



**Payment Card Industry (PCI)
Datensicherheitsstandard
PCI-DSS-Navigation**

Verständnis der Intention der Anforderungen

Version 2.0

Oktober 2010

Dokumentänderungen

<i>Datum</i>	<i>Version</i>	<i>Beschreibung</i>
<i>1. Oktober 2008</i>	<i>1.2</i>	<i>Angleichen von Inhalten an den neuen PCI-DSS v1.2 und Implementieren kleinerer Änderungen an der Ursprungsversion v1.1.</i>
<i>28. Oktober 2010</i>	<i>2.0</i>	<i>Angleichen von Inhalten an den neuen PCI-DSS v2.0</i>

Inhalt

Dokumentänderungen	2
Vorwort.....	4
<i>Virtualisierung</i>	<i>5</i>
Karteninhaberdaten und vertrauliche Authentifizierungselemente	6
<i>Speicherort von Karteninhaberdaten und vertraulichen Authentifizierungsdaten</i>	<i>8</i>
<i>Spur 1 vs. Spur 2 Daten</i>	<i>9</i>
Zugehörige Anleitungen für den PCI-Datensicherheitsstandard.....	10
Leitfaden für die Anforderungen 1 und 2: Erstellung und Aufrechterhaltung eines sicheren Netzwerks	11
<i>Anforderung 1: Installation und Aufrechterhaltung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten</i>	<i>11</i>
<i>Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden..</i>	<i>19</i>
Leitfaden für die Anforderungen 3 und 4: Schutz von Karteninhaberdaten	22
<i>Anforderung 3: Schutz gespeicherter Karteninhaberdaten</i>	<i>22</i>
<i>Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze</i>	<i>31</i>
Leitfaden für die Anforderungen 5 und 6: Unterhaltung eines Anfälligkeits-Managementprogramms.....	33
<i>Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware</i>	<i>33</i>
<i>Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen.....</i>	<i>35</i>
Leitfaden für die Anforderungen 7, 8 und 9: Implementierung starker Zugriffskontrollmaßnahmen.....	44
<i>Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf.....</i>	<i>44</i>
<i>Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff.....</i>	<i>46</i>
<i>Anforderung 9: Beschränken Sie den physischen Zugriff auf Karteninhaberdaten</i>	<i>51</i>
Leitfaden für die Anforderungen 10 und 11: Regelmäßige Überwachung und Testen von Netzwerken.....	55
<i>Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten</i>	<i>55</i>
<i>Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse.....</i>	<i>60</i>
Leitfaden für die Anforderung 12: Befolgung einer Informationssicherheits-Richtlinie.....	66
<i>Anforderung 12: Pflegen Sie eine Informationssicherheits-Richtlinie für das gesamte Personal</i>	<i>66</i>
Leitfaden für die Anforderung A.1: Zusätzliche PCI-DSS-Anforderungen für von mehreren Benutzern gemeinsam genutzte Hosting-Anbieter.....	73
Anhang A: PCI-Datensicherheitsstandard: Damit verbundene Dokumente	75

Vorwort

Dieses Dokument enthält eine Beschreibung der 12 Anforderungen in den Datensicherheitsstandards der Zahlungskartenindustrie (Payment Card Industry Data Security Standard, PCI-DSS) sowie einen Leitfaden, in dem der Zweck jeder einzelnen Anforderung beschrieben wird. Dieses Dokument ist als Hilfestellung für Händler, Dienstanbieter und Finanzinstitutionen gedacht, die sich näher über die Datensicherheitsstandards der Zahlungskartenindustrie, deren einzelne Bedeutung und den Zweck der ausführlichen Anforderungen zur Sicherung von Systemkomponenten (Server, Netzwerk, Anwendungen usw.) mit Datenumgebungen für Karteninhaberdaten informieren möchten.

HINWEIS: PCI DSS-Navigation: Das Dokument „Verständnis der Intention der Anforderungen“ ist nur zur Orientierung vorgesehen. Wenn Sie vor Ort eine PCI-DSS-Beurteilung oder einen Selbstbeurteilungsfragebogen ausfüllen, sind die archivierbaren Dokumente die PCI-DSS Anforderungen und Sicherheitsbeurteilungsverfahren sowie die PCI-DSS-Selbstbeurteilungsfragebögen 2.0.

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

- Netzwerkkomponenten umfassen unter anderem Firewalls, Switches, Router, Zugriffspunkte für drahtlose Netzwerke, Netzwerkgeräte und andere Sicherheitsgeräte.
- Zu Servertypen zählen unter anderem: Web, Anwendung, Datenbank, Authentifizierung, Mail, Proxy, Network Time Protocol (NTP) und Domain Name Server (DNS).
- Zu Anwendungen zählen unter anderem alle erworbenen und benutzerdefinierten Anwendungen, darunter auch interne und externe (z. B. Internet-)Anwendungen.

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

- Die betreffende Stelle identifiziert und dokumentiert sämtliche vorhandenen Karteninhaberdaten in ihrer Umgebung, um sicherzustellen, dass keine Karteninhaberdaten außerhalb der derzeit definierten Karteninhaberdaten-Umgebung (Englisch: Cardholder data environment, CDE) existieren.
- Sobald alle Speicherorte von Karteninhaberdaten identifiziert und dokumentiert sind, setzt die betreffende Stelle die entsprechenden Ergebnisse ein, um zu überprüfen, ob der PCI-DSS-Umfang angemessen ist (die Ergebnisse können z. B. in Form eines Diagramms oder eines Bestands der Speicherorte von Karteninhaberdaten dargestellt werden).
- Die Stelle prüft die Aufnahme aller lokalisierten Karteninhaberdaten in den Umfang der PCI-DSS-Bewertung und Teile der CDE, sofern diese Daten nicht gelöscht oder in die/der derzeit definierten CDE übertragen/konsolidiert wurden.

- Die Stelle bewahrt entsprechende Unterlagen auf, um nachzuweisen, wie der PCI-DSS-Umfang bestätigt wurde, sowie die Ergebnisse für eventuelle Kontrollen durch den Prüfer und/oder als Referenz für den Bestätigungsvorgang des PCI-DSS-Umfangs im Folgejahr.

Die Netzwerksegmentierung oder Isolierung (Segmentierung) der Karteninhaberdaten-Umgebung vom Rest des Unternehmensnetzwerks einer Stelle ist keine PCI-DSS-Anforderung. Sie wird jedoch unbedingt als Methode empfohlen, um den Umfang der Karteninhaberdaten-Umgebung einzuschränken. Ein qualifizierter Sicherheitsprüfer (Qualified Security Assessor oder QSA) kann bei der Bestimmung des Umfangs einer Karteninhaberdaten-Umgebung einer Stelle behilflich sein und Orientierungshilfe dazu bieten, wie der Umfang einer PCI-DSS-Bewertung durch die Implementierung einer geeigneten Netzwerksegmentierung eingeschränkt werden kann.

Bei Fragen, ob eine bestimmte Implementierung mit dem Standard übereinstimmt oder „konform“ mit einer spezifischen Anforderung ist, empfiehlt der PCI-SSC Unternehmen, einen QSA hinzuzuziehen, um ihre Implementierung der Technologie und Prozesse sowie die Konformität mit dem PCI-Datensicherheitsstandard zu bestätigen. Die Erfahrung des QSAs im Umgang mit komplexen Netzwerkumgebungen bereichert den Händler oder Dienstleister, der die Konformität mit den Richtlinien anstrebt, um bewährte Praktiken und Leitfäden. Die PCI-SSC-Liste qualifizierter Sicherheitsprüfer ist unter folgender Adresse abrufbar: <https://www.pcisecuritystandards.org>.

Virtualisierung

Wenn eine Virtualisierungstechnologie implementiert wird, müssen alle Komponenten innerhalb der virtuellen Umgebung, einschließlich einzelne virtuelle Hosts oder Geräte, Guest-Rechner, Anwendungen, Managementschnittstellen, zentrale Managementkonsolen, Hypervisoren usw. identifiziert und in der Überprüfung berücksichtigt werden. Alle Intra-Host-Kommunikationen und Datenflüsse sowie sämtliche Kommunikationen zwischen der virtuellen Komponente und anderen Systemkomponenten müssen identifiziert und dokumentiert werden.

Die Implementierung einer virtuellen Umgebung muss die Intentionen aller Anforderungen erfüllen, damit die virtualisierten Systeme tatsächlich als separate Hardware angesehen werden können. Beispielweise muss eine klare Segmentierung der Funktionen und Netzwerke mit verschiedenen Sicherheitsebenen vorhanden sein; die Segmentierung muss die Weitergabe von Produktions- und Test-/Entwicklungsumgebungen verhindern; die virtuelle Konfiguration muss so gesichert sein, dass Sicherheitslücken in einer Funktion nicht die Sicherheit anderer Funktionen in Mitleidenschaft ziehen können; und angeschlossene Gerät wie etwa USB-/serielle Geräte sollten nicht von allen virtuellen Instanzen erreichbar sein.

Darüber hinaus sollten alle virtuellen Protokolle der Managementschnittstelle in der Systemdokumentation enthalten sein und es müssen die Rollen und Berechtigungen für die Verwaltung virtueller Netzwerke und virtueller Systemkomponenten definiert werden. Virtualisierungsplattformen müssen in der Lage sein, die Trennung von Aufgaben und Mindestberechtigungen durchzusetzen, um die Verwaltung des virtuellen Netzwerkes von der Verwaltung des virtuellen Servers zu trennen.

Besondere Aufmerksamkeit ist auch bei der Implementierung von Authentifizierungssteuerungen gefragt, um sicherzustellen, dass sich die Benutzer in den richtigen virtuellen Systemkomponenten anmelden und dass zwischen den Guest-VMs (virtuelle Rechner, Englisch: virtual machines) und dem Hypervisor unterschieden wird.

Karteninhaberdaten und vertrauliche Authentifizierungsdatenelemente

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

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

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

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

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

In der folgenden Tabelle sind häufig verwendete Elemente an Karteninhaberdaten und vertraulichen Authentifizierungsdaten aufgeführt. Außerdem wird für jedes Datenelement angegeben, ob die **Speicherung** des jeweiligen Elements zulässig oder verboten ist und ob die einzelnen Datenelemente **geschützt** werden müssen. Diese Tabelle erhebt keinen Anspruch auf Vollständigkeit, sondern dient dazu, die verschiedenen Arten von Anforderungen darzustellen, die für jedes Datenelement gelten.

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

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

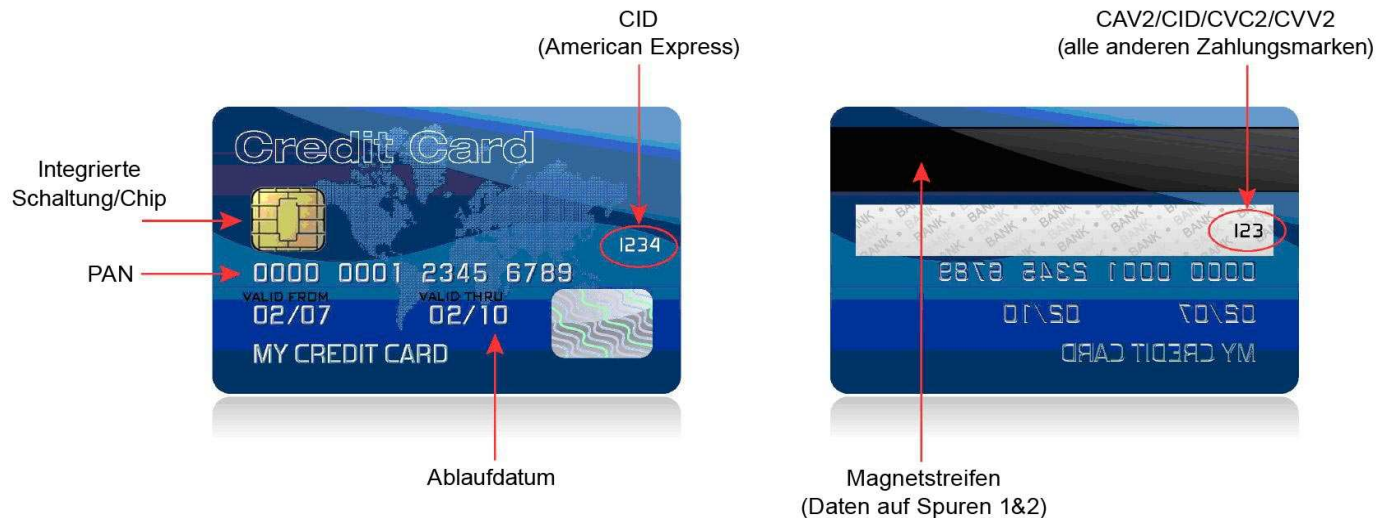
Der PCI-DSS **gilt nur**, wenn PANs gespeichert, verarbeitet und/oder übertragen werden.

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

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

Speicherort von Karteninhaberdaten und vertraulichen Authentifizierungsdaten

Vertrauliche Authentifizierungsdaten bestehen aus Magnetstreifendaten (oder Verfolgungsdaten)³, Kartvalidierungscode oder -wert⁴ und PIN-Daten⁵. **Die Speicherung vertraulicher Authentifizierungsdaten ist nicht zulässig!** Diese Daten sind für Personen mit böswilligen Absichten von großem Wert, zumal sie ihnen ermöglichen, gefälschte Zahlungskarten zu generieren und betrügerische Transaktionen zu erstellen. Für eine vollständige Definition des Begriffs „vertrauliche Authentifizierungsdaten“ konsultieren Sie das *Glossar, die Abkürzungen und Akronyme zum PCI-DSS und PA-DSS*. Die nachstehenden Abbildungen auf der Vorder- und Rückseite einer Kreditkarte zeigen die Speicherstelle der Karteninhaberdaten und der vertraulichen Authentifizierungsdaten.

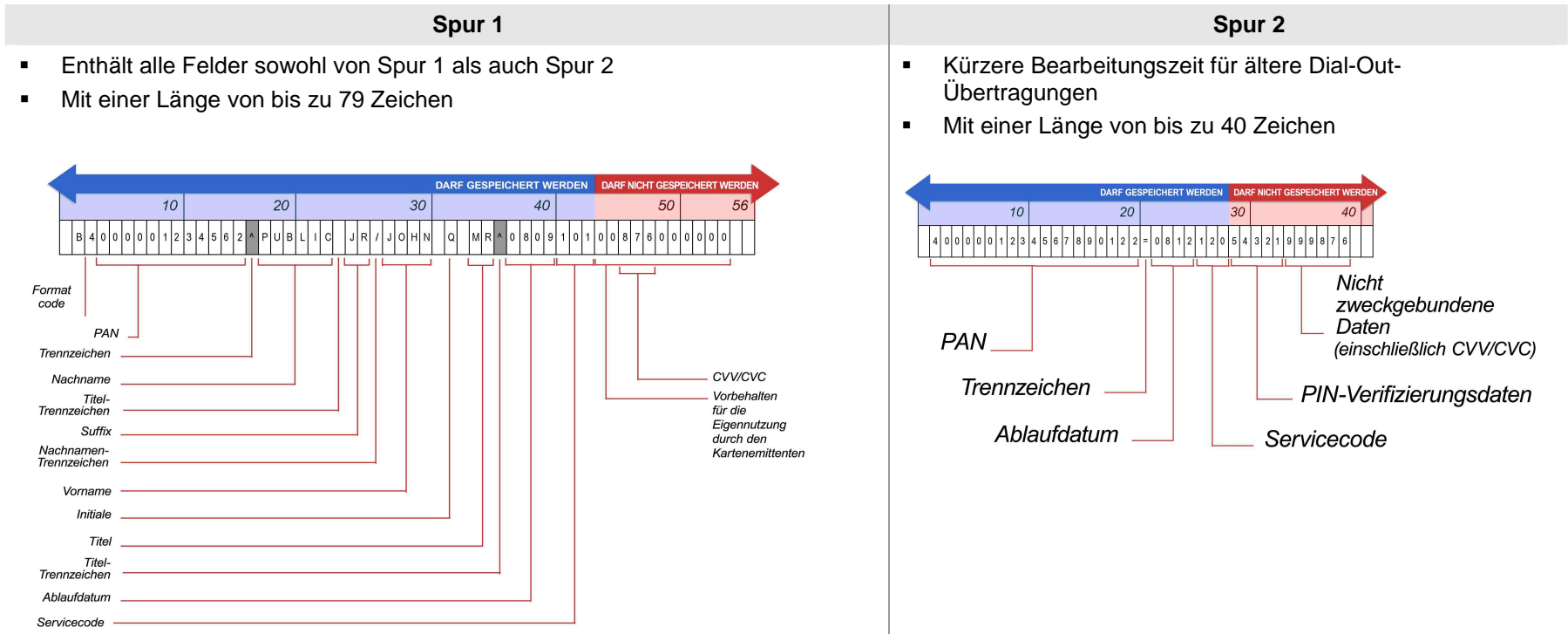


Hinweis: Der Chip enthält spurähnliche Daten sowie andere vertrauliche Daten, einschließlich dem Mikrochipkarten-Prüfwert (auch bekannt unter den Bezeichnungen Chip CVC, iCVV, CAV3 oder iCSC).

- ³ Im Magnetstreifen verschlüsselte Daten, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Diese Daten können auch auf einem Chip oder unter einem anderen Speicherort der Karte gespeichert werden. Einheiten dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifendaten speichern. Die einzigen Elemente der Verfolgungsdaten, die aufbewahrt werden dürfen, sind die primäre Kontonummer, der Name des Karteninhabers, das Ablaufdatum und der Servicecode.
- ⁴ Der drei- oder vierstellige Wert, der im oder rechts neben dem Unterschriftenfeld bzw. vorne auf einer Zahlungskarte aufgedruckt ist und zur Verifizierung von Transaktionen bei nicht vorliegender Karte verwendet wird.
- ⁵ Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht.

Spur 1 vs. Spur 2 Daten

Wenn vollständige Spurdaten (entweder Spur 1 oder Spur 2, vom Magnetstreifen, dem Magnetstreifenbild auf dem Chip oder anderswo) gespeichert werden, können böswillige Personen, die in den Besitz dieser Daten gelangen, Zahlungskarten reproduzieren und in aller Welt verkaufen. Ferner verstößt die Speicherung von vollständigen Spurdaten gegen die Betriebsordnung von Zahlungsmarken und kann zu Bußgeldern und Strafen führen. Die Illustration unten liefert Informationen über die Daten der Spur 1 und Spur 2 und deren Unterschiede und veranschaulicht ihre Anordnung so wie sie auf dem Magnetstreifen gespeichert werden.



Hinweis: Nicht zweckgebundene Datenfelder werden vom Kartenemittenten und/oder vom Kreditkartenunternehmen definiert. Vom Emittenten definierte Felder mit Daten, die vom Emittenten bzw. der Zahlungsmarke nicht als vertrauliche Authentifizierungsdaten angesehen werden, können auf der Spur in dem Teil mit den nicht zweckgebundenen Daten integriert werden. Zulässig wäre es auch, diese besonderen Daten unter bestimmten, vom Emittenten und/oder dem Kreditkartenunternehmen definierten Umständen und Bedingungen zu speichern.

Daten, die jedoch als vertrauliche Authentifizierungsdaten behandelt werden, ganz gleich, ob sie in einem zweckgebundenem Feld enthalten sind oder nicht, dürfen nach der Autorisierung nicht länger gespeichert werden.

Zugehörige Anleitungen für den PCI-Datensicherheitsstandard

Erstellung und Wartung eines sicheren Netzwerks

- Anforderung 1: Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
- Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden

Schutz von Karteninhaberdaten

- Anforderung 3: Schutz gespeicherter Karteninhaberdaten
- Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze

Unterhaltung eines Anfälligkeits-Managementprogramms

- Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware
- Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

Implementierung starker Zugriffskontrollmaßnahmen

- Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf
- Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff
- Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken

Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken

- Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
- Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

Befolgung einer Informationssicherheits-Richtlinie

- Anforderung 12: Pflegen Sie eine Informationssicherheits-Richtlinie für das gesamte Personal.

Leitfaden für die Anforderungen 1 und 2: Erstellung und Aufrechterhaltung eines sicheren Netzwerks

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

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

Eine Firewall untersucht den gesamten Netzwerkverkehr und blockiert die Übertragungen, die die angegebenen Sicherheitskriterien nicht erfüllen. Alle Systeme müssen vor dem unbefugten Zugriff von nicht vertrauenswürdigen Netzwerken geschützt werden, und zwar unabhängig davon, ob sie über das Internet als E-Commerce, über den Internetzugang der Mitarbeiter über Desktop-Browser, den E-Mail-Zugriff von Mitarbeitern, dedizierte Verbindungen, wie z. B. Business-to-Business-Verbindungen, über drahtlose Netzwerke oder über andere Quellen in das System gelangen. Häufig können scheinbar unbedeutende Wege in und aus nicht vertrauenswürdigen Netzwerken ungeschützte Wege in wichtige Systeme eröffnen. Firewalls sind für jedes Computernetzwerk ein wichtiger Schutzmechanismus.

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

Anforderung	Leitfaden
1.1 Festlegen von Standards für die Firewall- und Routerkonfiguration, die Folgendes beinhalten:	<p>Firewalls und Router sind zentrale Komponenten in der Architektur, die den Ein- und Ausgang des Netzwerks kontrollieren. Diese Einrichtungen sind Softwareprogramme oder Hardware-Geräte, die ungewünschte Zugriffe blockieren und zulässige ein- und ausgehende Zugriffe des Netzwerkes verwalten. Ohne entsprechende Richtlinien und Verfahren zur Dokumentation dessen, wie Mitarbeiter Firewalls und Router konfigurieren sollten, könnte ein Unternehmen leicht seine erste Verteidigungslinie in Sachen Datenschutz einbüßen. Dank dieser Richtlinien und Verfahren wird die erste Verteidigungslinie eines Unternehmens in Sachen Datenschutz aufrechterhalten.</p> <p>Virtuelle Umgebungen, in denen Datenflüsse kein physisches Netzwerk passieren, sollten bewertet werden, um sicherzustellen, dass eine angemessene Netzwerksegmentierung erreicht wurde.</p>
1.1.1 Ein offizieller Prozess zur Genehmigung und zum Testen aller Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration	<p>Eine Richtlinie und ein Prozess zur Genehmigung und Überprüfung aller Verbindungen und Änderungen, die an Firewalls und Routern vorgenommen wurden, helfen dabei, Sicherheitsprobleme durch Fehlkonfigurationen des Netzwerks, des Routers oder der Firewall zu vermeiden.</p> <p>In der Richtlinie und dem Prozess sollten auch Datenflüsse zwischen virtuellen Rechnern eingeschlossen werden.</p>

Anforderung	Leitfaden
<p>1.1.2 Ein aktuelles Netzwerkdiagramm mit allen Verbindungen mit Karteninhaberdaten einschließlich aller drahtlosen Netzwerke</p>	<p>Mithilfe von Netzwerkdiagrammen kann ein Unternehmen den Standort all seiner Netzwerkgeräte ermitteln. Darüber hinaus kann das Netzwerkdiagramm verwendet werden, um den Datenfluss von Karteninhaberdaten im Netzwerk und zwischen einzelnen Geräten abzubilden, um den Umfang der Karteninhaberdaten-Umgebung vollends zu erfassen. Ohne ein aktuelles Netzwerk- und Datenflussdiagramm können Geräte mit Karteninhaberdaten übersehen und unwissentlich nicht in die mehrstufigen, im Sinne des PCI-DSS implementierten, Sicherheitskontrollen eingeschlossen und somit anfällig für Sicherheitsrisiken gemacht werden.</p> <p>Netzwerk- und Datenflussdiagramme sollten virtuelle Systemkomponenten enthalten und Intra-Host-Datenflüsse dokumentieren.</p>
<p>1.1.3 Anforderungen für eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone</p>	<p>Durch den Einsatz einer Firewall für alle eingehenden (sowie ausgehenden) Verbindungen ermöglicht es das Netzwerk dem Unternehmen, ein- und ausgehende Zugriffe zu überwachen und zu kontrollieren und somit die Aussichten einer böswilligen Person dazu, sich Zugriff auf das interne Netzwerk zu verschaffen, zu minimieren.</p>
<p>1.1.4 Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die logische Verwaltung der Netzwerkkomponenten</p>	<p>Diese Beschreibung der Rollen und die Zuweisung von Verantwortlichkeiten gewährleisten, dass eine Person klar für die Sicherheit aller Komponenten verantwortlich und sich dieser Pflicht auch bewusst ist, außerdem bleiben somit keine Geräte unverwaltet.</p>

Anforderung	Leitfaden
<p>1.1.5 Dokumentation und Begründung für den Einsatz aller zulässigen Services, Protokolle und Ports, einschließlich der Dokumentation von Sicherheitsfunktionen für die Protokolle, die als unsicher gelten.</p> <p>Zu unsicheren Diensten, Protokollen oder Ports gehören unter anderem FTP, Telnet, POP3, IMAP und SNMP.</p>	<p>Sicherheitsverletzungen treten häufig durch unbenutzte oder unsichere Dienste und Ports auf, zumal diese nicht selten bekannte Sicherheitslücken aufweisen. Viele Unternehmen sind für derartige Sicherheitsverletzungen anfällig, da sie Schwachstellen in ungenutzten Diensten, Protokollen und Ports nicht mithilfe von Patches beheben (selbst wenn diese Sicherheitslücken noch immer vorzufinden sind). Alle Unternehmen sollten eine eindeutige Entscheidung darüber treffen, welche Dienste, Protokolle und Ports für ihre Geschäfte erforderlich sind und sie in ihren Unterlagen dokumentieren und letztendlich dafür sorgen, dass alle übrigen Dienste, Protokolle und Ports deaktiviert oder gelöscht werden. Außerdem sollten Unternehmen in Erwägung ziehen, allen Verkehr zu blockieren und diese Ports nur dann erneut zu öffnen, wenn deren Notwendigkeit festgestellt und dokumentiert wurde.</p> <p>Dann gibt es noch zahlreiche Dienste, Protokolle oder Ports, die ein Unternehmen unter Umständen benötigt (oder standardmäßig aktiviert hat) und die wiederholt von böswilligen Personen ausgenutzt werden, um ein Netzwerk zu beschädigen. Wenn diese unsicheren Dienste, Protokolle oder Ports für ein Unternehmen wichtig sind, muss das Risiko, das aus der Nutzung dieser Protokolle erwächst, verstanden und von dem Unternehmen akzeptiert werden und außerdem die Nutzung des Protokolls begründet und Sicherheitsfunktionen dokumentiert und implementiert werden, die eine sichere Nutzung dieser Protokolle gewährleisten. Wenn diese unsicheren Dienste, Protokolle oder Ports für ein Unternehmen nicht wesentlich sind, sollten sie deaktiviert oder gelöscht werden.</p>
<p>1.1.6 Anforderung zum Prüfen von Firewall- und Router-Regelsätzen mindestens alle sechs Monate</p>	<p>Diese Überprüfung bietet dem Unternehmen die Gelegenheit, mindestens alle sechs Monate sämtliche unnötigen, veralteten oder fehlerhaften Regeln zu entfernen und sicherzustellen, dass alle Regelsätze nur autorisierte Dienste und Ports zulassen, die einen Nutzen für das Unternehmen haben.</p> <p>Es empfiehlt sich, diese Überprüfungen häufiger durchzuführen, beispielsweise monatlich, um sicherzustellen, dass die Regelsätze aktuell sind und den Bedürfnissen des Unternehmens entsprechen, ohne Sicherheitslücken zu öffnen und unnötige Risiken einzugehen.</p>

