Ein priorisierter Ansatz für das Erreichen von PCI DSS-Compliance

Der Zahlungskartenbranche Datensicherheitsstandard (PCI DSS) stellt eine ausführliche Struktur bestehend aus 12 Anforderungen für den Schutz von Karteninhaberdaten dar, die von Händlern und anderen Unternehmen/Organisationen gespeichert, verarbeitet und/oder elektronisch übermittelt werden. Aufgrund seines umfassenden Geltungsbereichs bietet der Standard eine große Fülle von Informationen zum Themenkomplex Sicherheit. Diese Informationen sind dermaßen umfangreich, dass sich viele mit dem Schutz von Karteninhaberdaten befasste Personen fragen, an welcher Stelle sie mit der Einführung von Compliance beginnen sollen. Aus diesem Grund hat das PCI Security Standards Council den folgenden, so genannten „priorisierten Ansatz“ entwickelt, der Stakeholder dabei unterstützt, Ansatzpunkte für eine frühzeitige Risikominimierung im Compliance-Prozess zu identifizieren. Keiner der Meilensteine im priorisierten Ansatz sorgt für umfassende Sicherheit oder Compliance mit PCI DSS. Durch Befolgen des Ansatzes können Stakeholder jedoch den Prozess zum Schutz von Karteninhaberdaten beschleunigen.

HIGHLIGHTS

Unterstützt Händler beim Erkennen von Hochrisikozielen

Erläutert die grundlegenden Schritte bei der Implementierung von PCI DSS und Bewertungen

Händler können anhand von Meilensteinen ihren Fortschritt im Compliance-Prozess nachweisen

Was versteht man unter dem priorisierten Ansatz?

Der priorisierte Ansatz umfasst sechs Sicherheitsmeilensteine, mit denen Händler und andere Unternehmen/Organisationen auf ihrem Weg zu vollständiger PCI DSS-Compliance ihren Schutz gegen Hochrisikofaktoren Schritt für Schritt ausbauen und Bedrohungen eskalieren können. Der priorisierte Ansatz und seine Meilensteine (siehe Seite 2) bieten die folgenden Vorteile:

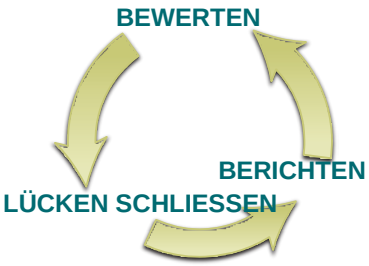
- Ein klar strukturierter Plan, den eine Organisation befolgen kann, um Risiken nach Prioritäten anzugehen
- Ein pragmatischer Ansatz, der schnelle Erfolge verspricht
- Unterstützung der finanziellen und betrieblichen Planung
- Vorgabe von Zielen mit messbaren Fortschrittsindikatoren
- Förderung von Konsistenz unter den Prüfern

Ziele des priorisierten Ansatzes

Der priorisierte Ansatz ist ein Fahrplan mit Compliance-Aktivitäten basierend auf den Risiken, die mit der Speicherung, Verarbeitung und/oder Übertragung von Karteninhaberdaten verbunden sind. Der Fahrplan ermöglicht eine Priorisierung von Schritten in Richtung Compliance, gibt Meilensteine vor und ermöglicht eine im Compliance-Prozess frühzeitige Minderung des Risikos von Sicherheitsverletzungen bei Karteninhaberdaten. Acquirer erhalten zudem eine Möglichkeit zur objektiven Messung von Compliance-Aktivitäten und der Risikoreduzierung durch Händler, Dienstanbieter und andere. Der priorisierte Ansatz wurde unter Einbeziehung von Erkenntnissen aus tatsächlichen Sicherheitsverletzungen sowie Rückmeldungen von Qualified Security Assessors, Forensic Investigators und dem PCI Security Standards Council Board of Advisors entwickelt. Er ist weder als Ersatz, Abkürzung oder Überbrückung für die Erreichung vollständiger PCI DSS-Compliance gedacht, noch handelt es sich dabei um eine allgemeingültige Rahmenvorgabe, die auf jede Organisation passt. Der priorisierte Ansatz eignet sich für Händler, die eine Vor-Ort-Bewertung durchführen oder SAQ D nutzen.

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.

DIE PCI DSS-COMPLIANCE IST EIN FORTLAUFENDER PROZESS



PCI SSC-GRÜNDER

TEILNEHMENDE UNTERNEHMEN/ORGANISATIONEN

Händler, Banken, Verarbeitungsunternehmen, Entwickler und Point-of-Sale-Anbieter

Haftungsausschluss

Zum Erreichen von PCI DSS-Compliance muss eine Organisation/ein Unternehmen alle PCI DSS-Anforderungen erfüllen. Die Reihenfolge, in der diese umgesetzt werden, oder ob die Organisation dabei dem priorisierten Ansatz für PCI DSS folgt, ist unerheblich. Mit diesem Dokument werden PCI DSS oder eine seiner Anforderungen weder abgeändert noch überbrückt. Das Dokument kann jederzeit ohne vorherige Ankündigung geändert werden.
PCI SSC ist nicht verantwortlich für Fehler oder Schäden jeglicher Art, die aus der Verwendung der hier enthaltenen Informationen entstehen. PCI SSC macht keine Zusicherungen und übernimmt keine Garantien für die Richtigkeit der hier dargebotenen Informationen und lehnt jede Verantwortung oder Haftung hinsichtlich des korrekten oder falschen Gebrauchs dieser Informationen ab.

Meilensteine für die Priorisierung der PCI DSS Compliance-Schritte

Der priorisierte Ansatz besteht aus sechs Meilensteinen. In der nachfolgenden Tabelle sind die allgemeinen Ziele und Vorsätze jedes Meilensteins beschrieben. Im restlichen Dokument werden diese Meilensteine in alle zwölf PCI DSS-Anforderungen und untergeordneten Anforderungen eingegliedert.

Meilenstein	Ziele
1	**Entfernen von vertraulichen Authentifizierungsdaten und Begrenzung des Datenaufbewahrungszeitraums.** Dieser Meilenstein zielt auf eines der Hauptrisiken ab, das in Organisationen/Unternehmen bereits zu Sicherheitsverletzungen geführt hat. Denken Sie daran: Vertrauliche Authentifizierungsdaten, die nicht gespeichert werden, mindern das Risiko einer Sicherheitsverletzung enorm. Daten, die nicht benötigt werden, sollten nicht gespeichert werden!
2	**Schützen von Systemen und Netzwerken und Maßnahmen zur Vorbereitung auf eine Sicherheitsverletzung.** Bei diesem Meilenstein geht es um die wirksame Kontrolle von Einfallspunkten und geeignete Reaktionen auf Sicherheitsverletzungen.
3	**Sichere Zahlungskartenanwendungen.** Dieser Meilenstein zielt auf Maßnahmen zur Kontrolle von Anwendungen, Anwendungsprozessen und Anwendungsservern ab. Schwächen in diesem Bereich öffnen Sicherheitsverletzungen und dem Diebstahl von Karteninhaberdaten Tür und Tor.
4	**Überwachung und Kontrolle des Zugriffs auf Systeme.** Die mit diesem Meilenstein umgesetzten Kontrollmaßnahmen ermöglichen es Ihnen festzustellen, welche Personen wann und wie auf welche Ressourcen, Ihr Netzwerk und Ihre CDE Zugriff haben.
5	**Schutz gespeicherter Karteninhaberdaten** Für Organisationen, die ihre Geschäftsprozesse analysiert und herausgefunden haben, dass sie PANs speichern müssen, beinhaltet der fünfte Meilenstein Hinweise zu Mechanismen zum Schutz dieser Daten.
6	**Finalisieren aller Compliance-Aufgaben und Sicherstellen, dass alle Kontrollmaßnahmen funktionieren.** Im sechsten Meilenstein geht es um die abschließende Umsetzung der PCI DSS-Anforderungen und die Erfüllung aller verbleibenden zugehörigen Richtlinien, Verfahren und Prozesse zum Schutz einer CDE.

