Zahlungskartenbranche (PCI)

Datensicherheitsstandard (DSS) und Zahlungsanwendung Datensicherheitsstandard (PA-DSS)

Glossar für Begriffe, Abkürzungen und Akronyme

Version 3.2

April 2016

Begriff	Definition
AAA	Akronym für „Authentication“ (Authentifizierung), „Authorization“ (Autorisierung) und „Accounting“ (Abrechnung). Protokoll zur Authentifizierung eines Benutzers basierend auf dessen nachweisbarer Identität, zur Autorisierung eines Benutzers auf Grundlage seiner Benutzerrechte und zur Nachverfolgung des Verbrauchs an Netzwerkressourcen durch den Benutzer.
Zugriffskontrolle	Ein Mechanismus zur Einschränkung der Verfügbarkeit von Informationen oder informationsverarbeitender Ressourcen ausschließlich auf autorisierte Personen oder Anwendungen.
Kontodaten	Kontodaten bestehen aus Karteninhaberdaten und/oder vertraulichen Authentifizierungsdaten. Siehe *Karteninhaberdaten* und *Vertrauliche Authentifizierungsdaten.*
Kontonummer	Siehe *Primary Account Number (PAN).*
Acquirer	Auch als „Handelsbank“, „erwerbende Bank“ bzw. „erwerbendes Finanzinstitut“ bezeichnet. Organisation, typischerweise eine Finanzinstitution, die Transaktionen mit Zahlungskarten für Händler abwickelt und von einer Zahlungsmarke als Acquirer definiert ist. Acquirer unterliegen Zahlungsmarkenregeln und -verfahren hinsichtlich der Händler-Compliance. Siehe auch *Abrechnungsstelle.*
Verwaltungszugriff	Höhere Berechtigungen, die einem Konto zugeteilt werden, damit dieses Systeme, Netzwerke und/oder Anwendungen verwalten kann. Verwaltungszugriffsberechtigungen können dem Konto einer Einzelperson oder einem integrierten Systemkonto zugeteilt werden. Konten mit Verwaltungszugriff werden oft als „superuser“, „root“, „administrator“, „admin“, „sysadmin“ oder „supervisor-state“ bezeichnet, je nach verwendetem Betriebssystem oder Organisationsstruktur.
Adware	Ein schädlicher Softwaretyp der, wenn er installiert wird, den Computer dazu zwingt, automatisch Werbung anzuzeigen oder herunterzuladen.
AES	Akronym für „Advanced Encryption Standard“ (Erweiterter Verschlüsselungsstandard). In der symmetrischen Schlüsselkryptographie verwendete Blockchiffrierung, übernommen von NIST im November 2001 unter der Bezeichnung U.S. FIPS PUB 197 (kurz „FIPS 197“). Siehe *Starke Kryptographie.*
ANSI	Akronym für „American National Standards Institute“ (US-amerikanisches Institut für Normung). Eine private, gemeinnützige Organisation, die das in den USA freiwillige Standardisierungs- und Konformitätsbewertungssystem verwaltet und koordiniert.

Begriff	Definition
Antivirus	Ein Programm oder eine Software, das/die verschiedene Formen schädlicher Software (auch bekannt unter der Bezeichnung „Malware“) erkennen und entfernen kann und vor ihnen Schutz bietet, unter anderem auch vor Viren, Würmern, Trojanern oder Trojanischen Pferden, Spyware, Adware und Rootkits.
AOC	Akronym für „Attestation of compliance“ (Konformitätsbescheinigung). Bei der Konformitätsbescheinigung handelt es sich um ein Formular für Händler und Dienstanbieter, in dem die Ergebnisse einer PCI-DSS-Beurteilung, wie im Selbstbeurteilungsfragebogen bzw. im Konformitätsbericht dokumentiert, dargelegt werden.
AOV	Akronym für „Attestation of validation“ (Validierungsbescheinigung). Bei der Validierungsbescheinigung handelt es sich um ein Formular für PA-QSAs, in dem die Ergebnisse einer PA-DSS-Beurteilung, wie im PA-DSS-Validierungsbericht dokumentiert, dargelegt werden.
Anwendung	Hierzu zählen alle erworbenen oder benutzerspezifischen Softwareprogramme oder Programmgruppen, einschließlich sowohl interne als auch externe (z. B. Web-) Anwendungen.
ASV	Akronym für „Approved Scanning Vendor“ (Zugelassener Scanning-Anbieter). Ein Unternehmen, das vom PCI SSC die Zulassung für externe Services zum Scannen von Anfälligkeiten erhalten hat.
Prüfprotokoll	Auch bezeichnet als „Audit-Trail“. Chronologische Einträge der Systemaktivitäten. Liefern ein unabhängig überprüfbares Trail, das umfassend genug ist, um eine Rekonstruktion, Überprüfung und Untersuchung der Sequenzen in den Umgebungen und den darin stattgefundenen Aktivitäten oder von Vorgängen durchzuführen, die Aufschluss auf den Betrieb, das Verfahren oder Ereignisse einer Transaktion von der Interzeption bis zu den Endergebnissen geben können.
Audit-Trail	Siehe *Prüfprotokoll.*
Authentifizierung	Ein Vorgang zur Überprüfung der Identität einer Person, eines Geräts oder eines Prozesses. Die Authentifizierung erfolgt üblicherweise unter Anwendung eines oder mehrerer der folgenden Authentifizierungsfaktoren: ▪ Etwas, das Sie wissen, wie zum Beispiel ein Kennwort oder ein Kennsatz; ▪ etwas, das Sie haben, wie zum Beispiel ein Token oder eine Smartcard; ▪ etwas, das Sie sind, wie zum Beispiel biometrische Daten.
Authentifizierungsinformationen	Eine Kombination aus dem Benutzernamen oder einer Konto-ID und dem/n eingesetzten Authentifizierungsfaktor/en, um eine Person, ein Gerät oder einen Prozess zu identifizieren.