Anforderung	Leitfaden
<p>1.2 Aufbauen von Firewall- und Router-Konfigurationen, die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der Karteninhaberdaten-Umgebung einschränken.</p> <p><i>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.</i></p>	<p>Es muss ein Netzwerkschutz installiert werden, und zwar eine Systemkomponente mit (mindestens) einer Stateful-Inspection-Firewall-Funktion zwischen dem internen, vertrauenswürdigen Netzwerk und anderen nicht vertrauenswürdigen Netzwerken, die extern aufgestellt und/oder nicht von der betreffenden Stelle kontrolliert oder verwaltet werden können. Wird es versäumt, diese Maßnahme korrekt zu implementieren, setzt sich die betreffende Stelle unerlaubten Zugriffen durch böswillige Personen oder schädliche Softwares aus.</p> <p>Wenn die Firewall-Funktion installiert ist, jedoch Regeln fehlen, die bestimmten Datenverkehr kontrollieren oder einschränken, sind böswillige Personen unter Umständen noch immer in der Lage, gefährdete Protokolle und Ports auszunutzen, um Ihr Netzwerk anzugreifen.</p>
<p>1.2.1 Beschränken des ein- und ausgehenden Netzwerkverkehrs auf den für die Karteninhaberdaten-Umgebung absolut notwendigen Verkehr.</p>	<p>Diese Anforderung soll verhindern, dass böswillige Personen auf das Netzwerk des Unternehmens über unerlaubte IP-Adressen zugreifen oder Dienste, Protokolle oder Ports auf missbräuchliche Art und Weise nutzen (z. B. indem sie Daten, an die sie über Ihr Netzwerk gelangt sind, an einen nicht vertrauenswürdigen Server senden).</p> <p>Alle Firewalls sollten eine Regel beinhalten, die unnötigen eingehenden und ausgehenden Datenverkehr ablehnt. Hierdurch werden unbeabsichtigte Sicherheitslücken vermieden, die anderweitigen, unerwünschten und möglicherweise schädlichen eingehenden sowie ausgehenden Datenverkehr zulassen.</p>
<p>1.2.2 Sichern und Synchronisieren von Router-Konfigurationsdateien.</p>	<p>Während ausgeführte Konfigurationsdateien normalerweise mit sicheren Einstellungen implementiert werden, können Startdateien (Router führen diese Dateien nur bei einem Neustart aus) nicht mit denselben sicheren Einstellungen implementiert werden, da sie nur gelegentlich ausgeführt werden. Wenn ein Router ohne die sicheren Einstellungen von ausgeführten Konfigurationsdateien neu gestartet wird, können daraus schwächere Regeln entstehen, die böswilligen Personen den Zugriff auf das Netzwerk ermöglichen, da die Startdateien nicht mit denselben sicheren Einstellungen wie die ausgeführten Konfigurationsdateien implementiert werden können.</p>

Anforderung	Leitfaden
<p>1.2.3 Installieren von Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der Karteninhaberdaten-Umgebung und Konfigurieren dieser Firewalls, sodass der gesamte Verkehr aus der drahtlosen Umgebung abgelehnt oder kontrolliert wird (sofern dieser Verkehr für Geschäftszwecke notwendig ist).</p>	<p>Die bekannte (oder nicht bekannte) Implementierung und Ausnutzung von Drahtlostechnologie in einem Netzwerk ist eine altbewährte Methode für böswillige Individuen, um sich Zugriff zu einem Netzwerk und zu Karteninhaberdaten zu verschaffen. Wenn ein drahtloses Gerät oder Netzwerk ohne das Wissen eines Unternehmens installiert wird, könnte sich eine böswillige Person mühelos und „heimlich“ Zugang zum Netzwerk verschaffen. Wenn Firewalls nicht den Zugriff von drahtlosen Netzwerken auf die Zahlungskarten-Umgebung einschränken, könnten sich böswillige Individuen, die sich unerlaubten Zugang zu dem drahtlosen Netzwerk verschafft haben, mit der Zahlungskarten-Umgebung verbinden und Kontoinformationen kompromittieren.</p> <p>Firewalls müssen zwischen allen drahtlosen Netzwerken und der Karteninhaberdaten-Umgebung installiert sein, unabhängig von der Aufgabe der Umgebung, mit der das drahtlose Netzwerk verbunden ist. Darunter fallen unter anderem Unternehmensnetzwerke, Einzelhandelsgeschäfte, Lager-Umgebungen usw.</p>
<p>1.3 Verboten des direkten öffentlichen Zugriffs zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung.</p>	<p>Der Zweck einer Firewall liegt darin, alle Verbindungen zwischen öffentlichen und internen Systemen zu verwalten und zu kontrollieren (insbesondere jene, die Karteninhaberdaten speichern, verarbeiten oder übertragen). Wenn Direktzugriffe zwischen öffentlichen Systemen und der Karteninhaberdaten-Umgebung zugelassen werden, kann der von der Firewall gebotene Schutz umgangen werden und Systemkomponenten, auf denen Karteninhaberdaten gespeichert werden, können Gefahren ausgesetzt sein.</p>
<p>1.3.1 Implementieren einer DMZ, um den eingehenden Datenverkehr auf Systemkomponenten zu beschränken, die zugelassene, öffentlich erhältliche Dienste, Protokolle und Ports anbieten.</p>	<p>Die DMZ ist der Teil des Netzwerkes, der die Verbindungen zwischen dem Internet (oder anderen nicht vertrauenswürdigen Netzwerken) und internen Diensten verwaltet, die ein Unternehmen der Öffentlichkeit zur Verfügung stellen muss (beispielsweise ein Webserver). Sie ist die erste Verteidigungslinie bei der Isolierung und Trennung des Datenverkehrs, der mit dem internen Netzwerk kommunizieren muss, von jedem Datenverkehr, der nicht mit dem internen Netzwerk kommuniziert.</p> <p>Diese Funktion soll verhindern, dass böswillige Personen auf das Netzwerk des Unternehmens über unerlaubte IP-Adressen zugreifen oder Dienste, Protokolle oder Ports auf missbräuchliche Art und Weise nutzen.</p>
<p>1.3.2 Beschränken des eingehenden Internetverkehrs auf IP-Adressen innerhalb der DMZ.</p>	<p>Die Bereitstellung von IP-Verbindungen zur DMZ bietet Gelegenheit zur Prüfung und Einschränkung von Quelle/Ziel und/oder zur Prüfung bzw. Blockierung von Inhalten, d. h. zur Vorbeugung ungefilterter Zugriffe zwischen nicht vertrauenswürdigen und bekannten Umgebungen.</p>

Anforderung	Leitfaden
<p>1.3.3 Keine direkten eingehenden oder ausgehenden Verbindungen für Datenverkehr zwischen dem Internet und der Karteninhaberdaten-Umgebung zulassen.</p>	<p>Die Bereitstellung von eingehenden und ausgehenden IP-Verbindungen bietet Gelegenheit zur Prüfung und Einschränkung von Quelle/Ziel und/oder zur Prüfung bzw. Blockierung von Inhalten, d. h. zur Vorbeugung ungefilterter Zugriffe zwischen nicht vertrauenswürdigen und bekannten Umgebungen. Hierdurch wird beispielsweise vermieden, dass böswillige Personen Daten, an die sie über Ihr Netzwerk gelangt sind, an einen externen nicht vertrauenswürdigen Server in einer unbekanntem Umgebung senden.</p>
<p>1.3.4 Nicht zulassen, dass interne Adressen aus dem Internet in die DMZ übergeben werden.</p>	<p>Normalerweise enthält ein Paket die IP-Adresse des Computers, von dem das Paket stammt. Hierdurch sind andere Computer im Netzwerk in der Lage, den Ursprung des Pakets zu erfahren. In bestimmten Fällen kann die IP-Adresse von böswilligen Personen gefälscht werden.</p> <p>Zum Beispiel senden böswillige Individuen ein Paket mit einer gefälschten Adresse, sodass (sofern Ihre Firewall dies nicht unterbindet) das Paket über das Internet in Ihr Netzwerk gelangen kann und zudem den Anschein erweckt, dass es sich um internen und somit zulässigen Datenverkehr handelt. Sobald sich der Angreifer Zugang zu Ihrem Netzwerk verschafft hat, ist er in der Lage, Ihre Systeme zu kompromittieren.</p> <p>Die Ingress-Filterung ist eine Technik, der Sie sich in Ihrer Firewall bedienen können, um Pakete zu filtern, die in Ihr Netzwerk gelangen, um unter anderem sicherzustellen, dass die Pakete nicht „gefälscht“ sind, um den Anschein zu erwecken, sie kämen aus Ihrem eigenen internen Netzwerk.</p> <p>Für ausführlichere Informationen zum Thema Paketfilterung informieren Sie sich bitte über die sogenannte „Ingress-Filterung“.</p>
<p>1.3.5 Keinen nicht autorisierten ausgehenden Datenverkehr von der Karteninhaberdaten-Umgebung zum Internet zulassen.</p>	<p>Der gesamte von der Karteninhaberdaten-Umgebung ausgehende Datenverkehr sollte ausgewertet werden, um sicherzustellen, dass er den implementierten, zugelassenen Regeln entspricht. Die Verbindungen sollten überprüft werden, um den Datenverkehr ausschließlich auf zugelassene Kommunikationen zu beschränken (z. B. indem Quell-/Ziel-Adressen bzw. Ports eingeschränkt und/oder Inhalte blockiert werden).</p> <p>In Umgebungen, in denen keine eingehenden Verbindungen zulässig sind, können ausgehende Verbindungen über Architekturen und Systemkomponenten erreicht werden, die die IP-Verbindungen unterbrechen und prüfen.</p>
<p>1.3.6 Implementieren der statusgesteuerten Inspektion, die auch als dynamische Paketfilterung bekannt ist. (Das bedeutet, dass nur „etablierte“ Verbindungen in das Netzwerk zulässig sind.)</p>	<p>Eine Firewall, die Stateful Packet Inspections ausführt, hält den „Zustand“ (oder den Status) aller Verbindungen zur Firewall. Indem der „Zustand“ gehalten wird, weiß die Firewall, ob es sich bei den vermeintlichen Antworten tatsächlich um Antworten auf eine vorige Verbindung (indem sie sich vorige Verbindungen „merkt“) oder um einen Angreifer oder eine schädliche Software handelt, der oder die versucht, die Firewall zu täuschen, damit sie die Verbindung zulässt.</p>

Anforderung	Leitfaden
<p>1.3.7 Speichern Sie Systemkomponenten, die Karteninhaberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauenswürdigen Netzwerken getrennt ist.</p>	<p>Karteninhaberdaten erfordern den höchsten Grad an Datenschutz. Wenn Karteninhaberdaten innerhalb einer DMZ gespeichert sind, ist es aufgrund der geringeren Schichten, in die es einzudringen gilt, für einen externen Angreifer einfacher, sich Zugriff auf diese Informationen zu verschaffen.</p> <p>Hinweis: Diese Anforderung umfasst nicht die Speicherung auf flüchtigen Arbeitsspeichern.</p>
<p>1.3.8 Geben Sie keine privaten IP-Adressen und Routing-Informationen an unbefugte Dritte weiter.</p> <p>Hinweis: Zu den Methoden zum Verbergen von IP-Adressen zählen unter anderem:</p> <ul style="list-style-type: none"> ▪ Network Address Translation (NAT) ▪ Das Platzieren von Servern mit Karteninhaberdaten hinter Proxy-Servern/Firewalls oder Inhalts-Caches, ▪ Löschen oder Filtern von Route-Advertisements für private Netzwerke, die registrierte Adressen verwenden, ▪ Interne Nutzung eines RFC1918-Adressraums anstatt registrierter Adressen. 	<p>Es ist von zentraler Bedeutung, die Übertragung von IP-Adressen einzuschränken, um zu verhindern, dass Hacker die IP-Adressen des internen Netzwerkes erfahren und diese Informationen nutzen, um sich Zugriff auf das Netzwerk zu verschaffen.</p> <p>Die jeweiligen Methoden, um den Zweck dieser Anforderung zu erfüllen, sind von der spezifischen, in Ihrer Umgebung eingesetzten Netzwerktechnologie abhängig. Beispielsweise können sich die zur Erfüllung dieser Anforderung in IPv4-Netzwerken eingesetzten Steuerungen von jenen in IPv6-Netzwerken unterscheiden.</p> <p>Eine Methode, um zu verhindern, dass Informationen zu IP-Adressen auf einem IPv4-Netzwerk bekannt werden, ist die Implementierung des Network Address Translation (NAT)-Verfahrens. NAT, das normalerweise von der Firewall verwaltet wird, ermöglicht es einem Unternehmen, interne Adressen nur im Netzwerk und externe Adressen nur außerhalb des Netzwerkes sichtbar zu machen. Wenn eine Firewall die IP-Adressen des internen Netzwerkes nicht ausblendet oder maskiert, kann eine böswillige Person unter Umständen interne IP-Adressen herausfinden und versuchen, auf das Netzwerk mithilfe einer gefälschten IP-Adresse zuzugreifen.</p> <p>Für IPv4-Netzwerke ist der RFC1918-Adressbereich für interne Adressen vorbehalten und sollte nicht über das Internet routbar sein. Aus diesem Grund wird er für IP-Adressen in internen Netzwerken vorgezogen. Allerdings gibt es auch Gründe, die für Unternehmen dafür sprechen, in internen Netzwerken nicht-RFC1918-Adressräume einzusetzen. Unter diesen Umständen müssen Route-Advertisements oder andere Techniken eingesetzt werden, um zu verhindern, dass interne Adressräume im Internet verbreitet oder an unbefugte Dritte weitergegeben werden.</p>

Anforderung	Leitfaden
<p>1.4 Installieren von persönlicher Firewallsoftware auf allen mobilen und Mitarbeitern gehörenden Computern mit direkter Verbindung mit dem Internet (z. B. Laptops, die von Mitarbeitern verwendet werden), die für den Zugriff auf das Unternehmensnetzwerk eingesetzt werden.</p>	<p>Wenn ein Computer nicht über eine installierte Firewall oder ein Antivirus-Programm verfügt, können unwissentlich Spyware, Trojaner, Viren, Würmer und Rootkits (Malware) heruntergeladen und/oder installiert werden. Der Computer ist sogar noch anfälliger, wenn er direkt und nicht durch die Firmen-Firewall geschützt mit dem Internet verbunden ist. Auf einen Computer heruntergeladene Malware kann dann, wenn nicht durch die Firewall des Unternehmens abgeschirmt, mit böswilligen Absichten Informationen aus dem Netzwerk anvisieren, wenn der Computer wieder mit dem Firmennetzwerk verbunden wird.</p> <p>Hinweis: Diese Anforderung bezieht sich auf Computer, mit denen sich per Fernzugriff in das Netzwerk eingeloggt wird, unabhängig davon, ob sie sich im Besitz eines Mitarbeiters oder des Unternehmens befinden. Systeme, die nicht mittels Unternehmensrichtlinien verwaltet werden können, schwächen den Netzwerkrand und bieten böswilligen Personen Angriffsmöglichkeiten.</p>

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

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

Anforderung	Leitfaden
<p>2.1 Ändern der vom Anbieter angegebenen Standardeinstellungen vor jeder Installation eines Systems im Netzwerk, einschließlich, jedoch nicht beschränkt auf die Einführung von Kennwörtern, SNMP-Community-Zeichenfolgen und Beseitigung nicht benötigter Konten.</p>	<p>Böswillige Personen (in einem Unternehmen und außerhalb) verwenden häufig Standardeinstellungen, -kontonamen und -kennwörter von Anbietern, um Systeme zu beeinträchtigen. Diese Einstellungen sind in der Hacker-Szene bekannt und machen Ihr System für Angriffe extrem anfällig.</p>
<p>2.1.1 Für drahtlose Umgebungen, die mit der Karteninhaberdaten-Umgebung verbunden sind oder Karteninhaberdaten übertragen, Ändern der drahtlosen Anbieterstandardeinstellungen, einschließlich, aber nicht beschränkt auf drahtlose Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen.</p>	<p>Viele Benutzer installieren diese Geräte ohne die Zustimmung der Geschäftsleitung und ändern danach nicht die Standardeinstellungen oder konfigurieren keine Sicherheitseinstellungen. Wenn keine Drahtlosnetzwerke mit ausreichenden Sicherheitskonfigurationen (einschließlich die Änderung von Standardeinstellungen) implementiert sind, können Wirelless-Sniffer den Datenverkehr belauschen, im Handumdrehen Daten und Kennwörter erfassen und sich Zugriff auf Ihr Netzwerk verschaffen und es schädigen. Darüber hinaus wurde das Schlüsselaustauschprotokoll der älteren 802.11x Verschlüsselung (WEP) geknackt und die Verschlüsselung somit nutzlos gemacht. Überprüfen Sie, ob die Firmware für Geräte aktualisiert ist und sichere Protokolle unterstützt (z. B. WPA2).</p>
<p>2.2 Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen.</p> <p>Zu den Quellen branchenweit akzeptierter Standards zur Systemstabilisierung zählen unter anderem:</p> <ul style="list-style-type: none"> ▪ Center for Internet Security (CIS) ▪ International Organization for Standardization (ISO) ▪ SysAdmin Audit Network Security (SANS) ▪ National Institute of Standards and Technology (NIST) 	<p>In vielen Betriebssystemen, Datenbanken und Firmenanwendungen gibt es bekannte Schwachstellen, welche mithilfe bestimmter Konfigurationen behoben werden können. Um jenen unter die Arme zu greifen, die keine Sicherheitsexperten sind, haben Sicherheitsunternehmen Empfehlungen zur Systemhärtung bereitgestellt, welche eine Anleitung zur Korrektur dieser Schwächen bieten. Wenn diese Schwachstellen nicht behoben werden – z. B. schwache Dateieinstellungen oder Standarddienste und -protokolle (für Dienste und Protokolle, die häufig nicht einmal benötigt werden) – kann ein Angreifer mehrere bekannte Verfahren einsetzen, um gefährdete Dienste und Protokolle anzugreifen und sich somit Zugriff zu Ihrem Unternehmensnetzwerk verschaffen. Unter anderen können Sie auf folgenden Websites Informationen über bewährte Verfahren der Branche einholen, die Ihnen dabei helfen, Konfigurationsstandards zu implementieren: www.nist.gov, www.sans.org, www.cisecurity.org, www.iso.org.</p> <p>Auch Systemkonfigurationsstandards müssen auf dem neuesten Stand gehalten werden, um sicherzustellen, dass neu entdeckte Sicherheitslücken geschlossen werden, bevor ein System auf dem Netzwerk installiert wird.</p>

Anforderung	Leitfaden
<p>2.2.1 Implementieren Sie nur eine primäre Funktion pro Server, um zu vermeiden, dass auf einem Server gleichzeitig mehrere Funktionen mit verschiedenen Sicherheitsniveaunanforderungen existieren. (Webserver, Datenbankserver und DNS sollten beispielsweise auf separaten Servern implementiert sein.)</p> <p><i>Hinweis: Wenn Virtualisierungstechnologien eingesetzt werden, implementieren Sie pro virtuelle Systemkomponente nur eine primäre Funktion.</i></p>	<p>Dies hat den Vorteil, dass die Systemkonfigurationsstandards Ihres Unternehmens sowie zugehörige Verfahren Serverfunktionen ansprechen, die verschiedene Sicherheitsebenen benötigen oder die Sicherheitslücken auf andere Funktionen auf demselben Server ausdehnen. Beispiel:</p> <ol style="list-style-type: none"> 1. Eine Datenbank, die starke Sicherheitsvorkehrungen benötigt, wäre gefährdet, wenn sie gemeinsam mit einer Web-Anwendung, die offen und direkt mit dem Internet verbunden sein muss, ein und denselben Server teilen würde. 2. Das Versäumen, einen Patch für eine scheinbar unwichtige Funktion anzuwenden, könnte eine Störung hervorrufen, die anschließend auch andere, wichtigere Funktionen (wie etwa Datenbanken) auf demselben Server in Mitleidenschaft zieht. <p>Diese Anforderung gilt für alle Server in der Karteninhaberdaten-Umgebung (normalerweise auf Unix, Linux oder Windows basierende Server). Diese Anforderung gilt nicht für Systeme, die nicht in der Lage sind, nativ Sicherheitsebenen auf einem einzigen Server zu implementieren (z. B. Großrechner).</p> <p>Wo immer Virtualisierungstechnologien eingesetzt werden, müssen alle virtuellen Komponenten (z. B. virtuelle Rechner, virtuelle Schalter, virtuelle Security Appliances usw.) als Server-Boundary angesehen werden. Einzelne Hypervisoren können verschiedene Funktionen unterstützen, aber für einzelne virtuelle Rechner sollte man sich an die Regel halten, nur eine primäre Funktion zu implementieren. In diesem Szenario könnte eine Schädigung des Hypervisors zu einer Beeinträchtigung der gesamten Systemfunktionen führen. Aus diesem Grund sollte auch auf die Höhe des Risikos geachtet werden, wenn es darum geht, mehrere Funktionen oder Komponenten auf einem einzigen physischen System zu platzieren.</p>
<p>2.2.2 Aktivieren Sie entsprechend des Bedarfs der Systemfunktion ausschließlich erforderliche und sichere Dienste, Protokolle, Daemons usw.</p> <p>Implementieren Sie Sicherheitsfunktionen für alle benötigten Dienste, Protokolle oder Daemons, die als unsicher eingestuft wurden. Verwenden Sie z. B. gesicherte Technologien wie etwa SSH, S-FTP, SSL oder IPSec VPN, um unsichere Dienste wie beispielsweise NetBIOS, File-Sharing, Telnet, FTP etc. zu schützen.</p>	<p>Wie bereits in der Anforderung 1.1.5 erwähnt, gibt es zahlreiche Protokolle, die ein Unternehmen unter Umständen benötigt (oder standardmäßig aktiviert hat) und die wiederholt von böswilligen Personen ausgenutzt werden, um ein Netzwerk zu beschädigen. Um sicherzustellen, dass ausschließlich notwendige Dienste und Protokolle aktiviert und dass alle unsicheren Dienste und Protokolle angemessen gesichert sind, bevor neue Server eingesetzt werden, sollte Ihr Unternehmen diese Anforderung in seine Konfigurationsstandards und zugehörigen Prozesse aufnehmen.</p>

Anforderung	Leitfaden
<p>2.2.3 Konfigurieren von Systemsicherheitsparametern, um Missbrauch zu verhindern.</p>	<p>Somit wird gewährleistet, dass die Systemkonfigurationsstandards Ihres Unternehmens sowie die zugehörigen Prozesse insbesondere jene Sicherheitseinstellungen und Parameter ansprechen, die sich bekanntermaßen auf die Sicherheit auswirken.</p>
<p>2.2.4 Entfernen aller unnötigen Funktionen wie z. B. Skripte, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver.</p>	<p>Die Standards zur Absicherung von Servern müssen Prozesse umfassen, die unnötige Funktionen ansprechen, die die Sicherheit gefährden können (z. B. indem FTP oder der Webserver gelöscht/deaktiviert wird, wenn der Server diese Funktionen nicht nutzt).</p>
<p>2.3 Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs mithilfe einer starken Kryptographie. Verwenden von Technologien wie SSH, VPN oder SSL/TLS für die webbasierte Verwaltung und sonstigen Nichtkonsolen-Verwaltungszugriff.</p>	<p>Wenn die Fernadministration nicht mit einer sicheren Authentifizierung und verschlüsselten Kommunikationen erfolgt, können vertrauliche administrative oder Informationen auf Betriebsebene (wie etwa Administrator-Kennwörter) Lauschangriffen ausgesetzt sein. Ein Angreifer könnte diese Informationen nutzen, um sich Zugang zum Netzwerk zu verschaffen, sich als Administrator auszugeben oder um Daten zu entwenden.</p>
<p>2.4 Gemeinsam verwendete Hosting-Anbieter müssen die gehostete Umgebung und Karteninhaberdaten aller Stellen schützen. Diese Anbieter müssen bestimmte Anforderungen erfüllen, wie in <i>Anhang A: Zusätzliche PCI-DSS-Anforderungen für gemeinsam verwendete Hosting-Provider</i> dargestellt.</p>	<p>Sie gelten für Hosting-Anbieter, die von mehreren Clients auf demselben Server genutzte Hosting-Umgebungen anbieten. Wenn sich alle Daten auf demselben Server befinden und von einer einzigen Umgebung gesteuert werden, lassen sich die Einstellungen auf diesen gemeinsam genutzten Servern vielmals nicht von einem einzigen Client verwalten, außerdem wird den Clients somit die Möglichkeit eingeräumt, unsichere Funktionen und Skripts hinzuzufügen, die die Sicherheit anderer Client-Umgebungen beeinträchtigen können und es somit einem Angreifer leicht machen, die Daten eines Clients zu beschädigen und sich anschließend Zugriff auf die Daten aller anderen Clients zu verschaffen. Siehe <i>Anhang A</i>.</p>

Leitfaden für die Anforderungen 3 und 4: Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

Schutzmethoden wie Verschlüsselung, Abkürzung, Maskierung und Hashing sind kritische Bestandteile des Schutzes von Karteninhaberdaten. Wenn ein Eindringling andere Sicherheitskontrollen umgeht und Zugriff auf verschlüsselte Daten ohne die entsprechenden kryptographischen Schlüssel erlangt, sind die Daten nicht leserlich und für diese Person unbrauchbar. Andere effektive Methoden zum Schutz gespeicherter Daten sollten als Möglichkeit zur Risikoabschwächung angesehen werden. Zu den Methoden zur Risikominimierung gehört es beispielsweise, Karteninhaberdaten nur zu speichern, wenn dies unbedingt erforderlich ist, Karteninhaberdaten abzukürzen, wenn die vollständige PAN nicht benötigt wird, und die unverschlüsselte PAN nicht mittels Messaging-Technologien für Endanwender wie etwa E-Mails oder Instant Messaging zu senden.

