



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

Verständnis der Intention der Anforderungen

Version 1.2

Oktober 2008

Dokumentänderungen

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

Inhalt

Dokumentänderungen	i
Einleitung	iii
Elemente von Karteninhaberdaten und vertraulichen Authentifizierungsdaten	1
<i>Position von Karteninhaberdaten und vertraulichen Authentifizierungsdaten.....</i>	<i>2</i>
<i>Track 1- vs. Track 2-Daten</i>	<i>3</i>
Zusätzliche Anweisungen für den PCI-Datensicherheitsstandard	4
Anweisungen für Anforderungen 1 und 2: Erstellung und Wartung eines sicheren Netzwerks	5
<i>Anforderung 1: Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten</i>	<i>5</i>
<i>Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden..</i>	<i>10</i>
Anweisungen für Anforderungen 3 und 4: Schutz von Karteninhaberdaten.....	13
<i>Anforderung 3: Schutz gespeicherter Karteninhaberdaten</i>	<i>13</i>
<i>Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze</i>	<i>19</i>
Anweisungen für Anforderungen 5 und 6: Wartung eines Anfälligkeits-Managementprogramms.....	21
<i>Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware</i>	<i>21</i>
<i>Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen.....</i>	<i>23</i>
Anweisungen für Anforderungen 7, 8 und 9: Implementierung starker Zugriffskontrollmaßnahmen	30
<i>Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf</i>	<i>30</i>
<i>Anforderung 8: Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff.....</i>	<i>32</i>
<i>Anforderung 9: Beschränkung des physischen Zugriffs auf Karteninhaberdaten.....</i>	<i>36</i>
Anweisungen für Anforderungen 10 und 11: Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken.....	41
<i>Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten</i>	<i>41</i>
<i>Anforderung 11: Regelmäßiges Testen der Sicherheitssysteme und -prozesse.....</i>	<i>44</i>
Anweisung für Anforderung 12: Befolgung einer Informationssicherheits-Richtlinie	47
<i>Anforderung 12: Befolgen einer Richtlinie zur Informationssicherheit für Mitarbeiter und Subunternehmer.....</i>	<i>47</i>
Anweisung für Anforderung A.1: Zusätzliche PCI-DSS-Anforderungen für gemeinsam genutzte Hosting-Anbieter	53
Anhang A: PCI-Datensicherheitsstandard: Damit verbundene Dokumente.....	55

Einleitung

In diesem Dokument werden die zwölf Anforderungen des Payment Card Industry-Datensicherheitsstandards („Payment Card Industry Data Security Standard“, kurz PCI-DSS) beschrieben. Es enthält zudem Anweisungen, die die Intention der einzelnen Anforderungen erläutern. Dieses Dokument wurde als Hilfe für Händler, Dienstanbieter und Finanzinstitutionen konzipiert, die den PCI-Datensicherheitsstandard sowie die Bedeutung und Intention der detaillierten Anforderungen, die die Sicherheit von Systemkomponenten (Server, Netzwerk, Anwendungen usw.) zur Unterstützung von Karteninhaberdaten-Umgebungen gewährleisten sollen, besser verstehen möchten.

HINWEIS: PCI-DSS-Navigation: Das Dokument *Verständnis der Intention der Anforderungen* dient lediglich als Hilfe. Bei der Durchführung einer PCI-DSS-Beurteilung vor Ort oder beim Ausfüllen eines Selbstbeurteilungs-Fragebogens (SBF) sollten die Dokumente *PCI-DSS-Anforderungen und -Sicherheitsbeurteilungsverfahren* („Payment Card Industry Data Security Standard (PCI-DSS) Requirements and Security Assessment Procedures“) sowie *PCI-DSS-Selbstbeurteilungs-Fragebogen v1.2* („PCI DSS Self-Assessment Questionnaires v1.2“) als Referenz herangezogen werden.

Die PCI-DSS-Anforderungen finden auf alle Systemkomponenten Anwendung, die in die Karteninhaberdaten-Umgebung eingebunden oder mit dieser verbunden sind. Die Karteninhaberdaten-Umgebung ist der Bestandteil des Netzwerks, der Karteninhaberdaten oder vertrauliche Authentifizierungsdaten, einschließlich Netzwerkkomponenten, Server und Anwendungen, beinhaltet.

- Netzwerkkomponenten können u. a. Firewalls, Switches, Router, Zugriffspunkte für drahtlose Netzwerke, Netzwerkgeräte und andere Sicherheitsgeräte umfassen.
- Servertypen können u. a. Folgendes beinhalten: Web, Datenbank, Authentifizierung, Mail, Proxy, Network Time Protocol (NTP) und Domain Name Server (DNS).
- Anwendungen können u. a. alle erworbenen und benutzerdefinierten Anwendungen, darunter auch interne und externe (Internet-) Anwendungen umfassen.

Eine geeignete Netzwerksegmentierung, durch die Systeme, die Karteninhaberdaten speichern, verarbeiten oder übertragen, von solchen Systemen isoliert werden, die dies nicht tun, kann den Umfang der Karteninhaberdaten-Umgebung reduzieren. Ein qualifizierter Sicherheitsprüfer (Qualified Security Assessor, QSA) kann dabei unterstützen, den Umfang innerhalb einer Karteninhaberdaten-Umgebung festzulegen und den Umfang einer PCI-DSS-Beurteilung durch die Implementierung einer korrekten Netzwerkumgebung zu beschränken. Bei Fragen, die sich darauf beziehen, ob eine spezielle Implementierung mit dem Standard übereinstimmt oder eine bestimmte Anforderung erfüllt, empfiehlt PCI SSC Unternehmen, sich an einen qualifizierten Sicherheitsprüfer zu wenden, um die Implementierung von Technologien und Prozessen sowie die Erfüllung des PCI-Datensicherheitsstandards zu überprüfen. Aufgrund ihrer Erfahrung mit komplexen Netzwerkumgebungen sind die qualifizierten Sicherheitsprüfer bestens geeignet, Händler oder Dienstanbieter bei ihrem Streben nach Konformität zu unterstützen und ihnen bewährte Methoden bereitzustellen. Die PCI SSC-Liste der qualifizierten Sicherheitsprüfer finden Sie hier: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

Elemente von Karteninhaberdaten und vertraulichen Authentifizierungsdaten

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

Unter Karteninhaberdaten sind die primäre Kontonummer (Primary Account Number, PAN, oder Kreditkartennummer) sowie andere im Zuge einer Zahlungstransaktion erhaltene Daten zu verstehen. Dazu zählen u. a. die folgenden Datenelemente (weitere Informationen finden Sie in der unten stehenden Tabelle):

- PAN
- Name des Karteninhabers
- Ablaufdatum
- Servicecode
- Vertrauliche Authentifizierungsdaten: (1) vollständige Magnetstreifendaten, (2) CAV2/CVC2/CVV2/CID und (3) PINs/PIN-Blöcke)

Die primäre Kontonummer (PAN) stellt den definierenden Faktor in Bezug auf die Anwendbarkeit der PCI-DSS-Anforderungen und des PA-DSS dar. Wird die PAN nicht gespeichert, verarbeitet oder übertragen, finden PCI-DSS und PA-DSS keine Anwendung.

	Datenelement	Speichern zulässig	Schutz erforderlich	PCI-DSS-Anf. 3, 4
Karteninhaberdaten	Primäre Kontonummer (PAN)	Ja	Ja	Ja
	Karteninhabername ¹	Ja	Ja ¹	Nein
	Servicecode ¹	Ja	Ja ¹	Nein
	Ablaufdatum ¹	Ja	Ja ¹	Nein
Vertrauliche Authentifizierungsdaten ²	Vollständige Magnetstreifendaten ³	Nein	Nicht zutr.	Nicht zutr.
	CAV2/CVC2/CVV2/CID	Nein	Nicht zutr.	Nicht zutr.
	PIN/PIN-Block	Nein	Nicht zutr.	Nicht zutr.

¹ Diese Datenelemente müssen geschützt werden, wenn sie in Verbindung mit der PAN gespeichert werden. Dieser Schutz sollte gemäß den PCI-DSS-Anforderungen für den allgemeinen Schutz der Karteninhaberdaten-Umgebung erfolgen. Darüber hinaus kann eine andere Gesetzgebung (z. B. im Zusammenhang mit dem Schutz persönlicher Verbraucherdaten, Datenschutz, Identitätsdiebstahl oder Datensicherheit) einen besonderen Schutz dieser Daten oder die ordnungsgemäße Weitergabe der Verfahren eines Unternehmens erfordern, wenn im Rahmen der Ausübung der geschäftlichen Tätigkeiten verbraucherbezogene persönliche Daten erfasst werden. Der PCI-DSS gilt jedoch nicht, wenn PANs nicht gespeichert, verarbeitet oder übertragen werden.

² Vertrauliche Authentifizierungsdaten dürfen nach der Autorisierung nicht gespeichert werden (auch wenn sie verschlüsselt wurden).

³ Vollständige Verfolgungsdaten vom Magnetstreifen, Magnetstreifenabbild auf dem Chip oder einem anderen Speicherort.

Position von Karteninhaberdaten und vertraulichen Authentifizierungsdaten

Vertrauliche Authentifizierungsdaten umfassen Magnetstreifendaten (bzw. Verfolgungsdaten)⁴, Kartvalidierungs-codes oder -werte⁵ sowie PIN-Daten⁶. **Das Speichern vertraulicher Authentifizierungsdaten ist verboten!** Diese Daten sind für böswillige Personen äußerst wertvoll, da sie mithilfe dieser Daten falsche Zahlungskarten erstellen und damit in betrügerischer Absicht Transaktionen durchführen können. Die vollständige Definition für „vertrauliche Authentifizierungsdaten“ finden Sie im *PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme*. Die folgenden Abbildungen der Rück- und Vorderseite einer Kreditkarte zeigen die Position von Karteninhaberdaten und vertraulichen Authentifizierungsdaten.



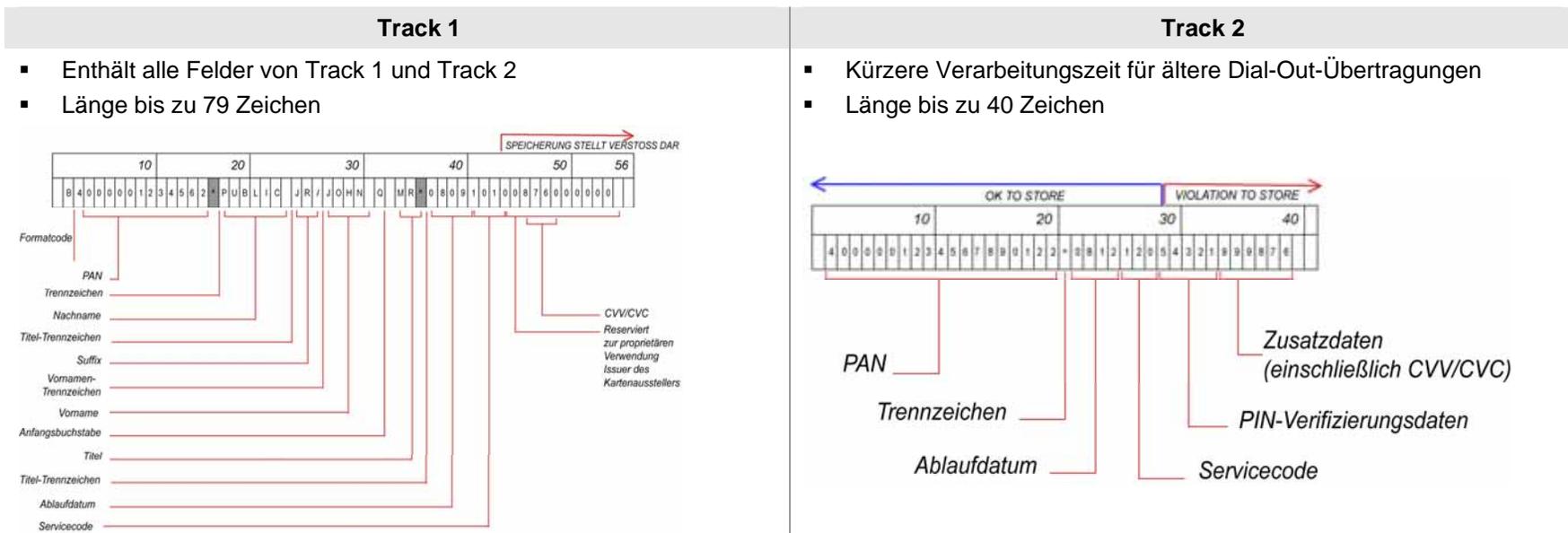
⁴ Im Magnetstreifen verschlüsselte Daten, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Diese Daten befinden sich außerdem in dem Magnetstreifenabbild auf dem Chip oder einem anderen Speicherort auf der Karte. Stellen dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifendaten speichern. Die einzigen Elemente der Verfolgungsdaten, die beibehalten werden dürfen, sind die primäre Kontonummer, der Karteninhabername, das Ablaufdatum sowie der Servicecode.

⁵ 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.

⁶ Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht.

Track 1- vs. Track 2-Daten

Werden vollständige Verfolgungsdaten (entweder Track 1 oder Track 2, vom Magnetstreifen, Magnetstreifenabbild auf dem Chip oder an einem anderen Speicherort) gespeichert, können böswillige Personen, die in den Besitz dieser Daten gelangen, Zahlungskarten reproduzieren und auf der ganzen Welt verkaufen. Darüber hinaus verstößt das Speichern der vollständigen Verfolgungsdaten gegen die Zahlungsmarkenbestimmungen und kann mit der Zahlung von Gebühren und Bußgeldern geahndet werden. In der unteren Abbildung werden Informationen zu den Track 1- und Track 2-Daten gegeben, wobei insbesondere die zwischen diesen Daten bestehenden Unterschiede beschrieben werden sowie eine Skizze der Speicherung der Daten auf dem Magnetstreifen dargestellt wird.



Zusätzliche Anweisungen 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

Wartung 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: Beschränkung des physischen Zugriffs auf Karteninhaberdaten

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: Befolgung einer Informationssicherheits-Richtlinie

Anweisungen für Anforderungen 1 und 2: Erstellung und Wartung eines sicheren Netzwerks

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

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

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 diese über das Internet als E-Commerce, über den Internetzugang der Mitarbeiter über Desktop-Browser, den E-Mail-Zugriff von Mitarbeitern, dedizierte Verbindungen, 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.

Anforderung	Anweisung
1.1 Festlegen von Standards für die Firewall- und Router-Konfiguration, die Folgendes beinhalten:	Firewalls und Router stellen Schlüsselkomponenten der Architektur dar, die den Zugang zum Netzwerk und das Verlassen des Netzwerks steuern. Bei diesen Geräten handelt es sich um Software oder Hardware, die den unerwünschten Zugang zum Netzwerk blockiert und den autorisierten Zugang in das Netzwerk sowie das Verlassen des Netzwerks regelt. Ohne Richtlinien und festgelegte Verfahren zum Konfigurieren von Firewalls und Routern besteht die Gefahr, dass ein Unternehmen seine erste Verteidigungslinie zum Schutz von Daten verliert. Diese Richtlinien und Verfahren gewährleisten eine starke erste Verteidigungslinie zum Schutz von Daten.
1.1.1 Einen offiziellen Prozess zur Genehmigung und zum Testen aller externen Netzwerkverbindungen und Änderungen an der Firewall- und Router-Konfiguration	Mithilfe von Richtlinien und festgelegten Verfahren zur Genehmigung und zum Testen aller Verbindungen und Änderungen an Firewalls und Routern können Sicherheitsprobleme infolge einer falschen Konfiguration von Netzwerk, Router oder Firewall verhindert werden.
1.1.2 Ein aktuelles Netzwerkdiagramm mit allen Verbindungen mit Karteninhaberdaten, einschließlich aller drahtlosen Netzwerke	Netzwerkdiagramme bieten dem Unternehmen die Möglichkeit, die Position aller Netzwerkgeräte zu bestimmen. Zudem lässt sich mithilfe des Netzwerkdiagramms der Datenfluss von Karteninhaberdaten innerhalb des Netzwerks und zwischen einzelnen Geräten abbilden. Auf diese Weise kann der Umfang der Karteninhaberdaten-Umgebung verständlich dargestellt werden. Ohne aktuelle Netzwerk- und Datenflussdiagramme besteht die Gefahr, dass Geräte mit Karteninhaberdaten übersehen und unbewusst nicht in die für den PCI-DSS implementierte mehrschichtige Sicherheitskontrolle eingebunden werden und somit für Sicherheitsverletzungen anfällig wären.

