenen Gebrauch entwickelt.
Medien	Physisches Material, einschließlich, aber nicht beschränkt auf elektronische Speichergeräte, entfernbare elektronische Medien und Berichte in Papierform.
MO/TO	Akronym für „Versandbestellung/Telefonbestellung.“
Multi-Faktor-Authentifizierung	Methode zur Authentifizierung eines Benutzers, bei dem mindestens zwei Faktoren verifiziert werden. Diese Faktoren umfassen etwas, das der Benutzer hat (wie eine Smartcard oder ein Dongle), etwas, das der Benutzer weiß (wie ein Passwort, eine Passphrase oder eine PIN) oder etwas, das der Benutzer ist oder tut (wie Fingerabdrücke und andere biometrische Elemente).

Begriff	Definition
Multi-Mandanten-Dienstleistungsanbieter	Eine Art von dritten Dienstleistungsanbietern, die verschiedene geteilte Dienstleistungen an Händler und andere Dienstleistungsanbieter anbietet, bei denen Kunden Systemressourcen gemeinsam nutzen (wie physische oder virtuelle Server), Infrastruktur, Anwendungen (einschließlich Software als eine Dienstleistung (SaaS)) und/oder DatenbankenDienstleistungen können Hosten von mehreren Entitäten auf einem einzigen geteilten Server, Bereitstellen von E-Commerce und/oder „Warenkorb"-Dienstleistungen, web-basierte Host-Dienstleistungen, Zahlungsanwendungen, verschiedene Cloudanwendungen und Dienstleistungen, und Verbindung zu Zahlungs-gateways und –prozessoren einschließen, sind aber nicht darauf beschränkt. Siehe Dienstleistungsanbieter und Dritte Dienstleistungsanbieter.
NAC	Akronym für „Netzwerkzugriffskontrolle."
Nachverfolgungsdaten	Auch als „vollständige Verfolgungsdaten" oder „Magnetstreifendaten" bezeichnet. Im Magnetstreifen oder Chip verschlüsselte Daten, die zur Authentifizierung und/oder Autorisierung bei Zahlungsvorgängen verwendet werden. Kann das Magnetstreifenbild auf einem Chip oder die Verfolgungsdaten auf dem Magnetstreifen sein.
NAT	Akronym für „Netzwerkadressübersetzung."
Netzwerkdiagramm	Ein Diagramm, das Systemkomponenten und Verbindungen innerhalb einer vernetzten Umgebung zeigt.
Netzwerksicherheitskontrollen (NSC)	Firewalls und andere Netzwerksicherheitstechnologien, die als Durchsetzungspunkte für Netzwerkrichtlinien fungieren. NSCs kontrollieren normalerweise den Netzwerkverkehr zwischen zwei oder mehr logischen oder physischen Netzwerksegmenten (oder Unternetzen) basierend auf vordefinierten Richtlinien oder Regeln.
Netzwerkverbindung	Ein logischer, physischer oder virtueller Kommunikationspfad zwischen Geräten, der das Senden und Empfangen von Netzwerkschichtpaketen gestattet.
Nicht vertrauenswürdiges Netzwerk	Jedes Netzwerk, das nicht der Definition eines „vertrauenswürdigen Netzwerks" erfüllt.
NIST	Akronym für „National Institute of Standards and Technology." Nicht regulierende Bundesbehörde in den USA Technologieadministration des Handelsministeriums.
NTP	Akronym für „Netzwerkzeitprotokoll".
Objekt auf Systemebene	Alles auf einer Systemkomponente, das für deren Betrieb erforderlich ist, einschließlich, aber nicht beschränkt auf ausführbare Anwendungsdateien und Konfigurationsdateien, Systemkonfigurationsdateien, statische und gemeinsam genutzte Bibliotheken und DLLs, ausführbare Systemdateien, Gerätetreiber und Gerätekonfigurationsdateien, und Komponenten von Dritten.