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

Anforderung	Leitfaden
<p>3.1 Beschränken Sie das Speichern von Karteninhaberdaten auf ein Minimum, indem Sie wie folgt Richtlinien und Verfahren zur Datenaufbewahrung und zum Löschen von Daten implementieren.</p> <p>3.1.1 Implementieren einer Richtlinie zur Datenaufbewahrung und zum Löschen von Daten, die folgende Punkte berücksichtigt:</p> <ul style="list-style-type: none"> ▪ Begrenzen der Speichermenge und der Aufbewahrungszeit auf die für rechtliche, gesetzliche oder geschäftliche Zwecke festgelegten Vorgaben. ▪ Prozesse zum Löschen von Daten, sobald diese nicht mehr benötigt werden. ▪ Spezifische Aufbewahrungsanforderungen für Karteninhaberdaten ▪ Ein vierteljährlicher automatischer oder manueller Prozess zur Identifizierung und sicheren Löschung gespeicherter Karteninhaberdaten, die den festgelegten Aufbewahrungszeitraum überschritten haben. 	<p>Eine formale Datenaufbewahrungsrichtlinie gibt an, welche Daten aufbewahrt werden müssen und wo sich diese Daten befinden, damit diese sicher vernichtet oder gelöscht werden können, sobald sie nicht mehr erforderlich sind. Um angemessene Aufbewahrungsanforderungen zu definieren, muss sich eine Stelle zunächst über ihre eigenen Betriebsbedürfnisse sowie jegliche Art von gesetzlichen oder behördlichen Pflichten im Klaren sein, die für ihre Branche und/oder den jeweiligen Datentyp gelten.</p> <p>Eine längere als entsprechend der Betriebsbedürfnisse erforderliche Speicherung von Karteninhaberdaten beschwört unnötige Risiken herauf. Die einzigen Karteninhaberdaten, die auch nach der Autorisierung gespeichert werden können, sind die primäre Kontonummer oder auch PAN genannt (in unleserlicher Form), Ablaufdatum, Name des Karteninhabers und der Servicecode.</p> <p>Der Einsatz sicherer Verfahren zum Löschen von Daten gewährleistet, dass diese nicht mehr wiederhergestellt werden können, wenn hierfür kein Bedarf mehr besteht.</p> <p>Denken Sie daran – wenn nicht benötigt, nicht speichern!</p>

Anforderung	Leitfaden
<p>3.2 Speichern Sie keine vertraulichen Authentifizierungsdaten nach der Autorisierung (auch wenn diese verschlüsselt sind).</p> <p>Vertrauliche Authentifizierungsdaten umfassen die Daten, die in den folgenden Anforderungen 3.2.1 bis 3.2.3 aufgeführt sind:</p> <p>Hinweis: Kartenemittenten und Unternehmen, die Ausstellungsdienste unterstützen, dürfen vertrauliche Authentifizierungsdaten speichern, wenn dafür eine Begründung vorliegt und die Daten sicher gespeichert werden.</p>	<p>Vertrauliche Authentifizierungsdaten bestehen aus Magnetstreifendaten (oder Verfolgungsdaten)⁶, Kartvalidierungscode oder -wert⁷ und PIN-Daten⁸. Die Speicherung vertraulicher Authentifizierungsdaten ist nach der Autorisierung nicht zulässig! Diese Daten sind für Personen mit böswilligen Absichten von großem Wert, zumal sie ihnen ermöglichen, gefälschte Zahlungskarten zu generieren und betrügerische Transaktionen zu erstellen. Eine Definition für „vertrauliche Authentifizierungsdaten“ finden Sie im <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>.</p> <p>Hinweis: Unternehmen, die Ausstellungsdienste anbieten, fördern oder unterstützen, dürfen vertrauliche Authentifizierungsdaten NUR speichern, WENN für die Speicherung dieser Daten eine betriebliche Begründung vorliegt. Hierbei sei angemerkt, dass für Emittenten alle PCI-DSS-Anforderungen gelten und dass die einzige Ausnahme darin besteht, dass Emittenten und zugehörige Dienstleister vertrauliche Authentifizierungsdaten speichern dürfen, wenn hierfür berechnete Gründe vorliegen. Ein berechtigter Grund beschreibt die Notwendigkeit zur Ausführung der Funktion des Emittenten und nicht für eine bequemere Ausführung der Arbeit.</p> <p><i>Diese Daten müssen sicher und gemäß dem PCI-DSS sowie den spezifischen Anforderungen der Zahlungsmarken gespeichert werden.</i></p>

⁶ Im Magnetstreifen verschlüsselte Daten, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Diese Daten können auch auf einem Chip oder an einem anderen Speicherort der Karte gespeichert werden. Einheiten dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifendaten speichern. Die einzigen Elemente der Verfolgungsdaten, die aufbewahrt werden dürfen, sind die primäre Kontonummer, der Name des Karteninhabers, das Ablaufdatum und der Servicecode.

⁷ Der drei- oder vierstellige Wert, der im oder rechts neben dem Unterschriftenfeld bzw. vorne auf einer Zahlungskarte aufgedruckt ist und zur Verifizierung von Transaktionen bei nicht vorliegender Karte verwendet wird.

⁸ Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht.

Anforderung	Leitfaden
<p>3.2.1 Speichern Sie nicht den gesamten Inhalt einer Spur (auf dem Magnetstreifen auf der Kartenrückseite, in einem Chip oder an anderer Stelle). Diese Daten werden auch als Full Track, Track, Track 1, Track 2 und Magnetstreifendaten bezeichnet.</p> <p><i>Hinweis: Beim normalen Geschäftsverlauf müssen evtl. folgende Datenelemente aus dem Magnetstreifen gespeichert werden:</i></p> <ul style="list-style-type: none"> ▪ <i>Der Name des Karteninhabers</i> ▪ <i>Primäre Kontonummer (Englisch: Primary Account Number, PAN)</i> ▪ <i>Ablaufdatum</i> ▪ <i>Servicecode</i> <p><i>Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.</i></p>	<p>Wenn vollständige Spurdaten gespeichert werden, sind Angreifer, die Zugriff zu diesen Daten haben, in der Lage, Zahlungskarten zu reproduzieren und zu verkaufen.</p>
<p>3.2.2 Speichern Sie nicht den Kartenprüfcode oder -wert (drei- oder vierstellige Zahl auf der Vorder- oder Rückseite der Zahlungskarte), der zur Verifizierung bei Transaktionen verwendet wird, bei denen die Karte nicht physisch vorliegt.</p>	<p>Der Zweck des Kartenvalidierungscodes liegt im Schutz von Transaktionen, bei denen weder der Kunde anwesend ist noch die Karte vorliegt – Auftragsabwicklungen über das Internet oder per E-Mail/Telefon. Diese Art von Transaktionen können nur authentifiziert werden, indem der Kartenvalidierungscode angefragt wird, zumal der Karteninhaber die Karte in der Hand hält und den Wert ablesen kann. Wenn diese verbotenen Daten gespeichert und anschließend entwendet werden, sind Betrüger in der Lage, Aufträge über das Internet und per E-Mail oder Telefon abzuwickeln.</p>
<p>3.2.3 Speichern Sie keine persönlichen Identifizierungsnummern (PIN) oder den verschlüsselten PIN-Block.</p>	<p>Diese Werte sollten ausschließlich dem Karteninhaber und der Bank, die die Karte ausgestellt hat, bekannt sein. Wenn diese verbotenen Daten gespeichert und anschließend entwendet werden, sind Betrüger in der Lage, PIN-basierte Lastschriften auszuführen (z. B. Abhebungen an Geldautomaten).</p>

Anforderung	Leitfaden
<p>3.3 Verbergen Sie die PAN bei der Anzeige (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden).</p> <p>Hinweise:</p> <ul style="list-style-type: none"> ▪ Diese Anforderung gilt nicht für Mitarbeiter und andere Parteien, die die vollständige PAN aus rechtmäßigen geschäftlichen Gründen einsehen müssen. ▪ Diese Anforderung ersetzt nicht strengere Anforderungen im Hinblick auf die Anzeige von Karteninhaberdaten – z. B. für POS-Belege. 	<p>Die Anzeige der vollständigen PAN beispielweise auf Computerbildschirmen, Zahlungsbestätigungen, Faxmitteilungen oder Berichten in Papierform kann dazu führen, dass diese Daten in die Hände von unbefugten Personen gelangen, die diese dann in betrügerischer Absicht nutzen. Die PAN kann in voller Länge auf dem „Verkäufer-Ausdruck“ angezeigt werden; allerdings sollte man sich bei gedruckten Bestätigungen an dieselben Sicherheitsvorkehrungen wie auch bei elektronischen Kopien halten und die Richtlinien des PCI-Datensicherheitsstandards befolgen, insbesondere die Anforderung 9 zum Thema physische Sicherheit. Die PAN kann auch in voller Länge angezeigt werden, wenn es sich um Personen handelt, die die vollständige PAN aus rechtmäßigen geschäftlichen Gründen einsehen müssen.</p> <p>Diese Anforderung bezieht sich auf den Schutz von PANs, die auf Bildschirmen, Belegen usw. <u>abgebildet</u> sind und darf nicht mit der Anforderung 3.4 zum Schutz der in Dateien, Datenbanken usw. <u>gespeicherten</u> PANs verwechselt werden.</p>
<p>3.4 Machen Sie die PAN überall dort unleserlich, wo sie gespeichert wird (auch auf tragbaren digitalen Medien, Sicherungsmedien und in Protokollen). Setzen Sie dazu eines der folgenden Verfahren ein:</p> <ul style="list-style-type: none"> ▪ Unidirektionale Hashes, die auf einer starken Kryptographie basieren (es muss von der vollständigen PAN ein Hash erstellt werden) ▪ Abkürzung (die Hash-Funktion kann nicht verwendet werden, um das abgekürzte Segment der PAN zu ersetzen) ▪ Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden) ▪ Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren. <p>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 Einheit nebeneinander bestehen, müssen zusätzliche Kontrollen eingesetzt werden, um sicherzustellen, dass gehashte und abgekürzte Versionen nicht verglichen werden können, um die originale PAN zu rekonstruieren.</p>	<p>Mangelnder Schutz der PANs ermöglicht es böswilligen Personen, diese Daten anzuzeigen oder gar herunterzuladen. PANs, die in einem Hauptspeicher (Datenbanken oder einfache Dateien, wie etwa Textdateien oder Tabellen) oder auch in nicht-Hauptspeichern (Sicherungskopien, Audit-Protokolle, Ausnahme- oder Fehlerbehebungsprotokolle) gespeichert werden, müssen entsprechend geschützt werden. Schäden durch Diebstahl oder Verlust von Sicherungsbändern während des Transports können reduziert werden, indem die PANs mithilfe von Verschlüsselungs-, Abkürzungs- oder Hashing-Techniken unleserlich gemacht werden. Da Audit-, Fehlerbehebungs- und Ausnahmeprotokolle ausbewahrt werden müssen, können Sie der Enthüllung von Daten in Protokollen vorbeugen, indem Sie die PANs in den Protokollen unleserlich machen (oder sie entfernen).</p> <p>Wenn ein Angreifer die gehashte und die abgekürzte Version einer bestimmten PAN miteinander vergleicht, kann er im Handumdrehen den ursprünglichen PAN-Wert ableiten. Um sicherzustellen, dass die ursprüngliche PAN unleserlich bleibt, können Kontrollen hilfreich sein, die vermeiden, dass diese Daten einander zugeordnet werden.</p> <p>Die Definition für „starke Kryptographie“ finden Sie im <i>Glossar, Abkürzungen und Akronyme zum PCI-DSS und DA-DSS</i>.</p>

Anforderung	Leitfaden
<ul style="list-style-type: none"> Unidirektionale Hashes, die auf einer starken Kryptographie basieren (es muss von der vollständigen PAN ein Hash erstellt werden) 	<p>Unidirektionale Hash-Funktionen, die auf einer starken Kryptographie basieren, wie etwa Secure Hash Algorithm (SHA), können verwendet werden, um die Karteninhaberdaten unleserlich zu machen. Hash-Funktionen eignen sich, wenn kein Bedarf besteht, die ursprüngliche Nummer abzurufen (unidirektionale Hashes können nicht rückgängig gemacht werden).</p> <p>Um die Erstellung von Rainbow Tables zu erschweren, empfiehlt es sich (es ist jedoch keine Anforderung), zusätzlich zu der PAN einen Salt-Wert in die Hash-Funktion einzugeben.</p>
<ul style="list-style-type: none"> Abkürzung (die Hash-Funktion kann nicht verwendet werden, um das abgekürzte Segment der PAN zu ersetzen) 	<p>Das Ziel der Abkürzung liegt darin, nur einen Teil (nicht mehr als die ersten sechs und die letzten vier Ziffern) der PAN zu speichern. Dieses Verfahren unterscheidet sich von der Maskierung insofern, als bei Letzterem die vollständige PAN gespeichert, sie jedoch maskiert angezeigt wird (d. h. es wird nur ein Teil der PAN auf Bildschirmen, Berichten, Belegen usw. angezeigt).</p> <p>Diese Anforderung bezieht sich auf den Schutz von PANs, die in Dateien, Datenbanken usw. <u>gespeichert</u> werden und darf nicht mit der Anforderung 3.3 zum Schutz der auf Bildschirmen, Belegen usw. <u>angezeigten</u> PANs verwechselt werden.</p>
<ul style="list-style-type: none"> Index-Tokens und -Pads (Pads müssen sicher aufbewahrt werden) 	<p>Auch Index-Tokens und -Pads können eingesetzt werden, um die Karteninhaberdaten unleserlich zu machen. Ein Index-Token ist ein kryptographisches Token, das die PAN anhand eines bestimmten Index für einen unvorhersehbaren Wert ersetzt. Ein Einmal-Pad ist ein System, bei dem ein per Zufallsgenerator erstellter privater Schlüssel nur einmal benutzt wird, um eine Nachricht zu verschlüsseln, welche anschließend mit einem entsprechenden Einmal-Pad und Schlüssel wieder entschlüsselt wird.</p>
<ul style="list-style-type: none"> Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren. 	<p>Das Ziel der starken Kryptographie (die Definition und Schlüssellängen finden Sie im <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>) liegt darin, dass die Verschlüsselung auf der Grundlage branchenbewährter und akzeptierter Algorithmen erfolgt (keine firmeneigenen oder gar individuellen Algorithmen).</p>

Anforderung	Leitfaden
<p>3.4.1 Wenn Datenträgerverschlüsselung verwendet wird (anstelle der Datenbankverschlüsselung auf Datei- oder Spaltenebene), muss der logische Zugriff unabhängig von nativen Zugriffskontrollmechanismen des Betriebssystems verwaltet werden (z. B. indem lokale Benutzerkontodatenbanken nicht verwendet werden). Entschlüsselungsschlüssel dürfen nicht mit Benutzerkonten verknüpft sein.</p>	<p>Der Zweck dieser Anforderung ist es, die Annehmbarkeit von Datenträgerverschlüsselungen, mit denen Karteninhaberdaten unleserlich gemacht werden, anzusprechen. Bei der Datenträgerverschlüsselung werden auf einer Massenspeichereinheit eines Computers gespeicherte Daten verschlüsselt und automatisch entschlüsselt, wenn ein Benutzer einen solchen Befehl eingibt. Systeme zur Datenträgerverschlüsselung fangen Lese- und Schreibvorgänge des Betriebssystems ab und führen die entsprechenden kryptographischen Umwandlungen ohne jegliches Zutun des Benutzers, außer der Eingabe eines Kennworts oder Kennsatzes zu Beginn der Sitzung, aus. Basierend auf den Eigenschaften der Datenträgerverschlüsselung darf die jeweilige Datenträgerverschlüsselungsmethode, um der vorliegenden Anforderung zu entsprechen, folgende Elemente nicht aufweisen:</p> <ol style="list-style-type: none"> 1) Eine direkte Verbindung zum Betriebssystem oder 2) Dechiffrierschlüssel, die mit den Benutzerkonten verbunden sind.
<p>3.5 Schützen Sie Schlüssel, die für den Schutz der Karteninhaberdaten eingesetzt werden, vor Weitergabe und Missbrauch:</p> <p><i>Hinweis: Diese Anforderung gilt auch für Schlüssel zum Verschlüsseln von Schlüsseln, die zum Schutz von Schlüsseln zum Verschlüsseln von Daten verwendet werden—diese Schlüssel zum Verschlüsseln von Schlüsseln müssen mindestens so sicher wie der Schlüssel zum Verschlüsseln von Daten sein.</i></p>	<p>Kryptographische Schlüssel müssen dringend geschützt werden, da Personen, die in deren Besitz gelangen, in der Lage sind, Daten zu entschlüsseln. Schlüssel zum Verschlüsseln von Schlüsseln, falls verwendet, müssen mindestens so sicher wie Schlüssel zum Verschlüsseln von Daten sein, um einen angemessenen Schutz sowohl des Schlüssels zum Verschlüsseln von Daten als auch der Daten, die mit diesem Schlüssel verschlüsselt wurden, zu gewährleisten.</p> <p>Die Anforderung, Schlüssel vor Weitergabe und Missbrauch zu schützen, gilt sowohl für Schlüssel zum Verschlüsseln von Daten als auch für Schlüssel zum Verschlüsseln von Schlüsseln. Da ein Schlüssel zum Verschlüsseln von Schlüsseln Zugriff auf eine Vielzahl von Schlüsseln zum Verschlüsseln von Daten ermöglicht, ist es notwendig, die Schlüssel zum Verschlüsseln von Schlüsseln mithilfe strenger Schutzvorkehrungen zu sichern. Zu den Methoden für eine sichere Speicherung von Schlüsseln zum Verschlüsseln von Schlüsseln gehören unter anderem Hardware Security Modules (HSMs) und das Sichern von Speicherplätzen mittels dualer Kontrollen und geteiltem Wissen.</p>
<p>3.5.1 Schränken Sie den Zugriff auf kryptographische Schlüssel auf die unbedingt notwendige Anzahl von Wächtern ein.</p>	<p>Es sollten möglichst wenige Personen Zugriff auf die kryptographischen Schlüssel haben, und vorzugsweise ausschließlich Personen, die als Schlüsselwächter eingesetzt wurden.</p>

Anforderung	Leitfaden
<p>3.5.2 Speichern Sie kryptographische Schlüssel sicher an möglichst wenigen Speicherorten und in möglichst wenigen Formen.</p>	<p>Kryptographische Schlüssel müssen sicher gespeichert werden, d. h. verschlüsselt mithilfe Schlüsseln zum Verschlüsseln von Schlüsseln und an nur sehr wenigen Speicherorten aufbewahrt werden. Zwar ist es nicht vorgesehen, dass Schlüssel zum Verschlüsseln von Schlüsseln selbst verschlüsselt werden, allerdings müssen sie gemäß Anforderung 3.5 vor Weitergabe und Missbrauch geschützt werden. Durch das Speichern von Schlüsseln zum Verschlüsseln von Schlüsseln an physisch und/oder logisch von Schlüsseln zum Verschlüsseln von Daten getrennten Speicherorten kann das Risiko unerlaubter Zugriffe auf beide Schlüssel reduziert werden.</p>
<p>3.6 Dokumentieren und implementieren Sie alle Schlüsselverwaltungsprozesse und -verfahren für kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, einschließlich der Folgenden:</p> <p><i>Hinweis: Zahlreiche Branchenstandards für die Schlüsselverwaltung sind über verschiedene Ressourcen verfügbar, unter anderem über NIST (unter http://csrc.nist.gov).</i></p>	<p>Die Art und Weise, in der kryptographische Schlüssel verwaltet werden, spielt in der Sicherheit der Verschlüsselungslösung eine wichtige Rolle. Ein guter Schlüsselverwaltungsprozess, ganz gleich, ob als Teil des Verschlüsselungsprodukts manueller oder automatischer Natur, basiert auf Branchenstandards und spricht alle in 3.6.1 bis 3.6.8 aufgeführten Schlüsselemente an.</p>
<p>3.6.1 Erstellung starker kryptographischer Schlüssel</p>	<p>Die Verschlüsselungslösung muss, so wie unter dem Begriff „starke Kryptographie“ im <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i> definiert, in der Lage sein, starke Schlüssel zu generieren.</p>
<p>3.6.2 Sichere Verteilung kryptographischer Schlüssel</p>	<p>Die Verschlüsselungslösung muss sicher Schlüssel verteilen können, d. h. dass Schlüssel nicht in Klartext und nur an die in 3.5.1 festgelegten Wächter verteilt werden dürfen.</p>
<p>3.6.3 Sicheres Speichern kryptographischer Schlüssel</p>	<p>Die Verschlüsselungslösung muss Schlüssel sicher speichern können, d. h. dass sie nicht in Klartext gespeichert werden (sie müssen mithilfe eines Schlüssels zum Verschlüsseln von Schlüsseln verschlüsselt werden).</p>

Anforderung	Leitfaden
<p>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. <i>NIST Special Publication 800-57</i>).</p>	<p>Die Schlüssellebensdauer beschreibt die Zeitspanne, in der ein bestimmter kryptographischer Schlüssel für den ihm vorbestimmten Zweck eingesetzt werden kann. Bei der Bestimmung der Schlüssellebensdauer müssen unter anderem die Stärke des zugrundeliegenden Algorithmus, die Größe oder Länge des Schlüssels, das Risiko für eine Kompromittierung des Schlüssels und die Vertraulichkeit der zu verschlüsselnden Daten berücksichtigt werden.</p> <p>Das regelmäßige Ändern der Verschlüsselungsschlüssel, wenn diese das Ende ihrer Schlüssellebensdauer erreicht haben, ist von zentraler Bedeutung, um das Risiko, dass sich unbefugte Personen Zugriff auf Verschlüsselungsschlüssel verschaffen und Daten entschlüsseln, zu minimieren.</p> <p>Wenn diese von einem Anbieter von Verschlüsselungsanwendungen geliefert wurden, befolgen Sie die dokumentierten Prozesse und Empfehlungen zur regelmäßigen Änderung von Schlüsseln. Der ernannte Schlüsselinhaber oder Wächter kann auch bewährte Branchenverfahren zu kryptographischen Algorithmen und zum Thema Schlüsselverwaltung, z. B. <i>NIST Special Publication 800-57</i> für eine Anleitung zur angemessenen Schlüssellebensdauer für verschiedene Algorithmen und Schlüssellängen konsultieren.</p> <p>Diese Anforderung gilt für Schlüssel, die zur Verschlüsselung gespeicherter Karteninhaberdaten dienen sowie für sämtliche Schlüssel zum Verschlüsseln von Schlüsseln.</p>
<p>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, usw.) oder Grund zur Annahme besteht, dass bestimmte Schlüssel beschädigt sind.</p> <p>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.</p>	<p>Alte Schlüssel, die nicht länger genutzt oder gebraucht werden, sollten entfernt oder vernichtet werden, um sicherzustellen, dass sie nicht länger benutzt werden. Falls alte Schlüssel aufbewahrt werden müssen (z. B. zur Unterstützung archivierter, verschlüsselter Daten), sind diese mittels strenger Sicherheitsvorkehrungen zu schützen. (Siehe Anforderung 3.6.6 unten.) Die Verschlüsselungslösung sollte die Möglichkeit zur Implementierung eines Prozesses zum Austauschen von Schlüsseln, die bekanntermaßen oder vermutlich kompromittiert worden sind, einräumen und unterstützen.</p>

Anforderung	Leitfaden
<p>3.6.6 Wenn manuelle Verwaltungsvorgänge kryptographischer Klartext-Schlüssel verwendet werden, müssen diese Vorgänge mittels einer geteilten Kenntnis und doppelten Kontrollen verwaltet werden (z. B. zwei oder drei Personen, die jeweils nur ihren eigenen Bestandteil des Schlüssels kennen, um den gesamten Schlüssel neu zu erstellen).</p> <p><i>Hinweis: Zu den manuellen Verfahren zur Schlüsselverwaltung zählen unter anderen: Schlüsselgenerierung, Übertragung, Ladung, Speicherung und Vernichtung.</i></p>	<p>Geteiltes Wissen und duale Schlüsselkontrollen werden benutzt, um zu verhindern, dass eine Person Zugriff auf den vollständigen Schlüssel hat. Diese Kontrolle gilt für manuelle Schlüsselverwaltungsverfahren oder für Verschlüsselungsprodukte, die keine Schlüsselverwaltung bieten.</p>
<p>3.6.7 Verhindern der unbefugten Ersetzung kryptographischer Schlüssel.</p>	<p>Die Verschlüsselungslösung sollte keine Auswechselungen von Schlüsseln autorisieren, die aus nicht zugelassenen Quellen oder unerwarteten Prozessen stammen.</p>
<p>3.6.8 Wächter kryptographischer Schlüssel müssen formal bestätigen, dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen.</p>	<p>Dieser Prozess gewährleistet, dass sich Personen, die als Schlüsselwächter fungieren, an ihre Rolle als Schlüsselwächter halten und die damit verbundenen Verantwortlichkeiten verstehen.</p>