Anforderung	Anweisung
<p>1.1.3 Anforderungen für eine Firewall an jeder Internetverbindung und zwischen jeder demilitarisierten Zone (DMZ) und der internen Netzwerkzone</p>	<p>Mit einer Firewall für jede Verbindung in das (und aus dem) Netzwerk hat das Unternehmen die Möglichkeit, den Zugang in das Netzwerk und das Verlassen des Netzwerks zu überwachen und die Gefahr zu reduzieren, dass böswillige Personen Zugang zum internen Netzwerk erhalten.</p>
<p>1.1.4 Beschreibung der Gruppen, Rollen und Verantwortungsbereiche für die logische Verwaltung der Netzwerkkomponenten</p>	<p>Dank der Beschreibung von Rollen und Verantwortungsbereichen wird sichergestellt, dass eine Person eindeutig für die Sicherheit aller Komponenten verantwortlich ist, dass sich diese Person ihrer Verantwortung auch bewusst ist und dass alle Geräte einbezogen werden.</p>
<p>1.1.5 Dokumentation und Begründung für den Einsatz aller zulässigen Dienste, Protokolle und Ports, einschließlich der Dokumentation von Sicherheitsfunktionen für die Protokolle, die als unsicher gelten</p>	<p>Sicherheitsverletzungen sind häufig die Folge von nicht genutzten oder unsicheren Diensten und Ports, denn ihre Anfälligkeiten sind oft bekannt. Viele Unternehmen sind für diese Arten der Sicherheitsverletzung anfällig, da sie ihre Sicherheitslücken für nicht genutzte Dienste, Protokolle und Ports nicht schließen (auch wenn Sicherheitslücken immer noch vorhanden sind). Jedes Unternehmen sollte eindeutig festlegen, welche Dienste, Protokolle und Ports für sein Geschäft erforderlich sind, diese für seine Unterlagen dokumentieren und sicherstellen, dass alle anderen Dienste, Protokolle und Ports deaktiviert oder entfernt werden. Des Weiteren sollten Unternehmen in Erwägung ziehen, sämtlichen Datenverkehr zu blockieren und diese Ports erst dann wieder zu öffnen, wenn die Notwendigkeit zum Öffnen festgelegt und dokumentiert wurde.</p> <p>Darüber hinaus existieren viele Dienste, Protokolle oder Ports, die ein Unternehmen möglicherweise benötigt (oder die standardmäßig aktiviert sind), die jedoch häufig von böswilligen Personen genutzt werden, um auf ein Netzwerk zuzugreifen. Benötigt das Unternehmen diese unsicheren Dienste, Protokolle und Ports, sollte sich das Unternehmen des Risikos bewusst sein, das durch die Nutzung dieser Protokolle besteht, und dieses Risiko ernst nehmen. Die Nutzung des Protokolls sollte begründet sein, und die Sicherheitsfunktionen, die eine sichere Nutzung dieser Protokolle ermöglichen, sollten dokumentiert und implementiert werden. Nicht benötigte unsichere Dienste, Protokolle und Ports sollten deaktiviert oder entfernt werden.</p>
<p>1.1.6 Anforderung zum Prüfen von Firewall- und Router-Regelsätzen mindestens alle sechs Monate</p>	<p>Dank dieser Prüfung hat das Unternehmen mindestens alle sechs Monate die Möglichkeit, nicht benötigte, veraltete oder falsche Regeln zu beseitigen und sicherzustellen, dass alle Regelsätze nur autorisierte, mit den Begründungen des Unternehmens in Einklang stehende Dienste und Ports zulassen.</p> <p>Es wird empfohlen, diese Prüfungen häufiger durchzuführen, beispielsweise monatlich, um zu gewährleisten, dass die Regelsätze aktuell sind und den Erfordernissen des Unternehmens entsprechen, damit keine Sicherheitslücken entstehen oder unnötige Risiken eingegangen werden.</p>

Anforderung	Anweisung
<p>1.2 Aufbauen einer Firewall-Konfiguration, die Verbindungen zwischen nicht vertrauenswürdigen Netzwerken und allen Systemkomponenten in der Karteninhaberdaten-Umgebung einschränkt</p> <p><i>Hinweis: Ein „nicht vertrauenswürdige 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 ist außerordentlich wichtig, einen Netzwerkschutz, d. h. eine Firewall, zwischen dem internen, vertrauenswürdigen Netzwerk und anderen, nicht vertrauenswürdigen Netzwerken einzurichten, die extern sind und/oder die die Einheit nicht kontrollieren oder steuern kann. Wird kein wirksamer Schutz eingerichtet, ist das Unternehmen für den unbefugten Zugriff durch böswillige Personen oder Software anfällig.</p> <p>Wird eine Firewall installiert, die nicht über Regeln zur Kontrolle und Begrenzung bestimmten Datenverkehrs verfügt, sind böswillige Personen möglicherweise weiterhin in der Lage, Sicherheitslücken bei Protokollen und Ports auszunutzen und Ihr Netzwerk anzugreifen.</p>
<p>1.2.1 Beschränkung des ein- und ausgehenden Netzwerkverkehrs auf den für die Karteninhaberdaten-Umgebung absolut notwendigen Datenverkehr</p>	<p>Diese Anforderung zielt darauf ab, den Zugriff von böswilligen Personen auf das Unternehmensnetzwerk über nicht autorisierte IP-Adressen sowie die unbefugte Nutzung von Diensten, Protokollen oder Ports (z. B. Senden von unberechtigterweise aus Ihrem Netzwerk gesammelten Daten an einen nicht vertrauenswürdigen Server) zu verhindern.</p> <p>Alle Firewalls sollten eine Regel enthalten, wodurch der gesamte nicht unbedingt benötigte ein- und ausgehende Netzwerkverkehr verweigert wird. Dadurch werden ungewollte Sicherheitslücken vermieden, die anderen, unerwünschten und potenziell gefährlichen ein- und ausgehenden Datenverkehr zulassen würden.</p>
<p>1.2.2 Sichern und Synchronisieren von Router-Konfigurationsdateien.</p>	<p>Während ausgeführte Konfigurationsdateien in der Regel mit Sicherheitseinstellungen implementiert werden, werden Startdateien (Router führen diese Dateien nur bei einem Neustart aus) möglicherweise nicht mit denselben Sicherheitseinstellungen implementiert, da sie nur gelegentlich ausgeführt werden. Erfolgt der Neustart eines Routers ohne dieselben Sicherheitseinstellungen wie bei ausgeführten Konfigurationsdateien, führt dies möglicherweise zu abgeschwächten Regeln, die böswilligen Personen den Zugriff auf das Netzwerk ermöglichen, da die Startdateien womöglich nicht mit denselben Sicherheitseinstellungen wie die ausgeführten Konfigurationsdateien implementiert wurden.</p>
<p>1.2.3 Installation von Umkreis-Firewalls zwischen allen drahtlosen Netzwerken und der Karteninhaberdaten-Umgebung und Konfigurieren dieser Firewalls in der Art, dass der gesamte Datenverkehr aus der drahtlosen Umgebung abgelehnt oder kontrolliert wird (sofern dieser Datenverkehr für die Geschäftszwecke notwendig ist).</p>	<p>Die bekannte (oder unbekannt) Implementierung und Nutzung drahtloser Technologien innerhalb eines Netzwerks stellt einen häufig genutzten Weg für böswillige Personen dar, um auf das Netzwerk und Karteninhaberdaten zuzugreifen. Wird ein drahtloses Gerät oder Netzwerk ohne das Wissen eines Unternehmens installiert, kann eine böswillige Person ganz leicht und „unsichtbar“ in das Netzwerk gelangen. Wenn der Zugriff von drahtlosen Netzwerken auf die Zahlungskartenumgebung nicht durch Firewalls beschränkt wird, können böswillige Personen, die unberechtigten Zugriff auf das drahtlose Netzwerk erhalten, ganz einfach eine Verbindung zu der Zahlungskartenumgebung herstellen und Kontoinformationen ausspähen.</p>

Anforderung	Anweisung
<p>1.3 Verboten des direkten öffentlichen Zugriffs zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdaten-Umgebung.</p>	<p>Der Zweck einer Firewall besteht in der Steuerung und Kontrolle aller Verbindungen zwischen öffentlichen Systemen und internen Systemen (insbesondere solchen Systeme, die Karteninhaberdaten speichern). Wird ein direkter Zugriff zwischen öffentlichen Systemen und Systemen, auf denen Karteninhaberdaten gespeichert werden, gewährt, wird der Firewall-Schutz übergangen. Die Folge ist, dass Systemkomponenten, auf denen Karteninhaberdaten gespeichert werden, Sicherheitsangriffen ausgesetzt sein können.</p>
<p>1.3.1 Implementieren einer DMZ, um ein- und ausgehenden Datenverkehr auf Protokolle zu beschränken, die für die Karteninhaberdaten-Umgebung erforderlich sind.</p>	<p>Diese Anforderung zielt darauf ab, den Zugriff von böswilligen Personen auf das Unternehmensnetzwerk über nicht autorisierte IP-Adressen sowie die unbefugte Nutzung von Diensten, Protokollen oder Ports (z. B. Senden von unberechtigterweise aus Ihrem Netzwerk gesammelten Daten an einen externen, nicht vertrauenswürdigen Server in einem nicht vertrauenswürdigen Netzwerk) zu verhindern.</p>
<p>1.3.2 Beschränken des eingehenden Internetverkehrs auf IP-Adressen innerhalb der DMZ.</p>	
<p>1.3.3 Keine direkten eingehenden oder ausgehenden Routen für Datenverkehr zwischen dem Internet und der Karteninhaberdaten-Umgebung zulassen.</p>	<p>Die DMZ ist der Teil der Firewall, der auf das öffentliche Internet ausgerichtet ist und Verbindungen zwischen dem Internet und internen Diensten steuert, die ein Unternehmen für die Öffentlichkeit bereitstellen muss (z. B. ein Webserver). Sie stellt die erste Verteidigungslinie bei der Trennung des Datenverkehrs, der mit dem internen Netzwerk kommunizieren muss, von dem Datenverkehr, der dies nicht tun muss, dar.</p>
<p>1.3.4 Nicht zulassen, dass interne Adressen aus dem Internet in die DMZ übergeben werden.</p>	<p>In der Regel enthält ein Paket die IP-Adresse des Computers, der es ursprünglich gesendet hat. Auf diese Weise wissen die anderen Computer innerhalb des Netzwerks, woher es stammt. In einigen Fällen wird jedoch von böswilligen Personen eine gefälschte IP-Adresse gesendet.</p> <p>Zum Beispiel: Böswillige Personen senden ein Paket mit einer gefälschten IP-Adresse, sodass das Paket (sofern Ihre Firewall dies nicht verbietet) aus dem Internet in Ihr Netzwerk gelangen kann, da der Eindruck entsteht, es handle sich um internen und damit rechtmäßigen Datenverkehr. Sobald böswillige Personen in Ihr Netzwerk eingedrungen sind, können sie Ihr System ausspähen und gefährden.</p> <p>Das „Ingress Filtering“ (Filtern des eingehenden Datenstroms) stellt eine bei der Firewall einsetzbare Methode zum Filtern von in das Netzwerk eingehenden Paketen dar. Dadurch kann u. a. sichergestellt werden, dass Pakete nicht so „manipuliert“ werden, dass der Eindruck entsteht, es handle sich um Pakete aus Ihrem eigenen Netzwerk.</p> <p>Wenn Sie sich eingehender über das Filtern von Paketen informieren möchten, können Sie sich auch mit dem „Egress Filtering“ (Filtern des ausgehenden Datenstroms) befassen.</p>
<p>1.3.5 Beschränken des ausgehenden Datenverkehrs aus der Karteninhaberdaten-Umgebung in das Internet, sodass der ausgehende Datenverkehr nur auf IP-Adressen innerhalb der DMZ zugreifen kann.</p>	<p>Die DMZ sollte zudem sämtlichen ausgehenden Datenverkehr aus dem Netzwerk prüfen, um sicherzustellen, dass sämtlicher ausgehender Datenverkehr den festgelegten Regeln folgt. Um die Wirksamkeit dieser DMZ-Funktion zu erhöhen, sollten alle Verbindungen aus dem Netzwerk zu Adressen außerhalb des Netzwerks verboten werden, es sei denn, sie durchlaufen zunächst eine Legitimitätsprüfung durch die DMZ.</p>

Anforderung	Anweisung
<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 eine statusgesteuerte Paketinspektion durchführt, merkt sich den „Status“ jeder Verbindung zur Firewall. Dadurch weiß die Firewall, ob es sich bei einer Reaktion auf eine vorherige Verbindung auch tatsächlich um eine Reaktion handelt (da sie sich an die vorherige Verbindung „erinnert“) oder ob eine böswillige Person oder Software versucht, die Firewall zu täuschen oder auszutricksen, damit diese die Verbindung zulässt.</p>
<p>1.3.7 Platzieren der Datenbank in einer internen Netzwerkzone, die von der DMZ getrennt ist.</p>	<p>Karteninhaberdaten erfordern den größtmöglichen Schutz. Werden Karteninhaberdaten innerhalb der DMZ gespeichert, können externe Angreifer aufgrund der geringeren Anzahl an zu durchdringenden Schichten einfacher auf diese Informationen zugreifen.</p>
<p>1.3.8 Implementieren von IP-Maskierung unter Verwendung des RFC 1918-Adressraums, um zu verhindern, dass interne Adressen übersetzt und im Internet offengelegt werden können. Verwenden von NAT-Technologien (Network Address Translation), z. B. Port Address Translation (PAT).</p>	<p>Eine durch die Firewall gesteuerte IP-Maskierung ermöglicht, dass ein Unternehmen sowohl interne Adressen, die nur innerhalb des Netzwerks sichtbar sind, als auch externe Adressen, die außerhalb des Netzwerks sichtbar sind, besitzen kann. Wenn eine Firewall die IP-Adresse des internen Netzwerks nicht „versteckt“ bzw. tarnt, könnte eine böswillige Person die internen IP-Adressen entdecken und versuchen, über eine gefälschte IP-Adresse auf das Netzwerk zuzugreifen.</p>
<p>1.4 Installieren von persönlicher Firewall-Software auf allen mobilen und/oder 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>Ist auf einem Computer keine Firewall oder kein Virenschutzprogramm installiert, besteht die Gefahr, dass Spyware, Trojaner, Viren, Würmer und Rootkits (Malware) heruntergeladen und/oder unbewusst installiert werden. Ist der Computer unmittelbar an das Internet angeschlossen, ohne dass die Firewall des Unternehmens dazwischengeschaltet ist, ist der Computer sogar noch anfälliger. Wird Malware auf einen Computer geladen, wenn dieser nicht durch die Firewall des Unternehmens geschützt ist, kann die Malware in böswilliger Absicht Informationen innerhalb des Netzwerks abfangen, wenn der Computer wieder an das Unternehmensnetzwerk angeschlossen wird.</p>

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

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

Anforderung	Anweisung
<p>2.1 Ändern der vom Anbieter angegebenen Standardeinstellungen vor der Installation eines Systems im Netzwerk (z. B. durch die Einführung von Kennwörtern, SNMP-Community-Zeichenfolgen und Beseitigung nicht benötigter Konten).</p>	<p>Böswillige Personen (innerhalb und außerhalb eines Unternehmens) verwenden häufig Standardeinstellungen, -kontonamen und -kennwörter, um Systeme zu beeinträchtigen. Diese Einstellungen sind in Hacker-Gemeinschaften gut bekannt. Verwenden Sie diese Einstellungen, ist Ihr System in höchstem Maße anfällig für Angriffe.</p>
<p>2.1.1 Bei drahtlosen Umgebungen, die mit der Karteninhaberdaten-Umgebung verbunden sind oder Karteninhaberdaten übertragen, Ändern der Anbieterstandardeinstellungen für drahtlose Umgebungen, einschließlich drahtloser Verschlüsselungsschlüssel, Kennwörter und SNMP-Community-Zeichenfolgen. Sicherstellen, dass die Sicherheitseinstellungen bei drahtlosen Geräten für eine starke Verschlüsselungstechnologie zur Authentifizierung und Übertragung aktiviert sind.</p>	<p>Viele Benutzer installieren diese Geräte ohne Genehmigung durch das Management. Zudem ändern sie weder die Standardeinstellungen, noch konfigurieren sie die Sicherheitseinstellungen. Wenn drahtlose Netzwerke nicht mit einer ausreichenden Sicherheitskonfiguration implementiert werden (einschließlich Ändern der Standardeinstellungen), können Wireless Sniffer den Datenverkehr belauschen, Daten und Kennwörter ganz einfach erfassen und in Ihr Netzwerk eindringen und dieses angreifen. Darüber hinaus wurde das Schlüsselaustauschverfahren für die ältere Version der 802.11x Verschlüsselung (WEP) geknackt, wodurch die Verschlüsselung nutzlos werden kann. Überprüfen Sie, ob die Firmware für Ihre Geräte aktuell ist und mehr Sicherheitsprotokolle wie WPA/WPA2 unterstützt.</p>

Anforderung	Anweisung
<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>Viele Schwachstellen von Betriebssystemen, Datenbanken und Unternehmensanwendungen sind bekannt. Doch es existieren auch Methoden, um diese Systeme so zu konfigurieren, dass Sicherheitslücken geschlossen werden. Um Personen zu unterstützen, die keine Sicherheitsexperten sind, haben Sicherheitsunternehmen Empfehlungen zur Systemstabilisierung aufgestellt, die eine Anleitung zur Behebung dieser Schwachstellen bieten. Werden die Schwachstellen von Systemen nicht behoben – z. B. schwache Dateieinstellungen oder Dienst- und Protokollstandardeinstellungen (für häufig nicht benötigte Dienste oder Protokolle) –, kann ein Angreifer mehrere, bekannte Exploits nutzen, um anfällige Dienste und Protokolle anzugreifen und so Zugang zu Ihrem Unternehmensnetzwerk zu erhalten. Auf den folgenden drei Websites können Sie sich über die branchenüblichen bewährten Methoden informieren, die Sie bei der Implementierung von Konfigurationsstandards unterstützen können: www.nist.gov, www.sans.org, www.cisecurity.org.</p>
<p>2.2.1 Implementieren nur einer primären Funktion pro Server.</p>	<p>Damit soll sichergestellt werden, dass die Systemkonfigurationsstandards Ihres Unternehmens sowie damit verbundene Prozesse Serverfunktionen angehen, die über verschiedene Sicherheitsstufen verfügen müssen oder die Sicherheitsschwächen bei anderen Funktionen auf demselben Server verursachen können. Beispiel:</p> <ol style="list-style-type: none"> 1. Eine Datenbank erfordert starke Sicherheitsmaßnahmen. Würde eine Datenbank einen Server mit einer Webanwendung teilen, die offen und unmittelbar an das Internet angebunden sein muss, wäre die Datenbank einem hohen Risiko ausgesetzt. 2. Wird versäumt, einen Patch für eine scheinbar unwichtige Funktion anzuwenden, könnte dies zu einem Sicherheitsangriff führen, durch den andere, wichtigere Funktionen (z. B. eine Datenbank) auf demselben Server beeinträchtigt würden. <p>Diese Anforderung bezieht sich auf Server (in der Regel Unix-, Linux- oder Windows-basiert) und nicht auf Mainframe-Systeme.</p>

Anforderung	Anweisung
<p>2.2.2 Deaktivieren aller unnötigen und unsicheren Dienste und Protokolle (nicht direkt für die Ausführung der spezifischen Gerätefunktion erforderliche Funktionen)</p>	<p>Wie unter 1.1.7 ausgeführt, existieren viele Protokolle, die ein Unternehmen möglicherweise benötigt (oder die standardmäßig aktiviert sind), die jedoch häufig von böswilligen Personen genutzt werden, um auf ein Netzwerk zuzugreifen. Um sicherzustellen, dass diese Dienste und Protokolle stets deaktiviert sind, wenn neue Server eingerichtet werden, sollte diese Anforderung Bestandteil der Konfigurationsstandards Ihres Unternehmens sowie damit verbundener Prozesse sein.</p>
<p>2.2.3 Konfigurieren von Systemsicherheitsparametern, um Missbrauch zu verhindern.</p>	<p>Hierdurch soll sichergestellt werden, dass die Systemkonfigurationsstandards Ihres Unternehmens sowie damit verbundene Prozesse speziell auf Sicherheitseinstellungen und Parameter ausgerichtet sind, für die bekannte Sicherheitsprobleme bestehen.</p>
<p>2.2.4 Entfernen aller unnötigen Funktionen, z. B. Skripte, Treiber, Features, Untersysteme, Dateisysteme und unnötige Webserver.</p>	<p>Die Standards zur Serverstabilisierung müssen Prozesse beinhalten, die auf unnötige Funktionen mit speziellen Sicherheitsproblemen ausgerichtet sind (z. B. Entfernen/Deaktivieren der FTP-Funktion oder der Webserver-Funktion, wenn der Server diese Funktionen nicht ausführt).</p>
<p>2.3 Verschlüsseln des gesamten Nichtkonsolen-Verwaltungszugriffs. Verwenden von Technologien wie SSH, VPN oder SSL/TLS für die webbasierte Verwaltung und sonstigen Nichtkonsolen-Verwaltungszugriff.</p>	<p>Erfolgt die Remote-Administration nicht über eine sichere Authentifizierung und eine verschlüsselte Kommunikation, können vertrauliche Verwaltungs- oder Betriebsinformationen (z. B. Kennwörter des Administrators) abgefangen werden. Eine böswillige Person könnte diese Informationen nutzen, um ins Netzwerk zu gelangen, Administrator zu werden und Daten zu stehlen.</p>
<p>2.4 Gemeinsam genutzte Hosting-Anbieter müssen die gehostete Umgebung und die gehosteten Daten jeder Einheit schützen. Diese Anbieter müssen bestimmte Anforderungen erfüllen, wie in „Anhang A: Zusätzliche PCI-DSS-Anforderungen für gemeinsam genutzte Hosting-Anbieter“ ausgeführt.</p>	<p>Dies richtet sich an Hosting-Anbieter, die gemeinsam genutzte Hosting-Umgebungen für mehrere Clients auf demselben Server bereitstellen. Wenn sich sämtliche Daten auf demselben Server befinden und von einer einzigen Umgebung gesteuert werden, sind die Einstellungen auf diesen gemeinsam genutzten Servern häufig nicht von den einzelnen Clients kontrollierbar. Es besteht die Möglichkeit, dass Clients unsichere Funktionen und Skripte hinzufügen, die die Sicherheit aller anderen Client-Umgebungen beeinträchtigen. Dadurch wird es für eine böswillige Person einfacher, Zugriff auf die Daten eines Clients und somit auch auf die Daten aller anderen Clients zu erhalten. Siehe Anhang A.</p>

Anweisungen für Anforderungen 3 und 4: Schutz von Karteninhaberdaten

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

Schutzmaßnahmen wie Verschlüsselung, Abkürzung, Maskierung und Hashing sind wichtige Bestandteile des Schutzes von Karteninhaberdaten. Wenn ein Eindringling andere Netzwerksicherheitskontrollen 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 PAN nicht in unverschlüsselten E-Mails zu senden.