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
Anforderung 1: Installation und Aufrechterhaltung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten						
1.1 Festlegen von Standards für die Firewall- und Router-Konfiguration, die Folgendes beinhalten:						
1.1.1 Förmlicher Prozess zur Genehmigung und zum Testen aller Netzwerkverbindungen und Änderungen an der Firewall-und Router-Konfiguration						6
1.1.2 Ein aktuelles Netzwerkdiagramm mit allen Verbindungen zwischen der CDE und anderen Netzwerken, einschließlich aller drahtlosen Netzwerke	1					
1.1.3 Aktuelles Diagramm mit den system- und netzwerkübergreifenden Flüssen von Karteninhaberdaten	1					
1.1.4 Einrichtung einer Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone		2				
1.1.5 Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die Verwaltung der Netzwerkkomponenten						6
1.1.6 Dokumentation der Begründung und Genehmigung für den Einsatz aller zulässigen Services, Protokolle und Ports, einschließlich der Dokumentation von Sicherheitsfunktionen für die Protokolle, die als unsicher gelten.		2				
1.1.7 Prüfung der Firewall- und Router-Regelsätze mindestens alle sechs Monate						6
1.2 Aufbau von Firewall- und Router-Konfigurationen, die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der CDE einschränken. *Hinweis: Ein „nicht vertrauenswürdiges Netzwerk" ist jedes Netzwerk, das außerhalb der Netzwerke liegt, die zu der geprüften Einheit gehören und/oder das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Einheit liegt.*						
1.2.1 Beschränken des ein- und ausgehenden Datenverkehrs auf das für die CDE notwendige Maß und ausdrückliche Ablehnung des gesamten sonstigen Datenverkehrs.		2				
1.2.2 Sichern und Synchronisieren von Router-Konfigurationsdateien.		2				
1.2.3 Installieren von Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der CDE und Konfigurieren dieser Firewalls, sodass der gesamte Verkehr zwischen der drahtlosen Umgebung und der CDE abgelehnt bzw. nur dann zugelassen wird, wenn es sich um autorisierten und für die Geschäftszwecke notwendigen Datenverkehr handelt.		2				
1.3 Verbieten des direkten öffentlichen Zugriffs zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung.						
1.3.1 Implementieren einer DMZ, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene, öffentlich zugängliche Dienste, Protokolle und Ports anbieten.		2				
1.3.2 Beschränken des eingehenden Internetverkehrs auf IP-Adressen innerhalb der DMZ.		2				
1.3.3 Implementierung von Anti-Spoofing-Maßnahmen zur Erkennung und Blockierung gefälschter Quell-IP-Adressen, über die auf das Netzwerk zugegriffen wird. (So kann beispielsweise der Datenverkehr blockiert werden, der trotz einer internen Quelladresse über das Internet zuzugreifen versucht.)		2				
1.3.4 Unterbindung von nicht autorisiertem ausgehenden Datenverkehr von der CDE zum Internet.		2				
1.3.5 Lassen Sie nur "etablierte" Verbindungen zum Netzwerk zu.		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
1.3.6 Speichern von Systemkomponenten mit Karteninhaberdaten (z. B. Datenbank) in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauenswürdigen Netzwerken getrennt ist.		2				
1.3.7 Vermeidung der Weitergabe privater IP-Adressen und Routing-Informationen an unbefugte Dritte. *Hinweis: Zu den Methoden zum Verbergen von IP-Adressen zählen unter anderem:* • *Network Address Translation (NAT);* • *Platzieren von Servern mit Karteninhaberdaten hinter Proxy-Servern/Firewalls;* • *Löschen oder Filtern von Route-Advertisements für private Netzwerke, die registrierte Adressen verwenden;* • *Interne Nutzung eines RFC1918-Adressraums anstatt registrierter Adressen.*		2				
1.4 Installieren von persönlicher Firewall-Software oder einer gleichwertige Funktion auf allen mobilen und/oder den Mitarbeitern gehörenden Geräten, die außerhalb des Netzwerks auf das Internet zugreifen (z. B. Laptops, die von Mitarbeitern verwendet werden) und die auch für den Zugriff auf das CDE eingesetzt werden. Firewall (oder gleichwertige Funktion) Konfigurationen umfassen: • Spezifische Konfigurationseinstellungen sind definiert. • Die persönliche Firewall (oder gleichwertige Funktion) ist aktiv. • Die persönliche Firewall (oder gleichwertige Funktion) kann nicht von Benutzern des mobilen Computergerätes geändert werden.		2				
1.5 Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung der Firewalls müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.		2				
Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden						
2.1 Änderung der Standardeinstellungen des Anbieters und Entfernung bzw. Deaktivierung unnötiger Standardkonten stets vor der Installation eines Systems im Netzwerk. Dies gilt für SÄMTLICHE Standardkennwörter, wie etwa die von Betriebssystemen, Sicherheitssoftware, Anwendungs-und Systemkonten, POS (Point of Sale, Verkaufsstelle)-Terminals, Zahlungsanwendungen, SNMP (Simple Network Management Protocol)-Community-Zeichenfolgen usw.).		2				
2.1.1 Ändern SÄMTLICHER Standardeinstellungen der Anbieter von Drahtlossystemen, einschließlich der Standard-Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen bei drahtlosen Umgebungen, die mit der CDE verbunden sind oder Karteninhaberdaten übertragen.		2				
2.2 Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Schwachstellen adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit akzeptierter Standards zur Systemstabilisierung zählen unter anderem: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institut • National Institute of Standards and Technology (NIST)			3			

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
2.2.1 Implementieren Sie nur eine primäre Funktion pro Server, um zu vermeiden, dass auf einem Server gleichzeitig mehrere Funktionen mit verschiedenen Sicherheitsniveauanforderungen existieren. (Webserver, Datenbankserver und DNS sollten beispielsweise auf separaten Servern implementiert sein.) *Hinweis: Wenn Virtualisierungstechnologien eingesetzt werden, implementieren Sie pro virtuelle Systemkomponente nur eine primäre Funktion.*			3			
2.2.2 Ausschließliches Aktivieren notwendiger Dienste, Protokolle, Daemons usw. entsprechend dem Bedarf der Systemfunktion.			3			
2.2.3 Implementieren Sie zusätzliche Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft werden. *Hinweis: Wenn SSL/eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 erfüllt werden.*		2				
2.2.4 Konfigurieren von Systemsicherheitsparametern zur Missbrauchsvermeidung.			3			
2.2.5 Entfernen aller unnötigen Funktionen wie z. B. Skripts, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver.			3			
2.3 Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs mithilfe einer starken Kryptographie. *Hinweis: Wenn SSL/eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 erfüllt werden.*		2				
2.4 Pflege eines Bestands an Systemkomponenten für den PCI-DSS.		2				
2.5 Sicherheitsrichtlinien und betriebliche Verfahren zur Verwaltung von Anbieterstandards und sonstigen Sicherheitsparametern müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.		2				
2.6 Anbieter von gemeinsam genutzten Hosting-Services müssen die gehostete Umgebung und Karteninhaberdaten aller Einheiten schützen. Diese Anbieter müssen bestimmte Anforderungen erfüllen, wie in Anhang A1: Zusätzliche PCI DSS-Anforderungen für gemeinsam verwendete Hosting-Anbieter.			3			
Anforderung 3: Schutz gespeicherter Karteninhaberdaten						
3.1 Beschränkung der Speicherung von Karteninhaberdaten auf ein Minimum durch Implementierung von Richtlinien und Verfahren zur Datenaufbewahrung und -löschung, die zumindest folgende Punkte für die Speicherung von Karteninhaberdaten umfassen: • Begrenzen der Speichermenge und der Aufbewahrungszeit auf die für rechtliche, gesetzliche und/oder geschäftliche Zwecke festgelegten Vorgaben. • Spezifische Aufbewahrungsanforderungen für Karteninhaberdaten • Prozesse zum Löschen von Daten, sobald diese nicht mehr benötigt werden. • Ein vierteljährlicher Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten, die den festgelegten Aufbewahrungszeitraum überschritten haben.	1					
3.2 Speichern Sie keine vertraulichen Authentifizierungsdaten nach der Autorisierung (auch wenn diese verschlüsselt sind). Falls vertrauliche Authentifizierungsdaten empfangen werden, müssen sämtliche Daten nach Abschluss des Autorisierungsprozesses so gelöscht werden, dass sie nicht wiederhergestellt werden können. Kartenemittenten und Unternehmen, die Ausstellungsdienste unterstützen, dürfen in den folgenden Fällen vertrauliche Authentifizierungsdaten speichern: • wenn es eine geschäftliche Begründung gibt • wenn die Daten sicher gespeichert werden Vertrauliche Authentifizierungsdaten umfassen die Daten, die in den folgenden Anforderungen 3.2.1 bis 3.2.3 aufgeführt sind:	1					

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
3.2.1 Speichern Sie nach der Autorisierung nicht den gesamten Inhalt einer Spur (auf dem Magnetstreifen auf der Kartenrückseite, in einem Chip oder an anderer Stelle). Diese Daten werden auch als Spurdaten, Full-Track-Daten, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet. Hinweis: Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden: • Der Name des Karteninhabers • Primäre Kontonummer (Englisch: Primary Account Number, PAN) • Ablaufdatum • Servicecode Um das Risiko zu minimieren, speichern Sie nur die betrieblich benötigten Datenelemente.	1					
3.2.2 Speichern Sie nach der Autorisierung nicht den Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte, der zur Verifizierung bei Transaktionen verwendet wird, bei denen die Karte nicht physisch vorliegt).	1					
3.2.3 Speichern Sie nach der Autorisierung keine persönlichen Identifizierungsnummern (PIN) oder verschlüsselten PIN-Blöcke.	1					
3.3 Maskieren Sie die PAN bei der Anzeige (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden), so dass nur Mitarbeiter mit einem rechtmäßigen geschäftlichen Grund mehr als die ersten sechs/die letzten vier Ziffern der PAN einsehen können. *Hinweis: Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten – z. B. bei juristischen Anforderungen und Anforderungen der Kreditkartenunternehmen an POS-Belege.*					5	
3.4 Unleserlich machen der PAN an allen Speicherorten (auch auf tragbaren digitalen Medien, Sicherungsmedien und in Protokollen). Setzen Sie dazu eines der folgenden Verfahren ein: • Unidirektionale Hashes, die auf einer starken Kryptographie basieren (es muss von der vollständigen PAN ein Hash erstellt werden); • Abkürzung (Hashing kann nicht verwendet werden, um das abgekürzte Segment der PAN zu ersetzen); • Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden); • Starke Kryptographie mit entsprechenden Schlüsselverwaltungsprozessen und -verfahren. *Hinweis: Für eine Person mit böswilligen Absichten ist es eine relativ einfache Übung, die originalen PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die abgekürzte als auch auf die Hash-Version einer PAN hat. Wenn die gehashte und die abgekürzte Version derselben PAN in der Umgebung derselben Stelle nebeneinander bestehen, müssen zusätzliche Kontrollen eingesetzt werden, damit die originale PAN nicht durch den Vergleich von gehashten und abgekürzten Versionen rekonstruiert werden kann.*					5	
3.4.1 Wenn Festplattenverschlüsselung verwendet wird (anstelle der Datenbankverschlüsselung auf Datei- oder Spaltenebene), muss der logische Zugriff unabhängig von nativen Authentifizierungs- und Zugriffskontrollmechanismen des Betriebssystems verwaltet werden (z. B. indem lokale Benutzerkontodatenbanken und allgemeine Netzwerkanmeldedaten nicht verwendet werden). Dechiffrierschlüssel dürfen nicht mit Benutzerkonten verbunden werden. *Hinweis: Diese Anforderung gilt zusätzlich zu allen anderen PCI-DSS-Anforderungen und Schlüsselverwaltungsanforderungen.*					5	
3.5 Dokumentieren und implementieren Sie Verfahren zum Schutz von Schlüsseln, die für die Sicherheit gespeicherter Karteninhaberdaten eingesetzt werden, vor Weitergabe und Missbrauch: *Hinweis: Diese Anforderung gilt für Schlüssel zum Verschlüsseln gespeicherter Karteninhaberdaten und auch für Schlüsselverschlüsselungsschlüssel, die zum Schutz von Datenverschlüsselungsschlüsseln verwendet werden. Diese Schlüsselverschlüsselungsschlüssel müssen mindestens so sicher wie der Datenverschlüsselungsschlüssel sein.*						