Organisatorische Unabhängigkeit	Eine organisatorische Struktur, die sicherstellt, dass kein Interessenkonflikt zwischen der Person oder Abteilung, die die Aktivität durchführt, und der Person oder Abteilung, die die Aktivität bewertet, besteht. Zum Beispiel sind Personen, die Bewertungen durchführen, organisatorisch von der Verwaltung der zu bewertenden Umgebung getrennt.
OWASP	Akronym für „Offenes Webanwendungs-Sicherheitsprojekt."

Begriff	Definition
PAN	Akronym für „Primäre Kontonummer (PAN).” Eindeutige Zahlungskartennummer (Kredit-, Debit- oder Prepaid-Karten usw.), die den Aussteller und das Karteninhaberkonto identifiziert.
Passwort / Passphrase	Eine Zeichenfolge, die als Authentifizierungsfaktor für einen Benutzer oder ein Konto dient.
Patch	Vorhandene Software aktualisieren, um Funktionen hinzuzufügen oder einen Fehler zu korrigieren.
PCI DSS	Akronym für „Payment Card Industry Data Security Standard“ (Zahlungskartenbranche Datensicherheitsstandard).
Personal	Vollzeit- und Teilzeitbeschäftigte, Zeitarbeitskräfte, Auftragnehmer und Berater mit Sicherheitsverantwortungen für den Schutz von Kontodaten oder die sich auf die Sicherheit von Kontodaten auswirken können.
Physische Zugriffskontrolle	Mechanismen, die den Zugriff auf einen physischen Raum oder eine Umgebung nur Mechanismen, die den Zugang zu einem physischen Raum oder einer Umgebung nur auf autorisierte Personen beschränken. Siehe Logische Zugriffskontrolle.
PIN	Akronym für "persönliche Identifizierungsnummer."
PIN-Block	Ein Datenblock, der zum Einkapseln einer PIN während der Verarbeitung verwendet wird. Das PIN-Blockformat definiert den Inhalt des PIN-Blocks und wie er verarbeitet wird, um die PIN abzurufen. Der PIN-Block besteht aus der PIN, der PIN-Länge und kann die PAN (oder eine Kürzung davon) enthalten, abhängig von dem verwendeten zugelassenen ISO-PIN-Blockformat.
POI	Akronym für „Punkt der Wechselwirkung“, der Ausgangspunkt, an dem Daten von einer Karte gelesen werden.
Punkt des Verkaufs-System (POS)	Hardware und Software, die von Händlern verwendet wird, um Zahlungen von Kunden zu akzeptieren. Kann-POI-Geräte, Pin-Pads, elektronische Bargeldregister usw. Einschließen.
Privilegierter Benutzer	Ein Benutzerkonto mit mehr als grundlegenden Zugriffsprivilegien. Diese Konten haben typischerweise erhöhte oder erweiterte Privilegien mit mehr Rechten als ein Standardbenutzerkonto. Der Umfang der Privilegien über verschiedene privilegierte Konten hinweg kann jedoch je nach Organisation, Jobfunktion oder Rolle und verwendeter Technologie stark variieren.
Protokoll	Siehe Audit-Protokoll.
QIR	Akronym für „Qualifizierter Integrator oder Wiederverkäufer.“ Siehe das QIR Program Guide auf der PCI SSC-Website für mehr Informationen.
QSA	Akronym für „Qualifizierter Sicherheitsbewerter.“ QSAs sind vom PCI SSC für die Durchführung von PCI DSS-Bewertungen vor Ort qualifiziert. Siehe dazu die QSA Qualifizierungsanforderungen über Details zu den Anforderungen für QSA-Unternehmen und -Mitarbeiter.

Begriff	Definition
Risikobewertung	Unternehmensweiter Prozess, der wertvolle Systemressourcen und Bedrohungen identifiziert; quantifiziert Verlustexpositionen (d. h. das Verlustpotenzial) basierend auf geschätzten Häufigkeiten und Kosten des Auftretens; und empfiehlt (optional), wie Ressourcen für Gegenmaßnahmen zugeordnet werden, um die Gesamtexposition zu minimieren. Siehe Gezielte Risikoanalyse. Prozess der Risikoklassifizierung, um Elemente in der Reihenfolge ihrer Wichtigkeit zu identifizieren, zu priorisieren und zu adressieren.