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

Anforderung	Anweisung
<p>3.1 Beschränken des Speicherns von Karteninhaberdaten auf ein Minimum. Entwickeln einer Richtlinie zur Datenaufbewahrung und zum Löschen von Daten. Begrenzen der Speichermenge und der Aufbewahrungszeit auf das für geschäftliche, rechtliche und/oder gesetzliche Zwecke Erforderliche, wie in der Richtlinie zur Datenaufbewahrung dokumentiert.</p>	<p>Die erweiterte Speicherung von Karteninhaberdaten, die über das für geschäftliche Zwecke Erforderliche hinausgeht, stellt ein unnötiges Risiko dar. Nur die folgenden Karteninhaberdaten sollten gespeichert werden: primäre Kontonummer bzw. PAN (unleserlich gemacht), Ablaufdatum, Name und Servicecode. Zur Erinnerung: Falls nicht benötigt, nicht speichern!</p>
<p>3.2 Kein Speichern vertraulicher Authentifizierungsdaten nach der Autorisierung (auch wenn diese verschlüsselt sind). Vertrauliche Authentifizierungsdaten umfassen die Daten, die in den folgenden Anforderungen 3.2.1 bis 3.2.3 aufgeführt sind:</p>	<p>Vertrauliche Authentifizierungsdaten umfassen Magnetstreifendaten (bzw. Verfolgungsdaten)⁷, Kartvalidierungscode oder -werte⁸ sowie PIN-Daten⁹. Das Speichern vertraulicher Authentifizierungsdaten nach der Autorisierung ist verboten! Diese Daten sind für böswillige Personen äußerst wertvoll, da sie mithilfe dieser Daten falsche Zahlungskarten erstellen und damit in betrügerischer Absicht Transaktionen durchführen können. Die vollständige Definition für „vertrauliche Authentifizierungsdaten“ finden Sie im <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>.</p>

⁷ Im Magnetstreifen verschlüsselte Daten, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Diese Daten befinden sich außerdem in dem Magnetstreifenabbild auf dem Chip oder an einem anderen Speicherort auf der Karte. Stellen dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifendaten speichern. Die einzigen Elemente der Verfolgungsdaten, die beibehalten werden dürfen, sind die primäre Kontonummer, der Karteninhabername, das Ablaufdatum sowie der Servicecode.

⁸ 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.

⁹ Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht.

Anforderung	Anweisung
<p>3.2.1 Nicht den gesamten Inhalt einer Spur auf dem Magnetstreifen (auf der Kartenrückseite, auf einem Chip oder an anderer Stelle) speichern. 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"> ▪ Name des Karteninhabers ▪ primäre Kontonummer (Primary Account Number, PAN) ▪ Ablaufdatum und ▪ Servicecode <p><i>Um das Risiko zu minimieren, speichern Sie nur die für das Geschäft erforderlichen Datenelemente.</i></p> <p><i>Hinweis: Weitere Informationen finden Sie im PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme.</i></p>	<p>Werden vollständige Verfolgungsdaten (Full Track) gespeichert, können böswillige Personen, die in den Besitz dieser Daten gelangen, Zahlungskarten reproduzieren und auf der ganzen Welt verkaufen.</p>
<p>3.2.2 Kartvalidierungscode 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, nicht speichern.</p> <p><i>Hinweis: Weitere Informationen finden Sie im PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme.</i></p>	<p>Der Zweck des Kartvalidierungscodes besteht im Schutz von Transaktionen, bei denen die Karte nicht physisch vorliegt: Transaktionen per Internet oder Post-/Telefonbestellung (MOTO). In diesen Fällen sind weder der Verbraucher noch die Karte physisch anwesend. Diese Transaktionsarten lassen sich allein durch das Anfordern des Kartvalidierungscodes authentifizieren und auf den Karteninhaber zurückführen, da der Karteninhaber die Karte in den Händen hält und den Wert ablesen kann. Wenn diese verbotenen Daten gespeichert und anschließend gestohlen werden, können böswillige Personen in betrügerischer Weise Transaktionen per Internet oder Post-/Telefonbestellung (MOTO) durchführen.</p>
<p>3.2.3 Keine persönlichen Identifizierungsnummern (PIN) oder verschlüsselten PIN-Blocks speichern.</p>	<p>Diese Werte sollten nur dem Karteninhaber oder der Bank, die die Karte ausgestellt hat, bekannt sein. Wenn diese verbotenen Daten gespeichert und anschließend gestohlen werden, können böswillige Personen in betrügerischer Weise PIN-basierte Abbuchungstransaktionen (z. B. Abheben am Bankautomat) durchführen.</p>

Anforderung	Anweisung
<p>3.3 Tarnen der PAN bei der Anzeige (es dürfen maximal die ersten sechs und die letzten vier Stellen angezeigt werden) <i>Hinweise:</i></p> <ul style="list-style-type: none"> ▪ <i>Diese Anforderung gilt nicht für Mitarbeiter und andere Parteien, die aus bestimmten Gründen die vollständige PAN einsehen müssen.</i> ▪ <i>Diese Anforderung ersetzt nicht strengere Anforderungen für die Anzeige von Karteninhaberdaten – z. B. für POS-Belege.</i> 	<p>Die Anzeige der vollständigen PAN auf Elementen wie Computerbildschirmen, Zahlungskartenbelegen, Faxseiten oder Berichten auf Papier kann zur Folge haben, dass nicht autorisierte Personen in den Besitz dieser Daten gelangen und diese in betrügerischer Weise nutzen. Die vollständige PAN kann auf den „Händlerkopie“-Belegen angezeigt werden, doch sollten Papierbelege die gleichen Sicherheitsanforderungen erfüllen wie elektronische Kopien und die Richtlinien des PCI-Datensicherheitsstandards, insbesondere Anforderung 9 im Hinblick auf die physische Sicherheit, befolgen. Darüber hinaus kann die vollständige PAN auch Personen angezeigt werden, die aus rechtmäßigen geschäftlichen Gründen die vollständige PAN einsehen müssen.</p>
<p>3.4 PAN mindestens überall dort unleserlich machen, wo sie gespeichert wird (auch auf tragbaren digitalen Medien, Sicherungsmedien, 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 ▪ Abkürzung ▪ Index-Token und -Pads (Pads müssen sicher aufbewahrt werden) 	<p>Werden PANs nur unzureichend geschützt, können böswillige Personen diese Daten einsehen und herunterladen. PANs, die im Hauptspeicher gespeichert werden (Datenbanken oder einfache Dateien (Flat Files) wie Textdateien oder Tabellen), und PANs, die nicht im Hauptspeicher gespeichert werden (Sicherungen, Audit-Protokolle, Fehler- und Fehlerbehebungsprotokolle), müssen geschützt werden. Schäden infolge von Diebstahl oder Verlust von Sicherungsbändern während eines Transports können reduziert werden, indem PANs mittels Verschlüsselung, Abkürzung oder Hashing unleserlich gemacht werden. Audit-, Fehlerbehebungs- und Fehlerprotokolle müssen aufbewahrt werden. Doch Sie können die Offenlegung von in Protokollen enthaltenen Daten vermeiden, indem die PANs in den Protokollen unleserlich gemacht (oder entfernt oder getarnt) werden. Die Definition für „starke Kryptographie“ finden Sie im <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>.</p> <p>Mithilfe von auf einer starken Kryptographie basierenden unidirektionalen Hashes (z. B. SHA-1) lassen sich Karteninhaberdaten unleserlich machen. Hash-Funktionen sind dann geeignet, wenn keine Notwendigkeit besteht, die ursprüngliche Nummer abzufragen (unidirektionale Hashes sind nicht umkehrbar).</p> <p>Der Zweck der Abkürzung besteht darin, dass nur ein Teil der PAN (maximal die ersten sechs und letzten vier Stellen) gespeichert wird. Diese Methode unterscheidet sich von der Methode der Tarnung (Masking), bei der zwar die vollständige PAN gespeichert, jedoch bei der Anzeige getarnt wird (d. h. nur ein Teil der PAN wird auf Bildschirmen, Berichten, Belegen usw. angezeigt).</p> <p>Auch mithilfe von Index-Token und -Pads lassen sich Karteninhaberdaten unleserlich machen. Bei einem Index-Token handelt es sich um einen kryptographischen Token, durch den die PAN anhand eines bestimmten Index durch einen unvorhersehbaren Wert ersetzt wird. Ein One-Time-Pad (Einmalverschlüsselung) stellt ein System dar, bei dem ein persönlicher Schlüssel zufällig generiert wird. Dieser Schlüssel wird nur ein einziges Mal zur Verschlüsselung einer Nachricht verwendet, die anschließend unter Verwendung eines One-Time-Pads und eines Schlüssels wieder entschlüsselt wird.</p>

Anforderung	Anweisung
<ul style="list-style-type: none"> ▪ Starke Kryptographie mit entsprechenden Schlüsselmanagementprozessen und -verfahren <p><i>Unter den Kontoinformationen MUSS MINDESTENS die PAN unleserlich gemacht werden.</i></p> <p><i>Hinweise:</i></p> <ul style="list-style-type: none"> ▪ <i>Informationen für den Fall, dass ein Unternehmen die PAN aus irgendeinem Grund nicht unleserlich machen kann, finden Sie in „Anhang B: Kompensationskontrollen“.</i> ▪ <i>Eine Definition für „starke Kryptographie“ finden Sie im PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme.</i> 	<p>Bei der starken Kryptographie (die Definition und Schlüssellänge finden Sie im <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>) erfolgt die Verschlüsselung auf der Grundlage eines branchenweit getesteten und anerkannten Algorithmus (kein proprietärer oder „hauseigener“ Algorithmus).</p>
<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>Diese Anforderung zielt darauf ab, die Akzeptanz der Datenträgerverschlüsselung zur Unkenntlichmachung von Karteninhaberdaten zu erhöhen. Bei der Datenträgerverschlüsselung werden im Massenspeicher eines Computers gespeicherte Daten verschlüsselt und bei der Abfrage durch einen autorisierten Benutzer automatisch entschlüsselt. Datenträgerverschlüsselungssysteme unterbrechen die vom Betriebssystem durchgeführten Lese- und Schreiboperationen und führen die entsprechende kryptographische Umwandlung durch. Hierzu muss der Benutzer lediglich zu Beginn der Sitzung ein Kennwort oder eine Kennwortphrase eingeben. Damit diese Anforderung erfüllt wird, gilt für die Datenträgerverschlüsselungsmethode aufgrund ihrer Merkmale Folgendes:</p> <ol style="list-style-type: none"> 1) Es darf keine direkte Verbindung zum Betriebssystem bestehen. 2) Sie darf keine Entschlüsselungsschlüssel besitzen, die mit Benutzerkonten verbunden sind.
<p>3.5 Schutz von kryptographischen Schlüsseln, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, vor der Weitergabe und vor Missbrauch:</p>	<p>Kryptographische Schlüssel bedürfen eines starken Schutzes, da diese Schlüssel von allen Personen, die Zugang zu ihnen erhalten, zur Entschlüsselung von Daten genutzt werden können.</p>
<p>3.5.1 Beschränken des Zugriffs auf kryptographische Schlüssel auf die unbedingt notwendige Anzahl von Wächtern.</p>	<p>Der Zugang zu kryptographischen Schlüsseln sollte auf wenige Personen, in der Regel nur auf Personen mit einer Verantwortung als Schlüsselwächter beschränkt sein.</p>
<p>3.5.2 Sicheres Speichern von kryptographischen Schlüsseln an möglichst wenigen Speicherorten und in möglichst wenig Formen.</p>	<p>Kryptographische Schlüssel müssen sicher, in der Regel unter Verwendung von Schlüsseln zum Verschlüsseln von Schlüsseln und an verschiedenen Orten gespeichert werden.</p>

Anforderung	Anweisung
3.6 Vollständiges Dokumentieren und Implementieren aller Schlüsselverwaltungsprozesse und -verfahren für kryptographische Schlüssel, die für die Verschlüsselung von Karteninhaberdaten verwendet werden, z. B.:	Die Art und Weise, wie kryptographische Schlüssel verwaltet werden, stellt einen wichtigen Bestandteil der kontinuierlichen Sicherheit der Verschlüsselungslösung dar. Ein guter Schlüsselverwaltungsprozess, unabhängig davon, ob dieser manuell oder automatisch als Bestandteil des Verschlüsselungsprodukts durchgeführt wird, berücksichtigt alle unter 3.6.1 bis 3.6.8 aufgeführten Schlüsselemente.
3.6.1 Generierung starker kryptographischer Schlüssel	Die Verschlüsselungslösung muss starke Schlüssel generieren, wie unter „starke Kryptographie“ im <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i> definiert.
3.6.2 Sichere Verteilung kryptographischer Schlüssel	Die Verschlüsselungslösung muss die Schlüssel auf einem sicheren Wege verteilen, d. h., die Schlüssel werden nicht ungeschützt und nur an die unter 3.5.1 genannten Wächter verteilt.
3.6.3 Sichere Aufbewahrung kryptographischer Schlüssel	Die Verschlüsselungslösung muss Schlüssel sicher speichern, d. h., die Schlüssel werden nicht ungeschützt gespeichert (Verschlüsselung mit einem Schlüssel zur Verschlüsselung von Schlüsseln).
3.6.4 Regelmäßige Änderungen kryptographischer Schlüssel <ul style="list-style-type: none"> • Wie von der jeweiligen Anwendung als notwendig erachtet und empfohlen (z. B. erneute Schlüsselvergabe), vorzugsweise automatisch • Mindestens jährlich 	Befolgen Sie, sofern vorhanden, die vom Anbieter der Verschlüsselungsanwendung bereitgestellten Prozesse oder Empfehlungen für das regelmäßige Ändern von Schlüsseln. Es ist unbedingt erforderlich, dass die Verschlüsselungsschlüssel mindestens einmal im Jahr geändert werden, um das Risiko zu reduzieren, dass eine nicht befugte Person in den Besitz der Verschlüsselungsschlüssel gelangt und Daten entschlüsseln kann.
3.6.5 Entfernung oder Austausch von alten oder vermeintlich beschädigten kryptographischen Schlüsseln	Alte, nicht mehr verwendete oder benötigte Schlüssel sollten entfernt und zerstört werden, um sicherzustellen, dass die Schlüssel nicht weiter verwendet werden können. Wenn alte Schlüssel aufbewahrt werden müssen (z. B. zur Unterstützung archivierter verschlüsselter Daten), sollten sie stark geschützt werden. (Siehe 3.6.6 weiter unten.) Die Verschlüsselungslösung sollte zudem einen Prozess zum Ersetzen von Schlüsseln, von denen bekannt ist oder bei denen vermutet wird, dass sie Sicherheitsangriffen ausgesetzt sind, beinhalten und unterstützen.

Anforderung	Anweisung
<p>3.6.6 Geteiltes Wissen und Festlegen dualer Schlüsselkontrolle</p>	<p>Mit der Methode des geteilten Wissens und der dualen Schlüsselkontrolle soll verhindert werden, dass eine Person Zugriff auf den gesamten Schlüssel hat. Diese Kontrolle findet in der Regel bei manuellen Schlüsselverschlüsselungssystemen Anwendung. Darüber hinaus wird sie angewandt, wenn die Schlüsselverwaltung nicht im dem Verschlüsselungsprodukt implementiert ist. Diese Art der Kontrolle wird im Allgemeinen innerhalb von Hardware-Sicherheitsmodulen implementiert.</p>
<p>3.6.7 Verhinderung des nicht autorisierten Ersatzes von kryptographischen Schlüsseln</p>	<p>Die Verschlüsselungslösung sollte den Ersatz von Schlüsseln, die aus nicht autorisierten Quellen oder unerwarteten Prozessen stammen, nicht zulassen.</p>
<p>3.6.8 Wächter von kryptographischen Schlüsseln müssen ein Formular unterzeichnen, das besagt, dass sie ihre Verantwortung als Schlüsselwächter voll und ganz verstehen und übernehmen.</p>	<p>Durch diesen Prozess wird sichergestellt, dass die betreffende Person ihre Rolle als Schlüsselwächter wahrnimmt und ihre damit verbundene Verantwortung versteht.</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 können zu dauerhaften Zielen böswilliger Personen werden, die diese Sicherheitslücken ausnutzen, um sich privilegierten Zugriff auf Karteninhaberdaten-Umgebungen zu verschaffen.