Begriff	Definition
Autorisierung	Im Zusammenhang mit der Zugriffskontrolle ist die Autorisierung die Gewährung des Zugangs bzw. anderer Rechte eines Benutzers, Programms oder Prozesses. Die Autorisierung bestimmt, wozu eine Person oder ein Programm nach der erfolgreichen Authentifizierung berechtigt ist. Bei einer Transaktion mit einer Zahlungskarte findet die Autorisierung in dem Moment statt, in dem ein Händler die Transaktionsgenehmigung erhält, nachdem der Acquirer die Transaktion beim Kartenemittenten/Verarbeitungsunternehmen gegengeprüft hat.
Sicherheitskopie	Eine zweite Datenkopie zu Archivzwecken oder um sich vor Schadensfällen oder Verlust zu schützen.
BAU	Akronym für „business as usual“ (normaler Betrieb). Unter „BAU“ werden die täglichen betrieblichen Aufgaben in einem Unternehmen zusammengefasst.
Bluetooth	Drahtlosprotokolle, die kurzreichweitige Kommunikationstechnologien für Datenübertragungen über kurze Distanzen einsetzen.
Pufferüberlauf	Ein Sicherheitsrisiko, das durch unsichere Codierungsmethoden verursacht wird. Es beschreibt den Fall, dass ein Programm mit dem Puffer nicht auskommt und Daten einfach in den angrenzenden Speicherbereich schreibt. Pufferüberläufe werden von Angreifern dazu genutzt, sich unerlaubten Zugriff auf Systeme oder Daten zu verschaffen.
Karten-Skimmer	Ein Gerät, das häufig an einem offiziellen Kartenlesegerät angebracht wird und mit dem Zahlungskarteninformationen auf illegale Weise erfasst und/oder gespeichert werden.

Begriff	Definition
Kartenverifizierungscode oder -wert	Auch bekannt als Kartenvalidierungscode oder -wert oder Kartenprüfnummer. Bezieht sich entweder auf: (1) Magnetstreifendaten oder (2) aufgedruckte Sicherheitsmerkmale. (1) Ein Datenelement auf dem Magnetstreifen einer Karte, das die Integrität der Daten auf dem Magnetstreifen mit einem sicheren Verschlüsselungsprozess gewährleistet und mit dem sich jegliche Art von Manipulation oder Fälschung feststellen lässt. Je nach Kreditkartenunternehmen wird dies als CAV, CVC, CVV oder CSC bezeichnet. In der folgenden Liste sind die Begriffe für sämtliche Kreditkartenunternehmen aufgeführt: ▪ **CAV –** Card Authentication Value (JCB-Zahlungskarten) ▪ **PAN CVC –** Card Validation Code (MasterCard-Zahlungskarten) ▪ **CVV –** Card Verification Value (Visa und Discover-Zahlungskarten) ▪ **CSC –** Card Security Code (American Express) (2) Bei Discover, JCB, MasterCard und Visa-Zahlungskarten ist der zweite Typ des Kartenverifizierungswerts oder -codes der rechte dreistellige Wert, der in dem Unterschriftfeld auf der Rückseite der Karte aufgedruckt ist. Bei American Express-Zahlungskarten besteht dieser Code aus vier Ziffern, die über der PAN auf der Vorderseite der Karten aufgedruckt sind. Der Code wird einmalig einem Kartenrohling zugeteilt und bindet die PAN an diesen Rohling. In der folgenden Liste sind die Begriffe für sämtliche Kreditkartenunternehmen aufgeführt: ▪ **CID –** Card Identification Number (American Express und Discover-Zahlungskarten) ▪ **CAV2 –** Card Authentication Value 2 (JCB-Zahlungskarten) ▪ **PAN CVC2 –** Card Validation Code 2 (MasterCard-Zahlungskarten) ▪ **CVV2 –** Card Verification Value 2 (Visa und Discover-Zahlungskarten)
Karteninhaber	Nichtverbraucher oder Verbraucher, denen eine Zahlungskarte ausgestellt wird oder Personen, die befugt sind, die Zahlungskarte zu benutzen.
Karteninhaberdaten	Karteninhaberdaten bestehen mindestens aus der vollständigen PAN. Karteninhaberdaten können auch die vollständige PAN einschließlich folgende Datenelemente umfassen: Name des Karteninhabers, Verfallsdatum und/oder Servicecode Für weitere Datenelemente, die bei einer Zahlungstransaktion übertragen oder verarbeitet (jedoch nicht gespeichert) werden können, siehe *Vertrauliche Authentifizierungsdaten*.