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

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

Anforderung	Leitfaden
<p>4.1 Verwenden Sie starke Kryptographie- und Sicherheitsprotokolle (z. B. SSL/TLS, IPsec, SSH usw.), damit sensible Karteninhaberdaten während der Übertragung über offene und öffentliche Netzwerke geschützt sind.</p> <p><i>Beispiele für offene, öffentliche Netzwerke, die in den Umfang des PCI-DSS fallen, sind unter anderem:</i></p> <ul style="list-style-type: none"> ▪ <i>Das Internet</i> ▪ <i>Drahtlose Technologien</i> ▪ <i>GSM-Kommunikationen (Global System for Mobile)</i> ▪ <i>General Packet Radio Service (GPRS).</i> 	<p>Vertrauliche Informationen müssen während der Übertragung über öffentliche Netzwerke verschlüsselt werden, da böswillige Personen Daten während der Übertragung mühelos abfangen und/oder umleiten können.</p> <p>Secure Sockets Layer (SSL) z. B. verschlüsselt Websites sowie die darin eingegebenen Daten. Wenn Sie mit SSL gesicherte Websites verwenden, stellen Sie sicher, dass „https“ Teil der URL ist.</p> <p>Beachten Sie, dass einige Protokollimplementierungen (z. B. SSL Version 2.0 und SSH Version 1.0) bekannte Sicherheitslücken wie etwa Pufferüberläufe aufweisen, welche von einem Angreifer ausgenutzt werden könnten, um die Kontrolle über das betroffene System zu erlangen. Ganz gleich, welches Sicherheitsprotokoll eingesetzt wird, stellen Sie sicher, dass es so konfiguriert ist, ausschließlich sichere Konfigurationen und Versionen zu verwenden, um zu vermeiden, dass eine unsichere Verbindung verwendet wird.</p>

Anforderung	Leitfaden
<p>4.1.1 Stellen Sie sicher, dass drahtlose Netzwerke, die Karteninhaberdaten übertragen oder mit der Karteninhaberdaten-Umgebung verbunden sind, bewährte Branchenverfahren (z. B. IEEE 802.11i) einsetzen, um die starke Verschlüsselung für die Authentifizierung und Übertragung zu implementieren.</p> <p>Hinweis: Die Nutzung von WEB als Sicherheitskontrolle ist seit dem 30. Juni 2010 untersagt.</p>	<p>Böswillige Personen verwenden kostenlose und allseits verfügbare Tools, um Drahtloskommunikationen zu belauschen. Durch den Einsatz einer starken Kryptographie kann die Weitergabe vertraulicher Informationen über das Netzwerk eingeschränkt werden. Viele bekannte Gefahren für Karteninhaberdaten, die ausschließlich im Kabelnetzwerk gespeichert sind, entstehen, wenn ein böswilliger Benutzer den Zugriff über ein unsicheres Drahtlosnetzwerk erweitert. Beispiele für drahtlose Implementierungen, die eine starke Kryptographie erfordern, sind unter anderem GPRS, GSM, WIFI, Satellit und Bluetooth.</p> <p>Um zu vermeiden, dass sich böswillige Benutzer Zugriff auf das Drahtlosnetzwerk und damit auf die darauf befindlichen Daten verschaffen oder die Drahtlosnetzwerke verwenden, um andere internen Netzwerke oder Daten zu erreichen, muss zum Schutz der Karteninhaberdaten eine starke Kryptographie zur Authentifizierung und Übertragung eingesetzt werden. Die WEP-Verschlüsselung sollte niemals als einzige Methode zur Verschlüsselung von Daten verwendet werden, da sie nicht als starke Kryptographie angesehen und aufgrund schwacher Initialisierungsvektoren im WEP-Schlüsselaustauschverfahren extrem anfällig ist und darüber hinaus nicht die erforderliche Schlüsselrotation unterstützt. Ein Angreifer kann ungehindert frei verfügbare Brute-Force-Cracking-Tools einsetzen, um in die WEP-Verschlüsselung einzudringen.</p> <p>Aktuelle Drahtlosgeräte sollten aufgerüstet werden (Beispiel: rüsten Sie die Zugriffspunkt-Firmware auf WPA2 auf), damit sie eine starke Verschlüsselung unterstützen können. Wenn aktuelle Geräte nicht aufgerüstet werden können, sollte entweder eine neue Ausrüstung gekauft oder andere kompensierende Steuerungen implementiert werden, um eine starke Verschlüsselung zu erreichen.</p>
<p>4.2 Versenden Sie niemals ungeschützte PANs über Messaging-Technologien für Endbenutzer (z. B. E-Mail, Instant Messaging, Chat usw.).</p>	<p>E-Mail, Instant Messaging und Chats können in internen und öffentlichen Netzwerken während der Übertragung mithilfe von Paket-Sniffing leicht abgefangen werden. Nutzen Sie diese Nachrichten-Tools nicht, um PANs zu versenden, sofern sie keine starke Verschlüsselung bieten.</p>

Leitfaden für die Anforderungen 5 und 6: Unterhaltung eines Anfälligkeits-Managementprogramms

Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware

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

Anforderung	Leitfaden
<p>5.1 Implementieren von Virenschutzsoftware auf allen Systemen, die häufig von böswilliger Software befallen werden (insbesondere Personal Computer und Server).</p>	<p>Es werden kontinuierlich Angriffe mithilfe weit verbreiteter Verfahren gegen anderweitig gesicherte Systeme durchgeführt. Häufig handelt es sich hierbei um „0-Day“-Angriffe, d. h. Sicherheitslücken, die innerhalb einer Stunde nach ihrer Entdeckung in den Netzwerken veröffentlicht und verbreitet werden. Ohne eine regelmäßig aktualisierte Antivirus-Software sind diese neuen Arten von Malware in der Lage, Ihr Netzwerk anzugreifen und sogar auszuschalten.</p> <p>Eine schädliche Software kann unwissentlich aus dem Internet heruntergeladen und/oder installiert werden. Allerdings sind Computer jedoch auch durch die Nutzung von Wechselspeichermedien wie etwa CDs oder DVDs, USB-Speichergeräten und Festplatten, Digitalkameras, PDAs und anderen Peripheriegeräten gefährdet. Ohne eine installierte Antivirus-Software könnten diese Computer in Ihrem Netzwerk zu Zugriffspunkten werden und/oder Informationen innerhalb des Netzwerks bedrohen.</p> <p>Da Systeme, die häufig von Malware betroffen sind, keine Mainframes und auch nicht die meisten Unix Systeme beinhalten (nachstehend finden Sie ausführlichere Informationen zu diesem Thema), müssen alle Stellen entsprechend der PCI-DSS-Anforderung 6.2 einen Prozess zur Identifizierung und Korrektur neuer Sicherheitslücken implementieren und dementsprechend ihre Konfigurationsstandards und Verfahren aktualisieren. Sollte eine andere Lösung dieselben Bedrohungen mit einer anderen Methode als dem signaturbasierten Ansatz abwenden, kann auch sie mit dieser Anforderung konform sein.</p> <p>Die im Zusammenhang mit den Betriebssystemen, die eine Stelle verwendet, beschriebenen Malware-Trends müssen in der Identifizierung neuer Sicherheitslücken eingegliedert sein und auch Methoden zur Korrektur neuer Trends sollten je nach Bedarf in die Konfigurationsstandards und Schutzmechanismen eines Unternehmens aufgenommen werden.</p> <p>Folgende Betriebssysteme sind normalerweise nur selten von Malware betroffen: Mainframes und bestimmte Unix Server (z. B. AIX, Solaris und HP-Unix). Allerdings können sich Branchentrends in Sachen Malware schnell ändern und alle Unternehmen müssen mit der Anforderung 6.2 konform sein, um neue</p>

Anforderung	Leitfaden
	Sicherheitsrisiken zu erkennen und zu beheben und ihre Konfigurationsstandards und Verfahren dementsprechend zu aktualisieren.
<p>5.1.1 Stellen Sie sicher, dass alle Virenschutzprogramme in der Lage sind, alle bekannten Malware-Typen zu erkennen, zu entfernen und davor zu schützen.</p>	<p>Es ist wichtig, sich gegen ALLE Arten und Formen von Malware zu schützen.</p>
<p>5.2 Stellen Sie sicher, dass alle Antivirenmechanismen auf dem Laufenden sind, aktiv ausgeführt werden und in der Lage sind, Audit-Protokolle zu generieren.</p>	<p>Selbst die beste Antivirus-Software ist in ihrer Wirksamkeit beschränkt, wenn sie nicht über aktuelle Antivirus-Signaturen verfügt oder in dem Netzwerk oder auf dem Computer einer Person nicht aktiviert wurde.</p> <p>Audit-Protokolle ermöglichen die Überwachung der Virus-Aktivität und Antivirus-Antworten. Folglich muss die Antivirus-Software so konfiguriert werden, dass sie Audit-Protokolle generiert und diese Protokolle im Sinne der Anforderung 10 verwaltet werden.</p>

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

Skrupellose Personen nutzen Sicherheitslücken aus, um sich einen privilegierten Zugriff auf Systeme zu verschaffen. Zahlreiche dieser Sicherheitslücken werden durch Sicherheitspatches geschlossen, die vom Anbieter bereitgestellt werden und von den Einheiten installiert werden müssen, die die Systeme verwalten. Alle kritischen Systeme müssen mit den neuesten Versionen der entsprechenden Software-Patches für den Schutz vor Ausnutzung und Beeinträchtigung von Karteninhaberdaten durch böswillige Personen und Software versehen sein.

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

Anforderung	Leitfaden
<p>6.1 Stellen Sie sicher, dass alle Systemkomponenten und Softwareanwendungen vor bekannten Sicherheitslücken mithilfe der neuesten Sicherheitspatches des jeweiligen Herstellers geschützt sind. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden.</p> <p><i>Hinweis: Ein Unternehmen kann den Einsatz eines risikobasierten Ansatzes in Erwägung ziehen, um seine Patch-Installationen zu priorisieren. Beispielsweise kann kritischer Infrastruktur (z. B. öffentliche Geräte und Systeme, Datenbanken) eine höhere Priorität eingeräumt werden als weniger kritischen internen Geräten, um zu gewährleisten, dass Systeme und Geräte mit hoher Priorität innerhalb eines Monats und weniger kritische Geräte und Systeme innerhalb von drei Monaten adressiert werden.</i></p>	<p>Bei einer Vielzahl von Angriffen werden weit verbreitete Verfahren gegen anderweitig gesicherte Systeme durchgeführt. Hierbei handelt es sich nicht selten um „0-Day“-Angriffe, d. h. Sicherheitslücken, die innerhalb einer Stunde veröffentlicht werden. Wenn nicht immer so bald wie möglich die neuesten Patches auf wichtigen Systemen implementiert werden, kann sich eine böswillige Personen dieser Verfahren bedienen, um das Netzwerk anzugreifen und auszuschalten. Erwägen Sie, die Änderungen nach ihrer Dringlichkeit zu ordnen, sodass wichtige Sicherheitspatches auf wichtigen oder gefährdeten Systemen innerhalb von 30 Tagen und andere weniger risikoreiche Änderungen innerhalb von 2-3 Monaten installiert werden.</p>

Anforderung	Leitfaden
<p>6.2 Erstellen Sie einen Prozess zur Identifizierung und Bestimmung einer Risikobewertung für neu festgestellte Sicherheitslücken.</p> <p>Hinweise: <i>Die Risikobewertungen müssen auf den Best Practices der Branche aufbauen. Ein Kriterium, um eine Schwäche mit einem „hohen“ Risiko einzustufen, könnte beispielsweise eine CVSS-Grundbewertung von 4.0 oder höher sein und/oder ein Patch von einem Anbieter, das als „kritisch“ bewertet wird, und/oder eine Schwäche, die eine wichtige Systemkomponente betrifft.</i> <i>Die in 6.2.a beschriebene Bewertung von Sicherheitslücken wird bis 30. Juni 2012 als Best Practices angesehen, danach wird sie zu einer Anforderung.</i></p>	<p>Der Zweck dieser Anforderung besteht darin, dass ein Unternehmen stets auf dem neuesten Stand bezüglich Sicherheitsrisiken ist, die dessen Umgebung gefährden könnten.</p> <p>Ebenso wichtig wie die Verfolgung von Bekanntgaben durch Anbieter zu Neuigkeiten über Sicherheitslücken und Patches für ihre Produkte ist es, sich über Newsgroups und Mailinglisten zu in der Branchen gängigen Sicherheitsrisiken und potentiellen Übergangslösungen zu informieren, die dem Anbieter unter Umständen noch nicht bekannt sind oder von ihm noch nicht gelöst werden konnten.</p> <p>Sobald ein Unternehmen eine Schwachstelle entdeckt, die seine Umgebung beeinträchtigen könnte, muss das Risiko dieser Schwachstelle bewertet und entsprechend eingestuft werden. Voraussetzung hierfür ist, dass das Unternehmen über eine einheitliche Methode zur Analyse und Risikobewertung von Schwachstellen verfügt. Obwohl die meisten Unternehmen wahrscheinlich aufgrund ihrer einzigartigen Karteninhaberdaten-Umgebung unterschiedliche Methoden zur Analyse und Risikobewertung von Sicherheitslücken haben, ist es möglich, auf in der Branche gängigen und zugelassenen Risikobewertungssystemen, wie etwa CVSS. 2.0, NIST SP 800-30 usw. aufzubauen.</p> <p>Durch die Einstufung von Risiken (z. B. als „schwerwiegend“, „mäßig“ oder „niedrig“) ist ein Unternehmen in der Lage, schneller Risiken höchster Priorität zu erkennen und zu beheben und somit die Wahrscheinlichkeit zu reduzieren, dass Schwachstellen, die ein großes Risiko darstellen, tatsächlich ausgenutzt werden können.</p>
<p>6.3 Entwickeln Sie Softwareanwendungen (interne und externe, einschließlich Web-Administrationszugriff auf die Anwendungen) gemäß PCI-DSS (z. B. sichere Authentifizierung und Protokollierung) und auf Grundlage von Best Practices der Branche und implementieren Sie Vorkehrungen zur Informationssicherheit während des Systementwicklungszyklus. Diese Prozesse müssen Folgendes umfassen:</p>	<p>Ohne die Einbindung von Informationssicherheitsmaßnahmen während der Definition der Anforderungen sowie der Design-, Analyse- und Testphasen in der Softwareentwicklung können Sicherheitslücken ungewollt oder in bössartiger Absicht in die Produktionsumgebung eingeschleust werden.</p>
<p>6.3.1 Löschung benutzerdefinierter Anwendungskonten, Benutzernamen und Kennwörter, bevor Anwendungen aktiv oder an Kunden freigegeben werden</p>	<p>Benutzerspezifische Anwendungskonten, Benutzernamen und Kennwörter sollten aus dem Seriencode gelöscht werden, bevor die Anwendung aktiviert oder an die Kunden ausgegeben wird, zumal diese Elemente Informationen über die Funktionsweise der Anwendung preisgeben können. Personen, die in den Besitz derartiger Informationen gelangen, könnten die Anwendung sowie zugehörige Karteninhaberdaten gefährden.</p>

Anforderung	Leitfaden
<p>6.3.2 Überprüfung benutzerdefinierter Programmcodes vor der Freigabe für die Produktion oder an Kunden, um alle potenziellen Programmanfälligkeiten zu identifizieren.</p> <p><i>Hinweis: Diese Anforderung für Code-Prüfungen gilt für den gesamten benutzerdefinierten (internen und öffentlichen) Code als Teil des Systementwicklungszyklus. Code-Prüfungen können durch qualifiziertes internes Personal oder durch Dritte ausgeführt werden. Webanwendungen unterliegen auch zusätzlichen Kontrollen, wenn sie öffentlich sind, um laufende Bedrohungen und Sicherheitslücken nach der Implementierung gemäß der Definition in PCI-DSS-Anforderung 6.6 zu adressieren.</i></p>	<p>Sicherheitslücken in benutzerspezifischen Codes werden von böswilligen Individuen häufig ausgenutzt, um sich Zugriff auf ein Netzwerk zu verschaffen und Karteninhaberdaten zu kompromittieren.</p> <p>Code-Prüfungen können entweder manuell oder mithilfe automatischer Überprüfungs-Tools vorgenommen werden. Automatische Überprüfungs-Tools verfügen über Funktionen, die Codes auf verbreitete Programmierfehler oder Schwachstellen untersuchen. Obwohl die automatische Überprüfung ein nützliches Instrument darstellt, sollte man sich zum Zweck der Code-Prüfung nicht alleinig auf diese Methode verlassen. Im Überprüfungsprozess sollte eine kompetente und erfahrene Person eingebunden werden, um selbst solche Codeprobleme erkennen zu können, die für ein automatisches Tool nur schwer oder gar unmöglich zu identifizieren sind. Indem die Code-Überprüfungen einer anderen Person als dem Entwickler des Codes aufgetragen werden, wird eine unabhängige und objektive Überprüfung gewährleistet.</p>
<p>6.4 Befolgen von Änderungskontrollprozessen und -verfahren für alle Änderungen an Systemkomponenten. Die Prozesse müssen Folgendes umfassen:</p>	<p>Ohne angemessene Änderungskontrollen können Sicherheitsfunktionen ungewollt oder wissentlich ausgelassen oder gar funktionsunfähig gemacht werden. Außerdem könnten Unregelmäßigkeiten in der Verarbeitung auftreten oder schädliche Codes eingeführt werden.</p>
<p>6.4.1 Separate Entwicklungs-, Test- und Produktionsumgebungen</p>	<p>Aufgrund des sich fortwährend ändernden Status von Entwicklungs- und Testumgebungen sind sie oft unsicherer als die Produktionsumgebung. Ohne eine angemessene Trennung der Umgebungen ist es möglich, dass die Produktionsumgebung und die Karteninhaberdaten aufgrund von Sicherheitslücken in einer Test- oder Entwicklungsumgebung beschädigt werden.</p>
<p>6.4.2 Trennung der Aufgaben zwischen Entwicklungs-, Test- und Produktionsumgebungen</p>	<p>Indem die Personenzahl, die Zugriff auf die Produktionsumgebung und die Karteninhaberdaten hat, eingeschränkt wird, kann das Risiko minimiert und sichergestellt werden, dass der Zugriff ausschließlich auf Personen mit einem geschäftlichen Informationsbedarf beschränkt ist.</p> <p>Der Zweck dieser Anforderung liegt darin, sicherzustellen, dass die Entwicklungs-/Testfunktionen von den Produktionsfunktionen getrennt werden. Ein Entwickler könnte beispielsweise in der Entwicklungsumgebung ein Konto auf Administratorebene mit erweiterten Rechten einsetzen und ein separates Konto mit Zugriff auf Benutzerebene zu der Produktionsumgebung haben.</p> <p>In Umgebungen, in denen eine einzige Person mehrere Funktionen erfüllt (z. B. die Anwendungsentwicklung und die Implementierung von Updates in Produktionssystemen), sollten die Aufgaben so verteilt werden, dass niemand die End-to-End-Kontrolle eines Prozesses ohne einen unabhängigen Kontrollpunkt innehat. Erteilen Sie z. B. Entwicklungs-, Autorisierungs- und Überwachungsaufgaben verschiedenen Personen.</p>

Anforderung	Leitfaden
<p>6.4.3 Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet</p>	<p>In der Entwicklungsumgebung sind die Sicherheitskontrollen normalerweise weniger streng. Die Verwendung von Produktionsdaten bietet böswilligen Personen die Gelegenheit, sich unbefugten Zugriff auf Produktionsdaten (Karteneinhaberdaten) zu verschaffen.</p> <p>Kreditkartenunternehmen und eine Vielzahl von Acquireern sind in der Lage, für Tests geeignete Kontonummern bereitzustellen, falls Sie vor der Veröffentlichung realistische PANs zum Testen der Systemfunktionalität benötigen.</p>
<p>6.4.4 Löschung von Testdaten und -konten, bevor Produktionssysteme aktiv werden</p>	<p>Testdaten und -konten sollten aus dem Seriencode gelöscht werden, bevor die Anwendung aktiviert, zumal diese Elemente Informationen über die Funktionsweise der Anwendung preisgeben können. Personen, die in den Besitz derartiger Informationen gelangen, könnten die Anwendung sowie zugehörige Karteneinhaberdaten gefährden.</p>
<p>6.4.5 Änderung von Kontrollverfahren für die Implementierung von Sicherheitspatches und Softwareänderungen. Die Verfahren müssen Folgendes umfassen:</p>	<p>Ohne angemessene Änderungskontrollen können Sicherheitsfunktionen ungewollt oder wissentlich ausgelassen oder gar funktionsunfähig gemacht werden. Außerdem könnten Unregelmäßigkeiten in der Verarbeitung auftreten oder schädliche Codes eingeführt werden. Ebenso kann eine Änderung eine Sicherheitsfunktion eines Systems beeinträchtigen. In diesem Fall muss die Änderung rückgängig gemacht werden.</p>
<p>6.4.5.1 Dokumentation der Auswirkungen.</p>	<p>Die Auswirkungen der Änderung sollten dokumentiert werden, sodass alle betroffenen Parteien angemessene Änderungen in der Verarbeitung vorausplanen können.</p>
<p>6.4.5.2 Dokumentierte Genehmigung von Änderungen durch autorisierte Parteien.</p>	<p>Die Genehmigung durch eine autorisierte Partei deutet darauf hin, dass es sich um eine zulässige und von dem Unternehmen genehmigte Änderung handelt.</p>
<p>6.4.5.3 Testen der Funktionalität, um sicherzustellen, dass die Änderung nicht die Sicherheit des Systems beeinträchtigt.</p>	<p>Es sollten eingehende Tests durchgeführt werden, um sicherzustellen, dass die Sicherheit durch diese Änderung nicht herabgesetzt wird. Die Tests sollten überprüfen, ob alle vorhandenen Sicherheitsvorkehrungen bestehen bleiben, durch ebenso starke Kontrollen ersetzt werden oder nach jeglichen Änderungen in der Umgebung sogar intensiviert werden müssen.</p> <p>Bei Änderungen an benutzerspezifischen Codes muss im Zuge der Tests überprüft werden, dass durch die Änderung keine Programmierschwächen eingeführt worden sind.</p>
<p>6.4.5.4 Back-Out-Verfahren.</p>	<p>Für alle Änderungen müssen Verfahren etabliert sein, um die Änderung, für den Fall, dass diese fehlschlägt, rückgängig zu machen und den vorherigen Zustand wiederherzustellen.</p>

Anforderung	Leitfaden
<p>6.5 Entwickeln Sie Anwendungen auf der Grundlage sicherer Programmierungsrichtlinien. Vorbeugung häufiger Programmierungsanfälligkeiten in Softwareentwicklungsprozessen, einschließlich der folgenden Punkte:</p> <p><i>Hinweis: Die unter 6.5.1 bis 6.5.9 aufgeführten Schwachstellen entsprechen zum Zeitpunkt der Veröffentlichung dieser Version des PA-DSS den Best Practices der Branche. Da jedoch die Best Practices der Branche im Anfälligkeits-Management aktualisiert werden (z. B. der OWASP Leitfaden, SANS CWE Top 25, CERT Secure Coding, usw.), müssen für diese Anforderungen die aktuellen Best Practices verwendet werden.</i></p>	<p>Die Anwendungsschicht ist einem hohen Risiko ausgesetzt und ist sowohl durch interne als auch externe Bedrohungen gefährdet. Ohne eine geeignete Sicherheitslösung sind Karteninhaberdaten und andere vertrauliche Unternehmensinformationen und somit auch das Unternehmen selbst, dessen Kunden und Ruf gefährdet.</p> <p>So wie bei allen PCI-DSS-Anforderungen handelt es sich bei den Anforderungen 6.5.1 bis 6.5.5 und 6.5.7 bis 6.5.9 lediglich um die <i>Mindestkontrollen</i>, welche implementiert werden müssen. Diese Liste umfasst die zum Zeitpunkt der Veröffentlichung dieser PCI-DSS-Version verbreitetsten zugelassenen und sicheren Codierungsverfahren. Bei einer Änderung der branchenweit anerkannten sicheren Codierungsverfahren müssen die unternehmensweiten Codierungsverfahren entsprechend aktualisiert werden.</p> <p>Die aufgeführten Beispiele für sichere Codierungsressourcen (SANS, CERT und OWASP) sind lediglich Bezugsquellen und dienen ausschließlich zur Orientierung. Ein Unternehmen sollte basierend auf der jeweiligen Technologie in seiner Umgebung passende sichere Codierungsverfahren implementieren.</p>

Anforderung	Leitfaden
<p>6.5.1 Injektionsfehler, insbesondere bei der SQL-Injektion. Injektion von Betriebssystembefehlen, LDAP- und Xpath-Injektionsfehler sowie andere Injektionsfehler sind ebenfalls zu berücksichtigen.</p>	<p>Validieren Sie die Eingabe, um zu überprüfen, dass Benutzerdaten nicht die Bedeutung von Befehlen und Abfragen ändern können. Injektionsfehler, insbesondere die SQL-Injektion, sind eine häufig eingesetzte Methode, um Anwendungen zu beschädigen. Injektionen treten auf, wenn vom Benutzer übermittelte Daten als Teil eines Befehls oder einer Anfrage an einen Interpreter gesendet werden. Die schädlichen Daten des Angreifers verleiten den Interpreter unwissentlich dazu, Befehle auszuführen oder Daten zu ändern, was es dem Angreifer ermöglicht, die Komponenten im Netzwerk über die Anwendung anzugreifen, Angriffe wie beispielsweise Pufferüberläufe einzuleiten oder sowohl vertrauliche Informationen als auch Anwendungsfunktionen des Servers zu enthüllen. Das ist auch eine verbreitete Methode, um betrügerische Transaktionen in Online-Shops auszuführen. Die Informationen aus Anfragen müssen, bevor sie an die Anwendung weitergeleitet werden, kontrolliert werden, beispielsweise indem nur alphabetische, eine Kombination aus alphabetischen und numerischen Zeichen usw. überprüft werden.</p>
<p>6.5.2 Pufferüberlauf</p>	<p>Stellen Sie sicher, dass die Anwendungen nicht anfällig für Angriffe durch Pufferüberläufe sind. Pufferüberläufe treten auf, wenn eine Anwendung auf ihrem Pufferspeicherplatz nicht über eine geeignete Bereichsüberprüfung verfügt. Um einen Schwachstelle durch einen Pufferüberlauf auszunutzen, schickt ein Angreifer einer Anwendung eine größere Datenmenge als einer ihrer Puffer in der Lage ist zu bearbeiten. Das kann dazu führen, dass die Informationen in dem Puffer aus dem Pufferspeicherplatz auf einen ausführbaren Speicherbereich verdrängt werden. In diesem Fall ist der Angreifer in der Lage, schädliche Codes an das Ende eines Puffers zu hängen und diesen Code anschließend, indem der Puffer zum Überlaufen gebracht wird, in einen ausführbaren Speicherbereich einzuschleusen. Der schädliche Code wird dann ausgeführt und gewährt dem Angreifer den rechnerfernen Zugriff auf die Anwendung und/oder das betroffene System.</p>
<p>6.5.3 Unsicherer kryptographischer Speicher</p>	<p>Verhindern Sie kryptographische Fehler. Anwendungen, die keine starken kryptographischen Funktionen zur angemessenen Speicherung ihrer Daten einsetzen, sind einem erhöhten Risiko für Kompromittierungen und Freigaben ihrer Karteninhaberdaten ausgesetzt. Wenn ein Angreifer schwache kryptographische Prozesse ausnutzen kann, könnte er unter Umständen auch in der Lage sein, verschlüsselte Daten in Klartext anzuzeigen.</p>