ROC	Akronym für „Bericht zur Einhaltung." Berichtstool zur Dokumentation detaillierter Ergebnisse der PCI DSS-Bewertung einer Entität.
RSA	Algorithmus zur Öffentlicher Schlüssel-Verschlüsselung. Siehe Starke Kryptographie.
SAQ	Akronym für „Fragebogen zur Selbstbewertung". Berichtstool zur Dokumentation von Ergebnissen der PCI DSS-Selbstbewertung einer Entität.
Schlüsselverwalter	Eine Rolle, bei der eine oder mehrere Personen mit der Erfüllung von Schlüsselverwaltungsaufgaben betraut und dafür verantwortlich sind, die geheime und/oder private Schlüssel, Schlüsselanteile oder Schlüsselkomponenten im Namen einer Entität einbeziehen.
Schlüsselverwaltungssystem	Eine Kombination aus Hardware und Software, die einen integrierten Ansatz zum Generieren, Verteilen und/oder Verwalten kryptografischer Schlüssel für Geräte und Anwendungen bereitstellt.
Scoping	Prozess zur Identifizierung aller Systemkomponenten, Personen und Prozesse, die in eine PCI DSS-Bewertung einbezogen werden sollen. Siehe „Geltungsbereich der PCI-DSS-Anforderungen" in den PCI DSS-Anforderungen und Sicherheitsbewertungsprozeduren.
Segmentierung	Wird auch als „Netzwerksegmentierung" oder „Isolation" bezeichnet. Segmentierung isoliert Systemkomponenten, die Karteninhaberdaten speichern, verarbeiten oder übertragen, von Systemen, die dies nicht tun. Siehe „Segmentierung" in dem PCI DSS-Abschnitt: 4 Scope von PCI DSS-Anforderungen.
Sensible Authentifizierungsdaten (SAD)	Sicherheitsbezogene Informationen, die verwendet werden, um Karteninhaber zu authentisieren und/oder Zahlungskartentransaktionen autorisieren. Diese Informationen umfassen, sind aber nicht beschränkt auf Verifizierungscodes/-werte für die Kartenvalidierung, vollständige Verfolgungsdaten (vom Magnetstreifen oder einem gleichwertigen Chip), PINs und PIN-Sperren.

Begriff	Definition
Sensibler Bereich	Ein sensibler Bereich ist in der Regel eine Teilmenge der CDE und jeder Bereich, in dem sich Systeme befinden, die als kritisch für die CDE betrachtet werden. Dies umfasst Rechenzentren, Serverräume, Backoffice-Räume an Einzelhandelsstandorten und alle Bereiche, die die Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten konzentriert oder zusammenfasst. Sensible Bereiche umfassen auch Bereiche, die Systeme unterbringen, die die Sicherheit der CDE verwalten oder aufrechterhalten (zum Beispiel solche, die Netzwerksicherheitskontrollen bereitstellen oder die physische oder logische Sicherheit verwalten). Davon ausgenommen sind Bereiche, in denen nur Verkaufsstellen-Terminals vorhanden sind, wie die Kassenbereiche in einem Einzelhandelsgeschäft oder Callcenter, in denen Agenten Zahlungen entgegennehmen.
Sichere Codierung	Der Prozess der Erstellung und Implementierung von Anwendungen, die gegen Manipulation und/oder Kompromittierung resistent sind.
Sicherheitsbeauftragter	Primäre Person, die für die Sicherheit einer Entität verantwortlich ist.
Sicherheitsereignis.	Ein Vorfall, der von einer Organisation als potenzielle Auswirkungen auf die Sicherheit für ein System oder seine Umgebung zu haben angesehen wird. Im Zusammenhang mit PCI DSS identifizieren Sicherheitsereignisse verdächtige oder anomale Aktivitäten.
SNMP	Akronym für „Einfaches Netzwerkverwaltungsprotokoll“.