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
3.5.1 Zusätzliche Anforderung nur für Dienstanbieter: Pflegen Sie eine dokumentierte Beschreibung der kryptographischen Architektur, die folgende Elemente enthält: • Details aller Algorithmen, Protokolle und Schlüssel, einschließlich der Schlüssellänge und dem Ablaufdatum, die für den Schutz der Karteninhaberdaten verwendet werden • Beschreibung der Verwendung für jeden Schlüssel. • Bestand eines HSM und anderen SCD, die für die Schlüsselverwaltung verwendet werden *Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*					5	
3.5.2 Einschränken des Zugriff auf kryptographische Schlüssel auf die unbedingt notwendige Anzahl von Personen.					5	
3.5.3 Geheime und private Schlüssel zur Ver- und Entschlüsselung von Karteninhaberdaten müssen stets in einer (oder mehreren) der folgenden Formen gespeichert werden: • Verschlüsselung mit einem Schlüsselverschlüsselungsschlüssel, der mindestens so sicher wie der Datenverschlüsselungsschlüssel ist und separat von diesem gespeichert wird • Speicherung in einem sicheren kryptographischen System (wie einem HSM (Host Security Module, Host-Sicherheitsmodul) oder einem für PTS zugelassenen POI-Gerät (Point Of Interaction, Interaktionspunkt) • Speicherung gemäß branchenweit akzeptierter Methoden in mindestens zwei Schlüsselkomponenten voller Länge oder in Schlüssel-Shares *Hinweis: Öffentliche Schlüssel müssen nicht in dieser Form gespeichert werden.*					5	
3.5.4 Speichern kryptographischer Schlüssel an möglichst wenigen Speicherorten.					5	
3.6 Dokumentieren und implementieren Sie alle Schlüsselverwaltungsprozesse und -verfahren für kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, wie z. B.: *Hinweis: Zahlreiche Branchenstandards für die Schlüsselverwaltung sind über verschiedene Ressourcen verfügbar, unter anderem über NIST (unter http://csrc.nist.gov).*						
3.6.1 Erstellung starker kryptographischer Schlüssel					5	
3.6.2 Sichere Verteilung kryptographischer Schlüssel					5	
3.6.3 Sicheres Speichern kryptographischer Schlüssel					5	
3.6.4 Änderungen kryptographischer Schlüssel für Schlüssel, die das Ende ihrer Schlüssellebensdauer erreicht haben (z. B. nach Ablauf einer festgelegten Zeitspanne und/oder nachdem von einem bestimmten Schlüssel eine gegebene Menge an Geheimtext generiert wurde), so wie von dem entsprechenden Anwendungsanbieter oder Schlüsselinhaber definiert und entsprechend bewährter Branchenverfahren und -richtlinien (z. B. NIST Special Publication 800-57).					5	
3.6.5 Entfernung oder Austausch (z. B. mittels Archivierung, Vernichtung und/oder Rückruf) von Schlüsseln je nach Notwendigkeit, wenn die Integrität des Schlüssels gefährdet ist (z. B. Ausscheiden eines Mitarbeiters, der einen Klartext-Schlüssel kennt) oder Grund zur Annahme besteht, dass bestimmte Schlüssel beschädigt sind. Hinweis: Wenn entfernte oder ausgetauschte kryptographische Schlüssel aufbewahrt werden müssen, sind diese Schlüssel auf eine sichere Art und Weise zu archivieren (z. B. mittels Schlüssel zum Verschlüsseln von Schlüsseln). Archivierte kryptographische Schlüssel dürfen nur zu Entschlüsselungs-/Überprüfungszwecken verwendet werden.					5	

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
3.6.6 Bei einer manuellen Verwaltung kryptographischer Klartext-Schlüssel gilt das Prinzip der geteilten Kenntnis und doppelten Kontrollen. Hinweis: Zu den manuellen Verfahren zur Schlüsselverwaltung zählen unter anderen das Generieren, Übertragen, Laden, Speichern und Vernichten von Schlüsseln.					5	
3.6.7 Verhindern der unbefugten Ersetzung kryptographischer Schlüssel.					5	
3.6.8 Aufbewahrer kryptographischer Schlüssel müssen formal bestätigen, dass sie ihre Verantwortung als Aufbewahrer verstehen und annehmen.					5	
3.7 Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz gespeicherter Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.					5	
Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze						
4.1 Verwenden starker Kryptographie und Sicherheitsprotokolle zum Schutz sensibler Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke: • Es werden ausschließlich vertrauenswürdige Schlüssel und Zertifikate akzeptiert. • Das verwendete Protokoll unterstützt ausschließlich sichere Versionen oder Konfigurationen. • Für die verwendete Verschlüsselungsmethode wird die richtige Verschlüsselungsstärke verwendet. *Hinweis: Wenn SSL/eine frühe Version von TLS verwendet wird, müssen die Anforderungen aus Anhang A2 erfüllt werden. Zu den offenen, öffentlichen Netzwerken zählen unter anderem:* • *Das Internet* • *Drahtlose Technologien wie 802.11 und Bluetooth* • *Mobilfunktechnologien wie GSM (Global System for Mobile Communications) und CDMA (Code Division Multiple Access)* • *General Packet Radio Service (GPRS).* • *Satellitenverbindungen*		2				
4.1.1 Stellen Sie sicher, dass drahtlose Netzwerke, die Karteninhaberdaten übertragen oder mit der CDE verbunden sind, mittels bewährter Branchenverfahren eine starke Verschlüsselung für die Authentifizierung und Übertragung implementieren.		2				
4.2 Versenden Sie niemals ungeschützte PANs über Messaging-Technologien für Endbenutzer (z. B. E-Mail, Instant Messaging, SMS, Chat usw.).		2				
4.3 Sicherheitsrichtlinien und betriebliche Verfahren zur Verschlüsselung der Übertragung von Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.		2				
Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware						
5.1 Implementieren von Antivirensoftware auf allen Systemen, die häufig von böswilliger Software befallen werden (insbesondere Personal Computer und Server).		2				
5.1.1 Sorgen Sie dafür, dass die Antivirenprogramme in der Lage sind, alle bekannten Malware-Typen zu erkennen, zu entfernen und davor zu schützen.		2				
5.1.2 Bei Systemen, die in der Regel nicht von Malware befallen sind, muss regelmäßig geprüft werden, ob sich die Malware-Bedrohung erhöht hat oder weiterhin keine Antivirensoftware auf diesen Systemen installiert werden muss.		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
5.2 Bei sämtlichen Antivirensystemen muss Folgendes beachtet werden: • Die Systeme müssen auf dem neuesten Stand gehalten werden. • Es müssen regelmäßige Suchläufe stattfinden. • Es sind Prüfprotokolle zu erstellen, die gemäß PCI-DSS-Anforderung 10.7 aufbewahrt werden müssen.		2				
5.3 Stellen Sie sicher, dass die Antivirensysteme aktiv ausgeführt werden und von den Benutzern weder deaktiviert noch verändert werden können, sofern keine fallweise Ausnahmegenehmigung der Geschäftsführung für einen beschränkten Zeitraum vorliegt. *Hinweis: Antivirenlösungen dürfen nur dann vorübergehend deaktiviert werden, wenn es einen triftigen technischen Grund dafür gibt. Hierzu ist für jeden Einzelfall die Genehmigung der Geschäftsführung einzuholen. Wenn der Virenschutz aus bestimmten Gründen deaktiviert werden muss, ist hierfür eine förmliche Autorisierung erforderlich. Möglicherweise sind außerdem für den Zeitraum, in dem der Virenschutz nicht aktiv ist, zusätzliche Sicherheitsmaßnahmen zu treffen.*		2				
5.4 Sicherheitsrichtlinien und betriebliche Verfahren zum Schutz von Systemen vor Malware müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.		2				
Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen						
6.1 Einrichtung eines Prozesses zur Ermittlung von Sicherheitsrisiken auf der Grundlage verlässlicher Quellen und Einteilung neu ermittelter Sicherheitsrisiken in verschiedene Risikostufen (hoch/mittel/niedrig). *Hinweis: Die Risikostufen sollten auf den bewährten Verfahren der Branche beruhen und die potenziellen Auswirkungen berücksichtigen. So könnten der CVSS-Basiswert und/oder die Klassifizierung durch den Anbieter sowie die Art der betroffenen Systeme als Kriterien für die Einteilung der Sicherheitsrisiken in verschiedene Stufen dienen.* *Die Methoden zur Bewertung der Sicherheitsrisiken und zur Einteilung in Sicherheitsstufen hängen von der Unternehmensumgebung und der Strategie zur Risikobewertung ab. Bei der Risikoeinstufung müssen zumindest die Sicherheitsrisiken ermittelt werden, die als „hohes Risiko" für die Umgebung gelten. Zusätzlich zu der Risikoeinstufung können einzelne Sicherheitsrisiken als „kritisch" betrachtet werden, falls sie eine unmittelbare Bedrohung der Umgebung darstellen, sich auf wichtige Systeme auswirken und/oder eine potenzielle Gefährdung darstellen, wenn nicht auf sie eingegangen wird. Beispiele für wichtige Systeme sind Sicherheitssysteme, öffentlich zugängliche Geräte und Systeme, Datenbanken und andere Systeme, in denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden.*			3			
6.2 Alle Systemkomponenten und Softwareanwendungen müssen vor bekannten Sicherheitsrisiken mithilfe der neuesten Sicherheitspatches des jeweiligen Anbieter geschützt werden. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden. *Hinweis: Kritische Sicherheitspatches müssen gemäß dem in Anforderung 6.1 festgelegten Prozess zur Risikoeinstufung ermittelt werden.*			3			
6.3 Sichere Entwicklung von Softwareanwendungen (interne und externe, inklusive Web-Administrationszugriff auf die Anwendungen) unter Berücksichtigung der folgenden Punkte: • Werden Softwareanwendungen gemäß dem PCI-DSS entwickelt (z. B. sichere Authentifizierung und Protokollierung)? • Basieren die Entwicklungsprozesse auf Branchenstandards und/oder bewährten Verfahren? • Integration von Informationssicherheit über den gesamten Softwareentwicklungszyklus hinweg *Hinweis: Diese Anforderungen gelten für alle intern entwickelten Softwareanwendungen sowie individuell von Drittanbietern entwickelte Software.*			3			
6.3.1 Löschen Sie Konten, Benutzer-IDs und Kennwörtern für Entwicklung, Tests und/oder individuelle Anwendungen, bevor die Anwendungen aktiv oder für Kunden freigegeben werden.			3			