Begriff	Definition
CDE	Akronym für „Cardholder Data Environment“ (Karteninhaberdaten-Umgebung). Personen, Prozesse und Technologien, die Karteninhaberdaten oder vertrauliche Authentifizierungsdaten speichern, verarbeiten oder übertragen.
Mobilfunktechnologien	Mobile Datenübertragung über Drahtlos-Telefonnetze wie z. B. GSM (Global System for Mobile communications), CDMA (Code Division Multiple Access) und GPRS (General Packet Radio Service).
CERT	Akronym für das „Computer Emergency Response Team“ (Computer-Notfallteam) der Carnegie Mellon University. Das CERT-Programm entwickelt und fördert die Nutzung angemessener Technologie- und Systemverwaltungspraktiken, mit denen Systeme Angriffen auf vernetzte Systeme widerstehen. Dadurch lassen sich eventuelle Schäden eindämmen und die Kontinuität wichtiger Systeme gewährleisten.
Änderungskontrolle	Prozesse und Verfahren zur Prüfung und Genehmigung von Änderungen an Systemen und Software vor der Implementierung.
CIS	Akronym für „Center for Internet Security“ (Zentrum für Internetsicherheit). Ein gemeinnütziges Unternehmen, das Organisationen dabei unterstützt, das Risiko von Unterbrechungen des Geschäfts- und E-Commerce-Betriebs aufgrund von unzureichenden technischen Sicherheitskontrollen zu reduzieren.
Verschlüsselung auf Datenbankspaltenebene	Eine Technik oder Technologie (entweder Software oder Hardware) zum Verschlüsseln von Inhalten einer spezifischen Spalte in einer Datenbank im Gegensatz zur Verschlüsselung des gesamten Inhalts der kompletten Datenbank. Alternativ siehe *Festplattenverschlüsselung* oder *Verschlüsselung auf Dateiebene.*