Software von Dritten	Software, die von einer Entität erworben, aber nicht ausdrücklich für diese entwickelt wurde. Es kann Offene Quelle, Freeware, Shareware oder gekauft sein.
Spaltenebene Datenbankverschlüsselung	Technik oder Technologie (entweder Software oder Hardware) zum Verschlüsseln des Inhalts einer bestimmten Spalte in einer Datenbank gegen den vollständigen Inhalt der gesamten Datenbank. Alternativ siehe Festplattenverschlüsselung und Verschlüsselung auf Dateiebene.
SQL	Akronym für „Strukturierte Abfragesprache."
SSH	Abkürzung für „Secure Shell“.
SSL	Akronym für „Secure Sockets Layer.”
Standardkonto	Anmeldekonto, das in einem System, einer Anwendung, oder einem Gerät vordefiniert ist, um den anfänglichen Zugriff zu gestatten, wenn das System zum ersten Mal in Betrieb genommen wird. Als Teil des Installationsvorgangs können auch zusätzliche Standardkonten vom System generiert werden.
Standardpasswort	Passwort für Systemadministration, Benutzer oder Dienstleistungskonten die in einem System, einer Anwendung, oder einem Gerät vordefiniert sind; das normalerweise mit dem Standardkonto verbunden ist. Standardkonten und Passwörter sind veröffentlicht und bekannt und daher leicht zu erraten.

Begriff	Definition
Starke Kryptographie	Kryptographie ist eine Methode zum Schutz von Daten durch einen umkehrbaren Verschlüsselungsprozess und ein grundlegendes Primitiv, das in vielen Sicherheitsprotokollen und -dienstleistungen verwendet wird. Starke Kryptografie basiert auf branchengetesteten und anerkannten Algorithmen zusammen mit Schlüssellängen, die mindestens 112 Bit effektive Schlüsselstärke und ordnungsgemäße Schlüsselverwaltungspraktiken bereitstellen. Die effektive Schlüsselstärke kann kürzer sein als die tatsächliche „Bit"-Länge des Schlüssels, was dazu führen kann, dass Algorithmen mit größeren Schlüsseln einen geringeren Schutz bieten als Algorithmen mit kleineren tatsächlichen, aber größeren effektiven Schlüsselgrößen. *Es wird empfohlen, dass alle neuen Implementierungen eine effektive Schlüsselstärke von mindestens 128 Bit verwenden.* Beispiele für Branchenreferenzen zu kryptografischen Algorithmen und Schlüssellängen umfassen: • *NIST Special Publication 800-57 Teil 1*, • *BSI TR-02102-1*, • *ECRYPT-CSA D5.4 Algorithms, Key Size and Protocols Report (2018)*, und • *ISO/IEC 18033- Encryption Algorithms, und* • *ISO/IEC 14888-3:2-81 IT Security techniques – Digital signatures with appendix Teil 3: Discrete logarithm based mechanisms*
Systemkomponenten	Alle Netzwerkgeräte, Server, Computergeräte, virtuellen Komponenten oder Software, die in der CDE enthalten oder mit ihr verbunden sind oder die sich auf die Sicherheit der CDE auswirken könnten.
TDES	Akronym für „Triple Data Encryption Standard." Auch als „3DES" oder „Triple DES" bezeichnet.
Teilnehmende Zahlungsmarke	Auch als „Zahlungsmarke" bezeichnet. Eine Zahlungskartenmarke, die zum fraglichen Zeitpunkt dann offiziell als (oder ein verbundenes Unternehmen von) Mitglied des PCI SSC gemäß seinen maßgeblichen Dokumenten zugelassen wird. Zum Zeitpunkt der Abfassung dieses Berichts gehören zu den teilnehmenden Zahlungsmarken PCI SSC-Gründungsmitglieder und strategische Mitglieder.
Telnet	Abkürzung für „Telefon-Netzwerk-Protokoll."
TLS	Akronym für „Sicherheit der Transportschicht".