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
6.3.2 Prüfung des individuellen Programmcodes vor der Freigabe für Produktion oder Kunden (entweder mithilfe manueller oder automatischer Prozesse) auf alle potenziellen Sicherheitsrisiken; dabei sind mindestens die folgenden Punkte zu berücksichtigen: • Codeänderungen werden von anderen Personen geprüft als dem ursprünglichen Ersteller des Codes, außerdem von Personen, die mit Verfahren zur Codeprüfung und sicheren Codierungsverfahren vertraut sind. • Mit Codeprüfungen wird sichergestellt, dass der Code gemäß sicheren Codierungsrichtlinien erstellt wird. • Vor der Freigabe werden entsprechende Korrekturen implementiert. • Ergebnisse der Codeprüfung werden vor der Freigabe vom Management geprüft und genehmigt. *Hinweis: Diese Vorschrift von Code-Prüfungen gilt für den gesamten benutzerdefinierten (internen und öffentlichen) Code im Rahmen des Systementwicklungszyklus. Code-Prüfungen können durch qualifiziertes internes Personal oder durch Dritte ausgeführt werden. Für die Öffentlichkeit bestimmte Webanwendungen unterliegen auch zusätzlichen Kontrollen, um laufende Bedrohungen und Sicherheitsrisiken nach der Implementierung gemäß der Definition in PCI DSS-Anforderung 6.6 anzugehen.*			3			
6.4 Befolgen von Änderungskontrollprozessen und -verfahren für alle Änderungen an Systemkomponenten. Die Prozesse müssen Folgendes umfassen:			3			
6.4.1 Trennung der Entwicklungs-/Testumgebungen von der Produktionsumgebung und Durchsetzung dieser Trennung mittels Zugriffskontrolle.			3			
6.4.2 Trennung der Aufgaben zwischen Entwicklungs-, Test- und Produktionsumgebungen			3			
6.4.3 Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet			3			
6.4.4 Löschung von Testdaten und -konten aus Systemkomponenten, bevor das System aktiv wird/in Produktion geht.			3			
6.4.5 Verfahren zur Änderungskontrolle müssen folgende Elemente beinhalten:						6
6.4.5.1 Dokumentation der Auswirkungen.						6
6.4.5.2 Dokumentierte Genehmigung von Änderungen durch autorisierte Parteien.						6
6.4.5.3 Testen der Funktionalität, damit die Änderung nicht die Sicherheit des Systems beeinträchtigt.						6
6.4.5.4 Back-Out-Verfahren.						6
6.4.6 Nach Abschluss einer signifikanten Änderung müssen alle relevanten PCI-DSS-Anforderungen auf allen neuen oder veränderten Systemen und Netzwerken implementiert, und die Dokumentation entsprechend aktualisiert sein. *Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*						6
6.5 Gehen Sie häufige Sicherheitsrisiken in Softwareentwicklungsprozessen an, einschließlich der folgenden Punkte: • Entwickler müssen mindestens jährlich auf aktuelle Techniken zur sicheren Programmierung, einschließlich dem Vorbeugen häufiger Schwachstellen, geschult werden. • Entwicklung von Anwendungen aufgrund sicherer Programmierungsrichtlinien. *Hinweis: Die unter 6.5.1 bis 6.5.10 aufgeführten Sicherheitsrisiken entsprachen zum Zeitpunkt der Veröffentlichung dieser Version des PCI-DSS den bewährten Verfahren der Branche. Da jedoch die bewährten Verfahren der Branche beim Management von Sicherheitsrisiken aktualisiert werden (z. B. der OWASP Leitfaden, SANS CWE Top 25, CERT Secure Coding usw.), sind für diese Anforderungen die jeweils gültigen bewährten Verfahren zu verwenden.*			3			
Hinweis: Die Anforderungen 6.5.1 bis 6.5.6 gelten für alle Anwendungen (intern oder extern).						

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
6.5.1 Injektionsfehler, insbesondere bei der SQL-Injektion. Injektion von Betriebssystembefehlen, LDAP- und Xpath-Injektionsfehler sowie andere Injektionsfehler sind ebenfalls zu berücksichtigen.			3			
6.5.2 Pufferüberläufe			3			
6.5.3 Unsicherer kryptographischer Speicher			3			
6.5.4 Unsichere Mitteilungen			3			
6.5.5 Inkorrekte Fehlerhandhabung			3			
6.5.6 Alle „schwerwiegenden" Sicherheitsrisiken werden entsprechend dem Identifikationsprozess ermittelt (wie in der PCI-DSS-Anforderung 6.1 definiert).			3			
Hinweis: Die nachstehenden Anforderungen 6.5.7 bis 6.5.10 gelten für Webanwendungen und Anwendungsschnittstellen (intern oder extern):						
6.5.7 Site-übergreifendes Scripting (XSS)			3			
6.5.8 Kontrolle unangemessener Zugriffe (z. B. unsichere direkte Objektverweise, fehlende Einschränkung des URL-Zugriffs, Directory Traversal und fehlende Einschränkung des Benutzerzugriffs auf bestimmte Funktionen).			3			
6.5.9 Cross-Site Request Forgery (CSRF)			3			
6.5.10 Geknackte Authentifizierungs- und Sitzungsverwaltung			3			
6.6 Kontinuierliche Betrachtung neuer Bedrohungen und Sicherheitsrisiken bei öffentliche Webanwendungen Schutz dieser Anwendungen vor bekannten Angriffen mithilfe einer der folgenden Methoden: • Prüfen öffentlicher Webanwendungen durch manuelle oder automatisierte Tools oder Methoden zum Bewerten der Anwendungssicherheit mindestens jährlich sowie nach Änderungen *Hinweis: Diese Bewertung ist nicht mit den für Anforderung 11.2 durchgeführten Schwachstellenprüfungen identisch.* • Installation einer automatischen technischen Lösung zur Erkennung und Verhinderung webbasierter Angriffe (z. B. eine Webanwendungs-Firewall) bei öffentlichen Webanwendungen zur kontinuierlichen Prüfung des Datenverkehrs			3			
6.7 Die Sicherheitsrichtlinien und betrieblichen Verfahren zum Aufbau und zur Wahrung sicherer Systeme und Anwendungen müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.			3			
Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf						
7.1 Beschränken des Zugriffs auf Systemkomponenten und Karteninhaberdaten auf die Personen, deren Tätigkeit diesen Zugriff erfordert.						
7.1.1 Definition der Zugriffsanforderungen für die einzelnen Rollen unter Berücksichtigung der folgenden Aspekte: • Systemkomponenten und Datenressourcen, die für die Ausführung der tätigkeitsbezogenen Funktionen benötigt werden • Erforderliche Berechtigungsstufe (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen				4		
7.1.2 Beschränkung des Zugriffs für Benutzer-IDs auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind.				4		
7.1.3 Zuweisung von Zugriffsberechtigungen aufgrund der Tätigkeitsklassifizierung und -funktion der einzelnen Mitarbeiter.				4		
7.1.4 Die Genehmigung durch autorisierte Parteien, in der die erforderlichen Berechtigungen angegeben sind, muss dokumentiert werden.				4		