Anforderung	Leitfaden
<p>6.5.4 Unsichere Mitteilungen</p>	<p>Verschlüsseln Sie alle authentifizierten und vertraulichen Mitteilungen ordnungsgemäß. Anwendungen, die es versäumen, den Netzwerkdatenverkehr mithilfe einer starken Kryptographie angemessen zu verschlüsseln, sind einem erhöhten Risiko für Kompromittierungen und Gefährdungen ihrer Karteninhaberdaten ausgesetzt. Wenn ein Angreifer schwache kryptographische Prozesse ausnutzen kann, könnte er unter Umständen auch in der Lage sein, die Kontrolle über eine Anwendung zu erlangen oder verschlüsselte Daten in Klartext anzuzeigen.</p>
<p>6.5.5 Inkorrekte Fehlerhandhabung</p>	<p>Geben Sie keine Informationen über Fehlermeldungen oder andere Mittel preis. Anwendungen können unbeabsichtigt Informationen über ihre Konfiguration und interne Anläufe preisgeben oder durch eine Vielzahl von Anwendungsproblemen gegen Datenschutzrichtlinien verstoßen. Angreifer nutzen diese Schwachstelle aus, um vertrauliche Informationen zu entwenden oder andere schwerwiegendere Angriffe auszuführen. Auch eine unsachgemäße Fehlerbehandlung gibt Informationen preis, die es Angreifern ermöglichen, dem System Schaden zuzufügen. Wenn eine böswillige Person Fehler einbauen kann, die die Anwendung anschließend nicht richtig behebt, ist sie auch in der Lage, an ausführliche Informationen über das System zu gelangen, Denial-of-Service-Unterbrechungen hervorzurufen, das Sicherheitssystem zum Scheitern oder den Server zum Abstürzen zu bringen. Zum Beispiel bestätigt die Meldung „falsches Kennwort“, dass der Benutzername korrekt war und der Angreifer seine Anstrengungen nur auf das Kennwort konzentrieren muss. Es wird empfohlen, allgemeinere Meldungen zu verwenden, wie z. B. „die Daten konnten nicht bestätigt werden“.</p>
<p>6.5.6 Alle „schwerwiegenden“ Schwächen werden entsprechend des Identifikationsprozesses von Schwächen dargelegt (wie in der PCI-DSS-Anforderung 6.2 definiert).</p> <p>Hinweis: Diese Anforderung wird bis zum 30. Juni 2012 als Best Practice angesehen, danach wird sie zu einer Anforderung.</p>	<p>Alle gemäß Anforderung 6.2 genannten schwerwiegenden Sicherheitslücken, die die Funktionsfähigkeit der Anwendung beeinträchtigen könnten, sollten während der Entwicklungsphase berücksichtigt werden. Beispielsweise sollte eine in einer Shared-Library oder in dem zugrundeliegenden Betriebssystem entdeckte Sicherheitslücke analysiert und, noch bevor die Anwendung an die Produktion freigegeben wird, korrigiert werden.</p>
<p>Für Web-Anwendungen und Anwendungsschnittstellen (intern und extern) gelten darüber hinaus folgende Anforderungen:</p>	<p>Web-Anwendungen sowohl intern als auch extern (öffentlich) sind aufgrund ihrer Architektur sowie der relativ einfachen Erstellung und der Häufigkeit von Angriffen einmaligen Sicherheitsrisiken ausgesetzt.</p>

Anforderung	Leitfaden
<p>6.5.7 Siteübergreifendes Scripting (XSS)</p>	<p>Vor der Aufnahme sollten alle Parameter zunächst überprüft werden. XSS-Fehler treten auf, wenn eine Anwendung vom Benutzer übermittelte Daten an einen Webbrowser sendet, ohne diese zuvor zu überprüfen oder deren Inhalt zu verschlüsseln. XSS ermöglicht es Angreifern im Browser eines betroffenen Benutzers Skripts auszuführen, wodurch unter anderem Benutzer-Sitzungen entführt, Websites unleserlich gemacht und möglicherweise Würmer eingeschleust werden können.</p>
<p>6.5.8 Kontrolle unangemessener Zugriffe (z. B. unsichere direkte Objektverweise, unterlassene Einschränkung des URL-Zugriffs und Directory Traversal)</p>	<p>Machen Sie interne Objektverweise nicht Benutzern zugänglich. Ein direkter Objektverweis entsteht, wenn ein Entwickler einen Verweis einem internen Implementierungsobjekt, wie etwa einer Datei, einem Verzeichnis, einem Datenbankeintrag oder einem Schlüssel, in Form einer URL oder eines Formparameters zugänglich macht. Angreifer können diese Verweise manipulieren, um unerlaubt auch auf andere Objekte zuzugreifen.</p> <p>Setzen Sie die Zugriffssteuerung konsistent in der Präsentationsebene und der Geschäftslogik für alle URLs durch. Oft schützt eine Anwendung eine empfindliche Funktion nur, indem sie verhindert, dass Links oder URLs unbefugten Benutzern angezeigt werden. Angreifer können diese Schwachstelle ausnutzen, um sich Zugriff auf Vorgänge zu verschaffen, für die sie keine Berechtigung besitzen, und diese anschließend auszuführen, indem sie diese URLs direkt aufrufen.</p> <p>Schützen Sie sich vor Directory Traversal. Ein Angreifer ist unter Umständen in der Lage, die Verzeichnisstruktur einer Website aufzulisten und zu durchsuchen und sich somit Zugriff auf vertrauliche Informationen zu verschaffen sowie tiefere Einblicke in die Funktionsweise der Site für spätere Angriffe zu gewinnen.</p>
<p>6.5.9 Cross-Site Request Forgery (CSRF)</p>	<p>Antworten Sie nicht auf Autorisierungsinformationen und Token, die automatisch von Browsern gesendet werden. Ein CSRF-Angriff zwingt den Browser eines angemeldeten Benutzers, eine noch nicht authentifizierte Anfrage an eine gefährdete Web-Anwendung zu senden, wodurch der Browser des Benutzers anschließend gezwungen wird, eine feindliche Aktion zum Vorteil des Angreifers auszuführen. CSRF kann genauso leistungsstark wie die angegriffene Web-Anwendung sein.</p>

Anforderung	Leitfaden
<p>6.6 Für öffentliche Webanwendungen laufende Adressierung neuer Bedrohungen und Schwachstellen und Gewährleisten, dass diese Anwendungen durch <i>eine</i> der folgenden Methoden geschützt werden:</p> <ul style="list-style-type: none">▪ Prüfen öffentlicher Webanwendungen durch manuelle oder automatisierte Tools oder Methoden zum Bewerten der Anwendungssicherheit mindestens jährlich sowie nach Änderungen▪ Installieren einer Webanwendungs-Firewall vor öffentlichen Webanwendungen	<p>Angriffe auf Webanwendungen sind nicht selten und häufig erfolgreich und werden durch schlechte Codierungsverfahren möglich gemacht. Diese Anforderung zur Überprüfung von Anwendungen oder Installation von Web Application Firewalls bezweckt, die Anzahl der Gefährdungen öffentlicher Web-Anwendungen zu reduzieren, durch die häufig Karteninhaberdaten kompromittiert werden.</p> <ul style="list-style-type: none">▪ Um diese Anforderung zu erfüllen, können manuelle oder automatisierte Tools oder Methoden zur Beurteilung der Anwendungssicherheit eingesetzt werden, da diese Anwendungen auf Sicherheitslücken überprüfen und/oder scannen.▪ Web Application Firewalls filtern und blockieren unnötigen Datenverkehr auf Anwendungsebene. Zusammen mit einer netzwerkbasieren Firewall kann eine angemessen konfigurierte Web Application Firewall Angriffe auf Anwendungsebene verhindern, sofern die Anwendungen entsprechend codiert oder konfiguriert sind.

Leitfaden für die Anforderungen 7, 8 und 9: Implementierung starker Zugriffskontrollmaßnahmen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

Um zu gewährleisten, dass nur autorisierte Mitarbeiter auf kritische Daten zugreifen können, müssen Systeme und Prozesse implementiert sein, die den Zugriff anhand des Informationsbedarfs und gemäß Zuständigkeiten beschränken. „Informationsbedarf“ besteht, wenn Zugriffsrechte nur auf die minimale Menge an Daten und Berechtigungen erteilt werden, die zum Ausüben einer Tätigkeit erforderlich sind.

Anforderung	Leitfaden
<p>7.1 Beschränken des Zugriffs auf Systemkomponenten und Karteninhaberdaten auf die Personen, deren Tätigkeit diesen Zugriff erfordert. Zugriffsbeschränkungen müssen Folgendes umfassen:</p> <p>7.1.1 Beschränkung von Zugriffsrechten für Benutzernamen auf Mindestberechtigungen, die zum Ausüben von tätigkeitsbezogenen Verpflichtungen erforderlich sind</p> <p>7.1.2 Die Zuweisung von Berechtigungen basiert auf der Tätigkeitsklassifizierung und -funktion einzelner Mitarbeiter</p> <p>7.1.3 Voraussetzung einer dokumentierten Genehmigung durch autorisierte Parteien, in der die erforderlichen Berechtigungen angegeben sind.</p> <p>7.1.4 Implementierung eines automatisierten Zugriffskontrollsystems</p>	<p>Je mehr Personen Zugriff auf die Karteninhaberdaten haben, desto höher ist das Risiko, dass das Konto eines Benutzers in böser Absicht ausgenutzt wird. Indem der Zugriff ausschließlich auf Personen beschränkt wird, die aus geschäftlichen Gründen Einsicht benötigen, ist Ihrem Unternehmen bereits geholfen, falsche Handhabungen der Karteninhaberdaten durch Unerfahrenheit oder Böswilligkeit zu vermeiden. Wenn Zugriffsberechtigungen nur für so wenig Daten und Rechte wie zur Ausführung einer Aufgabe erforderlich vergeben werden, handelt es sich um das sogenannte „Least Privilege“ und „Need to Know“-Prinzip, und wenn Berechtigungen an Personen entsprechend ihrer Tätigkeitskategorie und -funktion vergeben werden, spricht man von einer „Role-Based Access Control“ oder RBAC (zu Deutsch: Funktionsbasierte Zugriffskontrolle). Die Durchsetzung einer rollenbasierten Zugriffssteuerung ist nicht nur auf die Anwendungsebene oder spezifische Autorisierungslösungen beschränkt. Zum Beispiel sind unter anderem Verzeichnisdienste wie Active Directory oder LDAP, Access Control Lists (ACLs) und TACACS zuverlässige Lösungen, solange sie so konfiguriert sind, dass sie die „Least Privilege“ und „Need to Know“-Prinzipien durchsetzen.</p> <p>Unternehmen sollten mithilfe der rollenbasierten Zugriffssteuerung klare Richtlinien und Prozesse für Datenzugriffskontrollen basierend auf dem „Need to Know“-Prinzip, einschließlich angemessenen Verwaltungsautorisierungsverfahren, einrichten, um zu bestimmen, wem und wie Zugriff bewährt wird.</p>

Anforderung	Leitfaden
<p>7.2 Festlegen eines Zugriffskontrollsystems für Systemkomponenten mit mehreren Benutzern, das den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird.</p> <p>Dieses Zugriffskontrollsystem muss Folgendes umfassen:</p> <ul style="list-style-type: none"> 7.2.1 Abdeckung aller Systemkomponenten 7.2.2 Zuweisung von Berechtigungen zu einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion 7.2.3 Standardeinstellung „Alle ablehnen“ <p><i>Hinweis: Einige Zugriffskontrollsysteme sind standardmäßig auf „Alle zulassen“ gesetzt und lassen dadurch den Zugriff zu, bis eine Regel erstellt wird, die den Zugriff ausdrücklich ablehnt.</i></p>	<p>Ohne einen Mechanismus, um den Zugriff von Benutzern entsprechend ihres Informationsbedarfs einzuschränken, könnte einem Benutzer unter Umständen ungewollt Zugriff auf Dateninhaberdaten gewährt werden. Zur Verwaltung mehrerer Benutzer empfiehlt sich der Einsatz eines automatisierten Zugriffskontrollsystems oder -mechanismus. Dieses System sollte im Einverständnis mit den Zugriffskontrollrichtlinien und -prozessen des Unternehmens (einschließlich dem „Need to Know“-Prinzip und der „rollenbasierten Zugriffssteuerung“) eingerichtet werden und es sollte den Zugriff auf alle Systemkomponenten verwalten und über die Standardeinstellung „Alle ablehnen“ verfügen, um sicherzustellen, dass niemandem Zugriff gewährt wird, sofern nicht eine Regel eingesetzt wird, die diesen Zugriff ausdrücklich genehmigt.</p>

Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff

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

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

Anforderung	Leitfaden
<p>8.1 Zuweisen einer eindeutigen Benutzer-ID für alle Benutzer, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird.</p>	<p>Indem sichergestellt wird, dass jeder Benutzer eindeutig identifiziert ist – anstatt einen Benutzernamen für mehrere Mitarbeiter zu verwenden – kann ein Unternehmen Einzelne für ihre Handlungen zur Rechenschaft ziehen und pro Mitarbeiter einen effektiven Audit-Trail erstellen. Hierdurch können die Problembewältigung sowie der Einsatz von Vorbeugungsmaßnahmen im Falle von Missbrauch oder böswilligen Absichten beschleunigt werden.</p>
<p>8.2 Zuweisung einer eindeutigen ID und Einsatz von mindestens einer der folgenden Methoden zur Authentifizierung sämtlicher Benutzer:</p> <ul style="list-style-type: none"> ▪ Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennaussatz ▪ Etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard ▪ Etwas, das Sie sind, wie zum Beispiel biometrische Daten 	<p>Wenn diese Authentifizierungselemente zusammen mit einmaligen Benutzernamen eingesetzt werden, helfen sie dabei, die einmaligen Benutzernamen vor Angriffen zu schützen (zumal der Angreifer sowohl den einmaligen Benutzernamen als auch das Kennwort oder ein anderes Authentifizierungselement kennen muss).</p> <p>Solange es nur einmalig vergeben wird, ist ein digitales Zertifikat eine gute Option für eine Authentifizierung des Typs „Etwas, das Sie haben“.</p>

Anforderung	Leitfaden
<p>8.3 Authentifizierung anhand zweier Faktoren beim Remote-Zugriff (Netzwerkzugriff von außerhalb des Netzwerks) von Mitarbeitern, Administratoren und Dritten. (z. B. Remote-Authentifizierung und Einwahldienst (RADIUS) mit Tokens; Terminal Access Controller Access Control System (TACACS) mit Tokens oder andere Technologien, die eine Zwei-Faktor-Authentifizierung unterstützen.)</p> <p><i>Hinweis: Bei der Zwei-Faktor-Authentifizierung müssen zwei der drei Authentifizierungsmethoden (siehe PS-DSS-Anf. 8.2 für eine Beschreibung der Authentifizierungsmethoden) bei der Authentifizierung eingesetzt werden. Wenn ein Faktor zweimalig verwendet wird (z. B. wenn zwei separate Kennwörter eingesetzt werden) handelt es sich nicht um eine Zwei-Faktor-Authentifizierung.</i></p>	<p>Die Zwei-Faktor-Authentifizierung erfordert zwei verschiedene Authentifizierungen für Zugriffe mit einem höheren Risiko, wie etwa solche, die von außerhalb des Netzwerks getätigt werden. Für eine erhöhte Sicherheit kann Ihr Unternehmen auch in Betracht ziehen, beim Zugriff auf Netzwerke mit höheren Sicherheitsvorkehrungen von Netzwerken mit niedrigeren Sicherheitsvorkehrungen – z. B. von Unternehmens-Desktops (niedrigere Sicherheitsstandards) auf Produktionsserver/-datenbanken mit Karteninhaberdaten (hohe Sicherheitsstandards) – eine Zwei-Faktor-Authentifizierung zu verwenden.</p> <p>Diese Anforderung gilt für Benutzer, die einen Remote-Zugriff auf das Netzwerk besitzen und wo dieser Remote-Zugriff auch Zugang zu der Karteninhaberdaten-Umgebung gewähren könnte.</p> <p>In diesem Zusammenhang bezieht sich der Begriff Remote-Zugriff auf Zugriffe auf Netzwerkebene, die von außerhalb des Netzwerks einer Einheit getätigt werden, d. h. entweder über das Internet oder einem „nicht vertrauenswürdigen“ Netzwerk oder System, wie etwa durch einen Dritten oder einen Mitarbeiter, der mit seinem Laptop auf das Netzwerk der betreffenden Stelle zugreift. Interne LAN-auf-LAN-Zugriffe (z. B. zwischen zwei Büros über ein sicheres VPN) fallen in dieser Anforderung nicht unter den Begriff Remote-Zugriff.</p> <p>Wenn per Remote-Zugriff das Netzwerk einer Einheit mit angemessener Segmentierung aufgerufen wird, können diese Remote-Benutzer nicht auf die Karteninhaberdaten zugreifen oder diese gefährden. Folglich wäre für ein solches Netzwerk laut PCI-DSS keine Zwei-Faktor-Authentifizierung erforderlich. Nichtsdestotrotz ist eine Zwei-Faktor-Authentifizierung für alle Remote-Zugriffe auf Netzwerke mit Zugang auf die Karteninhaberdaten-Umgebung erforderlich und empfehlenswert für alle Remote-Zugriffe auf die Netzwerke der Einheit.</p>
<p>8.4 Geschützte Übertragung und Speicherung von Kennwörtern auf sämtlichen Systemkomponenten unter Verwendung einer sicheren Verschlüsselung.</p>	<p>Viele Netzwerkeinrichtungen und -anwendungen übertragen den Benutzernamen und das unverschlüsselte Kennwort über das Netzwerk und/oder speichern Kennwörter unverschlüsselt. Ein Angreifer kann leicht den unverschlüsselten oder lesbaren Benutzernamen und das Kennwort während der Übertragung mithilfe eines „Sniffers“ abfangen oder direkt auf die Benutzernamen und unverschlüsselte Kennwörter in gespeicherten Dateien zugreifen und diese gestohlenen Daten verwenden, um sich unbefugten Zugriff zu verschaffen. Während der Übertragung können entweder die Anmeldeinformationen von Benutzern oder der Tunnel verschlüsselt werden</p>
<p>8.5 Verwendung der geeigneten Benutzeridentifizierungs- und Authentifizierungsverwaltung für Nichtverbraucherbenutzer und Administratoren auf allen Systemkomponenten nach folgender Maßgabe:</p>	<p>Da der erste Schritt eines Angreifers zur Beschädigung eines Systems in der Ausnutzung schwacher oder nicht vorhandener Kennwörter liegt, ist es von großer Bedeutung, zuverlässige Verfahren zur Benutzeridentifizierung und Authentifizierungsverwaltung zu implementieren.</p>

Anforderung	Leitfaden
<p>8.5.1 Kontrollieren der Vorgänge zum Hinzufügen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsobjekten.</p>	<p>Um sicherzustellen, dass die Benutzer in Ihrem System alle gültige und anerkannte Benutzer sind, sollte die Eingabe, Löschung oder Änderung von Benutzernamen von einer kleinen Gruppe mit besonderen Befugnissen verwaltet und kontrolliert werden. Die Befugnis zur Verwaltung dieser Benutzernamen sollte ausschließlich dieser kleinen Gruppe vorbehalten sein.</p>
<p>8.5.2 Überprüfen der Benutzeridentität, bevor Kennwörter zurückgesetzt werden.</p>	<p>Viele Angreifer bedienen sich „Social Engineering“-Techniken,— zum Beispiel, indem sie den Helpdesk kontaktieren und sich als der entsprechende Benutzer ausgeben – um ein Kennwort zu ändern, damit sie einen bestimmten Benutzernamen verwenden können. Erwägen Sie den Einsatz von Sicherheitsfragen, die ausschließlich der jeweilige Benutzer beantworten kann, damit Administratoren den Benutzer eindeutig identifizieren können, bevor sie dessen Kennwort zurücksetzen. Stellen Sie sicher, dass diese Fragen angemessen gesichert und nicht weitergegeben werden.</p>
<p>8.5.3 Festlegen von Kennwörtern für die erste Verwendung und das Zurücksetzen dieser Kennwörter auf einen eindeutigen Wert für jeden Benutzer und sofortige Änderung nach der ersten Verwendung.</p>	<p>Wenn zur Einrichtung neuer Benutzer immer dasselbe Kennwort verwendet wird, könnte es einem internen Benutzer, einem früheren Mitarbeiter oder einem Angreifer bekannt sein oder in Erfahrung gebracht und eingesetzt werden, um auf die Konten zuzugreifen.</p>
<p>8.5.4 Sofortige Deaktivierung des Zugriffs ehemaliger Benutzer.</p>	<p>Wenn ein Mitarbeiter, der das Unternehmen verlassen hat, weiterhin Zugriff auf das Netzwerk über dessen Benutzerkonto besitzt, können unnötige Zugriffe oder Zugriffe in böswilligen Absichten auf Karteninhaberdaten eintreten. Diese Zugriffe könnten von einem früheren Mitarbeiter oder von einem Angreifer durchgeführt werden, der das alte und/oder ungenutzte Konto zu diesem Zweck missbraucht. Ziehen Sie in Erwägung, innerhalb der Personalabteilung einen Prozess zu implementieren, um direkt benachrichtigt zu werden, wenn ein Mitarbeiter das Unternehmen verlässt, sodass das Benutzerkonto umgehend gelöscht werden kann.</p>
<p>8.5.5 Entfernen bzw. Deaktivieren inaktiver Benutzerkonten mindestens alle 90 Tage.</p>	<p>Inaktive Konten ermöglichen es unbefugten Benutzern, die nicht genutzten Konten einzusetzen, um unter Umständen auf Karteninhaberdaten zuzugreifen.</p>

Anforderung	Leitfaden
<p>8.5.6 Aktivieren der von Anbietern für den Remote-Zugriff verwendeten Konten ausschließlich während der erforderlichen Zeit. Überwachung des aktiven Remote-Zugriffs auf Konten durch den Anbieter.</p>	<p>Wenn Sie Anbietern (wie etwa Anbieter von POS-Systemen) ermöglichen, an 7 Tagen in der Woche durchgehend auf Ihr Netzwerk zuzugreifen, um bei Bedarf Arbeiten an Ihrem System vorzunehmen, erhöht sich das Risiko für unbefugte Zugriffe entweder durch Benutzer aus der Umgebung des Anbieters oder durch eine böswillige Person, die diesen jederzeit verfügbaren externen Zugriffspunkt in Ihr Netzwerk ausnutzt.</p> <p>Die Überwachung des Zugriffs auf Karteninhaberdaten durch Anbieter gilt in gleicher Weise wie auch für andere Benutzer, wie etwa Mitarbeiter des Unternehmens. Dazu zählt auch die Überwachung und Protokollierung von Aktivitäten gemäß den PCI-DSS-Anforderungen 10.1 und 10.2 und die Kontrolle dazu, dass die Nutzung von Anbieter-Remote-Konten der in den Anforderungen 12.3.8 und 12.3.9 genannten Richtlinie entspricht.</p>
<p>8.5.7 Teilen Sie allen Benutzern, die Zugriff auf Karteninhaberdaten haben, die Authentifizierungsmethoden und -richtlinien mit.</p>	<p>Durch die Mitteilung von Kennwort-/Authentifizierungsverfahren an alle Benutzer sind diese in der Lage, die Richtlinien besser zu verstehen und sich an diese zu halten und wachsam zu sein, dass keine Angreifer ihre Kennwörter ausnutzen, um sich Zugriff auf die Karteninhaberdaten zu verschaffen (z. B. in dem ein Mitarbeiter angerufen und nach seinem Kennwort gefragt wird, um ein vermeintliches Problem zu lösen).</p>
<p>8.5.8 Verwenden Sie keine Konten und Kennwörter für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung oder andere Authentifizierungsmethoden.</p>	<p>Wenn mehrere Benutzer gemeinsam dieselben Anmeldeinformationen benutzen (z. B. Benutzerkonto und Kennwort), ist es nicht mehr möglich, Einzelne für ihre Aktionen zur Rechenschaft zu ziehen oder effektive Protokolle darüber zu führen, da die Aktion von jedem in der Gruppe, der die Anmeldeinformationen kennt, hätte durchgeführt werden können.</p> <p>Diese Anforderung für einmalige Benutzernamen und komplexe Kennwörter kann häufig innerhalb der Administration durch beispielsweise Sudo oder SSH eingehalten werden, indem sich der Administrator zunächst mit seinem eigenen einmaligen Benutzernamen und Kennwort anmeldet und dann über Sudo oder SSH eine Verbindung zum Administratorkonto herstellt. Nicht selten werden direkte Root-Anmeldungen deaktiviert, um die Nutzung des gemeinsamen Administratorkontos zu vermeiden. Auf diese Weise können Einzelverantwortung und Audit-Trails beibehalten werden. Allerdings sollten die aktuellen Administrator-Benutzernamen und Kennwörter trotz der Nutzung von Tools wie Sudo und SSH die PCI-DSS-Anforderungen (falls diese Konten nicht deaktiviert werden) einhalten, um zu verhindern, dass diese Informationen missbraucht werden können.</p>
<p>8.5.9 Ändern der Benutzerkennwörter mindestens alle 90 Tage.</p> <p>8.5.10 Festlegen einer Mindestlänge für Kennwörter von mindestens sieben Zeichen.</p>	<p>Starke Kennwörter sind die erste Verteidigungslinie eines Netzwerks, da Angreifer oft zunächst versuchen, Konten mit schwachen oder nicht vorhandenen Kennwörtern ausfindig zu machen. Es ist für eine Person mit böswilligen Absichten</p>