Token	Im Zusammenhang mit Authentifizierung und Zugriffskontrolle ist ein Token ein Wert, der von Hardware oder Software bereitgestellt wird, die mit einem Authentifizierungsserver oder VPN zusammenarbeitet, um eine dynamische oder Multi-Faktor-Authentifizierung durchzuführen.
Trennung von Aufgaben	Die Praxis, Schritte in einer Funktion auf mehrere Personen aufzuteilen, um zu verhindern, dass eine einzelne Person den Prozess untergräbt.
Überwachung der Dateiintegrität (FIM)	Eine Änderungserkennungslösung, die Änderungen, Hinzufügungen und Löschungen an kritischen Dateien überprüft, und benachrichtigt, wenn solche Änderungen erkannt werden.

Begriff	Definition
Verbraucher	Individueller Karteninhaber kauft Waren, Dienstleistungen oder beides.
Verletzlichkeit	Fehler oder Schwäche, die, wenn sie ausgenutzt wird, zu einer absichtlichen oder unabsichtlichen Kompromittierung eines Systems führen kann.
Verschlüsselter kryptographischer Hash	Eine Hashing-Funktion, die einen zufällig generierten geheimen Schlüssel enthält, um brutale Gewalt-Angriffs-Widerstand und die Integrität der geheimen Authentifizierung bereitzustellen. Geeignete verschlüsselte kryptografische Hashing-Algorithmen beinhalten, sind aber nicht beschränkt auf: HMAC, CMAC und GMAC mit einer effektiven kryptografischen Stärke von mindestens 128 Bit (NIST SP 800-131Ar2). Im Folgenden finden Sie weitere Informationen über HMAC, CMAC und GMAC: NIST SP 800-107r1, NIST SP 800-38B, und NIST SP 800-38D). Siehe NIST SP 800-107 (Revision 1): Empfehlung für Anwendungen, die zugelassene Hash-Algorithmen verwenden §5.3.
Verschlüsselung	Die (umkehrbare) Umwandlung von Daten durch einen kryptografischen Algorithmus, um Chiffretext zu erzeugen, d. h. den Informationsinhalt der Daten zu verbergen. Siehe Starke Kryptographie.
Verschlüsselung auf Dateiebene	Technik oder Technologie (entweder Software oder Hardware) zum Verschlüsseln des vollständigen Inhalts bestimmter Dateien. Alternativ siehe Festplattenverschlüsselung und Datenbankverschlüsselung auf Spaltenebene.
Verschlüsselungsalgorithmus	Siehe Kryptographischer Algorithmus.
Vertrauenswürdiges Netzwerk	Netzwerk einer Entität das von der Entität kontrolliert oder verwaltet werden kann und das die anwendbaren PCI DSS-Anforderungen erfüllt.
Verwaltung des kryptografischen Schlüssels	Der Satz von Prozessen und Mechanismen, die die Etablierung und Wartung kryptografischer Schlüssel unterstützen, einschließlich des Ersetzens älterer Schlüssel durch neue Schlüssel, falls erforderlich.
Verzeichnistoken	Ein Zufallswert aus einer Tabelle mit Zufallswerten, der einem bestimmten PAN entspricht.
Virtualization	Die logische Abstraktion von Rechenressourcen von physischen und/oder logischen Beschränkungen. Eine gängige Abstraktion wird als virtuelle Maschinen oder VMs bezeichnet, die den Inhalt einer physischen Maschine nimmt und ihr gestattet, auf unterschiedlicher physischer Hardware und/oder zusammen mit anderen virtuellen Maschinen auf derselben physischen Hardware zu arbeiten. Andere gängige Abstraktionen umfassen, sind aber nicht beschränkt auf Container, serverloses Computing oder Mikrodienstleistungen.
Virtuelles Zahlungsterminal	Im Zusammenhang mit dem Fragebogen zur Selbstbewertung (SAQ) C-VT, ist ein virtuelles Zahlungsterminal ein webbrowserbasierter Zugriff auf einen Erwerber, Verarbeiter oder die Website eines dritten Dientleistungsanbieters, um Zahlungskartentransaktionen zu autorisieren, wenn der Händler Zahlungskartendaten über einen Webbrowser manuell eingibt. Im Gegensatz zu physischen Terminals lesen virtuelle Zahlungsterminals die Daten nicht direkt von einer Zahlungskarte. Da Zahlungskartentransaktionen manuell eingegeben werden, werden in Händlerumgebungen mit geringem Transaktionsvolumen typischerweise virtuelle Zahlungsterminals anstelle von physischen Terminals verwendet.