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
7.1.4 Die Genehmigung durch autorisierte Parteien, in der die erforderlichen Berechtigungen angegeben sind, muss dokumentiert werden.				4		
7.2 Festlegen eines Zugriffskontrollsystems für Systemkomponenten, das den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem muss Folgendes umfassen:						
7.2.1 Abdeckung aller Systemkomponenten				4		
7.2.2 Zuweisung von Berechtigungen zu einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion.				4		
7.2.3 Standardeinstellung „Alle ablehnen“				4		
7.3 Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des Zugriffs auf Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.				4		
Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff						
8.1 Definition und Implementierung von Richtlinien und Verfahren zur geeigneten Benutzeridentifizierungsverwaltung für Nichtverbraucherbenutzer und Administratoren auf allen Systemkomponenten nach folgender Maßgabe:						
8.1.1 Zuweisen einer eindeutigen ID für alle Benutzer, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird.		2				
8.1.2 Kontrollieren Sie die Vorgänge des Hinzufügens, Löschens und Änderns von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsobjekten.		2				
8.1.3 Sofortige Deaktivierung des Zugriffs ehemaliger Benutzer.		2				
8.1.4 Entfernen bzw. Deaktivieren inaktiver Benutzerkonten innerhalb von 90 Tagen.		2				
8.1.5 Beim Management von IDs, die von Dritten für den Zugriff, den Support oder die Wartung von Systemkomponenten per Remote-Zugriff verwendet werden, müssen folgende Aspekte berücksichtigt werden: • Sie werden nur in dem Zeitraum aktiviert, in dem sie benötigt werden, und anschließend wieder deaktiviert. • Verwendete IDs werden überwacht.		2				
8.1.6 Begrenzen der wiederholten Zugriffsversuche durch Sperren der Benutzer-ID nach spätestens sechs Versuchen.		2				
8.1.7 Festlegen einer Aussperrdauer von mindestens 30 Minuten, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann.		2				
8.1.8 Nach mehr als 15-minütiger Inaktivität müssen sich die Benutzer erneut authentifizieren und das Terminal oder die Sitzung reaktivieren.		2				
8.2 Neben einer eindeutigen ID muss mindestens eine der folgenden Methoden zur Authentifizierung sämtlicher Benutzer zum Einsatz kommen, damit das Benutzerauthentifizierungsmanagement für Nichtverbraucherbenutzer und -Administratoren auf allen Systemkomponenten ordnungsgemäß verläuft: • Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz; • etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard; • Etwas, das Sie sind, wie zum Beispiel biometrische Daten.		2				
8.2.1 Nicht entschlüsselbare Übertragung und Speicherung von Kennwörtern und -sätzen auf sämtlichen Systemkomponenten unter Verwendung einer sicheren Verschlüsselung.		2				
8.2.2 Vor der Änderung von Authentifizierungsdaten muss die Benutzeridentität geprüft werden – beispielsweise beim Zurücksetzen von Kennwörtern, bei der Bereitstellung neuer Tokens oder bei der Erstellung neuer Schlüssel.		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
8.2.3 Kennwörter/Kennsatzsätze müssen die folgenden Anforderungen erfüllen: • Die Mindestlänge beträgt sieben Zeichen. • Es müssen sowohl Ziffern als auch Buchstaben verwendet werden. Alternativ müssen die Komplexität und Stärke eines Kennworts/Kennsatzes mindestens den oben angegebenen Parametern entsprechen.		2				
8.2.4 Änderung der Benutzerkennwörter/-sätze mindestens einmal alle 90 Tage.		2				
8.2.5 Neue Kennwörter/Kennsätze müssen sich von den letzten vier Kennwörtern/Kennsätzen unterscheiden.		2				
8.2.6 Festlegen von Kennwörtern/Kennsätzen für die erste Verwendung bzw. nach dem Zurücksetzen des Kennworts auf einen eindeutigen Wert für jeden Benutzer, der sofort nach der ersten Verwendung geändert werden muss.		2				
8.3 Sichern Sie alle Nichtkonsolen-Verwaltungszugriffe und Fernzugriffe auf das CDE durch Multi-Faktor-Authentifizierung. *Hinweis: Bei der Multi-Faktor-Authentifizierung müssen mindestens zwei der drei Authentifizierungsmethoden (siehe Anforderung 8.2 für eine Beschreibung der Authentifizierungsmethoden) bei der Authentifizierung eingesetzt werden. Wenn ein Faktor zweimalig verwendet wird (z. B. wenn zwei separate Kennwörter eingesetzt werden) handelt es sich nicht um eine Multi-Faktor-Authentifizierung.*						
8.3.1 Machen Sie die Multi-Faktor-Authentifizierung zum festen Bestandteil für alle Nichtkonsolen-Zugriffe auf das CDE durch Mitarbeiter mit Verwaltungszugriff. *Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*		2				
8.3.2 Integrieren Sie die Multi-Faktor-Authentifizierung als festen Bestandteil bei allen Fernzugriffen auf das Netzwerk durch interne Mitarbeiter (Benutzer und Administratoren) und Dritte von außerhalb des Netzwerkes (einschließlich Anbieterzugriff zu Support- oder Wartungszwecken).		2				
8.4 Dokumentation und Weitergabe der Richtlinien und Verfahren zur Authentifizierung an alle Benutzer unter Einschluss der folgenden Informationen: • Hinweise zur Auswahl starker Authentifizierungsinformationen • Hinweise zum Schutz der Authentifizierungsinformationen durch die Benutzer • Anweisungen zur Vermeidung wiederverwendeter Kennwörter • Anweisungen zur Änderung von Kennwörtern beim Verdacht einer Gefährdung				4		
8.5 Keine Verwendung von IDs und Kennwörtern für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder von anderen Authentifizierungsmethoden und Beachtung der folgenden Punkte: • Allgemeine Benutzer-IDs werden deaktiviert oder entfernt. • Es gibt keine gemeinsamen Benutzer-IDs für Systemadministrationsaufgaben und andere wichtige Funktionen. • Es werden keine gemeinsamen und allgemeinen Benutzer-IDs zur Administration von Systemkomponenten verwendet.				4		
8.5.1 Zusätzliche Anforderung nur für Dienstanbieter: Dienstanbieter mit Remote-Zugriff auf Kundensysteme (z. B. für den Support von POS-Systemen oder -Servern) benötigen für jeden Kunden eindeutige Authentifizierungsinformationen (wie etwa ein Kennwort oder einen Kennsatz). *Hinweis: Diese Anforderung gilt nicht für Anbieter von gemeinsam genutzten Hosting-Services, die auf ihre eigene Hosting-Umgebung, in der mehrere Kundenumgebungen gehostet werden, zugreifen möchten.*		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
8.6 Bei Verwendung anderer Authentifizierungsmethoden (z. B. Tokens für die physische/logische Sicherheit, Smartcards, Zertifikate usw.) muss die folgende Zuweisung beachtet werden: • Authentifizierungsinformationen müssen einem einzelnen Konto zugewiesen sein und dürfen nicht von mehreren Konten gemeinsam genutzt werden. • Mit physischen und/oder logischen Kontrollen muss gewährleistet werden, dass der Zugriff nur über das Konto erfolgen kann, für das die Authentifizierungsinformationen gedacht sind.				4		
8.7 Der gesamte Zugriff auf die Datenbank mit den Karteninhaberdaten (einschließlich des Zugriffs durch Anwendungen, Administratoren und alle anderen Benutzer) wird wie folgt beschränkt: • Sämtliche Zugriffe, Anfragen und Aktionen der Benutzer im Bezug auf die Datenbank erfolgen mittels programmierter Verfahren. • Nur Datenbankadministratoren können direkt auf die Datenbanken zugreifen und Abfragen durchführen. • Die Anwendungs-IDs für Datenbankanwendungen können nur von den Anwendungen (und nicht von Einzelbenutzern oder nicht zu den Anwendungen gehörenden Prozessen) verwendet werden.				4		
8.8 Sicherheitsrichtlinien und betriebliche Verfahren zur Identifizierung und Authentifizierung müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.				4		
Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken						
9.1 Verwenden angemessener Zugangskontrollen, um den physischen Zugriff auf Systeme in der CDE zu überwachen und zu beschränken.		2				
9.1.1 Überwachen des Zugangs zu zugangsbeschränkten Bereichen entweder mithilfe von Videokameras oder Kontrollsystemen (oder beidem). Überprüfen der gesammelten Daten und Korrelation mit anderen Daten. Speichern der Daten mindestens drei Monate lang, wenn dies gesetzlich zulässig ist. *Hinweis: „Sensible Bereiche" sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Nicht hierzu zählen die öffentlichen Bereiche, in denen lediglich POS-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).*		2				
9.1.2 Implementierung physischer und/oder logischer Kontrollen zur Beschränkung des Zugriffs auf öffentlich zugängliche Netzwerkbuchsen. Beispielsweise sollte die Möglichkeit bestehen, Netzwerkbuchsen in für Besucher zugänglichen Bereichen zu deaktivieren und nur dann zu aktivieren, wenn der Netzwerkzugriff ausdrücklich zugelassen ist. Alternativ können auch Prozesse implementiert werden, mit denen Besucher jederzeit in Bereiche mit aktiven Netzwerkbuchsen geleitet werden.		2				
9.1.3 Beschränkung des physischen Zugriffs auf WLAN-Zugriffspunkte, Gateways, Handgeräte, Netzwerk- und Kommunikationshardware und Telekommunikationsleitungen.		2				
9.2 Entwicklung von Verfahren mit den folgenden Elementen zur leichteren Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern: • Identifizierung von Besuchern und Mitarbeitern vor Ort (z. B. durch Vergabe von Ausweisen) • Änderungen bei den Zugangs- bzw. Zugriffsanforderungen • Rücknahme bzw. Beendigung der Identifizierung von Vor-Ort-Mitarbeitern und Besuchern (z. B. mittels Ausweis) bei Ablauf des Status					5	
9.3 Kontrolle des Zugangs von Vor-Ort-Personal zu den zugangsbeschränkten Bereichen gemäß den folgenden Anforderungen: • Der Zugang muss autorisiert sein und auf der jeweiligen tätigkeitsbezogenen Aufgabe basieren. • Die Zugangsberechtigung wird sofort nach dem Ende der Beschäftigung zurückgenommen, und sämtliche physischen Zugangssysteme wie Schlüssel, Karten usw. werden zurückgegeben oder deaktiviert.		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
9.4 Implementierung von Verfahren zur Identifizierung und Autorisierung von Besuchern. Die Verfahren müssen Folgendes umfassen:						
9.4.1 Besucher müssen vor dem Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder gepflegt werden, autorisiert und innerhalb dieser Bereiche jederzeit begleitet werden.					5	
9.4.2 Die Besucher werden identifiziert und mit einem Ausweis oder einer sonstigen Identifizierung versehen, mit der sie sich deutlich von den Vor-Ort-Mitarbeitern unterscheiden lassen.					5	
9.4.3 Die Besucher werden um Rückgabe des Ausweises bzw. der Identifizierung gebeten, wenn die Besucher die Einrichtung verlassen oder die Erlaubnis ausläuft.					5	
9.4.4 Die Aktivität der Besucher in der Einrichtung und in Computerräumen und Rechenzentren, in denen Karteninhaberdaten gespeichert oder übertragen werden, muss in einem Besucherprotokoll festgehalten werden. Dokumentieren Sie den Namen des Besuchers, den Firmennamen und den Namen des Mitarbeiters vor Ort, der dem Besucher Zugang gewährt. Aufbewahren des Besucherprotokolls für die Dauer von mindestens drei Monaten, wenn dies gesetzlich zulässig ist.					5	
9.5 Stellen Sie die physische Sicherheit aller Medien sicher.					5	
9.5.1 Aufbewahren von Sicherungskopien an einem sicheren Ort, vorzugsweise in einer anderen Einrichtung, wie z. B. an einem Alternativ- oder Backup-Standort oder bei einem kommerziellen Anbieter von Speicherkapazitäten. Überprüfen der Sicherheit dieses Standorts mindestens einmal pro Jahr.					5	
9.6 Durchführung strikter Kontrollen der internen bzw. externen Verteilung jeglicher Art von Medien, einschließlich der folgenden:						
9.6.1 Klassifizieren Sie die Medien, sodass das Gefährdungspotenzial der Daten bestimmt werden kann.					5	
9.6.2 Versenden Sie die Medien über einen sicheren Kurier oder eine andere Liefermethode, die präzise nachverfolgt werden kann.					5	
9.6.3 Das Management muss den Transfer sämtlicher Medien aus einem geschützten Bereich genehmigen (insbesondere, wenn die Medien an einzelne Personen weitergegeben werden).					5	
9.7 Strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien.						
9.7.1 Ordnungsgemäße Verwaltung von Medieninventurlisten und Durchführung von mindestens einer Medieninventur im Jahr.					5	
9.8 Vernichtung von Medien, die nicht mehr zu geschäftlichen oder juristischen Zwecken benötigt werden, nach folgenden Maßgaben:						
9.8.1 Papierausdrucke müssen in einer Form vernichtet werden, dass keine Karteninhaberdaten wiederhergestellt werden können. Container zur Aufbewahrung von zu vernichtendem Material müssen geschützt werden.	1					
9.8.2 Löschen von Karteninhaberdaten auf elektronischen Medien in einer Art und Weise, die eine Wiederherstellung der Daten unmöglich macht.	1					
9.9 Manipulations- und Austauschschutz von Geräten zur Erfassung von Zahlungskartendaten über eine direkte physische Interaktion mit der Karte. *Hinweis: Diese Anforderungen gelten für Kartenlesegeräte, die bei Transaktionen eingesetzt werden, bei denen die Karte am Point-of-Sale vorliegt und durch das Gerät gezogen oder in das Gerät eingesteckt werden muss. Diese Anforderung gilt nicht für Komponenten zur manuellen Eingabe wie Computertastaturen und POS-Ziffernblöcke.*						
9.9.1 Führen einer aktuellen Geräteliste. Die Liste muss folgende Punkte enthalten: • Fabrikat und Modell des Geräts • Standort des Geräts (zum Beispiel die Adresse des Standorts oder der Einrichtung, an der sich das Gerät befindet) • Seriennummer des Geräts oder andere Informationen zur eindeutigen Identifizierung.		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
9.9.2 Regelmäßige Untersuchung der Geräte auf Spuren von Manipulation (z. B. Anbringen von Skimming-Technik) oder Austausch (stimmen beispielsweise die Seriennummer oder andere Gerätemerkmale, oder wurde das Gerät durch ein anderes ausgetauscht?). *Hinweis: Anzeichen für eine Manipulation oder den Austausch von Geräten sind zum Beispiel unerwartete Anbauten oder Kabel, fehlende oder geänderte Sicherheitssiegel, beschädigte oder andersfarbige Gehäuse bzw. Änderungen bei der Seriennummer oder anderen externen Kennzeichen.*		2				
9.9.3 Personalschulungen zur Förderung des Bewusstseins im Hinblick auf Manipulations- oder Austauschversuche. Die Schulungen sollten Folgendes umfassen: • Prüfung der Identität von Dritten, die vorgeben, Reparatur- oder Wartungsarbeiten am Gerät vorzunehmen (diese Prüfung muss erfolgen, bevor diesen Personen erlaubt wird, an den Geräten zu arbeiten). • Prüfung der Geräte vor der Installation, dem Austausch und der Rückgabe. • Bewusstsein für verdächtiges Verhalten an den Geräten (z. B. Versuche, die Geräte auszustecken oder zu öffnen). • Meldung von verdächtigem Verhalten und von Anzeichen der Manipulation bzw. des Austauschs von Geräten an die entsprechenden Personen (z. B. Manager oder Sicherheitsbeauftragter).		2				
9.10 Sicherheitsrichtlinien und betriebliche Verfahren zur Beschränkung des physischen Zugangs zu Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.					5	
Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten						
10.1 Implementierung von Audit-Trails zur Verknüpfung des gesamten Zugriffs auf Systemkomponenten mit den einzelnen Benutzern.				4		
10.2 Implementierung automatisierter Audit-Trails für alle Systemkomponenten zur Rekonstruktion der folgenden Ereignisse:						
10.2.1 Alle individuellen Zugriffe auf Karteninhaberdaten				4		
10.2.2 Alle von einer Einzelperson mit Root- oder Administratorrechten vorgenommene Aktionen				4		
10.2.3 Zugriff auf alle Audit-Trails				4		
10.2.4 Ungültige logische Zugriffsversuche				4		
10.2.5 Verwendung der sowie Änderungen an Identifizierungs- und Authentifizierungsmechanismen (u. a. bei der Erstellung neuer Konten, Heraufstufung von Rechten usw.) und sämtliche Änderungen, Ergänzungen und Löschungen an bzw. von Konten mit „root“- oder Administratorrechten				4		
10.2.6 Initialisieren, Beenden oder Anhalten der Prüfprotokolle				4		
10.2.7 Erstellen und Löschen von Objekten auf Systemebene				4		
10.3 Aufzeichnen von mindestens den folgenden Audit-Trail-Einträgen für alle Systemkomponenten zu jedem Ereignis:						
10.3.1 Benutzeridentifizierung				4		
10.3.2 Ereignistyp				4		
10.3.3 Datum und Uhrzeit				4		
10.3.4 Angabe von Erfolgen oder Fehlschlägen				4		
10.3.5 Ereignisursprung				4		
10.3.6 Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen.				4		
10.3.6 Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen.				4		