Anforderung	Leitfaden
<p>8.5.11 Verwenden von Kennwörtern, die sowohl numerische als auch alphabetische Zeichen enthalten.</p>	<p>einfacher, diese schwachen Konten ausfindig zu machen und ein Netzwerk unter dem Deckmantel eines gültigen Benutzernamens zu kompromittieren, wenn die Kennwörter kurz und einfach zu erraten sind und über einen langen Zeitraum nicht gewechselt werden. Starke Kennwörter können unter diesen Anforderungen durchgesetzt und aufrechterhalten werden, indem die Kennwort- und Kontosicherheitsfunktionen, die in Ihrem Betriebssystem (z. B. Windows), Ihren Netzwerken, Datenbanken oder anderen Plattformen enthalten sind, aktiviert werden.</p>
<p>8.5.12 Festlegen, dass sich ein neues Kennwort von den letzten vier Kennwörtern unterscheiden muss.</p>	
<p>8.5.13 Begrenzen der wiederholten Zugriffsversuche durch Sperren der Benutzer-ID nach spätestens sechs Versuchen.</p>	<p>Ohne implementierte Mechanismen für Kontosperrungen kann ein Angreifer fortwährend versuchen, ein Kennwort über manuelle oder automatisierte Tools zu erraten (z. B. Kennwort-Cracking-Tools), bis er letztendlich Erfolg hatte und sich Zugriff auf das Konto eines Benutzers verschafft hat.</p>
<p>8.5.14 Festlegen einer Aussperrdauer von mindestens 30 Minuten, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann.</p>	<p>Wenn ein Konto gesperrt wurde, weil eine Person versucht hat, ein Kennwort zu erraten, unterbinden Steuerungen zur Hinauszögerung der Reaktivierung dieser gesperrten Konten, dass ein Angreifer weiter versucht, das Kennwort zu erraten (während eines Zeitraums von mindestens 30 Minuten können sie keine weiteren Eingaben tätigen, bis das Konto erneut aktiviert wird.) Darüber hinaus kann der Administrator oder Helpdesk, sollte die erneute Aktivierung beantragt werden müssen, nachprüfen, ob der Kontoinhaber der Auslöser für diese Sperrung war (indem er Fehler eintippt).</p>
<p>8.5.15 Festlegen, dass sich die Benutzer nach mehr als 15-minütiger Inaktivität erneut anmelden und das Terminal oder die Sitzung reaktivieren müssen.</p>	<p>Wenn sich ein Benutzer von seinem Rechner mit Zugriff auf ein wichtiges Netzwerk oder auf Karteninhaberdaten entfernt, kann der Rechner von anderen in Abwesenheit des Benutzers dazu verwendet werden, sich unbefugten Zugriff auf dessen Konto zu verschaffen und/oder es missbräuchlich einzusetzen.</p>
<p>8.5.16 Festlegen, dass für den gesamten Zugriff auf Datenbanken mit Karteninhaberdaten eine Authentifizierung erforderlich ist. (Dies umfasst Zugriff durch Anwendungen, Administratoren und alle anderen Benutzer.) Schränken Sie den Direktzugriff oder Datenbankabfragen auf Datenbankadministratoren ein.</p>	<p>Ohne eine Benutzerauthentifizierung für den Zugriff auf Datenbanken und Anwendungen erhöht sich das Risiko für unbefugte oder in böser Absicht getätigte Zugriffe. Darüber hinaus können diese Zugriffe nicht protokolliert werden, da sich der Benutzer nicht angemeldet hat und dem System folglich nicht bekannt ist. Auch der Zugriff auf Datenbanken sollte ausschließlich durch programmgesteuerte Methoden gewährt werden (z. B. mittels gespeicherter Verfahren), anstatt durch einen direkten Zugriff auf die Datenbank durch Endbenutzer (mit Ausnahme von DBAs, die direkten Zugriff auf die Datenbank zur Erfüllung ihrer administrativen Aufgaben haben müssen).</p>

Anforderung 9: Beschränken Sie den physischen Zugriff auf Karteninhaberdaten

Der physische Zugriff auf Daten oder Systeme mit Karteninhaberdaten bietet Einzelpersonen die Gelegenheit, auf Geräte oder Daten zuzugreifen und Systeme oder Ausdrücke zu entfernen. Daher sollte der physische Zugriff entsprechend beschränkt sein. Zum Zwecke der Anforderung 9 bezieht sich der Begriff „Mitarbeiter vor Ort“ hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter und Subunternehmen sowie Berater, die am Standort der jeweiligen Stelle arbeiten. Ein „Besucher“ wird als Lieferant, Gast eines Mitarbeiters vor Ort, Servicemitarbeiter oder jede Person definiert, die die Einrichtung für kurze Zeit betreten muss, meist nicht länger als einen Tag. Der Begriff „Medien“ bezieht sich auf alle Papierdokumente und elektronischen Medien mit Karteninhaberdaten.

Anforderung	Leitfaden
<p>9.1 Verwenden angemessener Zugangskontrollen, um den physischen Zugriff auf Systeme für Karteninhaberdaten zu überwachen und zu beschränken.</p>	<p>Ohne physische Zugriffssteuerungen könnten sich unbefugte Personen Zugriff auf das Gebäude und vertrauliche Informationen verschaffen, die Systemkonfigurationen verändern, Sicherheitslücken in das System einschleusen oder Betriebsmittel zerstören oder entwenden.</p>
<p>9.1.1 Überwachen des Zugangs zu zugangsbeschränkten Bereichen mithilfe von Videokameras und/oder Kontrollsystemen. Überprüfen der gesammelten Daten und Korrelation mit anderen Daten. Speichern der Daten mindestens drei Monate lang, wenn dies gesetzlich zulässig ist.</p> <p>Hinweis: „Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Nicht hierzu zählen die Bereiche, in denen lediglich Point-of-Sale-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).</p>	<p>Wenn Verletzungen der physischen Integrität untersucht werden, können diese Kontrollen dabei helfen, jene Personen auszumachen, die direkt auf diese vertraulichen Bereiche, in denen Karteninhaberdaten gespeichert werden, zugreifen. Solche vertraulichen Bereiche sind beispielsweise Serverräume für Unternehmensdatenbanken, Back-Ende-Serverräume von Einzelhandelsgeschäften, in denen Karteninhaberdaten gespeichert werden, sowie Speicherbereiche für große Mengen an Karteninhaberdaten.</p>
<p>9.1.2 Beschränken des physischen Zugriffs auf öffentlich zugängliche Netzwerkdaten.</p> <p>Beispielsweise sollten für Besucher zugängliche Bereiche keine aktiven Netzwerkports haben, sofern der Netzwerkzugriff nicht ausdrücklich zugelassen ist.</p>	<p>Indem der Zugriff auf Netzwerkdaten eingeschränkt wird, wird verhindert, dass böswillige Personen leicht zugängliche Netzwerkdaten ausnutzen und unter Umständen auf interne Netzwerkressourcen zugreifen. Ziehen Sie in Erwägung, die Netzwerkdaten, sofern nicht in Betrieb, abzuschalten und nur dann erneut zu aktivieren, wenn Sie sie benötigen. Richten Sie in öffentlichen Bereichen, wie etwa Konferenzräumen, private Netzwerke ein, um Anbietern und Besuchern zu ermöglichen, eine Verbindung zum Internet herzustellen, ohne gleichzeitig auch Zugriff auf Ihr internes Netzwerk zu haben.</p>

Anforderung	Leitfaden
<p>9.1.3 Beschränken Sie den physischen Zugriff auf WLAN-Zugriffspunkte, Gateways, Handgeräte, Netzwerk- und Kommunikationshardware und Telekommunikationsleitungen.</p>	<p>Wenn die Sicherheit nicht über die Zugriffsfreiheit auf drahtlose Komponenten und Geräte gestellt wird, sind böswillige Benutzer in der Lage, unbeaufsichtigte Drahtlosgeräte Ihres Unternehmens zu verwenden, um auf Ihre Netzwerkressourcen zuzugreifen oder sogar ihre eigenen Geräte an Ihr drahtloses Netzwerk anzuschließen, um sich unerlaubten Zugriff zu verschaffen. Darüber hinaus kann, indem Netzwerk- und Kommunikationshardware gesichert wird, verhindert werden, dass böswillige Benutzer den Netzwerkdatenverkehr belauschen oder ihre eigenen Geräte an Ihre drahtlosen Netzwerkressourcen anschließen.</p> <p>Ziehen Sie in Erwägung, drahtlose Zugangspunkte, Gateways sowie Netzwerk- und Kommunikationshardware in sicheren Lagerbereichen wie etwa abgeschlossenen Schränken oder Serverräumen einzurichten. Stellen Sie bei drahtlosen Netzwerken sicher, dass die starke Verschlüsselung aktiviert ist. Ziehen Sie auch in Betracht, automatische Sperren für drahtlose Handgeräte nach langen Inaktivitätszeiten einzurichten, und konfigurieren Sie Ihre Geräte so, dass beim Einschalten ein Kennwort abgefragt wird.</p>
<p>9.2 Entwickeln Sie Verfahren, die die Unterscheidung zwischen Mitarbeitern vor Ort und Besuchern erleichtern, insbesondere in Bereichen, in denen auf Karteninhaberdaten zugegriffen werden kann.</p>	<p>Ohne Ausweissysteme und Türkontrollen können sich unbefugte und böswillige Personen leicht Zugang zu Ihrer Einrichtung verschaffen, um wichtige Systeme und Karteninhaberdaten zu entwenden, zu stören, zu deaktivieren oder zu zerstören. Für eine optimale Kontrolle erwägen Sie, ein Ausweis- oder Magnetkartensystem in und außerhalb der Arbeitsbereiche, in denen Karteninhaberdaten gespeichert werden, zu implementieren.</p> <p>Indem Sie zugelassene Besucher anhand beispielsweise eines Ausweises kennzeichnen, damit sie leicht von den Mitarbeitern vor Ort unterschieden werden können, vermeiden Sie, dass unbefugten Besuchern Zugang auf Bereiche mit Karteninhaberdaten gewährt wird.</p>
<p>9.3 Stellen Sie sicher, dass alle Besucher wie folgt behandelt werden:</p>	<p>Besucherkontrollen sind von zentraler Bedeutung, um das Risiko zu reduzieren, dass sich unbefugte Personen in böser Absicht Zugang zu Ihren Einrichtungen (und unter Umständen auch auf Karteninhaberdaten) verschaffen.</p>
<p>9.3.1 Autorisierung zum Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder verwaltet werden</p>	<p>Besucherkontrollen sind auch wichtig, um sicherzustellen, dass Besucher ausschließlich Zugang zu Bereichen haben, die für diesen Zwecke freigegeben wurden, dass sie als Besucher zu erkennen sind, damit das Personal deren Aktivitäten überwachen kann, und dass ihre Zugangsberechtigung nur für die Länge des genehmigten Besuchs gültig ist.</p>
<p>9.3.2 Es wird ein physisches Token (z. B. ein Ausweis oder Zugangsgerät) mit begrenzter Gültigkeit und das Besucher als solche identifiziert, ausgeteilt.</p>	
<p>9.3.3 Bitte um Rückgabe der physischen Token, wenn die Besucher die Einrichtung verlassen oder die Erlaubnis ausläuft</p>	

Anforderung	Leitfaden
<p>9.4 Überprüfen Sie die Besucheraktivität anhand eines Besucherprotokolls. Dokumentieren Sie den Namen des Besuchers, den Firmennamen und den Namen des Mitarbeiters vor Ort, der dem Besucher Zugang gewährt. Aufbewahren des Besucherprotokolls für die Dauer von mindestens drei Monaten, wenn dies gesetzlich zulässig ist.</p>	<p>Ein Besucherprotokoll, das Mindestinformationen über den Besucher dokumentiert, ist einfach und kostengünstig zu verwalten und hilft im Falle potentieller Untersuchungen von Verletzungen der Datensicherheit bei der Identifizierung physischer Zutritte zu einem Gebäude oder eines Raums sowie möglicher Zugriffe auf Karteninhaberdaten. Erwägen Sie die Implementierung von Protokollen im Eingangsbereich und insbesondere in Bereichen, in denen Karteninhaberdaten aufbewahrt werden.</p>
<p>9.5 Aufbewahren von Sicherungskopien an einem sicheren Ort, vorzugsweise in einer anderen Einrichtung, wie z. B. an einer Alternativ- oder Backup-Stelle oder bei einem kommerziellen Anbieter von Speicherkapazitäten. Überprüfen der Sicherheit dieses Standorts mindestens einmal pro Jahr.</p>	<p>Wenn Sicherungskopien in einer nicht gesicherten Einrichtung gespeichert werden, können die Daten leicht verloren gehen oder in böser Absicht entwendet oder kopiert werden. Prüfen Sie die Möglichkeit, ein professionelles Datensicherungsunternehmen unter Vertrag zu nehmen ODER, in Falle kleinerer Stellen, ein Schließfach in einer Bank zu mieten.</p>
<p>9.6 Stellen Sie die physische Sicherheit aller Medien sicher.</p>	<p>Karteninhaberdaten sind durch unbefugte Zugriffe, unerlaubtes Kopieren oder Scannen gefährdet, wenn sie, während sie sich auf auswechselbaren oder tragbaren Datenträgern befinden, ausgedruckt oder auf einem Schreibtisch unbeaufsichtigt gelassen werden, nicht durch entsprechende Schutzmaßnahmen gesichert sind.</p>
<p>9.7 Führen Sie strikte Kontrollen der internen bzw. externen Verteilung jeglicher Art von Medien mit Karteninhaberdaten, einschließlich Folgender, durch:</p>	<p>Entsprechende Verfahren und Prozesse helfen dabei, Karteninhaberdaten auf Datenträgern zu schützen, wenn sie an interne und/oder externe Nutzer verteilt werden. Ohne solche Verfahren können Daten abhanden kommen oder entwendet und für betrügerische Zwecke eingesetzt werden.</p>
<p>9.7.1 Klassifizieren Sie die Medien, sodass die Sensibilität der Daten bestimmt werden kann.</p>	<p>Es ist wichtig, dass Datenträger so gekennzeichnet werden, dass ihre Klassifizierung leicht erkennbar ist. Datenträger, die nicht als vertraulich gekennzeichnet sind, werden unter Umständen nicht hinreichend geschützt oder können abhanden kommen oder gestohlen werden.</p>
<p>9.7.2 Versenden Sie die Medien über einen sicheren Kurier oder eine andere Liefermethode, die genau verfolgt werden kann.</p>	<p>Datenträger können abhanden kommen oder entwendet werden, wenn sie mit einer nicht nachverfolgbaren Methode wie etwa per Post gesendet werden. Nutzen Sie Services wie sichere Kurierdienste, um Datenträger mit Karteninhaberdaten zu verschicken, damit Sie deren Sendungsverfolgungssysteme einsetzen können, um über den Bestand und den Standort der Sendungen auf dem Laufenden zu bleiben.</p>
<p>9.8 Stellen Sie sicher, dass das Management den Transfer sämtlicher Medien aus einem geschützten Bereich genehmigt (insbesondere, wenn die Medien an einzelne Personen weitergegeben werden).</p>	<p>Karteninhaberdaten, die sichere Bereiche ohne einen durch die Unternehmensleitung genehmigten Prozess verlassen, können dazu führen, dass Daten verloren gehen oder gestohlen werden. Ohne einen verbindlichen Prozess können weder die Standorte von Datenträgern nachverfolgt werden noch gibt es ein Verfahren, um den Bestimmungsort der Daten oder deren Schutzmaßnahmen zu ermitteln.</p>

Anforderung	Leitfaden
<p>9.9 Führen Sie strikte Kontrollen der Aufbewahrung und des Zugriffs auf Medien durch.</p>	<p>Ohne sorgfältige Inventurmethode und Speicherkontrollen können entwendete oder abhanden gekommene Daten auf unbestimmte Zeit unbemerkt bleiben.</p>
<p>9.9.1 Stellen Sie eine ordnungsgemäße Verwaltung von Medieninventurlisten und die Durchführung mindestens einer jährlichen Medieninventur sicher.</p>	<p>Wenn keine Bestandsaufnahme der Datenträger durchgeführt wird, können entwendete oder abhanden gekommene Daten auf unbestimmte Zeit oder womöglich für immer unentdeckt bleiben.</p>
<p>9.10 Vernichten Sie Medien, wenn diese nicht mehr zu geschäftlichen oder juristischen Zwecken benötigt werden, wie folgt:</p>	<p>Wenn Informationen auf Festplatten, tragbaren Speichermedien, CD/DVDs oder Papier vor deren Entsorgung nicht vernichtet werden, sind Angreifer in der Lage, die Informationen von den entsorgten Datenträgern wieder herzustellen und die Datensicherheit zu gefährden. Beispielsweise könnten böswillige Personen die unter dem Namen „Dumpster Diving“ bekannte Technik einsetzen, bei der in Abfallbehältern nach passenden Informationen gesucht wird, um einen Angriff zu starten.</p>
<p>9.10.1 Setzen Sie Aktenvernichter für Papierausdrucke ein, sodass keine Karteninhaberdaten wiederhergestellt werden können.</p>	
<p>9.10.2 Löschen von Karteninhaberdaten auf elektronischen Medien in einer Art und Weise, die eine Wiederherstellung der Daten ausschließt.</p>	

Leitfaden für die Anforderungen 10 und 11: Regelmäßige Überwachung und Testen von Netzwerken

Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten

Protokollierungssysteme und die Möglichkeit, Benutzeraktivitäten nachzuverfolgen, sind wichtige Elemente bei dem Versuch, eine Zugriffsschutzverletzung zu verhindern oder aufzuspüren bzw. deren Auswirkungen so gering wie möglich zu halten. Durch Protokolle in den verschiedenen Umgebungen kann die Ursache von Problemen schnell gefunden werden. Außerdem können Warnmeldungen ausgegeben und Analysen erstellt werden. Die Ursache für eine Sicherheitsverletzung lässt sich ohne Protokolle der Systemaktivität nur sehr schwer oder sogar gar nicht ermitteln.

Anforderung	Leitfaden
<p>10.1 Einrichten eines Prozesses zur Verknüpfung des gesamten Zugriffs auf Systemkomponenten (insbesondere des Zugriffs mit Administratorprivilegien wie Root) mit den einzelnen Benutzern.</p>	<p>Es ist wichtig, über einen Prozess oder ein System zu verfügen, der/das den Benutzerzugriff mit den aufgerufenen Systemkomponenten verknüpft, insbesondere bei Benutzern mit Administratorrechten. Ein solches System generiert Audit-Protokolle und ermöglicht es, verdächtige Aktivitäten bis zu dem Benutzer zurückzuverfolgen, von dem diese ausgehen. Ursachenanalyseteams eines Vorfalls verlassen sich stark auf diese Protokolle zur Einleitung der Untersuchung.</p>
<p>10.2 Implementierung automatisierter Audit-Trails für alle Systemkomponenten zur Rekonstruktion der folgenden Ereignisse:</p>	<p>Indem Audit-Trails über verdächtige Aktivitäten erstellt werden, wird der Systemadministrator aufmerksam gemacht, es werden Daten an weitere Überwachungsmechanismen (wie etwa Eindringlingserfassungsmechanismen) gesendet und es wird ein Verlaufs-Trail für die Überprüfung im Anschluss des Vorfalls geliefert. Die Protokollierung folgender Ereignisse versetzt ein Unternehmen in die Lage, potentiell schädliche Aktivitäten zu erkennen und nachzuverfolgen.</p>
<p>10.2.1 Alle individuellen Zugriffe auf Karteninhaberdaten</p>	<p>Böswillige Individuen könnten Kenntnis über ein Benutzerkonto mit Zugriff auf Systeme in der CDE nehmen oder sie könnten ein neues, nicht genehmigtes Konto einrichten, um sich Zugriff auf die Karteninhaberdaten zu verschaffen. Einträge über alle einzelnen Zugriffe auf Karteninhaberdaten können Aufschluss darauf geben, welche Konten möglicherweise gefährdet oder missbräuchlich eingesetzt worden sind.</p>
<p>10.2.2 Alle von einer Einzelperson mit Root- oder Administratorrechten vorgenommene Aktionen</p>	<p>Konten mit erweiterten Rechten, wie etwa das Administrator- oder Root-Konto, können die Sicherheit und die betriebliche Funktionalität eines Systems ernstlich gefährden. Ohne ein Protokoll über sämtliche ausgeführten Aktivitäten kann ein Unternehmen Probleme, die durch einen Fehler des Administrators oder durch den Missbrauch von Rechten entstanden sind, nicht bis zu der entsprechenden Aktion oder der verantwortlichen Person zurückverfolgen.</p>

Anforderung	Leitfaden
10.2.3 Zugriff auf alle Audit-Trails	Böswillige Personen versuchen nicht selten, Audit-Protokolle zu verfälschen, um ihre Aktionen zu verbergen. Doch mittels Einträgen zu allen Zugriffen kann ein Unternehmen sämtliche Widersprüche oder potentielle Manipulationen der Protokolle bis zu einem einzelnen Konto zurückverfolgen.
10.2.4 Ungültige logische Zugriffsversuche	Angreifer werden häufig mehrere Versuche unternehmen, um auf die gewünschten Systeme zuzugreifen. Mehrere ungültige Anmeldeversuche können ein Hinweis darauf sein, dass ein unbefugter Benutzer versucht, das Kennwort über einen „Brute Force“-Angriff herauszufinden oder zu erraten.
10.2.5 Verwendung von Identifizierungs- und Authentifizierungsmechanismen	Wenn nicht bekannt ist, wer zu dem Zeitpunkt eines Vorfalls angemeldet war, ist es unmöglich, zu erkennen, welche Konten zu diesem Zweck benutzt werden konnten. Außerdem könnten Angreifer versuchen, die Authentifizierungskontrollen zu manipulieren, um sie entweder zu umgehen oder um sich als der Benutzer eines bestimmten gültigen Kontos auszugeben. Aktivitäten wie unter anderem Rechteeskalationen oder Änderungen an den Zugriffsberechtigungen können ein Hinweis auf eine nicht genehmigte Nutzung der Authentifizierungsmechanismen eines Systems sein.
10.2.6 Initialisierung der Audit-Protokolle	Ein beliebtes Ziel von Angreifern, die nicht entdeckt werden möchten, ist es, die Audit-Protokolle vor der Ausführung illegaler Aktivitäten auszuschalten. Die Initialisierung von Audit-Protokollen könnte darauf hinweisen, dass eine Protokollfunktion von einem Benutzer deaktiviert wurde, um seine Aktivitäten zu verbergen.
10.2.7 Erstellen und Löschen von Objekten auf Systemebene	Schädliche Software, wie etwa Malware, erstellt oder ersetzt oft Objekte auf Systemebene auf dem Zielsystem, um eine bestimmte Funktion oder einen Vorgang auf diesem System zu kontrollieren. Die Definition für den Begriff „Objekte auf Systemebene“ finden Sie im <i>Glossar, Abkürzungen und Akronyme zum PCI-DSS und DA-DSS</i> .
10.3 Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: 10.3.1 Benutzeridentifizierung 10.3.2 Ereignistyp 10.3.3 Datum und Uhrzeit 10.3.4 Angabe von Erfolgen oder Fehlschlägen 10.3.5 Ereignisursprung 10.3.6 Identität oder Namen der betroffenen Daten, Systemkomponenten oder Ressourcen	Indem diese Details für die protokollierenden Ereignisse unter 10.2 erfasst werden, kann eine potentielle Gefährdung schnell und mit Informationen zu dem Wer, Was, Wo, Wann und Wie erkannt werden.