Anforderung	Anweisung
<p>4.1 Verwenden von starker Kryptographie und Sicherheitsprotokollen wie SSL/TLS oder IPSEC, um vertrauliche Karteninhaberdaten während der Übertragung über offene, öffentliche Netzwerke zu schützen.</p> <p><i>Beispiele für offene, öffentliche Netzwerke, die in den Umfang des PCI-DSS fallen, sind:</i></p> <ul style="list-style-type: none"> ▪ <i>Das Internet</i> ▪ <i>Drahtlose Technologien</i> ▪ <i>GSM-Kommunikationen (Global System for Mobile) und</i> ▪ <i>General Packet Radio Service (GPRS)</i> 	<p>Vertrauliche Informationen müssen während der Übertragung über öffentliche Netzwerke verschlüsselt werden, da eine böswillige Person Daten in dieser Phase einfach und mühelos abfangen und/oder umleiten kann. Secure Sockets Layer (SSL) verschlüsselt Websites und auf ihnen eingegebene Daten. Bei der Verwendung von durch SSL gesicherten Websites muss sichergestellt werden, dass „https“ Bestandteil der URL ist.</p> <p>Beachten Sie, dass die SSL-Vorgängerversionen der Version v3.0 nachgewiesene Schwächen aufweisen, z. B. Pufferüberläufe, die ein Angreifer nutzen kann, um Kontrolle über das betreffende System zu erlangen.</p>

Anforderung	Anweisung
<p>4.1.1 Gewährleisten, 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> <ul style="list-style-type: none"> ▪ <i>Für neue drahtlose Implementierungen ist es nicht zulässig, WEP nach dem 31. März 2009 zu implementieren.</i> ▪ <i>Für bestehende drahtlose Implementierungen ist es nicht zulässig, WEP nach dem 30. Juni 2010 zu implementieren.</i> 	<p>Böswillige Benutzer verwenden frei verfügbare und leicht erhältliche Tools zum Abfangen drahtloser Kommunikation. Durch den Einsatz einer geeigneten Verschlüsselung können das Abfangen und die Offenlegung von vertraulichen Informationen innerhalb des Netzwerks vermieden werden. Viele bekannte Sicherheitsangriffe auf Karteninhaberdaten, die nur im verkabelten Netzwerk gespeichert waren, sind darauf zurückzuführen, dass ein böswilliger Benutzer den Zugang von einem unsicheren drahtlosen Netzwerk erweitert hat.</p> <p>Die starke Verschlüsselung für die Authentifizierung und Übertragung von Karteninhaberdaten ist erforderlich, um böswillige Benutzer daran zu hindern, Zugang zu einem drahtlosen Netzwerk – den Daten im Netzwerk – oder über die drahtlosen Netzwerke Zugang zu anderen internen Netzwerken oder Daten zu erhalten. WEP verwendet keine starke Verschlüsselung. Die WEP-Verschlüsselung sollte niemals als einzige Methode eingesetzt werden, da sie aufgrund von schwachen Initialisierungsvektoren (IV) im WEP-Schlüsselaustauschverfahren und der fehlenden erforderlichen Rotation der Schlüssel für Sicherheitsangriffe anfällig ist. Ein Angreifer kann unter Verwendung von frei verfügbaren Brute-Force-Cracking-Tools eine WEP-Verschlüsselung durchdringen.</p> <p>Die vorhandenen drahtlosen Geräte sollten aktualisiert werden (z. B. Aktualisieren der Access-Point-Firmware auf WPA), um eine starke Verschlüsselung zu unterstützen. Können die vorhandenen Geräte nicht aktualisiert werden, sollten neue Geräte angeschafft werden.</p> <p>Wenn die drahtlosen Netzwerke WEP-basiert sind, sollten diese nicht an Karteninhaberdaten-Umgebungen angeschlossen sein.</p>
<p>4.2 Kein Senden unverschlüsselter PANs über Messaging-Technologien für Endbenutzer (z. B. E-Mail, Instant Messaging, Chat)</p>	<p>Die Kommunikation über E-Mail, Instant Messaging und Chat kann während der Übermittlung zwischen internen und öffentlichen Netzwerken leicht mittels Packet-Sniffing abgefangen werden. Versenden Sie PANs nur dann unter Verwendung dieser Messaging-Tools, wenn sie über Verschlüsselungsfunktionen verfügen.</p>

Anweisungen für Anforderungen 5 und 6: **Wartung eines Anfälligkeits-Managementprogramms**

Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirensoftware

Bösartige 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. Antivirensoftware muss auf allen Systemen eingesetzt werden, die häufig von Malware befallen werden, um Systeme von aktuellen und zukünftigen Bedrohungen durch bösartige Software zu schützen.

Anforderung	Anweisung
<p>5.1 Implementieren von Antivirensoftware auf allen Systemen, die häufig von bösartiger Software befallen werden (insbesondere Personal Computer und Server).</p>	<p>Es finden fortlaufend zahlreiche Angriffe unter Verwendung von weit verbreiteten Exploits, häufig „O-Day-Exploits“ (Veröffentlichung und Verbreitung innerhalb von einer Stunde), gegen anders gesicherte Systeme statt. Ohne eine regelmäßig aktualisierte Antivirensoftware können diese neuen Formen bösartiger Software Ihr Netzwerk angreifen und lähmen.</p> <p>Bösartige Software kann unwissentlich aus dem Internet heruntergeladen und/oder installiert werden. Doch Computer sind auch dann anfällig für Sicherheitsangriffe, wenn austauschbare Speichergeräte wie CDs und DVDs, USB-Speichersticks und Festplatten, digitale Kameras, PDAs (Personal Digital Assistant) und andere Peripheriegeräte verwendet werden. Ohne eine Antivirensoftware können diese Computer Zugangspunkte zu Ihrem Netzwerk werden, und Informationen innerhalb des Netzwerks können in böswilliger Absicht abgefangen werden.</p> <p>Mainframes und die meisten Unix-Systeme gehören in der Regel nicht zu den Systemen, die häufig den Angriffen bösartiger Software ausgesetzt sind. Jede Einheit muss gemäß PCI-DSS-Anforderung 6.2 über einen Prozess zur Identifizierung neuer Sicherheitslücken und zum Umgang mit diesen sowie zur angemessenen Aktualisierung der Konfigurationsstandards und Prozesse verfügen. Auch Entwicklungen im Bereich der bösartigen Software, die sich auf die von der Einheit eingesetzten Betriebssysteme beziehen, sollten bei der Identifikation neuer Sicherheitslücken berücksichtigt werden. Zudem sollten bei Bedarf Methoden zum Umgang mit neuen Entwicklungen in die Konfigurationsstandards des Unternehmens und Schutzmechanismen eingebunden werden.</p> <p>Die folgenden Betriebssysteme sind in der Regel nicht häufig Angriffen durch bösartige Software ausgesetzt: Mainframes sowie bestimmte Unix-Server (z. B. AIX, Solaris und HP-Unix). Jedoch können sich die Branchenentwicklungen im Bereich der bösartigen Software schnell ändern. Daher muss jedes Unternehmen der Anforderung 6.2 entsprechen und über einen Prozess zur Identifizierung neuer Sicherheitslücken und zum Umgang mit diesen sowie zur angemessenen Aktualisierung der Konfigurationsstandards und Prozesse verfügen.</p>

Anforderung	Anweisung
5.1.1 Gewährleisten, dass alle Antivirenprogramme in der Lage sind, alle bekannten Malware-Typen zu erkennen, zu entfernen und davor zu schützen.	Es ist wichtig, dass ein Schutz gegen ALLE Typen und Formen von Malware eingerichtet wird.
5.2 Gewährleisten, dass alle Antivirenmechanismen aktuell sind, aktiv ausgeführt werden und in der Lage sind, Audit-Protokolle zu generieren.	Auch die beste Antivirensoftware kann ihre volle Wirksamkeit nur dann entfalten, wenn aktuelle Antivirensignaturen vorhanden sind oder wenn sie im Netzwerk oder auf einem einzelnen Computer aktiv ausgeführt wird. Mithilfe von Audit-Protokollen lassen sich die Virusaktivität sowie die Antivirusreaktionen überwachen.

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

Skrupellose Personen nutzen Sicherheitslücken aus, um sich 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 Softwarepatches für den Schutz vor Ausnutzung und Beeinträchtigung von Karteninhaberdaten durch böswillige Personen und bösartige Software versehen sein.

Hinweis: Geeignete Softwarepatches 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	Anweisung
<p>6.1 Gewährleisten, dass für alle Systemkomponenten und Softwareanwendungen die neuesten Sicherheitspatches des jeweiligen Herstellers installiert wurden. Wichtige 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>Es finden zahlreiche Angriffe unter Verwendung von weit verbreiteten Exploits, häufig „O-Day-Exploits“ (Veröffentlichung innerhalb einer Stunde), gegen anders gesicherte Systeme statt. Ohne die schnellstmögliche Implementierung der aktuellsten Patches für kritische Systeme, kann eine böswillige Person mithilfe dieser Exploits das Netzwerk angreifen und lähmen. Sie sollten auch die Priorisierung von Änderungen in Erwägung ziehen: Wichtige Sicherheitspatches für kritische oder gefährdete Systemen sollten im Abstand von 30 Tagen installiert werden, während Sicherheitspatches für weniger gefährdete Systeme auch im Abstand von 2 bis 3 Monaten installiert werden können.</p>
<p>6.2 Festlegen eines Prozesses zur Identifizierung neu festgestellter Sicherheitslücken (z. B. Abonnieren von im Internet frei verfügbaren Alarmdiensten). Aktualisieren von Konfigurationsstandards gemäß PCI-DSS-Anforderung 2.2, um neue Sicherheitslückenprobleme anzugehen.</p>	<p>Der Zweck dieser Anforderung besteht darin, dass Unternehmen in Bezug auf ihre Sicherheitslücken auf dem neuesten Stand sind, damit sie ihr Netzwerk angemessen schützen und neu entdeckte wichtige Sicherheitslücken in ihre Konfigurationsstandards einbeziehen können.</p>

Anforderung	Anweisung
<p>6.3 Entwickeln von Softwareanwendungen gemäß PCI-DSS (z. B. sichere Authentifizierung und Protokollierung) und anhand von bewährten Methoden der Branche und Integrieren von Informationssicherheit während des gesamten Softwareentwicklungszyklus. Diese Prozesse müssen Folgendes umfassen:</p>	<p>Wird der Sicherheitsaspekt bei der Festlegung der Anforderungen, der Designanalyse und der Testphase im Rahmen der Softwareentwicklung außer Acht gelassen, besteht die Gefahr, dass Sicherheitslücken versehentlich oder böswillig in die Produktionsumgebung eingeschleust werden.</p>
<p>6.3.1 Testen aller Sicherheitspatches und System- sowie Softwarekonfigurationsänderungen vor der Bereitstellung</p> <p>6.3.1.1 Validierung der gesamten Eingabe (zum Verhindern von siteübergreifender Skripterstellung, Injektionsfehlern, böswilliger Dateiausführung usw.)</p> <p>6.3.1.2 Validierung der ordnungsgemäßen Fehlerbehandlung</p> <p>6.3.1.3 Validierung des sicheren kryptographischen Speichers</p> <p>6.3.1.4 Validierung sicherer Mitteilungen</p> <p>6.3.1.5 Validierung der ordnungsgemäßen rollenbasierten Zugriffssteuerung (RBAC)</p>	<p>Sorgen Sie dafür, dass alle Installationen und Änderungen wunschgemäß funktionieren und dass keine unerwarteten, ungewollten oder schädlichen Funktionen durchgeführt werden.</p>
<p>6.3.2 Separate Entwicklungs-, Test- und Produktionsumgebungen</p>	<p>Entwicklungs- und Testumgebungen sind häufig nicht so sicher wie Produktionsumgebungen. Ohne eine angemessene Trennung können die Produktionsumgebung sowie Karteninhaberdaten aufgrund von Sicherheitslücken oder schwachen internen Prozessen dem Risiko eines Angriffs ausgesetzt sein.</p>
<p>6.3.3 Trennung der Aufgaben von Entwicklungs-, Test- und Produktionsumgebungen</p>	<p>Dadurch wird die Anzahl der Personen verringert, die Zugriff auf die Produktionsumgebung und auf die Karteninhaberdaten haben. Zudem wird sichergestellt, dass nur die Personen Zugriff haben, die diesen Zugriff wirklich benötigen.</p>
<p>6.3.4 Produktionsdaten (Live-PANs) werden nicht zum Testen oder zur Entwicklung verwendet</p>	<p>Die Sicherheitskontrollen in der Entwicklungsumgebung sind in der Regel nicht so strikt. Anhand von Produktionsdaten haben böswillige Personen die Möglichkeit, nicht autorisierten Zugriff auf Produktionsdaten (Karteninhaberdaten) zu erhalten.</p>

Anforderung	Anweisung
<p>6.3.5 Entfernen von Testdaten und -konten vor der Aktivierung der Produktionssysteme</p>	<p>Testdaten und -konten sollten vor der Aktivierung der Anwendung aus dem Produktionscode entfernt werden, da diese Elemente möglicherweise Informationen über die Funktionsweise der Anwendung bereitstellen. Durch den Besitz dieser Informationen könnte der Angriff auf die Anwendung und damit verbundene Karteninhaberdaten vereinfacht werden.</p>
<p>6.3.6 Entfernen benutzerdefinierter Anwendungskonten, Benutzer-IDs und Kennwörter vor der Aktivierung von Anwendungen oder deren Freigabe an Kunden</p>	<p>Benutzerdefinierte Anwendungskonten, Benutzer-IDs und Kennwörter sollten vor der Aktivierung der Anwendung oder ihrer Freigabe an den Kunden aus dem Produktionscode entfernt werden, da diese Elemente möglicherweise Informationen über die Funktionsweise der Anwendung bereitstellen. Durch den Besitz dieser Informationen könnte der Angriff auf die Anwendung und damit verbundene Karteninhaberdaten vereinfacht werden.</p>
<p>6.3.7 Überprüfung benutzerdefinierter Programmcodes vor der Freigabe an 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 gemäß PCI-DSS-Anforderung 6.3. Code-Prüfungen können durch qualifiziertes internes Personal ausgeführt werden. Webanwendungen unterliegen auch zusätzlichen Kontrollen, wenn sie öffentlich sind, um laufende Bedrohungen und Sicherheitslücken nach der Implementierung gemäß der Definition in der PCI-DSS-Anforderung 6.6 anzugehen.</i></p>	<p>Sicherheitslücken in benutzerdefinierten Codes werden häufig von böswilligen Individuen ausgenutzt, um Zugang zu einem Netzwerk zu erhalten und Karteninhaberdaten abzufangen und zu missbrauchen. Personen, die mit sicheren Codierungsverfahren vertraut sind, sollten den Code überprüfen, um potenzielle Sicherheitslücken zu ermitteln.</p>

Anforderung	Anweisung
<p>6.4 Befolgen von Änderungskontrollverfahren für alle Änderungen an Systemkomponenten. Die Verfahren müssen Folgendes umfassen:</p>	<p>Ohne geeignete Softwareänderungskontrollen könnten Sicherheitsfunktionen versehentlich oder absichtlich ausgelassen oder funktionsunfähig gemacht werden. Darüber hinaus könnten Verarbeitungsunregelmäßigkeiten auftreten, oder ein bössartiger Code könnte eingespeist werden. Existieren keine angemessenen Personalrichtlinien für Hintergrundinformationen und Systemzugriffskontrollen, besteht die Gefahr, dass nicht vertrauenswürdige und ungeübte Personen uneingeschränkten Zugriff auf den Softwarecode erhalten, dass entlassene Mitarbeiter die Systeme schädigen können und nicht autorisierte Aktionen unentdeckt bleiben.</p>
<p>6.4.1 Dokumentation der Auswirkungen</p>	<p>Die Auswirkungen der Änderung sollten dokumentiert werden, sodass alle betroffenen Parteien in der Lage sind, sich auf Prozessänderungen angemessen vorzubereiten.</p>
<p>6.4.2 Verwaltung der Abzeichnung durch die jeweiligen Parteien</p>	<p>Die Genehmigung durch das Management zeigt an, dass es sich um eine rechtmäßige, autorisierte und von dem Unternehmen genehmigte Änderung handelt.</p>
<p>6.4.3 Testen der Betriebsfunktionalität</p>	<p>Es sollten profunde Tests durchgeführt werden, um zu überprüfen, ob alle Aktionen gewollt sind, ob Berichte korrekt sind, ob alle möglichen Fehlerbedingungen richtig reagieren usw.</p>
<p>6.4.4 Back-Out-Verfahren</p>	<p>Für alle Änderungen sollten Back-Out-Verfahren eingerichtet sein, falls die Änderung fehlschlägt. Damit ist es möglich, den vorherigen Zustand wiederherzustellen.</p>
<p>6.5 Entwickeln aller Webanwendungen (intern und extern und einschließlich des Webverwaltungszugriffs auf die Anwendung) anhand sicherer Codierungsrichtlinien, z. B. des <i>Open Web Application Security Project Guide</i>. Berücksichtigen der Vorbeugung häufiger Programmierungsanfälligkeiten in Softwareentwicklungsprozessen, einschließlich der folgenden Punkte:</p> <p><i>Hinweis: Die unter 6.5.1 bis 6.5.10 aufgeführten Schwachstellen waren im OWASP-Handbuch zum Zeitpunkt der Veröffentlichung von PCI-DSS v1.2 aktuell. Wenn das OWASP-Handbuch aktualisiert wird, muss jedoch die aktuelle Version für diese Anforderungen verwendet werden.</i></p>	<p>Die Anwendungsebene ist stark gefährdet und kann sowohl internen als auch externen Bedrohungen ausgesetzt sein. Ohne angemessene Sicherheitsmaßnahmen können Karteninhaberdaten und andere vertrauliche Unternehmensinformationen offengelegt werden, was das Unternehmen, dessen Ruf und dessen Kunden schädigen kann.</p>