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
10.4 Synchronisieren Sie mit Technologien zur Zeitsynchronisierung alle wichtigen Systemuhren und -zeiten und stellen Sie sicher, dass folgende Elemente zur Ermittlung, Weitergabe und Speicherung der richtigen Zeit implementiert sind: *Hinweis: Eine Zeitsynchronisierungstechnologie ist beispielsweise das Network Time Protocol (NTP).*				4		
10.4.1 Auf wichtigen Systemen ist die Uhrzeit korrekt und einheitlich.				4		
10.4.2 Zeitinformationen sind geschützt.				4		
10.4.3 Zeiteinstellungen werden von branchenüblichen Zeitquellen empfangen.				4		
10.5 Schutz der Audit-Trails vor Veränderungen.						
10.5.1 Beschränkung der Anzeige der Audit-Trails auf Personen, die aus geschäftlichen Gründen darauf zugreifen müssen.				4		
10.5.2 Schutz von Audit-Trail-Dateien vor nicht autorisierten Änderungen.				4		
10.5.3 Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.				4		
10.5.4 Erstellung von Protokollen für nach außen gerichtete Technologien auf sicheren zentralen und internen Protokollservern oder Medien.				4		
10.5.5 Mithilfe von Software zur Dateiintegritätsüberwachung und zur Erfassung von Änderungen in Protokollen muss dafür gesorgt werden, dass bei der Änderung von bestehenden Protokolldaten ein Alarm ausgelöst wird (nicht jedoch bei der Eingabe neuer Daten).				4		
10.6 Überprüfung von Protokollen und Systemereignissen für alle Systemkomponenten auf Unregelmäßigkeiten oder verdächtige Aktivitäten. *Hinweis: Zur Einhaltung dieser Anforderung können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.*						
10.6.1 Prüfen Sie mindestens einmal täglich die folgenden Punkte: • Sämtliche Sicherheitsereignisse • Protokolle aller Systemkomponenten, die CHD und/oder SAD speichern, verarbeiten oder übertragen • Die Protokolle aller wichtigen Systemkomponenten • Die Protokolle aller Server- und Systemkomponenten, die Sicherheitsfunktionen ausführen (z. B. Firewalls, Systeme zur Erkennung/Verhinderung von Eindringversuchen (IDS/IPS), Authentifizierungsserver, E-Commerce-Umleitungsserver usw.).				4		
10.6.2 Regelmäßige Prüfung der Protokolle aller anderen Systemkomponenten auf der Grundlage der Richtlinien und der Risikomanagementstrategie des Unternehmens und gemäß der jährlichen Risikobewertung des Unternehmens.				4		
10.6.3 Nachverfolgung von bei der Prüfung ermittelten Ausnahmen und Unregelmäßigkeiten.				4		
10.7 Aufbewahrung der Audit-Trail-Verlaufsdaten für mindestens ein Jahr. Zur Analyse müssen diese Daten für einen Zeitraum von mindestens drei Monaten direkt zur Verfügung stehen (beispielsweise online, archiviert oder aus einer Sicherung wiederherstellbar).				4		