Anforderung	Leitfaden
<p>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:</p> <p><i>Hinweis: Eine Zeitsynchronisierungstechnologie ist beispielsweise das Network Time Protocol (NTP).</i></p> <p>10.4.1 Wichtige Systeme zeigen die richtige und gleichbleibende Uhrzeit an</p> <p>10.4.2 Zeitinformationen sind geschützt</p> <p>10.4.3 Zeiteinstellungen werden von branchenüblichen Zeitquellen empfangen</p>	<p>Technologien zur Zeitsynchronisierung werden verwendet, um die Uhren mehrerer Systeme zu synchronisieren. Wenn diese Technologie richtig eingesetzt wird, kann sie die Uhren auf einer Vielzahl von Systemen so genau synchronisieren, dass zwischen ihnen lediglich Unterschiede von Sekundenbruchteilen bestehen. Einige der Probleme, die auftreten können, wenn Uhren nicht angemessen synchronisiert werden, sind unter anderem, dass es schwierig, wenn nicht sogar unmöglich gemacht wird, Protokolldateien unterschiedlicher Systeme miteinander zu vergleichen und eine exakte Abfolge der Sequenzen herzuleiten (ein Punkt von entscheidender Bedeutung bei Ursachenanalysen im Falle eines Verstoßes) und dass kryptographische Protokolle wie z. B. SSH, die von der absoluten Zeit abhängig sind, nicht mehr richtig funktionieren. Für Ursachenanalyseteams nach einem Vorfall ist die Genauigkeit und Einheitlichkeit der Uhrzeit aller Systeme sowie die Uhrzeit der einzelnen Aktivitäten von zentraler Bedeutung, wenn es darum geht, festzustellen, wie die Systeme angegriffen wurden.</p> <p>Um eine einheitliche Uhrzeit zu gewährleisten, sollte es innerhalb einer Stelle idealerweise nur wenige interne (zentrale) Zeitserver geben. Diese Server erhalten direkt UTC (Koordinierten Weltzeit)-Daten von zuverlässigen, bekannten externen Zeitservern über spezielle Funkgeräte, GPS-Satelliten oder andere externe Netzwerkquellen und sie sorgen im Austausch untereinander für eine höchstmögliche Genauigkeit. Die anderen Systeme erhalten die Zeitangaben von diesen Servern.</p> <p>Wenn sich eine böswillige Person Zugriff zum Netzwerk verschafft hat, wird sie wahrscheinlich versuchen, in den Audit-Protokollen die Zeitstempel ihrer Aktionen zu ändern, um ihre Aktivitäten zu verhüllen. Ein Angreifer könnte auch versuchen, direkt die Uhr auf einer Systemkomponente zu ändern, um seine Anwesenheit zu verbergen – z. B. indem zu einem früheren Zeitpunkt die Systemuhr geändert wird. Aus diesen Gründen ist es besonders wichtig, dass die Uhrzeit auf allen Systemen korrekt ist und dass Zeitdaten vor unbefugten Zugriffen und Änderungen geschützt werden. Zu den Zeitdaten zählen die zur Einstellung jeder einzelnen Uhr verwendeten Parameter und Methoden.</p> <p>Ausführlichere Informationen zum NTP, einschließlich Informationen über Zeit, Zeitstandards und Server, finden Sie unter www.ntp.org.</p>
<p>10.5 Schützen Sie Audit-Trails vor Veränderungen.</p>	<p>Oft wird ein Angreifer, der sich Zugriff auf das Netzwerk verschafft hat, versuchen, die Audit-Protokolle zu bearbeiten, um die von ihm ausgeführten Vorgänge zu verbergen. Ohne entsprechende Schutzmaßnahmen für die Audit-Protokolle kann deren Vollständigkeit, Genauigkeit und Integrität nicht garantiert werden und darüber hinaus können die Audit-Protokolle als Überprüfungs-Tool nach einem Vorfall unbrauchbar gemacht werden.</p>

Anforderung	Leitfaden
<p>10.5.1 Beschränken Sie die Anzeige der Audit-Trails auf Personen, die aus geschäftlichen Gründen darauf zugreifen müssen.</p> <p>10.5.2 Schützen Sie Audit-Trail-Dateien vor nicht autorisierten Änderungen.</p> <p>10.5.3 Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.</p> <p>10.5.4 Erstellen Sie Protokolle für nach außen gerichtete Technologien auf einem Protokollserver im internen LAN.</p>	<p>Ein angemessener Schutz der Audit-Protokolle impliziert eine strenge Zugriffskontrolle (beschränken Sie den Zugriff auf Protokolle auf Personen mit einem geschäftlichen Informationsbedarf) und die Nutzung einer internen Trennung (damit die Protokolle schwerer zu finden und abzuändern sind). Durch das Schreiben von Protokollen über externe Technologien wie etwa Drahtlostechnologien, Firewalls, DNS und Mail-Server wird das Risiko für den Verlust oder den Diebstahl der Protokolle reduziert, zumal sie innerhalb des internen Netzwerks wesentlich sicherer sind.</p>
<p>10.5.5 Verwenden von Software zur Dateiintegritätsüberwachung und Änderungserfassung für Protokolle, damit bei der Änderung von bestehenden Protokolldateien ein Alarm ausgelöst wird (nicht jedoch bei der Eingabe neuer Daten).</p>	<p>Überwachungssysteme für die Integrität von Dateien suchen nach Änderungen an wichtigen Dateien und geben eine Warnmeldung aus, sobald derartige Änderungen entdeckt wurden. Um die Integrität von Dateien zu überwachen, überprüft eine Stelle normalerweise Dateien, die nur selten geändert werden und auf einen möglichen Angriff hinweisen, wenn tatsächlich eine Änderung vorgenommen wurde. Bei Protokolldateien (welche sich häufig ändern) sollte beispielsweise überwacht werden, ob eine Protokolldatei gelöscht wurde, plötzlich erheblich größer oder kleiner wird sowie andere Indikatoren dahingehend, dass eine böswillige Person eine Protokolldatei modifiziert hat. Für die Dateiintegritätsüberwachung gibt es sowohl serienmäßig produzierte Tools als auch Open-Source-Tools.</p>
<p>10.6 Überprüfen Sie die Protokolle für alle Systemkomponenten mindestens einmal täglich. Protokollüberprüfungen müssen die Server mit Sicherheitsfunktionen wie Intrusion Detection System (IDS) und Authentication, Authorization and Accounting (AAA)-Protokollserver (z. B. RADIUS) umfassen.</p> <p>Hinweis: Zur Konformität mit Anforderung 10.6 können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.</p>	<p>Viele Verstöße erstrecken sich über Tage oder Monate, bevor sie entdeckt werden. Durch das tägliche Kontrollieren der Protokolle können die Gefährdung und der Zeitraum, über den möglicherweise eine Sicherheitsverletzung stattfindet, reduziert werden. Der Überprüfungsprozess der Protokolle muss nicht manuell durchgeführt werden. Insbesondere für Stellen mit einer Vielzahl an Servern sollte der Einsatz von Protokoll-Harvesting-, -Analyse- und Alarmtools in Erwägung gezogen werden.</p>

Anforderung	Leitfaden
<p>10.7 Bewahren Sie die Audit-Trail-Verlaufsdaten für mindestens ein Jahr auf. Zur Analyse müssen diese Daten für einen Zeitraum von mindestens drei Monaten direkt zur Verfügung stehen (beispielsweise online, archiviert oder aus einer Sicherung wiederherstellbar).</p>	<p>Indem Protokolle mindestens ein Jahr aufbewahrt werden, wird der Tatsache Rechnung getragen, dass es oft eine Zeitlang dauert, bis eine bereits geschehene oder aktuelle Sicherheitsverletzung entdeckt wird. Außerdem ermöglicht der ausführliche Protokollverlauf es Prüfern, zu ermitteln, seit wann die Sicherheitsverletzung besteht und welche/s System/e möglicherweise betroffen ist/sind. Wenn Protokolle über mehrere Monate direkt verfügbar sind, kann eine Stelle schnell einen Verstoß gegen die Datensicherheit erkennen und die möglichen Konsequenzen minimieren. Das Speichern von Sicherungsbändern außerhalb der Stelle kann bewirken, dass die Wiederherstellung von Daten, die Durchführung von Analysen sowie die Identifizierung betroffener Systeme oder Daten wesentlich länger dauert.</p>

Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse

Schwachstellen in der Sicherheit bleiben meist nicht lange unentdeckt. Auch neue Software führt häufig zu zusätzlichen Gefahren. Systemkomponenten, Prozesse und individuelle Software müssen regelmäßig getestet werden, da nur so eine effektive Sicherheit in einer sich ändernden Umgebung erzielt werden kann.

Anforderung	Leitfaden
<p>11.1 Stellen Sie mithilfe von Tests fest, ob Zugriffspunkte für drahtlose Netzwerke vorhanden sind und suchen Sie vierteljährlich nach eventuellen nicht autorisierten Zugriffspunkten für drahtlose Netzwerke.</p> <p>Hinweis: Methoden, die sich hierfür anbieten, sind unter anderen Scans zur Feststellung drahtloser Netzwerke, physische/logische Überprüfungen der Systemkomponenten und Infrastruktur, Network Access Control (NAC) oder Wireless IDS/IPS-Systeme.</p> <p>Welche Methode auch immer verwendet wird, sie muss ausreichend sein, um jegliche nicht autorisierte Geräte zu erkennen und zu identifizieren.</p>	<p>Die Implementierung und/oder Ausnutzung von Drahtlostechnologie in einem Netzwerk ist eine altbewährte Methode für böswillige Individuen, um sich Zugriff zu einem Netzwerk und zu Karteninhaberdaten zu verschaffen. Wenn ein drahtloses Gerät oder Netzwerk ohne das Wissen eines Unternehmens installiert wird, könnte sich ein Angreifer mühelos und „heimlich“ Zugang zum Netzwerk verschaffen.</p> <p>Nicht zugelassene Drahtlosgeräte können versteckt in oder angeschlossen an einem Computer oder einer anderen Systemkomponente sein oder direkt an einen Netzwerk-Port oder ein Netzwerkgerät, wie etwa einen Schalter oder einen Router, angeschlossen werden. Diese Geräte könnten als nicht zugelassener Zugriffspunkt in die Umgebung fungieren.</p> <p>Aufgrund der Einfachheit, mit der ein drahtloser Zugriffspunkt an ein Netzwerk angeschlossen werden kann, dessen extrem komplizierter Erkennung und dem hohen Risiko durch nicht genehmigte Drahtlosgeräte, müssen diese Prozesse selbst dann ausgeführt werden, wenn eine Richtlinie implementiert ist, die die Nutzung von Drahtlostechnologien komplett untersagt.</p> <p>Die Größe und Komplexität einer bestimmten Umgebung geben Hinweise auf die erforderlichen Tools und Prozesse, die eingesetzt werden müssen, um ausreichend Sicherheit dahingehend zu bieten, dass in der Umgebung kein unbefugter drahtloser Zugriffspunkt installiert wurde.</p> <p>Beispiel: Im Falle eines einzelnen Verkaufskiosk in einem Einkaufszentrum, bei dem sich alle Kommunikationskomponenten innerhalb eines manipulationssicheren und sicherheitsverpackten Gehäuses befinden, mag eine physische Kontrolle des Kiosks ausreichend sein, um sicherzustellen, dass keine schädlichen drahtlosen Zugriffspunkte installiert oder angeschlossen wurden. Dahingegen ist es in einer Umgebung mit mehreren Knoten (z. B. in einem großen Einzelhandelsgeschäft, einem Callcenter, einem Serverraum oder Datacenter) aufgrund der Anzahl der Systemkomponenten und Netzwerkpunkten schwierig, eine ausführliche physische Überprüfung durchzuführen, um festzustellen, ob an ihnen schädliche drahtlose Zugriffspunkte installiert oder angeschlossen wurden. In diesem Fall bietet es sich an, mehrere Methoden miteinander zu kombinieren, um die Anforderung zu erfüllen, beispielsweise indem physische Systemüberprüfungen durchgeführt und mit den Ergebnissen eines Analysators für drahtlose Netzwerke kombiniert werden.</p> <p>Network Access Control (NAC) Lösungen eignen sich für die Geräteauthentifizierung und Konfigurationsverwaltung, um zu verhindern, dass unbefugte Systeme eine Verbindung zum Netzwerk herstellen oder nicht zugelassene Geräte an autorisierte Systeme im Netzwerk angeschlossen werden.</p> <p>Ein Unternehmen sollte im Rahmen seines Vorfalldaktionsplans über dokumentierte Verfahren verfügen, die für den Fall, dass ein unbefugter drahtloser Zugriffspunkt entdeckt wird, befolgt werden</p>

Anforderung	Leitfaden
	<p>müssen. Ein Wireless-IDS/IPS-System sollte so konfiguriert werden, dass es automatisch eine Warnmeldung ausgibt, allerdings sollte der Plan auch Reaktionsverfahren für den Fall dokumentieren, dass ein nicht zugelassenes Gerät während eines manuellen drahtlosen Scans entdeckt wird.</p>
<p>11.2 Ausführen interner und externer Netzwerkanfälligkeitsscans mindestens vierteljährlich und nach jeder signifikanten Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Änderung der Firewall-Regeln, Produkt-Upgrades).</p> <p>Hinweis: Es ist für die anfängliche PCI DSS-Konformität nicht erforderlich, dass vier bestandene vierteljährliche Scans abgeschlossen sein müssen, wenn der Prüfer überprüft, dass 1) das letzte Scan-Ergebnis ein positives Ergebnis war, 2) die Einheit über dokumentierte Richtlinien und Verfahren verfügt, die eine Fortsetzung der vierteljährlichen Scans erfordern, und 3) alle im ersten Scan festgestellten Anfälligkeiten korrigiert wurden, wie ein erneuter Scan beweist. Für die Folgejahre nach der ersten PCI-DSS-Prüfung müssen vier bestandene vierteljährliche Scans vorliegen.</p>	<p>Eine Schwachstellenprüfung ist ein automatisiertes Tool, das auf externen und internen Netzwerkgeräten und -servern ausgeführt wird und dazu dient, potentielle Schwachstellen in Netzwerken aufzudecken, die von böswilligen Personen erkannt und ausgenutzt werden könnten. Sobald diese Schwachstellen erkannt wurden, werden sie von der betreffenden Stelle behoben. Anschließend wird der Scan erneut ausgeführt, um sicherzustellen, dass die Sicherheitslücken auch tatsächlich geschlossen wurden.</p> <p>Zum Zeitpunkt der anfänglichen PCI-DSS-Beurteilung eines Unternehmens ist es durchaus möglich, dass die vier vierteljährlichen Scans noch nicht ausgeführt wurden. Wenn das letzte Scanergebnis die Kriterien erfüllt und bestanden hat und Richtlinien sowie Verfahren für spätere vierteljährliche Scans implementiert wurden, wird diese Anforderung als erfüllt betrachtet. Wenn diese Kriterien erfüllt sind, ist es bei dieser Anforderung nicht erforderlich, die Bewertung „Implementiert“ zu verschieben, nur weil die vier vierteljährlichen Scans nicht durchgeführt wurden.</p>

Anforderung	Leitfaden
<p>11.2.1 Führen Sie vierteljährlich interne Schwachstellenprüfungen durch.</p>	<p>Ein eindeutiges Verfahren zur Erkennung von Schwachstellen in internen Systemen innerhalb der CDE setzt voraus, dass vierteljährliche Scans durchgeführt werden. Die rechtzeitige Erkennung und Korrektur von Schwachstellen reduziert die Wahrscheinlichkeit, dass eine solche Sicherheitslücke ausgenutzt wird und eine Systemkomponente oder Karteninhaberdaten gefährdet werden.</p> <p>Jenen Schwachstellen, die ein besonders hohes Risiko für die Umgebung darstellen (z. B. Schwachstellen, die laut Anforderung 6.2 als „schwerwiegend“ klassifiziert wurden), sollte höchste Priorität eingeräumt werden.</p> <p>Da sich interne Netzwerke im Laufe des Jahres kontinuierlich verändern, ist es möglich, dass eine Stelle nicht durchgehend volle interne Anfälligkeitsscans durchführt. Das Ziel ist es, dass eine Stelle ein solides Anfälligkeits-Managementprogramm implementiert, um bekannte Schwachstellen in einem angemessenen Zeitraum zu beheben. Zumindest als „schwerwiegend“ eingestufte Schwachstellen müssen rechtzeitig angesprochen werden.</p> <p>Interne Anfälligkeits-Scans können von geschultem, internen Personal durchgeführt werden, das möglichst nicht direkt für die zu scannende/n Systemkomponente/n zuständig ist (z. B. sollte ein Firewall-Administrator nicht damit beauftragt werden, die Firewall zu scannen). Darüber hinaus bietet sich einer Einheit die Option, interne Anfälligkeits-Scans von einem vom PCI-SSC zugelassenen Scanninganbieter, einem QSA oder einem Unternehmen, das auf Anfälligkeits-Scans spezialisiert ist, durchführen zu lassen.</p>
<p>11.2.2 Führen Sie vierteljährlich externe Schwachstellenprüfungen über einen Scanninganbieter (ASV) durch, der vom Payment Card Industry Security Standards Council (PCI-SSC) zugelassen wurde.</p> <p>Hinweis: <i>Vierteljährliche externe Schwachstellenprüfungen müssen von einem Scanninganbieter (ASV) durchgeführt werden, der vom Payment Card Industry Security Standards Council (PCI-SSC) zugelassen wurde. Nach Netzwerkänderungen durchgeführte Scans können vom internen Personal ausgeführt werden.</i></p>	<p>Da externe Netzwerke eher durch Angriffe gefährdet sind, muss vierteljährlich ein externer Anfälligkeits-Scan von einem vom PCI-SSC zugelassenen Scanninganbieter (ASV) durchgeführt werden.</p> <p>ASV müssen die im PCI-SSC-Programmführer für zugelassene Scanninganbieter beschriebenen Scan- und Berichtskriterien erfüllen.</p>
<p>11.2.3 Führen Sie nach jeder wesentlichen Änderung interne und externe Scans durch.</p> <p>Hinweis: <i>Nach Änderungen durchgeführte Scans können vom internen Personal ausgeführt werden.</i></p>	<p>Durch das Scannen einer Umgebung nach der Durchführung signifikanter Änderungen wird gewährleistet, dass die Änderungen vollständig abgeschlossen wurden und die Sicherheit der Umgebung durch die Änderungen nicht herabgesetzt wurde. Nach einer Änderung ist es nicht zwingend notwendig, die ganze Umgebung zu scannen. Es müssen nur die von der Änderung betroffenen Systemkomponenten gescannt werden.</p>

Anforderung	Leitfaden
<p>11.3 Durchführen externer und interner Penetrationstests mindestens einmal im Jahr und nach jeder signifikanten Infrastruktur- oder Anwendungsaktualisierung oder -änderung (z. B. Betriebssystem-Upgrade, neues Teilnetzwerk oder neuer Webserver in der Umgebung). Diese Penetrationstests müssen Folgendes enthalten:</p> <p>11.3.1 Penetrationstests auf Netzwerkebene</p> <p>11.3.2 Penetrationstests auf Anwendungsebene</p>	<p>Der Zweck eines Penetrationstests ist es, eine reale Angriffssituation zu simulieren, um zu ermitteln, wie weit ein Angreifer in der Lage wäre, in das System einzudringen. Hierdurch erhält die jeweilige Stelle ein tieferes Verständnis des potentiellen Risikos, dem sie ausgesetzt ist und ist der Lage, eine entsprechende Strategie zu entwickeln, um sich vor Angriffen zu schützen.</p> <p>Ein Penetrationstest unterscheidet sich insofern von einem Anfälligkeits-Scan, als der Penetrationstest ein aktiver Prozess ist, bei dem unter anderem auch bekannte Schwachstellen ausgetestet werden. Oft ist die Durchführung eines Anfälligkeits-Scans der erste, jedoch nicht der einzige Schritt eines Penetrationstesters, um mögliche Angriffspläne zu durchkreuzen. Selbst wenn bei einem Anfälligkeits-Scan bekannte Schwachstellen nicht erkannt werden, erhält der Penetrationstester zumeist hinreichend Informationen über das System, um mögliche Sicherheitslücken zu erkennen.</p> <p>Penetrationstests sind überwiegend manuelle Prozesse. Obwohl auch einige automatisierte Tools verwendet werden können, muss der Prüfer dennoch seine Systemkenntnisse einsetzen, um in eine Umgebung einzudringen. Oft wird ein Prüfer mehrere Arten von Exploits miteinander verbinden, um verschiedene Sicherheitsschichten zu durchbrechen. Wenn ein Prüfer beispielsweise einen Weg findet, sich Zugriff auf einen Anwendungsserver zu verschaffen, wird er diesen gefährdeten Server als Ausgangspunkt für einen neuen Angriff abhängig von den Ressourcen, zu denen der Server Zugriff hat, nutzen. Mithilfe dieser Methode ist ein Prüfer in der Lage, die von einem Angreifer genutzten Methoden zu simulieren und somit in der Umgebung jegliche Bereiche mit Schwachstellen zu identifizieren, die behoben werden müssen.</p>

Anforderung	Leitfaden
<p>11.4 Nutzung von Systemen zur Erkennung und/oder Verhinderung von Angriffsversuchen zur Überwachung des kompletten Datenverkehrs in der Umgebung, in der sich Karteninhaberdaten befinden, sowie kritischer Punkte innerhalb der Karteninhaberdaten-Umgebung und Alarmierung des Personals bei mutmaßlichen Sicherheitsverletzungen.</p> <p>Ständige Aktualisierung der Angriffserfassungs- und -vorbeugungssysteme, Ausgangseinstellungen und Signaturen.</p>	<p>Eindringlingserkennungs- und/oder Eindringlingspräventionssysteme (IDS/IPS) vergleichen den vom Netzwerk stammenden Datenverkehr mit bekannten Signaturen und/oder Verhalten Tausender von Angriffstypen (Hacker-Tools, Trojaner und andere Malware) und schicken Warnmeldungen und/oder unterbinden den Versuch sofort. Ohne einen vorausschauenden Ansatz zur Erkennung unbefugter Aktivitäten mithilfe dieser Tools können Angriffe auf (oder Missbrauch von) Computerressourcen, während sie sich zutragen, unentdeckt bleiben. Die von diesen Systemen ausgehenden Sicherheitsalarmmeldungen sollten überwacht werden, damit Eindringlinge abgewehrt werden können.</p> <p>IDS/IPS-Geräte sollten so implementiert werden, dass sie eingehenden und ausgehenden Datenverkehr im Bereich der CDE sowie an kritischen Punkten innerhalb der CDE überwachen. Zu den kritischen Punkten innerhalb der CDE können unter anderem entsprechend der Umgebung der betreffenden Stelle sowie den Dokumentationen aus ihrer Risikobewertung Datenbankserver mit Karteninhaberdaten, Speicherplätze mit kryptographischen Schlüsseln, verarbeitende Netzwerke oder andere empfindliche Systemkomponenten zählen.</p> <p>Obwohl viele IDS-IPS-Geräte heutzutage in der Lage sind, mehrere Punkte in der CDE mit nur einem Gerät zu überwachen, ist es dennoch wichtig, das erhöhte Risiko, das durch einen eventuellen Ausfall dieses Geräts entstehen würde, nicht außer Acht zu lassen. Deshalb ist es wichtig, in der IDS/IPS-Infrastruktur entsprechende Redundanzen anzuordnen.</p> <p>Es gibt Tausende von Angriffstypen, und mit jedem Tag werden weitere entdeckt. Veraltete Signaturen und Scanning-Systeme auf IDS-IPS-Geräten sind nicht in der Lage, neue Schwachstellen zu erkennen, wodurch es zu unerkannten Sicherheitsverletzungen kommen könnte. Anbieter dieser Produkte liefern häufig, zumeist täglich Updates, die regelmäßig überprüft und angewendet werden sollten.</p>

Anforderung	Leitfaden
<p>11.5 Setzen Sie Tools zur Überwachung der Dateiintegrität ein, die das Personal über nicht autorisierte Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien alarmieren, und konfigurieren Sie die Software so, dass sie mindestens wöchentlich Vergleiche wichtiger Dateien herstellt.</p> <p><i>Hinweis: Für die Dateiintegritätsüberwachung 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. Produkte zur Dateiintegritätsüberwachung sind in der Regel mit wichtigen Dateien für das jeweilige Betriebssystem vorkonfiguriert. Andere wichtige Dateien wie solche für benutzerdefinierte Anwendungen müssen von der jeweiligen Stelle (Händler oder Dienstleister) beurteilt und definiert werden.</i></p>	<p>Überwachungs-Tools für die Integrität von Dateien (Englisch: File-Integrity Monitoring, FIM) suchen nach Änderungen an wichtigen Dateien und geben eine Warnmeldung aus, sobald derartige Änderungen entdeckt wurden. Für die Dateiintegritätsüberwachung gibt es sowohl serienmäßig produzierte Tools als auch Open-Source-Tools. Falls diese nicht korrekt implementiert sind und die Ergebnisse des FIM nicht überprüft werden, könnte ein Angreifer die Inhalte der Konfigurationsdateien, Betriebssystemprogramme oder ausführbare Anwendungsdateien ändern. Derartige unbefugte Änderungen könnten, falls sie unentdeckt bleiben, vorhandene Sicherheitskontrollen unwirksam machen und/oder dazu führen, dass Karteninhaberdaten ohne merkbare Auswirkungen auf die normale Verarbeitung gestohlen werden.</p>

Leitfaden für die Anforderung 12: Befolgung einer Informationssicherheits-Richtlinie

Anforderung 12: Pflegen Sie eine Informationssicherheits-Richtlinie für das gesamte Personal

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

Anforderung	Leitfaden
<p>12.1 Festlegen, Veröffentlichen, Verwalten und Verbreiten einer Sicherheitsrichtlinie mit den folgenden Zielen:</p> <p>12.1.1 Sie umfasst sämtliche PCI-DSS-Anforderungen.</p>	<p>Die Informationssicherheitsrichtlinie eines Unternehmens stellt die Grundlage zur Implementierung von Sicherheitsmaßnahmen zum Schutz wertvoller Unternehmensressourcen dar. Eine strenge Sicherheitsrichtlinie gibt den Takt für das gesamte Unternehmen vor und dient dem Personal als Richtschnur dazu, was von ihm verlangt wird. Alle Mitarbeiter sollten sich darüber im Klaren sein, dass Daten Gefahren ausgesetzt sind und dass sie für deren Schutz verantwortlich sind.</p>
<p>12.1.2 Sie umfasst einen jährlichen Prozess zur Ermittlung von Bedrohungen und Anfälligkeiten, der zu einer offiziellen Risikobeurteilung führt. (Beispiele von Risikobewertungsmethoden sind unter anderen OCTAVE, ISO 27005 und NIST SP 800-30.)</p>	<p>Eine Risikobewertung ermöglicht es einem Unternehmen, Bedrohungen und entsprechende Schwachstellen zu erkennen, welche den Betrieb des Unternehmens beeinträchtigen könnten. So können dann effektiv entsprechende Ressourcen eingesetzt werden, um Kontrollen zu implementieren, die die Wahrscheinlichkeit und/oder die möglichen Auswirkungen eines Angriffs minimieren.</p> <p>Jährliche Risikobewertungen ermöglichen es dem Unternehmen, stets auf dem neuesten Stand bezüglich organisatorischen Veränderungen sowie neuen Bedrohungen, Trends und Technologien zu bleiben.</p>
<p>12.1.3 Sie umfasst eine mindestens jährliche Überprüfung sowie Aktualisierungen bei Umgebungsänderungen.</p>	<p>Im Laufe eines Jahres erscheinen immer wieder neue Sicherheitsrisiken und Schutzmaßnahmen. Ohne regelmäßige Updates der Sicherheitsrichtlinie, um neue wichtige Änderungen aufzunehmen, können neue Schutzmaßnahmen zur Bekämpfung dieser Bedrohungen nicht berücksichtigt werden.</p>
<p>12.2 Entwickeln von Routineverfahren für die Betriebssicherheit, die den Anforderungen in dieser Spezifikation entsprechen (z. B. Benutzerkonto-Wartungsverfahren und Protokollüberprüfungsverfahren).</p>	<p>Tägliche Betriebssicherheitsverfahren dienen als Leitfaden für Mitarbeiter bei ihren täglichen Systemverwaltungs- und Wartungsaufgaben. Nicht dokumentierte Betriebssicherheitsverfahren führen dazu, dass sich Mitarbeiter des Gesamtumfangs ihrer Aufgaben nicht bewusst sind, diese Verfahren von neuen Mitarbeitern nicht reproduziert werden können und potentielle Lücken in den Verfahren es einem böswilligen Individuum ermöglichen, sich Zugriff auf wichtige Systeme und Ressourcen zu verschaffen.</p>