Begriff	Definition
VPN	Akronym für "virtuelles privates Netzwerk."
Web Anwendung	Eine Anwendung, auf die im Allgemeinen über einen Webbrowser oder über Webdienstleistungen zugegriffen wird. Webanwendungen können über das Internet oder ein privates, internes Netzwerk verfügbar sein.
Zahlungskarte	Für Zwecke des PCI DSS jeder Zahlungskarten-Formfaktor, der das Logo einer am PCI SSC teilnehmenden Zahlungsmarke trägt.
Zahlungskarten-Formfaktor	Umfasst physische Zahlungskarten sowie Geräte mit Funktionalität, die eine Zahlungskarte emulieren, um eine Zahlungstransaktion einzuleiten. Beispiele für solche Geräte umfassen, sind aber nicht beschränkt auf Smartphones, Smartwatches, Fitnessarmbänder, Schlüsselanhänger und Tragbares wie Schmuck.
Zahlungsmarke	Eine Organisation mit gebrandeten Zahlungskarten oder anderen Formfaktoren für Zahlungskarten. Zahlungsmarken regeln, wo und wie die Zahlungskarten oder andere Formfaktoren, die ihre Marke oder ihr Logo tragen, verwendet werden. Eine Zahlungsmarke kann eine am PCI SSC teilnehmende Zahlungsmarke oder eine andere globale oder regionale Zahlungsmarke, ein System oder ein Netzwerk sein.
Zahlungskanal	Methoden,. Die von Händlern verwendet werden, um Zahlungen von Kunden zu akzeptieren. Übliche Zahlungskanäle schließen Karte vorhanden (bei der Person), und Karte nicht vorhanden (E-Commerce unde MO/TO) ein.
Zahlungsseite	Eine webbasierte Benutzerschnittstelle, die ein oder mehrere Formelemente enthält, die Kontodaten von einem Verbraucher erfassen oder erfasste Kontodaten vorlegen sollen. Die Zahlungsseite kann wie folgt gerendert werden: • Ein einzelnes Dokument oder eine Instanz, • Ein Dokument oder eine Komponente, die in einem Inline-Rahmen innerhalb einer Nichtzahlungsseite angezeigt wird, Mehrere Dokumente oder Komponenten, die jeweils ein oder mehrere Formelemente enthalten, die in mehreren Inline-Rahmen innerhalb einer Nichtzahlungsseite enthalten sind.
Zahlungsseitenskripts	Alle Programmiersprachenbefehle oder Anweisungen auf einer Zahlungsseite, die vom Browser eines Verbrauchers verarbeitet und/oder interpretiert werden, einschließlich Befehlen oder Anweisungen, die mit dem Dokumentobjektmodell einer Seite interagieren. Beispiele für Programmiersprachen sind JavaScript und VB-Script; weder Markup-Sprachen (zum Beispiel HTML) noch Style-Regeln (zum Beispiel CSS) sind Programmiersprachen.
Zahlungsverarbeiter	Manchmal auch als „Zahlungs-Gateway“ oder „Zahlungsdienstleistungsanbieter (PSP)“ bezeichnet. Entität, die von einem Händler oder einer anderen Entität beauftragt wurde, Zahlungskartentransaktionen in deren Namen abzuwickeln. Siehe Erwerber.
Zugriff ohne Konsole	Logischer Zugriff auf eine Systemkomponente, der über eine Netzwerkschnittstelle statt über eine direkte, physische Verbindung zur Systemkomponente erfolgt. Der Zugriff ohne Konsole umfasst den Zugriff aus lokalen/internen Netzwerken sowie den Zugriff aus externen oder entfernten Netzwerken.