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
10.8 Zusätzliche Anforderung nur für Dienstanbieter: Implementieren Sie einen Prozess zur baldigen Ermittlung und Meldung von Ausfällen wichtiger Sicherheitskontrollsysteme, einschließlich Ausfälle der Folgenden: • Firewalls • IDS/IPS • FIM • Antivirus • Physische Zugangskontrollen • Logische Zugriffskontrollen • Mechanismen zur Audit-Protokollierung • Segmentierungskontrollen (falls verwendet) *Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*				4		
10.8.1 Zusätzliche Anforderung nur für Dienstanbieter: Reagieren Sie zügig auf Ausfälle wichtiger Sicherheitskontrollen. Die Reaktion auf Ausfälle bei den Sicherheitskontrollen muss die folgenden Prozesse umfassen: • Wiederherstellung der Sicherheitsfunktionen • Ermittlung und Dokumentierung der Dauer (Datum und Zeit von Anfang bis Ende) des Sicherheitsausfalls • Ermittlung und Dokumentierung der Ursache(n) des Ausfalls, einschließlich der Fehlerursache, und Dokumentierung der erforderlichen Maßnahmen zur Behebung der Fehlerursache • Ermittlung und Behebung von Sicherheitsproblemen, die während des Ausfalls aufgetreten sind • Durchführung einer Risikobeurteilung zur Feststellung, ob weitere Maßnahmen als Folge des Sicherheitsausfalls erforderlich sind • Implementierung von Kontrollen zur Verhinderung eines Wiederauftretens der Fehlerursache • Wiederaufnahme der Überwachung von Sicherheitskontrollen *Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*				4		
10.9 Sicherheitsrichtlinien und betriebliche Verfahren zur Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.				4		
Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse						
11.1 Implementierung von Prozessen, mit denen getestet wird, ob Zugriffspunkte für drahtlose Netzwerke (802.11) vorhanden sind, und vierteljährlich alle autorisierten und nicht autorisierten Zugriffspunkte für drahtlose Netzwerke gesucht werden. *Hinweis: Methoden, die sich hierfür anbieten, sind unter anderem Scans zur Feststellung drahtloser Netzwerke, physische/logische Überprüfungen der Systemkomponenten und Infrastruktur, Network Access Control (NAC) oder Wireless IDS/IPS-Systeme. Sie können sich für eine beliebige Methode entscheiden, solange damit autorisierte und nicht autorisierte Geräte erkannt und identifiziert werden können.*				4		
11.1.1 Inventarisierung von autorisierten WLAN-Zugriffspunkten mit dokumentierter geschäftlicher Begründung.				4		
11.1.2 Implementierung von Vorfallreaktionsverfahren für den Fall, dass nicht autorisierte WLAN-Zugriffspunkte entdeckt werden.		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
11.2 Ausführen interner und externer Netzwerkanfälligkeits-Scans mindestens einmal pro Quartal und nach jeder wesentlichen Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Änderung der Firewall-Regeln, Produkt-Upgrades). *Hinweis: Um beim vierteljährlichen Scan sämtliche Systeme und alle möglichen Sicherheitsrisiken zu berücksichtigen, können mehrere Scan-Berichte miteinander kombiniert werden. Es ist unter Umständen zusätzliche Dokumentation erforderlich, um zu belegen, dass bei noch nicht behobenen Sicherheitsrisiken erste Schritte unternommen wurden.* *Es ist für die anfängliche PCI DSS-Konformität nicht erforderlich, dass vier vierteljährliche Scans bestanden sein müssen, wenn der Prüfer feststellt, dass 1) das letzte Scan-Ergebnis ein positives Ergebnis war, 2) die Einheit über dokumentierte Richtlinien und Verfahren verfügt, die eine Fortsetzung der vierteljährlichen Scans erfordern, und 3) alle in den Scan-Ergebnissen festgestellten Sicherheitsrisiken nachweislich korrigiert wurden. Für die Folgejahre nach der ersten PCI-DSS-Prüfung müssen vier bestandene vierteljährliche Scans vorliegen.*		2				
11.2.1 Führen Sie vierteljährlich interne Schwachstellenprüfungen durch. Beheben Sie Schwachstellen und führen Sie erneute Scans durch, um sicherzustellen, dass alle „hohen" Sicherheitsrisiken gemäß der Risikogruppen der Einrichtung behoben wurden (gemäß Anforderung 6.1). Scans müssen von qualifizierten Mitarbeitern durchgeführt werden.		2				
11.2.2 Vierteljährliche externe Scans auf Sicherheitsrisiken, die von einem vom PCI SSC zugelassenen ASV durchgeführt werden. Nach Bedarf müssen erneute Scans durchgeführt werden, bis das Ergebnis „bestanden" lautet. *Hinweis: Vierteljährliche externe Schwachstellenprüfungen müssen von einem Scanninganbieter (Approved Scanning Vendor, ASV) durchgeführt werden, der vom Payment Card Industry Security Standards Council (PCI SSC) zugelassen wurde. Informationen zu den Scan-Kunden-Zuständigkeiten, der Scan-Vorbereitung usw. finden Sie im ASV-Programmführer auf der PCI-SSC-Website.*		2				
11.2.3 Führen Sie nach jeder wesentlichen Änderung interne und externe Scans und nach Bedarf erneute Scans durch. Scans müssen von qualifizierten Mitarbeitern durchgeführt werden.		2				
11.3 Implementierung einer Methodik für Penetrationstests, die die folgenden Elemente umfasst: • Die Methodik basiert auf branchenweit akzeptierten Verfahren für Penetrationstests (z. B. NIST SP800- 115). • Die Methodik umfasst die gesamte Umgebung der CDE und wichtige Systeme. • Es werden Tests innerhalb und außerhalb des Netzwerks durchgeführt. • Bei den Tests werden auch Kontrollen zur Segmentierung und zur Reduktion des Umfangs validiert. • Bei der Definition von Penetrationstests auf Anwendungsebene müssen mindestens die in Anforderung 6.5 aufgeführten Sicherheitsrisiken berücksichtigt werden. • Es müssen Penetrationstests auf Netzwerkebene definiert werden, die sämtliche Komponenten zur Unterstützung von Netzwerkfunktionen und Betriebssysteme enthalten. • Bei der Methodik müssen die in den letzten 12 Monaten aufgetretenen Bedrohungen und Sicherheitsrisiken berücksichtigt werden. • Es muss festgelegt sein, wo die Ergebnisse von Penetrationstests und Abhilfemaßnahmen gespeichert werden sollen.		2				
11.3.1 Durchführen externer Penetrationstests mindestens einmal im Jahr und nach jeder wesentlichen Infrastruktur- oder Anwendungsaktualisierung oder -änderung (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver in der Umgebung).		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
11.3.2 Durchführen interner Penetrationstests mindestens einmal im Jahr und nach jeder wesentlichen Infrastruktur- oder Anwendungsaktualisierung oder -änderung (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver in der Umgebung).		2				
11.3.3 Beim Penetrationstest ermittelte ausnutzbare Sicherheitsrisiken müssen behoben werden, und anschließend muss ein erneuter Test durchgeführt werden.		2				
11.3.4 Falls die CDE durch Segmentierung von anderen Netzwerken isoliert wird, muss bei mindestens jährlich und nach Änderungen an den Segmentierungskontrollen/-methoden durchzuführenden Penetrationstests geprüft werden, ob die Segmentierungsmethode funktioniert und effektiv ist und alle Systeme außerhalb des Bereichs von den Systemen innerhalb des CDE isoliert werden.		2				
11.3.4.1 Zusätzliche Anforderung nur für Dienstanbieter: Falls Segmentierung verwendet wird, bestätigen Sie den PCI-DSS-Umfang durch Durchführung von Penetrationstest an Segmentierungskontrollen, mindestens alle sechs Monate nach Änderungen an den Segmentierungsmethoden. *Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*		2				
11.4 Nutzung von Techniken zur Erkennung und/oder Verhinderung von Eindringversuchen in das Netzwerk. Überwachung des gesamten Datenverkehrs in der Umgebung der CDE sowie an kritischen Punkten innerhalb der CDE und Alarmierung des Personals bei mutmaßlichen Sicherheitsverletzungen. Ständige Aktualisierung der Systeme zur Erkennung und Verhinderung von Eindringversuchen, der Basis und der Signaturen.		2				
11.5 Bereitstellung von Systemen zur Erkennung von Änderungen (z. B. Tools zur Überwachung der Dateiintegrität), die das Personal über nicht autorisierte Änderungen (einschließlich Änderungen, Hinzufügungen und Löschungen) an wichtigen System-, Konfigurations- oder Inhaltsdateien alarmieren, und Konfiguration der Software für einen mindestens wöchentlich durchgeführten Vergleich wichtiger Dateien. *Hinweis: Zum Zwecke der Erkennung von Änderungen sind wichtige Dateien in der Regel Dateien, die sich nicht regelmäßig ändern, deren Änderung aber auf eine Sicherheitsverletzung im System oder auf das Risiko einer Verletzung hinweisen könnte. Systeme zur Änderungserkennung, wie beispielsweise Produkte zur Dateiintegritätsüberwachung, sind in der Regel bereits vorab mit wichtigen Dateien für das jeweilige Betriebssystem konfiguriert. Andere wichtige Dateien wie solche für benutzerdefinierte Anwendungen müssen von der jeweiligen Stelle (Händler oder Dienstanbieter) beurteilt und definiert werden.*				4		
11.5.1 Implementierung eines Prozesses zur Reaktion auf Alarme der Lösung zur Änderungserkennung.				4		
11.6 Die Sicherheitsrichtlinien und betrieblichen Verfahren zur Sicherheitsüberwachung und für Tests müssen dokumentiert sein, verwendet werden und allen Beteiligten bekannt sein.				4		
Anforderung 12: Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.						
12.1 Festlegen, Veröffentlichen, Verwalten und Verbreiten einer Sicherheitsrichtlinie.						6
12.1.1 Überarbeitung der Richtlinie mindestens einmal pro Jahr und Aktualisierung bei Umgebungsänderungen.						6

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
12.2 Implementierung eines Risikobewertungsprozesses, für den Folgendes gilt: • Der Prozess wird mindestens einmal im Jahr und nach wesentlichen Änderungen an der Umgebung (z. B. Übernahmen, Fusionen, Umzüge usw.) durchgeführt. • Beim Prozess werden wichtige Ressourcen, Bedrohungen und Sicherheitsrisiken ermittelt. • Der Prozess führt zu einer offiziellen, dokumentierten Risikoanalyse. Beispiele von Risikobewertungsmethoden sind unter anderen OCTAVE, ISO 27005 und NIST SP 800-30.	1					
12.3 Entwicklung von Verwendungsrichtlinien für wichtige Technologien und Definition der korrekten Verwendung dieser Technologien. *Hinweis: Beispiele für wichtige Technologien sind unter anderem Remotezugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, elektronische Wechselmedien, E-Mail-Programme und Internet-Anwendungen.* Die Verwendungsrichtlinien umfassen folgende Punkte:						6
12.3.1 Ausdrückliche Genehmigung durch autorisierte Parteien						6
12.3.2 Authentifizierung zur Verwendung der Technologie						6
12.3.3 Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff						6
12.3.4 Methode zur genauen und schnellen Bestimmung von Eigentümern, Kontaktinformationen und Zweck (z. B. Etikettierung und Codierung von Geräten sowie Einbuchung in den Bestand)						6
12.3.5 Akzeptable Verwendung der Technologie						6
12.3.6 Akzeptable Netzwerkorte für die Technologien						6
12.3.7 Liste der vom Unternehmen zugelassenen Produkte						6
12.3.8 Automatisches Trennen von Remotezugriff-Sitzungen nach einer bestimmten Zeit der Inaktivität						6
12.3.9 Aktivierung von Remotezugriff-Technologien für Anbieter und Geschäftspartner nur, wenn bei Anbietern und Geschäftspartnern ein dringender Bedarf besteht und die Technologie nach der Nutzung gleich wieder deaktiviert wird						6
12.3.10 Untersagen Sie Mitarbeitern, die auf Karteninhaberdaten per Remotezugriff zugreifen, die Daten auf lokale Festplatten und elektronische Wechselmedien zu kopieren, zu verschieben oder darauf zu speichern, sofern nicht ausdrücklich aufgrund bekannter geschäftlicher Bedürfnisse gestattet. Wenn ein bekanntes geschäftliches Bedürfnis besteht, muss in den Nutzungsrichtlinien festgelegt sein, dass die Daten entsprechend den geltenden PCI-DSS-Anforderungen geschützt werden.						6
12.4 Klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter in den Sicherheitsrichtlinien und Verfahren.						6
12.4.1 Zusätzliche Anforderung nur für Dienstanbieter: Die Geschäftsleitung hat die Verantwortung für den Schutz der Karteninhaberdaten und ein PCI-DSS-Konformitätsprogramm übernommen, das Folgendes beinhaltet: • Gesamtverantwortung für die Beibehaltung der PCI-PSS-Konformität • Definition einer Charta für das PCI-DSS-Konformitätsprogramm und die Kommunikation mit der Geschäftsleitung *Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*						6