Anforderung	Anweisung
<p>6.5.1 Siteübergreifendes Scripting (XSS)</p>	<p>Alle Parameter sollten vor der Einbindung überprüft werden. XSS-Lücken treten auf, wenn eine Anwendung vom Benutzer bereitgestellte Daten übernimmt und ohne vorherige Überprüfung oder Verschlüsselung des Inhalts an einen Webbrowser sendet. XSS ermöglicht Angreifern, Skripte im Browser des Opfers durchzuführen, was dazu führen kann, dass Benutzersitzungen angegriffen, Websites verunstaltet, mögliche Würmer eingeschleust werden usw.</p>
<p>6.5.2 Injektionsfehler, insbesondere bei der SQL-Injektion. 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 SQL-Injektionen, treten häufig bei Webanwendungen auf. Es kommt zu einer Injektion, wenn vom Benutzer bereitgestellte Daten im Rahmen eines Befehls oder einer Abfrage an ein interpretierendes Programm gesendet werden. Die feindlichen Daten des Angreifers tricksen das interpretierende Programm aus und veranlassen es, ungewollte Befehle durchzuführen oder Daten zu ändern. Der Angreifer hat die Möglichkeit, Komponenten innerhalb des Netzwerks über die Anwendung anzugreifen, Angriffe, z. B. Pufferüberläufe, einzuleiten oder sowohl vertrauliche Informationen als auch die Funktionen der Serveranwendung offenzulegen. Dies ist auch eine beliebte Methode, um Transaktionen auf Websites mit E-Commerce-Funktionalität in betrügerischer Absicht durchzuführen. Informationen, die aus Webabfragen stammen, sollten vor dem Senden an die Webanwendung validiert werden, z. B. Überprüfen aller alphabetischen Zeichen, der Kombination aus alphabetischen und numerischen Zeichen usw.</p>
<p>6.5.3 Böswillige Dateiausführung</p>	<p>Validieren Sie die Eingabe, um zu überprüfen, dass die Anwendung keine Dateinamen oder Dateien von Benutzern akzeptiert. Ein RFI-anfälliger (Remote File Inclusion) Code ermöglicht Angreifern, feindliche Codes oder Daten einzuschleusen, um zerstörerische Angriffe, z. B. eine vollständige Schädigung des Servers, durchzuführen. Angriffe auf der Basis einer böswilligen Dateiausführung befallen PHP, XML und jedes Framework, das Dateinamen oder Dateien von Benutzern akzeptiert.</p>
<p>6.5.4 Unsichere direkte Objektverweise</p>	<p>Machen Sie interne Objektverweise Benutzern nicht zugänglich. Es kommt zu einem direkten Objektverweis, wenn ein Entwickler einen Verweis zu einem internen Implementierungsobjekt offenlegt, z. B. eine Datei, ein Verzeichnis, ein Datenbankdatensatz oder ein Schlüssel wie eine URL oder ein Formparameter. Angreifer können diese Verweise manipulieren und sich so ohne Autorisierung Zugriff darauf verschaffen.</p>

Anforderung	Anweisung
<p>6.5.5 Cross-Site Request Forgery (CSRF)</p>	<p>Antworten Sie nicht auf Autorisierungsinformationen und Token, die von Browsern automatisch gesendet werden. Ein CSRF-Angriff veranlasst den Browser eines Opfers, eine vorher authentifizierte Abfrage an eine anfällige Webanwendung zu senden, die anschließend den Browser des Opfers veranlasst, eine feindliche Aktion zugunsten des Angreifers durchzuführen. CSRF kann ebenso leistungsfähig sein wie die angegriffene Webanwendung.</p>
<p>6.5.6 Informationslecks und unsachgemäße Fehlerbehandlung</p>	<p>Geben Sie keine Informationen über Fehlermeldungen oder andere Mittel preis. Anwendungen können unbeabsichtigt Informationen über ihre Konfiguration oder internen Abläufe preisgeben oder den Datenschutz durch eine Vielzahl von Anwendungsproblemen gefährden. Angreifer nutzen diese Schwäche aus, um vertrauliche Daten zu stehlen oder noch schwerwiegendere Angriffe durchzuführen. Darüber hinaus liefert die Fehlerbehandlung Informationen, anhand derer eine böswillige Person das System gefährden kann. Wenn eine böswillige Person Fehler erzeugt, die die Webanwendung nicht richtig handhaben kann, kann die Person in den Besitz von detaillierten Systeminformationen gelangen, Denial-of-Service-Unterbrechungen verursachen, ein Fehlschlagen der Sicherheitsmaßnahmen bewirken oder den Server zum Abstürzen bringen. Zum Beispiel: Die Nachricht „Falsches Kennwort“ vermittelt dem Angreifer, dass die Benutzer-ID richtig ist und dass er seine Anstrengungen nur auf das Kennwort ausrichten sollte. Verwenden Sie allgemeinere Fehlermeldungen, z. B. „Daten konnten nicht verifiziert werden“.</p>
<p>6.5.7 Geknackte Authentifizierungs- und Sitzungsverwaltung</p>	<p>Authentifizieren Sie Benutzer ordnungsgemäß, und schützen Sie Kontoanmeldeinformationen und Sitzungs-Token. Kontoanmeldeinformationen und Sitzungs-Token werden häufig nicht ausreichend geschützt. Angreifer hacken Kennwörter, Schlüssel oder Authentifizierungs-Token, um die Identität anderer Benutzer anzunehmen.</p>
<p>6.5.8 Unsicherer kryptographischer Speicher</p>	<p>Verhindern Sie kryptographische Fehler. Webanwendungen setzen kryptographische Funktionen nur selten richtig zum Schutz von Daten und Informationen ein. Angreifer nutzen schwach geschützte Daten, um Identitäten zu stehlen und andere Straftaten, z. B. Kreditkartenbetrug, zu begehen.</p>
<p>6.5.9 Unsichere Mitteilungen</p>	<p>Verschlüsseln Sie alle authentifizierte und vertraulichen Mitteilungen ordnungsgemäß. Anwendungen verschlüsseln den Netzwerkverkehr häufig nicht, wenn es notwendig wäre, vertrauliche Mitteilungen zu schützen.</p>

Anforderung	Anweisung
<p>6.5.10 Unterlassene Einschränkung des URL-Zugriffs</p>	<p>Setzen Sie die Zugriffssteuerung konsistent in der Präsentationsebene und der Geschäftslogik für alle URLs durch. Häufig schützt eine Anwendung vertrauliche Funktionen lediglich, indem sie verhindert, dass Links oder URLs nicht autorisierten Benutzern angezeigt werden. Angreifer können diese Schwäche ausnutzen und sich direkten Zugang zu diesen URLs verschaffen, um nicht autorisierte Aktionen durchzuführen.</p>
<p>6.6 Kontinuierliches Angehen neuer Bedrohungen und Schwachstellen bei öffentlichen Webanwendungen und Gewährleisten, dass diese Anwendungen durch eine 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 öffentliche Webanwendungen finden regelmäßig statt und sind häufig auch erfolgreich. Schlechte Codierungsverfahren machen dies möglich. Die Anforderung, Anwendungen zu überprüfen oder Webanwendungs-Firewalls zu installieren, verfolgt das Ziel, die Anzahl der Angriffe auf öffentliche Webanwendungen, die auf das Hacken von Karteninhaberdaten ausgerichtet sind, erheblich zu reduzieren.</p> <ul style="list-style-type: none"> ▪ Um diese Anforderung zu erfüllen, können manuelle oder automatisierte Tools oder Methoden zum Bewerten der Anwendungssicherheit eingesetzt werden, die Anwendungsschwachstellen prüfen bzw. nach ihnen suchen. ▪ Webanwendungs-Firewalls filtern und blockieren unwichtigen Datenverkehr auf der Anwendungsebene. Ist eine Webanwendungs-Firewall richtig konfiguriert und wird sie in Verbindung mit einer netzwerkbasierter Firewall eingesetzt, können Angriffe auf die Anwendungsebene verhindert werden, die stattfinden können, wenn Anwendungen unzureichend kodiert oder konfiguriert sind. <p><i>Weitere Informationen finden Sie im Informationsnachtrag: Anforderung 6.6 – Anwendungsprüfungen und Webanwendungs-Firewalls – Klärung (www.pcisecuritystandards.org).</i></p>

Anweisungen für 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 für die minimale Menge an Daten und Berechtigungen erteilt werden, die zum Ausüben einer Tätigkeit erforderlich sind.

Anforderung	Anweisung
<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 tätigkeitsbezogene 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 Anforderung für ein vom Management unterzeichnetes Autorisierungsformular, das erforderliche Berechtigungen angibt</p> <p>7.1.4 Implementierung eines automatisierten Zugriffskontrollsystems</p>	<p>Je mehr Personen Zugriff auf Karteninhaberdaten haben, desto größer ist das Risiko, dass ein Benutzerkonto in böswilliger Absicht genutzt wird. Durch die Beschränkung des Zugriffs auf Personen, die aus wichtigen Geschäftsgründen einen Zugriff benötigen, kann Ihr Unternehmen den aufgrund von Unerfahrenheit oder in böswilliger Absicht erfolgten falschen Umgang mit Karteninhaberdaten verhindern. Werden die Zugriffsrechte nur für die minimale Menge an Daten und Berechtigungen, die zur Durchführung einer Aufgabe erforderlich sind, erteilt, wird dies als „Informationsbedarf“ bezeichnet. Werden Berechtigungen auf der Grundlage der Tätigkeitsklassifizierung und -funktion eines Mitarbeiters zugewiesen, wird dies als „rollenbasierte Zugriffssteuerung“ oder RBAC („role-based access control“) bezeichnet. Ihr Unternehmen sollte anhand des Merkmals „Informationsbedarf“ eindeutige Richtlinien und Prozesse zur Datenzugriffssteuerung und anhand des Merkmals „rollenbasierte Zugriffssteuerung“ die Zugriffsart und die Personen, denen Zugriff gewährt wird, festlegen.</p>

Anforderung	Anweisung
<p>7.2 Festlegen eines Mechanismus für Systemkomponenten mit mehreren Benutzern, der den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem muss Folgendes umfassen:</p> <p><i>Hinweis: „Informationsbedarf“ besteht, wenn Zugriffsrechte nur auf die minimale Menge an Daten und Berechtigungen erteilt werden, die zum Ausüben einer Tätigkeit erforderlich sind.</i></p> <p>7.2.1 Abdeckung aller Systemkomponenten</p> <p>7.2.2 Zuweisung von Berechtigungen zu einzelnen Personen anhand der Tätigkeitsklassifizierung und -funktion</p> <p>7.2.3 Standardeinstellung „Alle ablehnen“</p>	<p>Ohne einen Mechanismus zur Beschränkung des Zugriffs anhand des Informationsbedarfs eines Benutzers kann einem Benutzer unwissentlich Zugriff zu Karteninhaberdaten gewährt werden. Der Einsatz eines automatisierten Zugriffskontrollsystems ist für die Verwaltung mehrerer Benutzer unerlässlich. Die Einrichtung dieses System sollte im Einklang mit den Zugriffskontrollrichtlinien und -verfahren Ihres Unternehmens (einschließlich der Berücksichtigung der Merkmale „Informationsbedarf“ und „rollenbasierte Zugriffssteuerung“) erfolgen. Zudem sollte dieses System den Zugriff auf alle Systemkomponenten verwalten und über die Standardeinstellung „Alle ablehnen“ verfügen, um sicherzustellen, dass einer Person nur dann der Zugriff erteilt wird, wenn der Zugriff durch eine entsprechende festgelegte Regel gewährt wird.</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.

Anforderung	Anweisung
<p>8.1 Zuweisen einer eindeutigen Benutzer-ID für alle Benutzer, bevor diesen der Zugriff auf Systemkomponenten oder Karteninhaberdaten gestattet wird.</p>	<p>Durch die Zuweisung einer eindeutigen Kennung für jeden einzelnen Benutzer – anstatt der Verwendung einer ID für mehrere Mitarbeiter – kann ein Unternehmen sicherstellen, dass jeder Einzelne für die eigenen Handlungen verantwortlich ist. Außerdem kann es auf diese Weise einen effektiven Audit-Trail für jeden Mitarbeiter einrichten. Dadurch lässt sich die Problemlösung und -begrenzung bei einem Missbrauch oder einem böswilligen Angriff beschleunigen.</p>
<p>8.2 Neben der Zuweisung einer eindeutigen ID Einsetzen mindestens einer der folgenden Methoden zur Authentifizierung aller Benutzer:</p> <ul style="list-style-type: none"> ▪ Kennwort oder Kennsatz ▪ Zwei-Faktor-Authentifizierung (z. B. Token-Geräte, Smartcards, biometrische Systeme oder öffentliche Schlüssel) 	<p>Werden diese Authentifizierungselemente zusätzlich zu eindeutigen IDs verwendet, trägt dies dazu bei, die eindeutigen Benutzer-IDs vor Angriffen zu schützen (da der Angreifer sowohl die eindeutige ID als auch das Kennwort oder das Authentifizierungselement kennen muss).</p>
<p>8.3 Zwei-Faktor-Authentifizierung beim Remote-Zugriff (Netzwerkzugriff von außerhalb des Netzwerks) von Mitarbeitern, Administratoren und Dritten. Verwenden von Technologien wie Remote-Authentifizierung und Einwähldienst (RADIUS) oder Terminal Access Controller Access Control System (TACACS) mit Token bzw. VPN (basiert auf SSL/TLS oder IPSEC) mit individuellen Zertifikaten.</p>	<p>Die Zwei-Faktor-Authentifizierung erfordert zwei Arten der Authentifizierung für Zugriffe mit einem höheren Risiko, z. B. für Zugriffe von außerhalb Ihres Netzwerks. Um mehr Sicherheit zu erreichen, kann Ihr Unternehmen die Zwei-Faktor-Authentifizierung auch dann einsetzen, wenn von weniger sicheren Netzwerken auf stark gesicherte Netzwerke zugegriffen wird, z. B. von Unternehmenscomputern (geringe Sicherheit) auf Produktionsserver/-datenbanken mit Karteninhaberdaten (hohe Sicherheit).</p>

Anforderung	Anweisung
<p>8.4 Geschützte Übertragung und Speicherung von Kennwörtern auf sämtlichen Systemkomponenten unter Verwendung einer sicheren Verschlüsselung (siehe <i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme</i>).</p>	<p>Zahlreiche Netzwerkgeräte und -anwendungen übertragen die Benutzer-ID und das unverschlüsselte Kennwort innerhalb des Netzwerks und/oder speichern die Kennwörter unverschlüsselt. Eine böswillige Person kann die unverschlüsselte oder lesbare Benutzer-ID sowie das Kennwort während der Übertragung unter Verwendung eines „Sniffers“ abfangen oder unmittelbar auf die Benutzer-ID und unverschlüsselten Kennwörter in den Dateien, in denen sie gespeichert sind, zugreifen und diese gestohlenen Daten anschließend nutzen, um sich nicht autorisierten Zugriff zu verschaffen.</p>
<p>8.5 Einrichten einer geeigneten Benutzerauthentifizierungs- und Kennwortverwaltung für Nichtverbraucherbenutzer und Administratoren auf allen Systemkomponenten auf die folgende Weise:</p>	<p>Da eine böswillige Person, die ein System angreift, zunächst versuchen wird, schwache oder nicht vorhandene Kennwörter zu hacken, ist die Implementierung geeigneter Benutzerauthentifizierungs- und Kennwortverwaltungsverfahren von großer Bedeutung.</p>
<p>8.5.1 Kontrollieren der Vorgänge zum Hinzufügen, Löschen und Ändern von Benutzer-IDs, Anmeldeinformationen und anderen Identifizierungsobjekten.</p>	<p>Um sicherzustellen, dass es sich bei den zu Ihrem System hinzugefügten Benutzern um gültige und anerkannte Benutzer handelt, sollte das Hinzufügen, Löschen und Ändern von Benutzer-IDs von einer kleinen Gruppe von Personen mit spezieller Berechtigung verwaltet und gesteuert werden. Die Berechtigung zur Verwaltung dieser Benutzer-IDs sollte auf diese kleine Gruppe beschränkt sein.</p>
<p>8.5.2 Überprüfen der Benutzeridentität, bevor Kennwörter zurückgesetzt werden.</p>	<p>Viele böswillige Personen setzen das „Social Engineering“ ein (z. B. Anruf beim Helpdesk und Auftreten als rechtmäßiger Benutzer), um ein Kennwort zu ändern und so eine Benutzer-ID verwenden zu können. Stellen Sie sicher, dass solche Fragen angemessen geschützt sind und nicht von mehreren Personen gemeinsam verwendet werden.</p>
<p>8.5.3 Festlegen eindeutiger Werte für die anfänglichen Kennwörter der einzelnen Benutzer und sofortige Änderung nach der ersten Verwendung.</p>	<p>Wird für jeden neu eingerichteten Benutzer dasselbe Kennwort verwendet, könnte ein interner Benutzer, ein ehemaliger Mitarbeiter oder eine böswillige Person dieses Kennwort entweder bereits kennen oder leicht herausfinden und es anschließend nutzen, um sich Zugriff auf Konten zu verschaffen.</p>