Anforderung	Leitfaden
<p>12.3 Entwickeln Sie Verwendungsrichtlinien für wichtige Technologien (z. B. Remotезugriffs- und Wireless-Technologien, elektronische Wechselmedien, Laptops, Tablets, PDAs, E-Mail-Programme und Internet), und beschreiben Sie die korrekte Verwendung dieser Technologien. Die Verwendungsrichtlinien umfassen folgende Punkte:</p>	<p>Verwendungsrichtlinien für das Personal können entweder die Nutzung bestimmter Geräte oder Technologien untersagen, sollte dies von der Unternehmensrichtlinie vorgeschrieben sein, oder das Personal über die korrekte Nutzung und Implementierung informieren. Sind keine Verwendungsrichtlinien implementiert, könnte das Personal die Technologien entgegen der Unternehmensrichtlinie nutzen und Angreifern den Weg zu wichtigen Systemen und Karteninhaberdaten freimachen. Beispielsweise könnten unwissentlich Drahtlosnetzwerke ohne jegliche Sicherheitsvorkehrungen eingerichtet werden. Um sicherzustellen, dass die Unternehmensstandards befolgt und ausschließlich zugelassene Technologien implementiert werden, ziehen Sie in Erwägung, ausschließlich der IT-Abteilung eine Befugnis für die Implementierung zu erteilen und ungeschultem/allgemeinem Personal zu untersagen, diese Technologien zu installieren.</p>
<p>12.3.1 Ausdrückliche Genehmigung durch autorisierte Parteien</p>	<p>Wird keine entsprechende Genehmigung für Implementierungen vorausgesetzt, können einzelne Personen in gutem Glauben eine Lösung für einen vermuteten Unternehmensbedarf installieren, jedoch gleichzeitig eine nicht unerhebliche Sicherheitslücke öffnen, die wichtige Systeme und Daten böswilligen Personen aussetzt.</p>
<p>12.3.2 Authentifizierung zur Verwendung der Technologie</p>	<p>Wenn Technologien ohne eine entsprechende Authentifizierung implementiert werden (Benutzernamen und Kennwörter, Tokens, VPNs, usw.), können Angreifer diese ungeschützte Technologie mühelos ausnutzen, um auf wichtige Systeme und Karteninhaberdaten zuzugreifen.</p>
<p>12.3.3 Liste aller betroffenen Geräte und aller Mitarbeiter mit Zugriff</p>	<p>Böswillige Personen können physische Sicherheitsvorrichtungen durchbrechen und ihre eigenen Geräte an das Netzwerk anschließen, um sich somit ein Hintertürchen offen zu halten. Auch Mitarbeiter können sich unter Umständen über die Verfahren hinwegsetzen und Geräte installieren. Durch mithilfe einer punktgenauen Bestandsaufnahme und Kennzeichnung der Geräte können nicht zugelassene Installationen schnell entdeckt werden. Ziehen Sie die Festlegung einer offiziellen Namenskonvention für Geräte in Betracht und kennzeichnen und protokollieren Sie alle Geräte im Sinne der eingeführten Bestandskontrollen. Eine logische Kennzeichnung mit Informationen, wie etwa Codes, die Aufschluss auf den Besitzer, dessen Kontaktinformationen und den Zweck des Geräts geben, könnten als Alternative in Erwägung gezogen werden.</p>
<p>12.3.4 Etikettierung von Geräten, um Eigentümer, Kontaktinformationen und Zweck zu bestimmen</p>	
<p>12.3.5 Akzeptable Verwendung der Technologie</p>	<p>Indem die zulässige betriebliche Nutzung und der Standort der vom Unternehmen genehmigten Geräte und Technologien definiert werden, ist das Unternehmen besser vorbereitet, um Lücken in Konfigurationen und Betriebskontrollen zu bewältigen und zu kontrollieren und um sicherzustellen, dass Angreifern keine Hintertürchen geöffnet werden, um sich Zugriff auf wichtige Systeme und Karteninhaberdaten zu verschaffen.</p>
<p>12.3.6 Akzeptable Netzwerkkarte für die Technologien</p>	
<p>12.3.7 Liste der vom Unternehmen zugelassenen Produkte</p>	
<p>12.3.8 Automatisches Trennen von Remotезugriff-Sitzungen</p>	<p>Remotезugriff-Technologien stellen nicht selten Hintertürchen zu wichtigen</p>

Anforderung	Leitfaden
<p>nach einer bestimmten Zeit der Inaktivität</p> <p>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</p>	<p>Ressourcen und Karteninhaberdaten dar. Wenn Remotezugriff-Technologien jedoch ausgeschaltet werden, wenn sie nicht in Verwendung sind (z. B. jene, die Ihr POS-Anbieter, andere Anbieter oder Geschäftspartner verwenden, um Ihre Systeme zu warten), können die Zugriffe auf die Netzwerke und die entsprechenden Risiken minimiert werden. Ziehen Sie in Betracht, Kontrollen einzusetzen, die Geräte nach einer Inaktivitätszeit von 15 Minuten automatisch abschalten. Für weitere Informationen zu diesem Thema lesen Sie die Anforderung 8.5.6.</p>
<p>12.3.10 Untersagen Sie Mitarbeitern, die auf Karteninhaberdaten per Remotezugriff zugreifen, Karteninhaberdaten auf lokale Festplatten und elektronische Wechselmedien zu kopieren, zu verschieben oder zu speichern, sofern nicht ausdrücklich aufgrund bekannter Geschäftsbedürfnisse gestattet.</p>	<p>Um sicherzustellen, dass sich alle Mitarbeiter ihrer Pflicht dahingehend, keine Karteninhaberdaten auf ihren lokalen PCs oder andere Datenträgern zu speichern oder zu kopieren, bewusst sind, sollte Ihre Richtlinie ein derartiges Vorgehen strikt untersagen, ausgenommen für Personal, das hierfür eine ausdrückliche Genehmigung besitzt. Diese autorisierten Mitarbeiter sind ihrerseits dafür verantwortlich, zu gewährleisten, dass die in ihrem Besitz befindlichen Karteninhaberdaten im Sinne aller PCI-DSS-Anforderungen gehandhabt werden, da dieses Personal nun als Teil der Karteninhaberdaten-Umgebung des Unternehmens betrachtet wird.</p>
<p>12.4 Stellen Sie sicher, dass die Sicherheitsrichtlinien und Verfahren eine klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter beinhalten</p>	<p>Wenn keine klar definierten Sicherheitsrollen und -verantwortlichkeiten zugewiesen werden, könnte die Folge ein widersprüchliches Zusammenwirken mit der IT-Sicherheitsabteilung sein und daraus anschließend unsichere Implementierungen von Technologien oder die Nutzung veralteter oder nicht gesicherter Technologien entstehen.</p>
<p>12.5 Weisen Sie einer Einzelperson oder einem Team folgende Managementverantwortungsbereiche in puncto Informationssicherheit zu:</p> <p>12.5.1 Festlegen, Dokumentieren und Verteilen von Sicherheitsrichtlinien und -verfahren.</p> <p>12.5.2 Überwachen und analysieren Sie Sicherheitsalarme und -informationen und verteilen Sie sie an das entsprechende Personal.</p> <p>12.5.3 Festlegen, Dokumentieren und Weitergeben von Reaktions- und Eskalationsverfahren für Sicherheitsvorfälle, die eine rechtzeitige und effektive Vorgehensweise in allen Situationen gewährleisten.</p> <p>12.5.4 Verwalten Sie Benutzerkonten, einschließlich Ergänzungen, Löschungen und Änderungen</p> <p>12.5.5 Überwachen und kontrollieren Sie den gesamten</p>	<p>Jede Person oder jedes Team, das für das Management der Informationssicherheit zuständig ist, sollte seine Verantwortlichkeiten und Aufgaben durch das Hinzuziehen einer spezifischen Richtlinie kennen. Ohne eine derartige Verpflichtung können Verfahrenslücken den Zugriff auf wichtige Ressourcen oder Karteninhaberdaten ermöglichen.</p>

Anforderung	Leitfaden
<p>Datenzugriff.</p>	
<p>12.6 Implementieren Sie ein offizielles Sicherheitsbewusstseinsprogramm, durch das allen Mitarbeitern die Bedeutung der Sicherheit der Karteninhaberdaten vermittelt wird.</p>	<p>Wenn das Personal nicht bezüglich seiner Verantwortlichkeiten in punkto Sicherheit und implementierte Sicherheitsvorkehrungen und -verfahren geschult wird, kann es dem Unternehmen durch unterlaufene Fehler oder vorsätzliche Handlungen schaden.</p>
<p>12.6.1 Führen Sie Mitarbeiterschulungen bei der Einstellung und danach mindestens einmal im Jahr durch.</p> <p><i>Hinweis: Die Methoden sind abhängig von der Funktion der Mitarbeiter und deren Zugriffsrechte auf Karteninhaberdaten.</i></p>	<p>Wenn das Sicherheitsbewusstseinsprogramm nicht von regelmäßigen Auffrischkursen begleitet wird, geraten wichtige Sicherheitsprozesse und -verfahren in Vergessenheit oder werden umgangen und zentrale Ressourcen und Karteninhaberdaten werden Gefahren ausgesetzt. Die Ausrichtung und Vollständigkeit der ersten Schulung und des Auffrischkurses ist abhängig von der Funktion der Mitarbeiter und sollte den Bedürfnissen der Zielgruppe angepasst werden. Beispielsweise sollten Schulungen für Datenbankadministratoren auf spezifische technische Kontrollen und Prozesse ausgerichtet werden, während Kurse für Kassierer den Schwerpunkt auf sichere Transaktionsverfahren setzen könnten</p> <p>Ziehen Sie in Erwägung, kontinuierliche Aktualisierungen der Sensibilisierungsprogramme einzurichten, um die Mitarbeiter bezüglich aktueller Richtlinien und Verfahren stets auf dem neuesten Stand zu halten. Auch die Form der Schulungen kann je nach Zielgruppe und Kurs variieren. Zum Beispiel können anfängliche und jährliche Schulungen als formelle praktische Kurse oder computerbasierte Ausbildungsschulungen durchgeführt werden und regelmäßige Aktualisierungen per E-Mail, Poster oder Newsletter usw. bekannt gegeben werden.</p>
<p>12.6.2 Fordern Sie von den Mitarbeitern mindestens einmal pro Jahr eine schriftliche Bestätigung dazu, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens gelesen und verstanden haben.</p>	<p>Auch die Aufforderung an das Personal, eine schriftliche oder elektronische Bestätigung abzugeben, hilft dabei, sicherzustellen, dass die Sicherheitsrichtlinien und -verfahren gelesen und verstanden wurden und dass in der Vergangenheit sowie in Zukunft alles daran gesetzt wurde bzw. wird, diese Richtlinien</p>

Anforderung	Leitfaden
<p>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.)</p> <p><i>Hinweis: Für potentielle neue Mitarbeiter wie z. B. Kassierer, die nur Zugriff auf jeweils eine Kartenummer gleichzeitig haben, wenn eine Transaktion durchgeführt wird, ist diese Anforderung lediglich eine Empfehlung.</i></p>	<p>einzuhalten.</p> <p>Indem gründliche Hintergrundrecherchen über Mitarbeiter durchgeführt werden, die möglicherweise angestellt werden sollen und später Zugriff auf Karteninhaberdaten hätten, wird das Risiko der unerlaubten Nutzung von PANs und anderen Karteninhaberdaten durch Individuen mit fragwürdigem oder gar kriminellern Hintergrund minimiert. Es wird erwartet, dass ein Unternehmen über eine Richtlinie und Prozesse für Hintergrundrecherchen verfügt, einschließlich eigenen Entscheidungsprozessen darüber, welche Ergebnisse derartiger Überprüfungen die Entscheidung einer möglichen Anstellung beeinflussen (und welche Auswirkungen diese Ergebnisse haben).</p> <p>Die Genauigkeit dieser Hintergrundrecherchen sollte aus Effizienzgründen der jeweiligen Position entsprechen. Beispielsweise erfordern Positionen mit höherer Verantwortung oder die Administratorzugriff auf wichtige Daten oder Systeme haben, eine gründlichere Hintergrundrecherche als Positionen mit weniger Verantwortung oder Zugriffsrechten. In diesem Prozess sollten auch interne Versetzungen berücksichtigt werden, das heißt, dass Mitarbeiter in weniger risikobehafteten Positionen und die sich bereits einer ausführlichen Hintergrundrecherche unterzogen haben, auf Positionen mit einem größeren Verantwortungsbereich und erweiterten Zugriffsrechten befördert oder versetzt werden.</p>
<p>12.8 Wenn Karteninhaberdaten gemeinsam mit Dienstanbietern genutzt werden, müssen Richtlinien und Verfahren zur Verwaltung von Dienstanbietern umgesetzt und eingehalten werden. Hierunter fallen die folgenden Punkte:</p>	<p>Wenn ein Händler oder Dienstanbieter Karteninhaberdaten gemeinsam mit einem anderen Dienstanbieter verwendet, gelten bestimmte Anforderungen, um den dauerhaften Schutz dieser Daten durch diese Dienstanbieter zu gewährleisten.</p>
<p>12.8.1 Stellen Sie eine Liste der Dienstanbieter auf.</p>	<p>Behalten Sie alle Dienstanbieter im Auge, bei denen ein potentielles Risiko nicht nur innerhalb des Unternehmens erkannt wurde.</p>
<p>12.8.2 Unterhalten Sie eine schriftliche Vereinbarung mit einer Bestätigung dazu, dass der Dienstanbieter für die Sicherheit der Karteninhaberdaten in seinem Besitz haftet.</p>	<p>Diese Bestätigung der Dienstanbieter unterstreicht deren Engagement, die Karteninhaberdaten, die sie von ihren Kunden anvertraut bekommen, entsprechend zu schützen, und nimmt sie für die Einhaltung dieser Vereinbarung in die Pflicht.</p>
<p>12.8.3 Festlegung eines eindeutigen Verfahrens für die Inanspruchnahme von Dienstanbietern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht.</p>	<p>Das Verfahren gewährleistet, dass jegliche Einbindungen von Serviceanbietern intern vom Unternehmen geprüft werden, dazu zählt auch eine Risikoanalyse vor der Vereinbarung einer formalen Beziehung zu dem Serviceanbieter.</p>
<p>12.8.4 Richten Sie ein Programm zur mindestens einmal jährlichen Überwachung der Dienstanbieter-Konformität mit dem PCI-Datensicherheitsstandard ein.</p>	<p>Wenn Sie den PCI-DSS-Compliance-Status Ihres Serviceanbieters kennen, können Sie sich sicher sein, dass er denselben Anforderungen wie auch Ihr Unternehmen unterliegt.</p> <p>Sollte der Serviceanbieter verschiedene Dienstleistungen anbieten, gilt diese Anforderung nur für jene Dienste, die der Kunde tatsächlich in Anspruch</p>

Anforderung	Leitfaden
	<p>genommen hat und die in den Umfang der PCI-DSS-Bewertung des Kunden fallen. Wenn ein Anbieter beispielsweise Firewall/IDS- und IPS-Dienste anbietet, würde ein Kunde, der nur den Firewall/IDS-Dienst in Anspruch genommen hat, auch nur diesen Service in seine PCI-DSS-Bewertung aufnehmen.</p>
<p>12.9 Implementieren Sie einen Vorfalldaktionsplan. Bereiten Sie sich auf eine sofortige Reaktion auf Sicherheitsverletzungen im System vor.</p>	<p>Ohne einen ausführlichen Vorfalldaktionsplan, der an die verantwortlichen Parteien weitergeleitet, gelesen und verstanden wurde, können Verwirrung und eine fehlende einheitliche Reaktion dem Unternehmen zusätzliche Ausfallszeiten, unnötige Medienpräsenz sowie neue rechtliche Haftungen bescheren.</p>
<p>12.9.1 Erstellen Sie den Vorfalldaktionsplan, der im Falle einer Sicherheitsverletzung im System eingesetzt wird. Stellen Sie sicher, dass der Plan mindestens die folgenden Punkte umfasst:</p> <ul style="list-style-type: none"> ▪ Rollen, Verantwortungsbereiche und Kommunikations- sowie Kontaktstrategien bei einer Verletzung der Systemsicherheit, einschließlich Benachrichtigung der Zahlungsmarken ▪ Konkrete Verfahren für die Reaktion auf Vorfälle ▪ Verfahren zur Wiederaufnahme und Fortsetzung des Geschäftsbetriebs ▪ Verfahren zur Datensicherung ▪ Analyse der gesetzlichen Bestimmungen hinsichtlich der Offenlegung von Sicherheitsverletzungen ▪ Abdeckung sämtlicher wichtigen Systemkomponenten ▪ Verweis auf oder Einbeziehung von Verfahren der Zahlungsmarken zur Reaktion auf Vorfälle 	<p>Der Vorfalldaktionsplan sollte gut durchdacht sein und alle Schlüsselemente enthalten, die es Ihrem Unternehmen ermöglichen, effektiv potentiellen Verstößen zu begegnen, die die Karteninhaberdaten betreffen könnten.</p>
<p>12.9.2 Testen Sie den Plan mindestens einmal im Jahr.</p>	<p>Ohne entsprechende Tests könnte die Implementierung wichtiger Schritte versäumt werden, wodurch während eines Vorfalls hohe Risiken entstehen können.</p> <p>Wenn innerhalb des letzten Jahres der Vorfalldaktionsplan komplett mit allen Komponenten des Plans aktiviert wurde, ist eine ausführliche Überprüfung des aktuellen Vorfalls sowie der entsprechenden Reaktion als Test vollkommen ausreichend. Wenn nur einige der Komponenten in der jüngsten Vergangenheit aktiviert wurden, müssen trotzdem noch die restlichen Komponenten getestet werden. Wenn in den letzten 12 Monaten keine Komponenten des Plans aktiviert wurden, müssen bei dem alljährlichen Test alle Komponenten des Plans eingeschlossen werden.</p>

Anforderung	Leitfaden
<p>12.9.3 Stellen Sie sicher, dass rund um die Uhr Mitarbeiter eingesetzt sind, die auf mögliche Warnmeldungen reagieren.</p>	<p>Ohne ein entsprechend ausgebildetes und stets verfügbares Team zur Durchsetzung der Vorfalldaktionspläne könnten größere Schäden am Netzwerk verursacht und wichtige Daten und Systeme durch die unsachgemäße Handhabung der anvisierten Systeme „befallen“ werden. Hierdurch kann auch der Erfolg einer nachträglichen Ursachenanalyse eines Vorfalls vereitelt werden. Wenn keine internen Ressourcen verfügbar sind, ziehen Sie in Erwägung, einen entsprechenden Vertrag mit einem Anbieter solcher Dienste abzuschließen.</p>
<p>12.9.4 Führen Sie Schulungen für Mitarbeiter ein, die für die Reaktion auf Sicherheitsverletzungen verantwortlich sind.</p>	
<p>12.9.5 Achten Sie hierbei auch auf Alarme aus Systemen zur Erkennung und/oder Verhinderung von Angriffsversuchen und zur Überwachung der Dateiintegrität.</p>	<p>Diese Überwachungssysteme wurden konzipiert, um sich vorrangig auf potentielle Risiken für Daten zu konzentrieren, sie sind von zentraler Bedeutung, wenn es darum geht, eine Sicherheitsverletzung zu verhindern und müssen folglich in die Vorfalldaktionsprozesse aufgenommen werden.</p>
<p>12.9.6 Entwickeln Sie einen Prozesses zur Änderung und Weiterentwicklung des Vorfalldaktionsplans entsprechend Ihrer eigenen Erfahrungen und integrieren Sie Branchenentwicklungen.</p>	<p>Durch die Eingliederung der eigenen Erfahrungen in den Vorfalldaktionsplan nach einem Vorfall wird der Plan aktualisiert und in die Lage versetzt, auch auf aufkommende Bedrohungen und Sicherheitstrends zu reagieren.</p>

Leitfaden für die Anforderung A.1: Zusätzliche PCI-DSS-Anforderungen für von mehreren Benutzern gemeinsam genutzte Hosting-Anbieter

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

Wie in Anforderung 12.8 erläutert, müssen sämtliche Dienstleister, die auf Karteninhaberdaten zugreifen können (auch gemeinsam genutzte Hosting-Anbieter), den PCI-Datensicherheitsstandard erfüllen. Außerdem geht aus Anforderung 2.4 hervor, dass gemeinsam genutzte Hosting-Anbieter die gehostete Umgebung und die Daten jeder Stelle schützen müssen. Aus diesem Grund müssen die Hosting-Anbieter auch die Anforderungen in diesem Anhang erfüllen.

Anforderung	Leitfaden
<p>A.1 Schutz der gehosteten Umgebung und der Daten jeder Stelle (d. h. Händler, Dienstleister oder eine andere Stelle) gemäß A.1.1 bis A.1.4:</p> <p>Ein Hosting-Anbieter muss diese Anforderungen sowie die anderen relevanten Abschnitte des PCI-Datensicherheitsstandards erfüllen.</p> <p>Hinweis: Auch wenn ein Hosting-Anbieter diese Anforderungen erfüllt, ist nicht garantiert, dass die Stelle, die den Hosting-Anbieter nutzt, die Konformitätskriterien erfüllt. Jede Stelle muss PCI-DSS-konform arbeiten und die Konformität von Fall zu Fall beurteilen.</p>	<p>Der <i>Anhang A</i> des PCI-DSS gilt für von mehreren Benutzern genutzte Hosting-Anbieter, die den Kunden Ihrer Händler und/oder Serviceanbieter eine PCI-DSS konforme Hosting-Umgebung bieten möchten. Zusätzlich zu allen anderen gültigen PCI-DSS-Anforderungen sollten auch die nachfolgenden Schritte befolgt werden:</p>
<p>A.1.1 Stellen Sie sicher, dass an den einzelnen Stellen nur Prozesse ausgeführt werden, die Zugriff auf die Karteninhaberdaten-Umgebung dieser Stelle haben.</p>	<p>Wenn ein Händler oder Dienstleister berechtigt ist, seine eigenen Anwendungen auf dem gemeinsam genutzten Server auszuführen, sollten diese mit dem Benutzernamen des Händlers oder Serviceanbieters anstatt als Benutzer mit besonderen Rechten ausgeführt werden. Ein Benutzer mit besonderen Rechten hat Zugriff auf die eigenen Karteninhaberdaten-Umgebungen sowie jene aller anderen Händler und Serviceanbieter.</p>
<p>A.1.2 Beschränken des Zugriffs und der Rechte der einzelnen Stellen auf die eigene Umgebung mit Karteninhaberdaten.</p>	<p>Um sicherzustellen, dass die Zugriffsberechtigungen und Rechte so eingeschränkt sind, dass alle Händler oder Serviceanbieter nur Zugang zu ihren eigenen Karteninhaberdaten haben, beachten Sie bitte Folgendes: (1) Berechtigungen des Webserver-Benutzernamens des Händlers oder Dienstleisters; (2) gewährte Berechtigungen zum Lesen, Schreiben und Ausführen von Dateien; (3) gewährte Berechtigungen zum Schreiben von Systemdateien; (4) gewährte Zugriffsberechtigungen auf die Protokolldateien von Händlern und Serviceanbietern; und (5) Kontrollen, um sicherzustellen, dass ein Händler oder Serviceanbieter nicht die kompletten Systemressourcen für sich in Anspruch nehmen kann.</p>
<p>A.1.3 Stellen Sie sicher, dass eindeutige, mit der PCI-DSS-Anforderung 10 konforme, Protokollierungs- und Audit-</p>	<p>Protokolle sollten in von mehreren Benutzern genutzten Hosting-Umgebungen verfügbar sein, damit die Händler und Serviceanbieter auf zu ihrer Karteninhaber-</p>

Anforderung	Leitfaden
Trails für die Karteninhaberdaten-Umgebung jeder Stelle aktiviert sind.	Umgebung zugehörige Protokolle zugreifen und diese überprüfen können.
A.1.4 Aktivieren Sie Prozesse für eine rechtzeitige Ursachenanalyse im Falle einer Sicherheitsverletzung bei einem gehosteten Händler oder Dienstanbieter.	Von mehreren Benutzern genutzte Hosting-Anbieter müssen über Prozesse mit einer entsprechenden Informationstiefe verfügen, um einerseits schnell und unkompliziert zu antworten, sollte eine Ursachenanalyse bezüglich eines Angriffs notwendig werden, und andererseits damit die Informationen zu den einzelnen Händlern oder Serviceanbietern ersichtlich werden.

Anhang A: PCI-Datensicherheitsstandard: Damit verbundene Dokumente

Die folgenden Dokumente wurden als Hilfe für Händler und Dienstanbieter entwickelt, damit sie besser über den PCI-Datensicherheitsstandard (DSS) und die Konformitätsanforderungen und Verantwortlichkeiten informiert werden.

Dokument	Publikum
<i>Anforderungen und Sicherheitsbeurteilungsverfahren des PCI-Datensicherheitsstandard</i>	Alle Händler und Dienstanbieter
<i>PCI-DSS-Navigation: Verständnis der Intention der Anforderungen</i>	Alle Händler und Dienstanbieter
<i>PCI-Datensicherheitsstandard: Richtlinien und Anleitungen zum Selbstbeurteilungs-Fragebogen</i>	Alle Händler und Dienstanbieter
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen A und Bescheinigung</i>	Verfügbare Händler ⁹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen B und Bescheinigung</i>	Verfügbare Händler ⁹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen C-VT und Bescheinigung</i>	Verfügbare Händler ⁹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen C und Bescheinigung</i>	Verfügbare Händler ⁹
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen D und Bescheinigung</i>	Verfügbare Händler und Dienstanbieter ⁹
<i>Der PCI-DSS und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>	Alle Händler und Dienstanbieter

⁹ Informationen zum Bestimmen des angemessenen Selbstbeurteilungs-Fragebogen finden Sie unter dem PCI-Datensicherheitsstandard: Anleitung und Richtlinien für den Selbstbeurteilungsfragebogen „Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind“.