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
12.5 Zuweisung der folgenden Managementverantwortungsbereiche in puncto Informationssicherheit zu einer Einzelperson oder einem Team:						6
12.5.1 Festlegen, Dokumentieren und Verteilen von Sicherheitsrichtlinien und -verfahren.						6
12.5.2 Überwachung und Analyse von Sicherheitsalarmen und -informationen und Verteilung an das entsprechende Personal.						6
12.5.3 Festlegen, Dokumentieren und Verteilen von Reaktions- und Eskalationsverfahren für Sicherheitsvorfälle, damit eine rechtzeitige und effektive Vorgehensweise in allen Situationen gewährleistet ist.		2				
12.5.4 Administration von Benutzerkonten, einschließlich Ergänzungen, Löschungen und Änderungen.						6
12.5.5 Überwachung und Kontrolle des gesamten Datenzugriffs.						6
12.6 Implementierung eines offiziellen Programms zur Förderung des Sicherheitsbewusstseins, das allen Mitarbeitern die Bedeutung der Sicherheitsrichtlinien und Verfahren für Karteninhaberdaten vermittelt.						6
12.6.1 Durchführung von Mitarbeiterschulungen bei der Einstellung und danach mindestens einmal im Jahr. Hinweis: Die Methoden sind abhängig von der Funktion der Mitarbeiter und deren Zugriffsrechten auf Karteninhaberdaten.						6
12.6.2 Die Mitarbeiter müssen mindestens einmal pro Jahr schriftlich bestätigen, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens gelesen und verstanden haben.						6
12.7 Überprüfen Sie potentielle neue Mitarbeiter, um das Risiko von Angriffen durch interne Quellen zu minimieren. (Beispiele für Hintergrundinformationen sind frühere Tätigkeiten, eventuelle Vorstrafen, die finanzielle Situation und Referenzen bisheriger Arbeitgeber.) *Hinweis: Für potentielle neue Mitarbeiter wie z. B. Kassierer, die nie Zugriff auf mehrere Kartennummern gleichzeitig haben, wenn eine Transaktion durchgeführt wird, ist diese Anforderung lediglich eine Empfehlung.*						6
12.8 Pflege und Implementierung von Richtlinien und Verfahren zur Verwaltung von Dienstanbietern, mit denen Karteninhaberdaten gemeinsam genutzt werden oder die Auswirkungen auf die Sicherheit von Karteninhaberdaten haben könnten, auf folgende Weise:		2				
12.8.1 Pflegen Sie eine Liste von Dienstanbietern mit Angabe der geleisteten Dienstleistungen.		2				
12.8.2 Aufbewahrung einer schriftlichen Vereinbarung mit einer Bestätigung dazu, dass der Dienstanbieter für die Sicherheit der Karteninhaberdaten haftet, die sich in seinem Besitz befinden bzw. die er für den Kunden speichert, verarbeitet oder überträgt, bzw. dahingehend, dass die Sicherheit der CDE betroffen sein könnte. *Hinweis: Der genaue Wortlaut einer Bestätigung hängt davon ab, was die beiden Parteien miteinander vereinbart haben, welche Dienste bereitgestellt wurden und welche Zuständigkeiten den Parteien zugewiesen wurden. Die Bestätigung muss nicht den exakten Wortlaut aus dieser Anforderung enthalten.*		2				
12.8.3 Festlegung eines eindeutigen Prozesses für die Inanspruchnahme von Dienstanbietern, der die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht.		2				
12.8.4 Einrichtung eines Programms zur mindestens einmal jährlichen Überwachung der Dienstanbieter-Konformität mit dem PCI-DSS.		2				
12.8.5 Verwaltung von Informationen darüber, welche PCI-DSS-Anforderungen von den einzelnen Dienstanbietern und welche von der Einheit verwaltet werden.		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein					
	1	2	3	4	5	6
12.9 Zusätzliche Anforderung nur für Dienstanbieter: Dienstanbieter bestätigen den Kunden gegenüber schriftlich, dass sie für die Sicherheit der Karteninhaberdaten haften, die sich in ihrem Besitz befinden bzw. die sie für den Kunden speichern, verarbeiten oder übertragen, bzw. dahingehend, dass die Sicherheit der CDE betroffen sein könnte. *Hinweis: Der genaue Wortlaut einer Bestätigung hängt davon ab, was die beiden Parteien miteinander vereinbart haben, welche Dienste bereitgestellt wurden und welche Zuständigkeiten den Parteien zugewiesen wurden. Die Bestätigung muss nicht den exakten Wortlaut aus dieser Anforderung enthalten.*		2				
12.10 Implementierung eines Vorfallreaktionsplans, der eine sofortige Reaktion auf Sicherheitsverletzungen im System ermöglicht.						
12.10.1 Erstellung des Vorfallreaktionsplans, der im Falle einer Sicherheitsverletzung im System eingesetzt wird. Der Plan umfasst mindestens die folgenden Punkte: • Rollen, Verantwortungsbereiche und Kommunikations-- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Kartenunternehmen • Konkrete Verfahren für die Reaktion auf Vorfälle • Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs • Verfahren zur Datensicherung • Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen • Abdeckung sämtlicher wichtigen Systemkomponenten • Verweis auf oder Einbeziehung von Verfahren der Kartenunternehmen zur Reaktion auf Vorfälle		2				
12.10.2 Überprüfen und testen Sie den Plan mindestens jährlich, einschließlich aller in Anforderung 12.10.1 genannter Elemente.		2				
12.10.3 Zur Reaktion auf Alarmmeldungen muss rund um die Uhr spezielles Personal verfügbar sein.		2				
12.10.4 Durchführung von Schulungen für Mitarbeiter, die für die Reaktion auf Sicherheitsverletzungen verantwortlich sind.		2				
12.10.5 Berücksichtigung von Alarmmeldungen aus Sicherheitsüberwachungssystemen wie IDS/IPS, Firewalls und Systemen zur Überwachung der Dateiintegrität.		2				
12.10.6 Entwicklung eines Prozesses zur Änderung und Weiterentwicklung des Vorfallreaktionsplans unter Berücksichtigung von eigenen Erkenntnissen und Branchenentwicklungen.		2				
12.11 Zusätzliche Anforderung nur für Dienstanbieter: Führen Sie mindestens einmal vierteljährlich Überprüfungen durch, um zu bestätigen, dass die Mitarbeiter den Sicherheitsrichtlinien und betrieblichen Verfahren folgen. Die Überprüfungen müssen die folgenden Prozesse abdecken: • Tägliche Überprüfung der Protokolle • Überprüfung der Firewall-Regelsätze • Anwendung von Konfigurationsstandards auf neue Systeme • Reaktion auf Sicherheitsalarme • Change-Management-Prozesse *Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*						6

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016

PCI-DSS-Anforderungen 3.2	Meilenstein 1	2	3	4	5	6
12.11.1 Zusätzliche Anforderung nur für Dienstanbieter: Pflegen Sie die Dokumentation des vierteljährlichen Überprüfungsprozesses, sodass diese Folgendes enthält: • Dokumentierung der Überprüfungsergebnisse • Überprüfung und Unterzeichnung der Ergebnisse durch Mitarbeiter, welchen die Verantwortung für das PCI-DSS-Konformitätsprogramm übertragen wurde *Hinweis: Diese Anforderung wird bis zum 31. Januar 2018 als bewährtes Verfahren betrachtet und anschließend zu einer vollwertigen Anforderung.*						6
Anhang A1: Zusätzliche PCI DSS-Anforderungen für gemeinsam verwendete Hosting-Anbieter						
A1 Schutz der gehosteten Umgebung und der Daten jeder Einheit (d. h. Händler, Dienstanbieter oder andere Einheiten) gemäß A1.1 bis A1.4: Ein Hosting-Anbieter muss diese Anforderungen sowie die anderen relevanten Abschnitte des PCI-Datensicherheitsstandards erfüllen. *Hinweis: Auch wenn ein Hosting-Anbieter diese Anforderungen erfüllt, ist nicht garantiert, dass die Stelle, die den Hosting-Anbieter nutzt, die Konformitätskriterien erfüllt. Jede Einheit muss PCI-DSS-konform arbeiten und die Konformität von Fall zu Fall beurteilen.*			3			
A1.1 In den einzelnen Einheiten dürfen nur Prozesse ausgeführt werden, die Zugriff auf die CDE dieser Einheit haben.			3			
A1.2 Beschränkung des Zugriffs und der Berechtigungen aller Einheiten auf die jeweils eigene CDE.			3			
A1.3 Für die CDE jeder Einheit müssen eindeutige, mit der PCI-DSS-Anforderung 10 konforme Protokollierungs- und Audit-Trails aktiviert sein.			3			
A1.4 Aktivierung von Prozessen für eine rechtzeitige Ursachenanalyse im Falle einer Sicherheitsverletzung bei einem gehosteten Händler oder Dienstanbieter.			3			
Anhang A2: Zusätzliche PCI-DSS-Anforderungen für Einheiten, die SSL/eine frühe Version von TLS verwenden *Hinweis: Dieser Anhang gilt für Einheiten, die SSL/eine frühe Version von TLS für den Schutz von CDE und/oder CHD verwenden*						
A2.1 Für POS-POI-Terminals (und die SSL/TLS Abschlusspunkte, mit welchen sich diese verbinden), die SSL und/oder eine frühe Version von TLS verwenden muss die Einheit entweder: • Bestätigen, dass die Geräte nicht anfällig für bekannte Sicherheitsrisiken dieser Protokolle sind. Oder: • Über einen offiziellen Plan zur Risikoabschwächung und Migration verfügen.		2				
A2.2 Einrichtungen mit vorhandenen Implementierungen (andere, als die in A2.1 erlaubten), die SSL und/oder frühe Versionen von TLS verwenden, müssen über einen offiziellen Plan zur Risikoabschwächung und Migration verfügen.		2				
A2.3 Zusätzliche Anforderung nur für Dienstanbieter: Alle Dienstanbieter müssen ab 30. Juni 2016 ein sicheres Serviceangebot vorhalten. *Hinweis: Vor dem 30. Juni 2016 muss der Dienstanbieter entweder die Option auf ein sicheres Protokoll in seinem Angebot einschließen, oder über einen dokumentierten Plan zur Risikoabschwächung und Migration (gemäß A2.2) verfügen, der einen Termin bis spätestens 30. Juni 2016 für die Einrichtung eines sicheren Protokolls vorsieht. Nach diesem Datum müssen alle Dienstanbieter die Option auf ein sicheres Protokoll für ihren Service vorhalten.*		2				

© 2016 PCI Security Standards Council LLC. Das vorliegende Dokument enthält ergänzende Informationen, die keinen Ersatz für die bestehenden PCI SSC Security Standards oder begleitende Dokumente darstellen.
Mai 2016