Anforderung	Anweisung
<p>8.5.4 Sofortige Deaktivierung des Zugriffs ehemaliger Benutzer.</p>	<p>Hat ein Mitarbeiter, der das Unternehmen verlassen hat, über sein Benutzerkonto weiterhin Zugang zum Netzwerk, könnte es zu einem unnötigen oder in böswilliger Absicht durchgeführten Zugriff auf Karteninhaberdaten kommen. Dieser Zugriff könnte durch einen ehemaligen Mitarbeiter oder eine böswillige Person, die das ältere und/oder ungenutzte Konto missbraucht, erfolgen. Ziehen Sie daher in Betracht, gemeinsam mit der Personalabteilung ein Verfahren zur sofortigen Benachrichtigung im Falle der Kündigung eines Mitarbeiters einzurichten, damit das Benutzerkonto umgehend deaktiviert werden kann.</p>
<p>8.5.5 Entfernen bzw. Deaktivieren inaktiver Benutzerkonten mindestens alle 90 Tage.</p>	<p>Mithilfe von inaktiven Konten kann ein nicht autorisierter Benutzer das ungenutzte Konto missbrauchen, um sich möglicherweise Zugriff auf Karteninhaberdaten zu verschaffen.</p>
<p>8.5.6 Aktivieren der von Anbietern/Lieferanten für die Remote-Wartung verwendeten Konten ausschließlich während der erforderlichen Zeit.</p>	<p>Wenn Sie Anbietern (z. B. POS-Anbietern) rund um die Uhr Zugang zu Ihrem Netzwerk gestatten, falls Ihre Systeme einen entsprechenden Support benötigen, wächst die Gefahr eines nicht autorisierten Zugriffs entweder durch einen Benutzer innerhalb der Anbieterumgebung oder durch eine böswillige Person, die diesen stets verfügbaren externen Zugriffspunkt zu Ihrem Netzwerk entdeckt und ausnutzt. Weitere Informationen zu diesem Thema finden Sie unter 12.3.8 und 12.3.9.</p>
<p>8.5.7 Vermitteln der geltenden Kennwortverfahren und -richtlinien an alle Benutzer mit Zugriff auf Karteninhaberdaten.</p>	<p>Durch das Vermitteln von Kennwortverfahren an alle Benutzer können diese Benutzer die Richtlinien besser verstehen und sich besser an diese halten. Zudem trägt dies zu einer erhöhten Wachsamkeit in Bezug auf Angriffe durch böswillige Personen bei, die möglicherweise versuchen, die Kennwörter der Benutzer auszunutzen, um sich Zugriff auf Karteninhaberdaten zu verschaffen (z. B. durch einen Anruf eines Mitarbeiters, um dessen Kennwort zu erfragen, damit der Anrufer „das Problem beheben“ kann).</p>
<p>8.5.8 Keine Vergabe von Konten und Kennwörtern für Gruppen bzw. mehrere Personen oder die allgemeine Nutzung.</p>	<p>Wenn mehrere Benutzer dasselbe Konto und Kennwort gemeinsam nutzen, ist es nicht mehr möglich, einen Einzelnen für seine Handlungen verantwortlich zu machen oder diese Handlungen effektiv zu protokollieren, denn jedes Mitglied der Gruppe, die das Konto und das Kennwort gemeinsam nutzt, hätte eine bestimmte Handlung durchführen können.</p>
<p>8.5.9 Ändern der Benutzerkennwörter mindestens alle 90 Tage.</p>	<p>Starke Kennwörter stellen die erste Verteidigungslinie für ein Netzwerk dar. Denn eine böswillige Person wird häufig zunächst versuchen, Konten mit</p>

Anforderung	Anweisung
8.5.10 Festlegen einer Mindestlänge für Kennwörter von 7 Zeichen.	schwachen oder nicht vorhandenen Kennwörtern zu finden. Sind Kennwörter kurz, leicht zu erraten oder für eine lange Zeit ohne Veränderung gültig, hat eine böswillige Person mehr Zeit, diese schwachen Konten ausfindig zu machen und, getarnt durch eine gültige Benutzer-ID, ein Netzwerk zu schädigen. Starke Kennwörter können gemäß diesen Anforderungen verstärkt und gepflegt werden, indem die Kennwort- und Kontosicherheitsfunktionen, die in Ihrem Betriebssystem (z. B. Windows) sowie in Ihren Netzwerken, Datenbanken und anderen Plattformen enthalten sind, aktiviert werden.
8.5.11 Verwenden von Kennwörtern, die sowohl numerische als auch alphabetische Zeichen enthalten.	
8.5.12 Festlegen, dass sich ein neues Kennwort von den letzten vier Kennwörtern unterscheiden muss.	
8.5.13 Begrenzen der wiederholten Zugriffsversuche durch Sperren der Benutzer-ID nach spätestens sechs Versuchen.	Sind keine Kontosperrverfahren eingerichtet, kann ein Angreifer laufend versuchen, ein Kennwort mithilfe von manuellen oder automatisierten Tools (z. B. Knacken des Kennwortes) so lange zu erraten, bis er Erfolg hat und Zugriff auf ein Benutzerkonto erlangt.
8.5.14 Festlegen einer Aussperrdauer von mindestens 30 Minuten, innerhalb derer die Benutzer-ID nur durch den Administrator reaktiviert werden kann.	Ist ein Konto infolge des fortlaufenden Versuchs, ein Kennwort zu erraten, gesperrt, hindern Verfahren zur Steuerung der Verschiebung einer Reaktivierung dieser gesperrten Konten die böswillige Person daran, weiterhin das Kennwort zu erraten (sie muss mindestens 30 Minuten warten, bis das Konto reaktiviert wird). Darüber hinaus kann der Administrator oder das Helpdesk, wenn eine Reaktivierung angefordert werden muss, überprüfen, ob der Kontoinhaber die Sperrung (durch Fehler bei der Eingabe) verursacht hat.
8.5.15 Festlegen, dass die Benutzer nach mehr als 15-minütiger Inaktivität das Kennwort erneut eingeben und das Terminal reaktivieren müssen.	Wenn sich ein Benutzer von einem öffentlichen Computer mit Zugang zu wichtigen Netzwerk- und Karteninhaberdaten entfernt, kann dieser Computer in der Abwesenheit des Benutzers von anderen Personen genutzt werden. Dies kann zu einem nicht autorisierten Zugriff auf das Konto und/oder Missbrauch des Kontos führen.
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.	Existiert keine Benutzerauthentifizierung für den Zugriff auf Datenbanken und Anwendungen, wächst das Risiko eines nicht autorisierten oder in böswilliger Absicht durchgeführten Zugriffs. Die Sperrung eines derart erfolgten Zugriffs ist nicht möglich, da der Benutzer nicht authentifiziert wurde und daher dem System nicht bekannt ist. Des Weiteren sollte der Datenbankzugriff ausschließlich programmgesteuert (z. B. über gespeicherte Verfahren) gewährt werden; der direkte Zugriff auf die Datenbank durch den Endbenutzer sollte nicht gestattet werden (mit Ausnahme von DBAs, die zur Durchführung ihrer Verwaltungsaufgaben direkten Zugriff auf die Datenbank haben können).

Anforderung 9: Beschränkung des physischen Zugriffs 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.

Anforderung	Anweisung
<p>9.1 Verwenden angemessener Zugangskontrollen, um den physischen Zugriff auf Systeme für Karteninhaberdaten zu überwachen und zu beschränken.</p>	<p>Ohne physische Zugangskontrollen könnten sich nicht autorisierte Personen potenziell Zugang zum Gebäude und zu vertraulichen Daten verschaffen und die Systemkonfigurationen ändern, Sicherheitslücken im Netzwerk einbauen oder Ausrüstung stehlen oder zerstören.</p>
<p>9.1.1 Überwachen des Zugangs zu zugangsbeschränkten Bereichen mithilfe von Videokameras und anderen Kontrollsystemen. Überprüfen der gesammelten Daten und Korrelation mit anderen Daten. Speichern der Daten mindestens drei Monate lang, wenn dies gesetzlich zulässig ist.</p> <p><i>Hinweis: „Zugangsbeschränkte Bereiche“ sind beispielsweise Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert werden. Hierzu zählen nicht die Bereiche, in denen lediglich Point-of-Sale-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).</i></p>	<p>Bei der Untersuchung physischer Sicherheitsverletzungen können diese Kontrollen bei der Identifizierung von Personen unterstützen, die in Bereiche eingedrungen sind, in denen Karteninhaberdaten gespeichert werden.</p>
<p>9.1.2 Beschränken des physischen Zugriffs auf öffentlich zugängliche Netzwerkbuchsen</p>	<p>Durch die Beschränkung des Zugriffs auf Netzwerkbuchsen werden böswillige Personen daran gehindert, Geräte an unmittelbar verfügbare Netzwerkbuchsen anzuschließen, über die sie möglicherweise Zugriff auf interne Netzwerkkressourcen erhalten könnten. Ziehen Sie in Betracht, ungenutzte Netzwerkbuchsen abzuschalten und nur bei Bedarf zu reaktivieren. In öffentlichen Bereichen, z. B. in Konferenzräumen, sollten Sie private Netzwerke einrichten, über die Anbietern und Besuchern ausschließlich der Zugang zum Internet gewährt wird. Auf diese Weise können Sie verhindern, dass diese Personen in Ihr internes Netzwerk gelangen.</p>

Anforderung	Anweisung
<p>9.1.3 Beschränken des physischen Zugriffs auf WLAN-Zugriffspunkte, Gateways und Handgeräte.</p>	<p>Existieren keine Sicherheitsmaßnahmen für den Zugriff auf drahtlose Komponenten und Geräte, könnten böswillige Benutzer die unbewachten drahtlosen Geräte Ihres Unternehmens nutzen, um sich Zugang zu Netzwerkressourcen zu verschaffen oder sogar um ihre eigenen Geräte an Ihr drahtloses Netzwerk anzuschließen und so nicht autorisierten Zugang zu erhalten. Sie sollten in Betracht ziehen, WLAN-Zugriffspunkte und Gateways an sicheren Orten einzurichten, z. B. in abgeschlossenen Schränken oder Serverräumen. Stellen Sie sicher, dass eine starke Verschlüsselung aktiviert ist. Aktivieren Sie eine automatische Gerätesperrung drahtloser Handgeräte, wenn diese längere Zeit nicht in Benutzung sind, und stellen Sie Ihre Geräte so ein, dass beim Einschalten eine Kennwortabfrage erfolgt.</p>
<p>9.2 Entwickeln von Verfahren, die es dem Personal erleichtern, zwischen Mitarbeitern und Besuchern zu unterscheiden, insbesondere in Bereichen, in denen auf Karteninhaberdaten zugegriffen werden kann. <i>„Mitarbeiter“ bezieht sich hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter und externe Mitarbeiter sowie Berater, die am Standort der jeweiligen Stelle „beheimatet“ sind. Ein „Besucher“ wird als Lieferant, Gast eines Mitarbeiters, Servicepersonal oder jede Person definiert, die die Einrichtung für kurze Zeit betreten muss, meist nicht länger als einen Tag.</i></p>	<p>Ohne Ausweissysteme und Türkontrollen können sich nicht autorisierte und böswillige Benutzer leicht Zugang zu Ihren Einrichtungen verschaffen und wichtige Systeme oder Karteninhaberdaten stehlen, deaktivieren, stören oder zerstören. Um eine optimale Kontrolle sicherzustellen, sollten Sie die Einrichtung von Ausweis- oder Kartenzugangssystemen innerhalb und außerhalb von Arbeitsbereichen, in denen Karteninhaberdaten aufbewahrt werden, in Betracht ziehen.</p>
<p>9.3 Sicherstellen, dass alle Besucher wie folgt behandelt werden:</p>	<p>Besucherkontrollen sind wichtig, um die Chancen von nicht autorisierten und böswilligen Personen zu verringern, Zugang zu Ihren Einrichtungen (und möglicherweise auch zu Karteninhaberdaten) zu erhalten.</p>

Anforderung	Anweisung
<p>9.3.1 Autorisierung vor Betreten von Bereichen, an denen Karteninhaberdaten verarbeitet oder gepflegt werden.</p> <p>9.3.2 Begrenzung der gültigen Zugangserlaubnis (z. B. Ausweis oder Zugangsgesamt) für Besucher, aus der hervorgeht, dass es sich nicht um Mitarbeiter handelt.</p> <p>9.3.3 Bitte um Rückgabe der Zugangserlaubnis, wenn die Besucher die Einrichtung verlassen oder die Erlaubnis ausläuft.</p>	<p>Besucherkontrollen sind wichtig, um sicherzustellen, dass Besucher nur in autorisierte Bereiche gelangen, dass sie als Besucher erkennbar sind, damit Mitarbeiter ihre Aktivitäten überwachen können, und dass der Zugang auf die Dauer eines rechtmäßigen Besuchs begrenzt ist.</p>
<p>9.4 Überprüfen der Besucheraktivität anhand eines Besucherprotokolls. Protokollieren des Namen des Besuchers, des Firmennamens und des Namens des Mitarbeiters, der dem Besucher Zugang gewährt. Aufbewahren des Besucherprotokolls für die Dauer von mindestens drei Monaten, wenn dies gesetzlich zulässig ist.</p>	<p>Ein Besucherprotokoll, in dem ein Mindestmaß an Informationen über den Besucher dokumentiert wird, ist einfach zu führen und nicht kostspielig. Es hilft im Rahmen der Untersuchung einer möglichen Datensicherheitsverletzung dabei, den physischen Zugang zu einem Gebäude oder einem Raum sowie einen möglichen Zugriff auf Karteninhaberdaten zu ermitteln. Sie sollten die Implementierung von Protokollen beim Eingang zu Einrichtungen, insbesondere in Bereichen, in denen Karteninhaberdaten aufbewahrt werden, in Betracht ziehen.</p>
<p>9.5 Aufbewahren von Sicherungsmedien an einem sicheren Ort, vorzugsweise in räumlicher Entfernung, z. B. an einem Alternativ- oder Backup-Standort oder bei einem kommerziellen Anbieter von Lagerkapazitäten. Überprüfen der Sicherheit dieses Standorts mindestens einmal pro Jahr.</p>	<p>Sicherungskopien, die Karteninhaberdaten enthalten und an einem unsicheren Ort aufbewahrt werden, können leicht verloren gehen oder in böswilliger Absicht gestohlen oder kopiert werden. Um eine sichere Aufbewahrung zu gewährleisten, sollten Sie in Erwägung ziehen, einen Vertrag mit einem kommerziellen Anbieter von Lagerkapazitäten zu schließen. Für eine kleinere Einheit käme auch ein Bankschließfach zur Aufbewahrung der Sicherheitskopien in Betracht.</p>

Anforderung	Anweisung
9.6 Sicherstellen der physischen Sicherheit aller Papierdokumente und elektronischen Medien mit Karteninhaberdaten.	Ungeschützte Karteninhaberdaten, die sich auf tragbaren Medien oder auf einem Papierausdruck befinden oder auf dem Schreibtisch einer Person liegengelassen werden, können durch nicht autorisierte Personen eingesehen, kopiert oder durchsucht werden. Sie sollten daher in Betracht ziehen, Verfahren und Prozesse zum Schutz von Karteninhaberdaten einzurichten, die auf an interne und/oder externe Benutzer verteilten Medien enthalten sind. Ohne solche Verfahren können Daten verloren gehen oder gestohlen und in betrügerischer Absicht verwendet werden.
9.7 Strikte Kontrolle der internen bzw. externen Verteilung dieser Art von Medien mit Karteninhaberdaten.	
9.7.1 Klassifizieren der Medien, damit sie als vertraulich identifiziert werden können.	Nicht als vertraulich identifizierte Medien werden möglicherweise nicht mit der notwendigen Sorgfalt behandelt und können verloren gehen oder gestohlen werden. Binden Sie in die in der oben aufgeführten Anforderung 9.6 empfohlenen Verfahren auch ein Medienklassifizierungsverfahren ein.
9.7.2 Senden der Medien per sicherem Kurier oder mit einer anderen Liefermethode, die präzise verfolgt werden kann.	Medien können verloren gehen oder gestohlen werden, wenn sie über eine nicht nachverfolgbare Methode, z. B. auf dem regulären Postweg, versendet werden. Greifen Sie bei der Versendung von Medien mit Karteninhaberdaten auf die Dienste eines sicheren Kurierdienstes zurück, damit Sie mithilfe seiner Nachverfolgungssysteme die Bestände und den Ort von Sendungen nachverfolgen können.
9.8 Sicherstellen, dass das Management den Transfer sämtlicher Medien mit Karteninhaberdaten aus einem geschützten Bereich genehmigen muss (insbesondere dann, wenn die Medien an Einzelne weitergegeben werden).	Karteninhaberdaten, die sichere Bereiche ohne einen durch das Management genehmigten Prozess verlassen, können verloren gehen oder gestohlen werden. Ohne einen soliden Prozess kann weder nachverfolgt werden, an welchem Ort sich die Medien befinden, noch wohin die Daten transferiert und wie sie geschützt werden. Binden Sie in die in der oben genannten Anforderung 9.6 empfohlenen Verfahren auch ein Managementgenehmigungsverfahren ein.
9.9 Strikte Kontrolle der Aufbewahrung und des Zugriffs auf Medien mit Karteninhaberdaten.	Ohne sorgfältige Inventurverfahren und Aufbewahrungskontrollen könnte der Diebstahl oder Verlust von Medien für eine unbestimmte Zeit unbemerkt bleiben. Binden Sie in die in der oben genannten Anforderung 9.6 empfohlenen Verfahren auch ein Verfahren zur Beschränkung des Zugriffs auf Medien mit Karteninhaberdaten ein.
9.9.1 Ordnungsgemäße Verwaltung von Medieninventurlisten und Durchführung mindestens einer jährlichen Medieninventur.	Erfolgt keine Medieninventur, dann bleibt der Diebstahl oder Verlust von Daten möglicherweise lange Zeit unentdeckt. Binden Sie in die in der oben genannten Anforderung 9.6 empfohlenen Verfahren auch ein Verfahren für Medieninventuren und eine sichere Aufbewahrung ein.

Anforderung	Anweisung
9.10 Löschen/Vernichten von Medien mit Karteninhaberdaten, sobald die Daten nicht mehr zu geschäftlichen oder juristischen Zwecken benötigt werden.	Werden auf PC-Festplatten, CDs und Papier enthaltene Daten nur gelöscht und nicht vollständig zerstört, besteht die Gefahr einer Sicherheitsverletzung sowie eines damit einhergehenden finanziellen Schadens und eines Imageverlusts. Böswillige Personen könnten beispielsweise die „Dumpster Diving“-Methode anwenden, bei der Abfalleimer und Papierkörbe durchsucht und gefundene Daten für einen Angriff verwendet werden. Binden Sie in die in der oben genannten Anforderung 9.6 empfohlenen Verfahren auch ein geeignetes Verfahren zur Zerstörung von Medien mit Karteninhaberdaten, einschließlich einer geeigneten Aufbewahrung dieser Medien bis zu ihrer Zerstörung, ein.
9.10.1 Einsatz von Aktenvernichtern für Ausdrücke usw.	
9.10.2 Löschen von Karteninhaberdaten auf elektronischen Medien in einer Art und Weise, die eine Wiederherstellung der Daten unmöglich macht.	

Anweisungen für Anforderungen 10 und 11: Regelmäßige Überwachung und regelmäßiges Testen von Netzwerken

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

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

Anforderung	Anweisung
<p>10.1 Einrichten eines Prozesses zur Verknüpfung des gesamten Zugriffs auf Systemkomponenten (insbesondere des Zugriffs mit Administratorberechtigungen wie root) mit den einzelnen Benutzern.</p>	<p>Die Einrichtung eines Prozesses oder Systems zur Verknüpfung des Benutzerzugriffs auf Systemkomponenten, insbesondere für Benutzer mit Administratorberechtigungen, ist von außerordentlicher Bedeutung. Dieses System erzeugt Audit-Protokolle und bietet die Möglichkeit, verdächtige Aktivitäten auf einen bestimmten Benutzer zurückzuführen. Forensik-Teams, die nach einem Vorfall eingesetzt werden, benötigen diese Protokolle dringend zur Einleitung einer Untersuchung.</p>
<p>10.2 Implementieren automatisierter Audit-Trails für alle Systemkomponenten, um folgende Ereignisse rekonstruieren zu können:</p> <ul style="list-style-type: none"> 10.2.1 Alle individuellen Benutzerzugriffe auf Karteninhaberdaten 10.2.2 Alle von einer Einzelperson mit root- oder Administratorrechten vorgenommene Aktionen 10.2.3 Zugriff auf alle Audit-Trails 10.2.4 Ungültige logische Zugriffsversuche 10.2.5 Verwendung von Identifizierungs- und Authentifizierungsmechanismen 10.2.6 Initialisierung der Audit-Protokolle 10.2.7 Erstellung und Löschen von Objekten auf Systemebene. 	<p>Böswillige Personen im Netzwerk unternehmen häufig mehrere Versuche, um Zugang zu den anvisierten Systemen zu erhalten. Durch die Generierung von Audit-Trails für verdächtige Aktivitäten wird nicht nur der Systemadministrator gewarnt, sondern es werden auch Daten an andere Überwachungssysteme gesendet (z. B. Systeme zur Erkennung von Eindringversuchen) und Verlaufsdaten für eine Nachverfolgung nach dem Vorfall bereitgestellt.</p>

Anforderung	Anweisung
<p>10.3 Aufzeichnen mindestens der folgenden Prüfverfahrenseinträge für alle Systemkomponenten zu jedem Ereignis:</p> <ul style="list-style-type: none"> 10.3.1 Benutzeridentifizierung 10.3.2 Ereignistyp 10.3.3 Datum und Uhrzeit 10.3.4 Erfolg oder Fehler 10.3.5 Ereignisursprung 10.3.6 Identität oder Name der betroffenen Daten, Systemkomponenten oder Ressourcen 	<p>Durch Aufzeichnen dieser Einträge für prüfbare Ereignisse unter 10.2 kann eine potenzielle Gefährdung schnell ausgemacht werden, mit detaillierten Informationen zum „wer, was, wo, wann und wie“.</p>
<p>10.4 Synchronisation aller kritischen Systemuhren und -zeiten.</p>	<p>Personen, die mit böswilligen Absichten auf Netzwerke zugreifen, versuchen oft, die Zeitangaben ihrer Aktionen innerhalb der Prüfprotokolle zu ändern, um zu vermeiden, dass ihre Aktivität entdeckt wird. Für Forensik-Teams, die nach einem Vorfall eingesetzt werden, ist der Zeitpunkt jeder Aktivität äußerst wichtig, um erkennen zu können, wie die Systeme beeinträchtigt wurden. Unter Umständen versuchen böswillige Personen auch, direkt die Uhr auf einem Zeitserver zu ändern, und setzen die Zeit bei mangelhaften Zugriffsbeschränkungen auf einen Zeitpunkt vor dem eigentlichen Zugriff der böswilligen Person zurück.</p>
<p>10.5 Schutz der Prüfverfahren vor Veränderungen.</p> <ul style="list-style-type: none"> 10.5.1 Beschränken der Anzeige der Prüfverfahren auf Personen mit arbeitsbedingtem Bedarf. 10.5.2 Schutz von Prüfverfahrensdateien vor nicht autorisierten Änderungen. 10.5.3 Sofortige Sicherung von Prüfverfahrensdateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen. 10.5.4 Erstellen von Protokollen für nach außen gerichtete Technologien auf einem Protokollserver im internen LAN. 	<p>Böswillige Personen, die auf ein Netzwerk zugegriffen haben, versuchen oft, die Prüfprotokolle zu bearbeiten, um ihre Aktivitäten zu verschleiern. Ohne einen angemessenen Schutz der Prüfprotokolle kann ihre Vollständigkeit, Genauigkeit und Integrität nicht gewährleistet werden. Damit können die Prüfprotokolle für Ermittlungen nach einem Angriff nutzlos werden.</p> <p>Zu einem angemessenen Schutz der Prüfprotokolle gehören eine starke Zugriffskontrolle (beschränken Sie den Zugriff auf Protokolle auf die Personen, die sie wirklich lesen müssen) und die Nutzung interner Trennung (damit die Protokolle schwerer zu finden und zu ändern sind). Durch Schreiben von Protokollen über nach außen gerichtete Technologien wie Drahtlostechnologie, Firewalls, DNS- und Mailserver lässt sich das Risiko eines Verlusts bzw. einer Änderung dieser Protokolle senken, da diese Technologien innerhalb des internen Netzwerks sicherer sind.</p>

Anforderung	Anweisung
<p>10.5.5 Verwendung von Software zur Dateiintegritätsüberwachung und zur Änderungserfassung für Protokolle, um zu gewährleisten, dass bestehende Protokoll Daten nicht geändert werden können, ohne dass Alarme ausgelöst werden (obgleich neue Daten ohne Auslösung von Alarmen hinzugefügt werden können).</p>	<p>Systeme zur Überwachung der Dateiintegrität überprüfen wichtige Dateien auf Änderungen und benachrichtigen den Benutzer, falls Änderungen gefunden wurden. Bei der Überwachung der Dateiintegrität werden üblicherweise Dateien überwacht, die sich nicht regelmäßig ändern. Findet dann doch eine Änderung statt, weist dies auf eine mögliche Gefährdung hin. Bei Protokolldateien (die sich ja häufig ändern) sollte beispielsweise überwacht werden, ob sie gelöscht werden, plötzlich deutlich anwachsen oder kleiner werden, sowie weitere Indikatoren dafür, dass eine Manipulation durch eine böswillige Person stattgefunden hat. Es sind sowohl Standard- als auch Open-Source-Tools für die Überwachung der Dateiintegrität erhältlich.</p>
<p>10.6 Untersuchung der 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. <i>Hinweis: Um die Konformität mit Anforderung 10.6 zu erzielen, können Protokoll-Harvesting-, -Analyse- und Alarmtools eingesetzt werden.</i></p>	<p>Zahlreiche Sicherheitsverletzungen geschehen Tage oder Monate, bevor sie entdeckt werden. Durch tägliches Überprüfen der Protokolle wird die Dauer und Schwere einer potenziellen Gefährdung minimiert. Der Protokollüberprüfungsprozess muss nicht manuell erfolgen. Gerade in Bereichen mit vielen Servern sollten Protokoll-Harvesting-, -Analyse- und Alarmtools in Betracht gezogen werden.</p>
<p>10.7 Aufbewahren der Prüfprotokoll-Verlaufsdaten für den Zeitraum mindestens eines Jahres, wobei ein mindestens dreimonatiger Zeitraum sofort für die Analyse bereitstehen muss (beispielsweise online, archiviert oder aus einer Sicherung wiederherstellbar).</p>	<p>Mit der Aufbewahrung von Protokollen für mindestens ein Jahr wird der Tatsache Rechnung getragen, dass es häufig einige Zeit dauert, bis eine Gefährdung erkannt wird. Ermittler verfügen so über einen genügend langen Protokollverlauf, um die Dauer einer potenziellen Gefährdung sowie die potenziell betroffenen Systeme besser feststellen zu können. Indem ein dreimonatiger Protokollverlauf immer umgehend verfügbar gemacht wird, können die betroffenen Bereiche Datensicherheitsverletzungen schnell erkennen und so die Auswirkungen minimieren. Die standortferne Speicherung von Sicherungsbändern kann zu einer längeren Dauer der Datenwiederherstellung, Analyse und Identifizierung betroffener Systeme oder Daten führen.</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	Anweisung
<p>11.1 Regelmäßige, mindestens einmal im Quartal erfolgende Tests auf WLAN-Zugriffspunkte mit einem Analysegerät oder Einsatz eines Wireless IDS/IPS-Systems zur Ermittlung aller im Betrieb befindlichen drahtlosen Geräte.</p>	<p>Die Implementierung und/oder Nutzung von drahtloser Technologie in einem Netzwerk führt besonders häufig zu Versuchen böswilliger Benutzer, Zugriff auf Netzwerke oder Karteninhaberdaten zu erlangen. Wird ein drahtloses Gerät oder Netzwerk ohne das Wissen eines Unternehmens installiert, kann ein Angreifer ganz leicht und „unsichtbar“ in das Netzwerk gelangen. Zusätzlich zu Analysegeräten können Port-Scanner und weitere Netzwerktools, die drahtlose Geräte erkennen, verwendet werden.</p> <p>Aufgrund der Leichtigkeit, mit der WLAN-Zugriffspunkte eines Netzwerks angegriffen werden können, aufgrund der Schwierigkeiten, solche Angriffe zu erkennen, sowie aufgrund des erhöhten Risikos, das von nicht autorisierten Drahtlosgeräten ausgeht, müssen diese Scans selbst dann durchgeführt werden, wenn die Verwendung von Drahtlostechnologie per Richtlinie untersagt ist.</p> <p>Es sollte zum Reaktionsplan eines Unternehmens gehören, über dokumentierte Verfahrensweisen zu verfügen, die befolgt werden, wenn ein nicht autorisierter WLAN-Zugriffspunkt entdeckt wird. Ein Wireless IDS/IPS-System sollte so konfiguriert werden, dass es automatisch einen Alarm ausgibt. Der Plan muss darüber hinaus aber auch Reaktionsverfahren für den Fall dokumentieren, dass im Zuge eines manuellen Scans ein nicht autorisiertes Gerät erkannt wird.</p>

Anforderung	Anweisung
<p>11.2 Ausführen interner und externer Netzwerkanfälligkeitsscans mindestens vierteljährlich und nach jeder signifikanten Netzwerkänderung (z. B. Installation neuer Systemkomponenten, Änderung der Netzwerktopologie, Modifizierungen von Firewall-Regeln, Produktupgrades).</p> <p><i>Hinweis: Vierteljährliche externe Netzwerkanfälligkeitsscans müssen von einem Approved Scanning Vendor (ASV) durchgeführt werden, der vom Payment Card Industry Security Standards Council (PCI SSC) zugelassen wurde. Nach Netzwerkänderungen durchgeführte Scans können vom internen Personal des Unternehmens ausgeführt werden.</i></p>	<p>Ein Netzwerkanfälligkeitsscan ist ein automatisches Tool, mit dem externe und interne Netzwerkgeräte und Server überprüft werden. Ziel ist es, potenzielle Schwachstellen zu finden und Netzwerk-Ports zu identifizieren, die von böswilligen Personen gefunden und ausgenutzt werden könnten. Werden Schwachstellen gefunden, können die entsprechenden Stellen sie beheben. Daraufhin wird der Scan wiederholt, um sicherzustellen, dass die Schwachstellen aus dem Weg geräumt wurden.</p> <p>Bei der ersten PCI-DSS-Bewertung eines Bereichs kann es sein, dass bislang noch keine vier vierteljährlichen Scans durchgeführt wurden. Wenn die neuesten Scan-Ergebnisse die Kriterien für ein Bestehen erfüllen und Richtlinien und Verfahrensweisen für zukünftige vierteljährliche Scans aufgestellt wurden, gilt diese Anforderung als erfüllt. Es ist nicht notwendig, eine Bewertung „vor Ort“ zu verschieben, um diese Anforderung aufgrund fehlender vier Scans zu erfüllen, wenn diese Bedingungen bereits erfüllt sind.</p>
<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). Diese Penetrationstests müssen Folgendes enthalten:</p> <ul style="list-style-type: none"> 11.3.1 Penetrationstests auf Netzwerkebene 11.3.2 Penetrationstests auf Anwendungsebene 	<p>Penetrationstests auf Netzwerk- und Anwendungsebene unterscheiden sich von Netzwerkanfälligkeitsscans darin, dass Penetrationstests eher manuell durchgeführt werden. Außerdem wird hierbei versucht, einige der bei Scans gefundenen Schwachstellen tatsächlich auszunutzen. Die Tests verwenden dafür Techniken, die auch böswillige Personen nutzen, um schwache Sicherheitssysteme oder -prozesse auszuschalten.</p> <p>Bevor Anwendungen, Netzwerkgeräte und Systeme in die Produktion gehen, sollten sie mithilfe bewährter Sicherheitsmethoden stabilisiert und gesichert werden (gemäß Anforderung 2.2). Mit Netzwerkanfälligkeitsscans und Penetrationstests werden sämtliche verbleibenden Schwachstellen, die später von Angreifern gefunden und ausgenutzt werden könnten, aufgezeigt.</p>

Anforderung	Anweisung
<p>11.4 Nutzung von Systemen zur Erkennung und/oder Verhinderung von Eindringversuchen zur Überwachung des kompletten Datenverkehrs in der Umgebung, in der sich Karteninhaberdaten befinden, und Alarmierung des Personals bei mutmaßlichen Sicherheitsverletzungen. Ständige Aktualisierung der Intrusionserfassungs- und -vorbeugungssysteme.</p>	<p>Diese Systeme vergleichen den im Netzwerk eingehenden Datenverkehr mit bekannten „Signaturen“ tausender Bedrohungstypen (Hackertools, Trojaner und andere Malware) und senden Alarme und/oder stoppen den Eindringversuch sofort. Ohne einen proaktiven Ansatz zur Erkennung nicht autorisierter Aktivitäten mithilfe dieser Tools können Angriffe auf (oder Missbrauch von) Computerressourcen unbemerkt bleiben. Die von diesen Tools generierten Sicherheitsalarme sollten überwacht werden, damit Eindringversuche gestoppt werden können.</p> <p>Es gibt tausende von Bedrohungstypen, und Tag für Tag kommen neue hinzu. Ältere Versionen dieser Systeme kennen die aktuellen „Signaturen“ nicht und können daher neue Schwachstellen, die zu einem unerkannten Datenzugriff führen könnten, nicht feststellen. Die Anbieter dieser Produkte stellen jedoch häufig Updates zur Verfügung, oftmals täglich.</p>
<p>11.5 Bereitstellen von Software zur Überwachung der Dateiintegrität, die einen Alarm ausgibt, wenn es zu nicht autorisierten Änderungen an wichtigen System-, Konfigurations- oder Inhaltsdateien kommt, und Konfiguration der Software für einen mindestens einmal pro Woche durchzuführenden Vergleich wichtiger Dateien.</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 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>Systeme zur Überwachung der Dateiintegrität überprüfen wichtige Dateien auf Änderungen und benachrichtigen den Benutzer, falls Änderungen gefunden wurden. Es sind sowohl Standard- als auch Open-Source-Tools für die Überwachung der Dateiintegrität erhältlich. Bei nicht ordnungsgemäßer Implementierung und Überwachung der Ausgabe von Systemen zur Dateiintegritätsüberwachung könnten böswillige Personen den Inhalt der Konfigurationsdatei, von Betriebssystemprogrammen oder Anwendungsdateien ändern. Solche nicht autorisierten Änderungen können, wenn sie nicht entdeckt werden, dazu führen, dass bestehende Sicherheitskontrollen wirkungslos werden oder dass Karteninhaberdaten ohne nachweisbare Beeinträchtigung der normalen Verarbeitung gestohlen werden.</p>

Anweisung für Anforderung 12: Befolgung einer Informationssicherheits-Richtlinie

Anforderung 12: Befolgen einer Richtlinie zur Informationssicherheit für Mitarbeiter und Subunternehmer

Eine strenge Sicherheitsrichtlinie gibt den Takt für das gesamte Unternehmen vor und dient den Mitarbeitern als Richtschnur dafür, was von ihnen verlangt wird. Sämtliche Mitarbeiter sollten sich darüber im Klaren sein, dass Daten Gefahren ausgesetzt sind und dass sie für deren Schutz verantwortlich sind. „Mitarbeiter“ bezieht sich hierbei auf Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter und externe Mitarbeiter sowie Berater, die am Standort der jeweiligen Stelle „beheimatet“ sind.

Anforderung	Anweisung
<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>12.1.2 Sie umfasst einen jährlichen Prozess zur Ermittlung von Bedrohungen und Anfälligkeiten, der zu einer offiziellen Risikobeurteilung führt.</p> <p>12.1.3 Sie umfasst eine Überprüfung mindestens einmal im Jahr und Aktualisierungen bei Umgebungsänderungen.</p>	<p>Die Unternehmensrichtlinien für Informationssicherheit sind der „Fahrplan“ für die Implementierung von Sicherheitsmaßnahmen, die die wichtigsten Güter des Unternehmens schützen sollen. Eine strenge Sicherheitsrichtlinie gibt den Takt für das gesamte Unternehmen vor und dient den Mitarbeitern als Richtschnur dafür, was von ihnen verlangt wird. Sämtliche Mitarbeiter sollten sich darüber im Klaren sein, dass Daten Gefahren ausgesetzt sind und dass sie für deren Schutz verantwortlich sind.</p> <p>Sicherheitsbedrohungen und Schutzmethoden entwickeln sich innerhalb eines Jahres rasant weiter. Ohne eine Aktualisierung der Sicherheitsrichtlinie mit Blick auf diese Änderungen kann der Kampf gegen neue Bedrohungen nicht gewonnen werden.</p>
<p>12.2 Entwicklung täglicher Betriebssicherheitsverfahren, die den Anforderungen in dieser Spezifikation entsprechen (z. B. Benutzerkonto-Wartungsverfahren und Protokollüberprüfungsverfahren).</p>	<p>Tägliche Betriebssicherheitsverfahren fungieren als „Schreibtischanweisungen“, die von Mitarbeitern in ihre täglichen Systemverwaltungs- und -wartungsaktivitäten eingebunden werden. Nicht dokumentierte Betriebssicherheitsverfahren können dazu führen, dass Mitarbeiter sich nicht über den vollen Umfang ihrer Aufgaben bewusst sind, dass Prozesse von neuen Mitarbeitern nicht einfach wiederholt werden können und dass potenzielle Sicherheitslücken innerhalb der Prozesse entstehen, über die Angreifer Zugriff auf wichtige Systeme und Ressourcen gewinnen können.</p>

Anforderung	Anweisung
<p>12.3 Entwickeln von Verwendungsrichtlinien für wichtige Technologien, mit denen die Mitarbeiter arbeiten (Remote-Zugriffs- und Wireless-Technologien, elektronische Wechselmedien, Notebooks, PDAs, E-Mail-Programme und Browser), und Definition der korrekten Verwendung dieser Technologien für Mitarbeiter und Subunternehmer. Die Verwendungsrichtlinien umfassen folgende Punkte:</p>	<p>Verwendungsrichtlinien für Mitarbeiter können entweder die Nutzung bestimmter Geräte oder sonstiger Technologien verbieten, falls dies die Unternehmensrichtlinien erfordern, oder Mitarbeitern Anweisungen zur richtigen Nutzung und Implementierung geben. Falls keine Verwendungsrichtlinien vorliegen, nutzen Mitarbeiter die Technologien eventuell nicht in Einklang mit den Unternehmensrichtlinien und verschaffen Angreifern so Zugriff auf wichtige Systeme oder Karteninhaberdaten. Beispielsweise könnten ohne Absicht ungesicherte Drahtlosnetzwerke eingerichtet werden. Um sicherzustellen, dass die Unternehmensvorgaben befolgt und ausschließlich genehmigte Technologien implementiert werden, sollte die Implementierung ausschließlich speziellen Betriebsteams vorbehalten sein und nicht von unqualifizierten Mitarbeitern vorgenommen werden.</p>
<p>12.3.1 Ausdrückliche Genehmigung durch das Management</p>	<p>Wenn nicht die ausdrückliche Genehmigung für eine Technologieimplementierung durch das Management erforderlich ist, können Mitarbeiter unter Umständen ohne böse Absicht Lösungen implementieren, die zwar notwendig erscheinen, gleichzeitig aber auch enorme Sicherheitslücken öffnen, über die Angreifer auf wichtige Systeme und Daten zugreifen können.</p>
<p>12.3.2 Authentifizierung zur Verwendung der Technologie</p>	<p>Wenn eine Technologie ohne ordnungsgemäße Authentifizierung (Benutzer-IDs und Kennwörter, Token, VPNs usw.) implementiert wird, können böswillige Personen diese ungeschützte Technologie leicht nutzen, um Zugriff auf wichtige Systeme und Karteninhaberdaten zu erlangen.</p>
<p>12.3.3 Liste aller Geräte und Mitarbeiter mit Zugriff</p>	<p>Böswillige Personen können physische Sicherheitsbarrieren überwinden und dann eigene Geräte als „Hintertür“ in das Netzwerk einbinden. Möglicherweise umgehen auch Mitarbeiter Verfahrensweisen und installieren eigene Geräte. Eine sorgfältig gepflegte Inventarliste mit korrekten Gerätebezeichnungen ermöglicht eine schnelle Erkennung nicht genehmigter Installationen. Es empfiehlt sich, eine offizielle Benennungskonvention für Geräte zu verabschieden und sämtliche Geräte zu kennzeichnen und im Rahmen von Inventuren zu protokollieren.</p>
<p>12.3.4 Etikettierung von Geräten mit Hinweis zu Eigner und Zweck sowie Kontaktinformationen</p>	
<p>12.3.5 Akzeptable Verwendungen dieser Technologien</p>	<p>Durch die Festlegung akzeptabler Geschäftsverwendungen und der Aufbewahrungsorte für vom Unternehmen genehmigte Geräte und Technologien kann das Unternehmen Lücken bei den Konfigurationen und Betriebssteuerungen besser verwalten und kontrollieren, um sicherzustellen, dass Angreifern keine „Hintertür“ zu wichtigen Systemen oder Karteninhaberdaten geöffnet wird.</p>
<p>12.3.6 Akzeptable Netzwerkorte für die Technologien</p>	
<p>12.3.7 Liste der vom Unternehmen zugelassenen Produkte</p>	

Anforderung	Anweisung
<p>12.3.8 Automatisches Trennen von Remote-Zugriffstechnologien nach einer bestimmten Zeit der Inaktivität</p>	<p>Remote-Zugriffstechnologien bieten häufig „Hintertüren“ zu wichtigen Ressourcen und Karteninhaberdaten. Durch Trennen der Remote-Zugriffstechnologien bei Inaktivität (etwa der Technologien, die Ihr POS- oder ein anderer Anbieter für Serviceleistungen an Ihren Systemen nutzt) werden der Zugriff auf und damit das Risiko für Netzwerke minimiert. Es empfiehlt sich, Geräte nach 15 Minuten Inaktivität zu trennen. Weitere Informationen zu diesem Thema finden Sie unter Anforderung 8.5.6.</p>
<p>12.3.9 Aktivierung von Remote-Zugriffstechnologien für Anbieter nur im Bedarfsfall und mit sofortiger Deaktivierung nach der Verwendung</p>	
<p>12.3.10 Karteninhaberdaten können bei einem Remote-Zugriff nicht auf lokale Festplatten und elektronische Wechselmedien kopiert oder verschoben werden.</p>	<p>Um sicherzugehen, dass Ihre Mitarbeiter sich über ihre Verantwortung, Karteninhaberdaten nicht auf ihren PCs oder anderen Medien zu speichern oder zu kopieren, im Klaren sind, sollte eine Unternehmensrichtlinie existieren, in der derartige Aktivitäten klar verboten werden.</p>
<p>12.4 Klare Definition der Sicherheitsverantwortlichkeit aller Mitarbeiter und Subunternehmer in den Sicherheitsrichtlinien und Verfahren.</p>	<p>Ohne klar definierte Sicherheitsrollen und zugewiesene Verantwortlichkeiten kann es zu inkonsistenten Interaktionen mit der Sicherheitsgruppe kommen, was die unsichere Implementierung von Technologien oder die Nutzung veralteter oder unsicherer Technologien zur Folge haben kann.</p>
<p>12.5 Zuweisen der folgenden Managementverantwortungsbereiche in puncto Informationssicherheit zu einer Einzelperson oder einem Team:</p> <p>12.5.1 Festlegen, Dokumentieren und Verteilen von Sicherheitsrichtlinien und -verfahren.</p> <p>12.5.2 Überwachung und Analyse von Sicherheitsalarmen und -informationen und Verteilung an das jeweilige Personal.</p> <p>12.5.3 Festlegen, Dokumentieren und Verteilen von Sicherheitsvorfallreaktions- und Eskalationsverfahren, um eine rechtzeitige und effektive Vorgehensweise in allen Situationen zu gewährleisten.</p> <p>12.5.4 Verwaltung von Benutzerkonten einschließlich Hinzufügen, Löschen und Ändern.</p> <p>12.5.5 Überwachung und Kontrolle des gesamten Datenzugriffs.</p>	<p>Jede Einzelperson oder jedes Team mit Verantwortung für das Management von Informationssicherheit sollte sich seiner Verantwortungsbereiche und Aufgaben dank einer spezifischen Richtlinie bewusst sein. Ist diese Verlässlichkeit nicht gewährleistet, können Prozesslücken entstehen, über die ein Zugriff auf wichtige Ressourcen oder Karteninhaberdaten möglich wird.</p>

Anforderung	Anweisung
12.6 Implementierung eines offiziellen Sicherheitsbewusstseinsprogramms, mit dem allen Mitarbeitern die Bedeutung der Sicherheit der Karteninhaberdaten vermittelt wird.	Wenn Benutzer nicht über ihre Verantwortung für die Sicherheit unterrichtet werden, verlieren Sicherheitsmaßnahmen und -Prozesse, die implementiert wurden, möglicherweise ihre Wirkung, da die Mitarbeiter nicht ordnungsgemäß damit umgehen können.
12.6.1 Schulung der Mitarbeiter bei Einstellung und danach mindestens einmal im Jahr.	Wenn das Sicherheitsbewusstseinsprogramm keine jährlichen Auffrischungen beinhaltet, können wichtige Sicherheitsprozesse und -verfahrensmöglichkeiten möglicherweise vergessen oder umgangen werden, was wiederum zu einer Offenlegung wichtiger Ressourcen und Karteninhaberdaten führen kann.
12.6.2 Mindestens einmal pro Jahr gegebene schriftliche Bestätigung der Mitarbeiter, dass sie die Sicherheitsrichtlinien und -verfahren des Unternehmens kennen.	Durch Anforderung einer (schriftlich oder elektronisch erstellten) Bestätigung Ihrer Mitarbeiter können Sie sicherstellen, dass die Sicherheitsrichtlinien bzw. -verfahrensmöglichkeiten gelesen und verstanden wurden und dass die Mitarbeiter sich verpflichten, diese Richtlinien einzuhalten.
12.7 Prüfen potenzieller Mitarbeiter (siehe Definition unter Punkt 9.2) vor der Einstellung, um das Risiko interner Angriffe so gering wie möglich zu halten. <i>Für Mitarbeiter wie Kassierer und Kassiererinnen, die nur Zugriff auf jeweils eine Kartennummer gleichzeitig haben, wenn eine Transaktion durchgeführt wird, ist diese Anforderung lediglich eine Empfehlung.</i>	Mit gründlichen Ermittlungen zum Hintergrund von potenziellen Mitarbeitern, die bei einer Einstellung Zugriff auf Karteninhaberdaten erhalten, vermindern Sie das Risiko einer nicht autorisierten Nutzung von PANs und anderen Karteninhaberdaten durch Personen mit fragwürdigem oder kriminellem Hintergrund. Es wird erwartet, dass Unternehmen Richtlinien und Verfahrensmöglichkeiten für Hintergrundüberprüfungen haben und genau wissen, welche Ergebnisse der Hintergrundüberprüfungen sich wie auf ihre Einstellungsentscheidung auswirken.
12.8 Umsetzung und Einhaltung von Richtlinien und Verfahren zur Verwaltung von Dienstleistern, falls diese ebenfalls Zugriff auf Karteninhaberdaten erhalten. Hierunter fallen die folgenden Punkte:	Wenn ein Händler oder Dienstleister Karteninhaberdaten mit einem anderen Dienstleister teilt, gelten gewisse Anforderungen, um sicherzustellen, dass die Daten von den Dienstleistern durchgehend geschützt werden.
12.8.1 Führen einer Liste mit Dienstleistern.	Wenn Sie die jeweiligen Dienstleister kennen, lassen sich Risiken, die außerhalb des Unternehmens entstehen können, besser einschätzen.
12.8.2 Schriftliche Vereinbarung, die eine Bestätigung umfasst, dass der Dienstleister für die Sicherheit der Karteninhaberdaten in seinem Besitz haftet.	Gibt der Dienstleister eine solche Bestätigung, zeigt dies, dass er die Sicherheit der ihm ausgehändigten Karteninhaberdaten ernst nimmt und somit als zuverlässig angesehen werden kann.

Anforderung	Anweisung
<p>12.8.3 Festlegung eines eindeutigen Verfahrens für die Inanspruchnahme von Dienstleistern, das die Wahrung der erforderlichen Sorgfalt bei der Wahl des Anbieters unterstreicht.</p>	<p>Hiermit wird sichergestellt, dass jede Inanspruchnahme von Dienstleistern vorher gründlich intern geprüft wird. Zur Prüfung sollte eine Risikoanalyse gehören, die vor dem Eingehen einer offiziellen Beziehung mit dem Dienstleister durchgeführt wird.</p>
<p>12.8.4 Nutzung eines Programms zur Überwachung der Dienstleister-Konformität mit dem PCI-Datensicherheitsstandard.</p>	<p>Mit der Überwachung der PCI-DSS-Konformität eines Dienstleiters kann sichergestellt werden, dass er dieselben Anforderungen erfüllt, die auch für das Unternehmen gelten.</p>
<p>12.9 Implementieren eines Vorfalldaktionsplans, der eine sofortige Reaktion auf Sicherheitsverletzungen im System ermöglicht.</p>	<p>Ohne einen umfassenden Vorfalldaktionsplan, der ordnungsgemäß verteilt und von den verantwortlichen Parteien gelesen und verstanden wird, können Verwirrungen und das Fehlen einer geltenden Reaktionsweise zusätzliche Ausfallzeiten, schlechte Presse und rechtliche Folgen haben.</p>
<p>12.9.1 Erstellen des Vorfalldaktionsplans, der im Falle einer Sicherheitsverletzung im System umgesetzt wird. Der Plan umfasst mindestens die folgenden Punkte:</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 umfassend sein und sämtliche Schlüsselemente enthalten, die Ihrem Unternehmen eine effektive Reaktion im Falle von Angriffen, die Karteninhaberdaten gefährden könnten, ermöglichen.</p>

Anforderung	Anweisung
12.9.2 Testen des Plans mindestens einmal im Jahr.	Ohne ordnungsgemäßes Testen kann es passieren, dass wichtige Schritte zur Risikominderung während eines Vorfalls vergessen werden.
12.9.3 Rund-um-die-Uhr-Bereitstellung von bestimmtem Personal, das auf Alarme reagiert.	Ohne ein geschultes und jederzeit bereites Vorfalldatenzentrum kann zusätzlicher Schaden am Netzwerk entstehen, und wichtige Daten und Systeme werden eventuell durch unsachgemäße Handhabung der Zielsysteme „verschmutzt“. Dies kann den Erfolg einer Ermittlung nach dem Vorfall zunichte machen. Wenn keine internen Ressourcen zur Verfügung stehen, empfiehlt sich die Beauftragung eines entsprechenden Diensteanbieters.
12.9.4 Schulung von Mitarbeitern mit Verantwortung im Bereich der Reaktion auf Sicherheitsverletzungen.	
12.9.5 Beachtung von Alarmen aus Systemen zur Erkennung und/oder Verhinderung von Eindringversuchen und zur Überwachung der Dateiintegrität.	Diese Überwachungssysteme sind darauf ausgelegt, sich auf potenzielle Datenrisiken zu konzentrieren und sind für eine schnelle Reaktion im Falle eines Angriffs unerlässlich. Sie müssen daher Teil der Vorfalldatenzentrenverfahren sein.
12.9.6 Entwickeln eines Prozesses zur Änderung und Weiterentwicklung des Vorfalldatenzentrenplans je nach eigenen Erfahrungen und Branchenentwicklungen.	Nach einem Vorfall „gelernte Lektionen“ sollten in den Vorfalldatenzentrenplan aufgenommen werden, um auf zukünftige Bedrohungen und Sicherheitstrends besser reagieren zu können.

Anweisung für Anforderung A.1: Zusätzliche PCI-DSS-Anforderungen für gemeinsam genutzte Hosting-Anbieter

Anforderung A.1: Gemeinsam genutzte Hosting-Anbieter schützen 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	Anweisung
<p>A.1 Schutz der gehosteten Umgebung und der Daten jeder Stelle (d. h. Händler, Dienstleister oder andere Stelle) entsprechend A.1.1 bis A.1.4: Ein Hosting-Anbieter muss diese Anforderungen sowie die anderen relevanten Abschnitte des PCI-Datensicherheitsstandards erfüllen. <i>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.</i></p>	<p>Anhang A des PCI-DSS wurde für gemeinsam genutzte Hosting-Anbieter verfasst, die Ihren Kunden (Händler und/oder Dienstleister) eine PCI-DSS-konforme Hosting-Umgebung bieten möchten. Diese Schritte sollten eingehalten werden, zusätzlich zu allen weiteren relevanten PCI-DSS-Anforderungen.</p>
<p>A.1.1 Sicherstellen, 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 die Erlaubnis hat, eigene Anwendungen auf dem gemeinsam genutzten Server auszuführen, sollte er diese mit seiner Benutzer-ID ausführen müssen und nicht als Benutzer mit besonderen Rechten. Ein Benutzer mit besonderen Rechten hätte Zugriff auf sämtliche Umgebungen mit Karteninhaberdaten – sowohl beim Händler bzw. Dienstleister als auch beim Unternehmen selbst.</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 Zugriff und Rechte derart eingeschränkt sind, dass jeder Händler oder Dienstleister nur auf die eigene Umgebung mit Karteninhaberdaten zugreifen kann, beachten Sie folgende Punkte: (1) die Berechtigungen der Webserver-Benutzer-ID des Händlers oder Dienstleisters; (2) erteilte Berechtigungen zum Lesen, Schreiben oder Ausführen von Dateien; (3) erteilte Berechtigungen zum Schreiben in Systemdateien; (4) erteilte Berechtigungen für die Protokolldateien des Händlers/Dienstleisters; (5) Kontrollen zur Sicherstellung, dass ein Händler oder Dienstleister keine Monopolstellung bezüglich der Systemressourcen innehaben kann.</p>

Anforderung	Anweisung
A.1.3 Aktivierung eindeutiger mit PCI-DSS-Anforderung 10 konformer Protokollierungs- und Prüfverfahren für die Karteninhaberdaten-Umgebung jeder Stelle.	Protokolle sollten in einer gemeinsam genutzten Hosting-Umgebung zur Verfügung stehen, damit Händler und Dienstanbieter darauf zugreifen und sie entsprechend der jeweiligen Karteninhaberdaten-Umgebung überprüfen können.
A.1.4 Implementieren von Prozessen, um eine rechtzeitige forensische Untersuchung zu ermöglichen, falls die Sicherheit bei einem gehosteten Händler oder Dienstanbieter verletzt wurde.	Gemeinsam genutzte Hosting-Anbieter müssen für den Fall, dass eine forensische Ermittlung erforderlich wird, über Prozesse zur schnellen und einfachen Reaktion verfügen. Diese Prozesse sollten im Detail individuell für den Händler oder Dienstanbieter angepasst sein.

Anhang A: PCI-Datensicherheitsstandard: Damit verbundene Dokumente

Die folgenden Dokumente wurden als Hilfe für Händler und Dienstleister entwickelt, damit sie besser über den PCI-Datensicherheitsstandard und die Anforderungen und Verantwortlichkeiten hinsichtlich der Konformität informiert werden.

Dokument	Publikum
<i>PCI-Datensicherheitsstandard – Anforderungen und Sicherheitsbeurteilungsverfahren</i>	Alle Händler und Dienstleister
<i>PCI-DSS-Navigation: Verständnis der Intention der Anforderungen</i>	Alle Händler und Dienstleister
<i>PCI-Datensicherheitsstandard: Anleitung und Richtlinien zur Selbstbeurteilung</i>	Alle Händler und Dienstleister
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen A und Bescheinigung</i>	Händler ¹⁰
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen B und Bescheinigung</i>	Händler ¹⁰
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen C und Bescheinigung</i>	Händler ¹⁰
<i>PCI-Datensicherheitsstandard: Selbstbeurteilungs-Fragebogen D und Bescheinigung</i>	Händler ¹⁰ und alle Dienstleister
<i>PCI-DSS- und PA-DSS-Glossar für Begriffe, Abkürzungen und Akronyme.</i>	Alle Händler und Dienstleister

¹⁰ Informationen zum Bestimmen des angemessenen Selbstbeurteilungs-Fragebogens finden Sie im Dokument *PCI-Datensicherheitsstandard: Anleitung und Richtlinien zur Selbstbeurteilung* unter „Auswahl des SBF und der Bescheinigung, die für Ihr Unternehmen am besten geeignet sind“.