Begriff	Definition
Kompensationskontrollen	Kompensationskontrollen können in den meisten Fällen, in denen eine Stelle eine explizite Anforderung aufgrund legitimer technischer oder dokumentierter geschäftlicher Einschränkungen nicht exakt erfüllen kann, in Erwägung gezogen werden. Voraussetzung hierfür ist jedoch, dass der mit der Nichterfüllung verbundene Risikozuwachs durch die Implementierung anderer Kontrollen kompensiert wird. Kompensationskontrollen müssen: (1) Der Absicht und Genauigkeit der ursprünglichen PCI-DSS-Anforderung entsprechen; (2) Ein ähnliches Verteidigungslevel wie die ursprüngliche PCI-DSS-Anforderung bieten; (3) Über andere PCI-DSS-Anforderungen hinausreichen (nicht nur mit anderen PCI-DSS-Anforderungen konform sein); und (4) Anpassung an das zusätzliche Risiko, das durch die Nichteinhaltung der PCI-DSS-Anforderung entsteht. Siehe „Kompensationskontrollen“ in Anhang B und C in *PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren* für eine Anleitung über die Nutzung von Kompensationskontrollen.
Sicherheitsverletzung	Auch als „Verletzung der Datensicherheit“ bezeichnet. Ein Zugriff auf ein Computersystem, bei dem es unter Umständen zu einer unbefugten Enthüllung von Daten bzw. einem Datendiebstahl, zu Modifikationen an oder zur Vernichtung von Karteninhaberdaten gekommen ist.
Konsole	Bildschirm und Tastatur, die den Zugriff auf und die Steuerung eines Servers, Großrechners oder eines anderen Systemtyps in einer vernetzten Umgebung ermöglichen.
Verbraucher	Eine Person, die Güter oder Services oder beides einkauft.
Kritische Systeme/kritische Technologien	Ein System oder eine Technologie, die von der Organisation als besonders wichtig erachtet wird. Ein kritisches System kann z. B. für die Leistungsfähigkeit eines Betriebsablaufs oder den Erhalt einer Sicherheitsfunktion von entscheidender Bedeutung sein. Beispiele für kritische Systeme sind Sicherheitssysteme, öffentlich zugängliche Geräte und Systeme, Datenbanken und Systeme, in denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Welche spezifischen Systeme und Technologien als kritisch erachtet werden, hängt von der Umgebung und Risikobewertungsstrategie der jeweiligen Organisation ab.
Cross-Site Request Forgery (CSRF)	Ein Sicherheitsrisiko aufgrund von unsicheren Codierungsmethoden. In diesem Fall können über eine authentifizierte Sitzung unerwünschte Aktionen durchgeführt werden. Eine CSRF ist häufig im Zusammenhang mit XSS und/oder SQL-Injektionen zu beobachten.

Begriff	Definition
Siteübergreifendes Scripting (XSS)	Ein Sicherheitsrisiko aufgrund von unsicheren Codierungstechniken, die zu einer unsachgemäßen Validierung der Eingaben führt. XSS ist häufig im Zusammenhang mit CSRF und/oder SQL-Injektionen zu beobachten.
Kryptographischer Schlüssel	Ein Wert, der bei der Verschlüsselung von unverschlüsseltem Text die Ausgabe eines Verschlüsselungsalgorithmus bestimmt. Die Länge des Schlüssels bestimmt in der Regel, wie schwierig die Entschlüsselung des Textes der jeweiligen Mitteilung ist. Siehe *Starke Kryptographie.*

Erstellung kryptografischer Schlüssel	Die Schlüsselerstellung gehört zu den Funktionen der Schlüsselverwaltung. Anerkannte Anleitungen für eine ordnungsgemäße Schlüsselerstellung finden Sie in den folgenden Dokumenten:
	• NIST Special Publication 800-133: Recommendation for Cryptographic Key Generation (Empfehlung für die Erstellung kryptografischer Schlüssel)
	• ISO 11568-2 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle (ISO 11568-2 Finanzservices – Schlüsselmanagement (Handel) – Teil 2: Symmetrische Verschlüsselungsmethoden, ihre Schlüsselverwaltung und Lebenszyklen
	  ○ 4.3 Schlüsselerstellung
	• ISO 11568-4 Financial services — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle (ISO 11568-4 Finanzservices – Schlüsselmanagement (Handel) – Teil 4: Asymmetrische Kryptosysteme – Schlüsselmanagement und Lebenszyklus)
	  ○ 6.2 Schlüssellebenszyklusphasen – Erstellung
	• European Payments Council EPC 342-08 Guidelines on Algorithms Usage and Key Management (Leitfaden zur Algorithmusverwendung und Schlüsselverwaltung)
	  ○ 6.1.1 Schlüsselerstellung [für symmetrische Algorithmen]
	  ○ 6.2.1 Schlüsselerstellung [für asymmetrische Algorithmen]

Management kryptographischer Schlüssel	Eine Reihe von Prozessen und Mechanismen, die die Erstellung und Pflege kryptographischer Schlüssel unterstützen und nach Bedarf ältere Schlüssel durch neue ersetzen.
Kryptographie	Eine Disziplin der Mathematik und der Computerwissenschaften, die sich mit der Informationssicherheit, insbesondere der Verschlüsselung und Authentifizierung, beschäftigt. In Anwendungen und in der Netzwerksicherheit ist es ein Tool zur Steuerung der Zugriffskontrolle sowie des Informationsgeheimnisses und der Datenintegrität.

Begriff	Definition
Schlüssellebensdauer	Die Zeitspanne, in der ein bestimmter kryptographischer Schlüssel für seinen vorbestimmten Zweck eingesetzt werden kann. Diese Zeitspanne basiert beispielsweise auf einem bestimmten Zeitraum und/oder einer bestimmten Menge an generiertem Geheimtext und entspricht bewährten Verfahren und Richtlinien der Branche (z. B. *NIST Special Publication 800-57*).
CVSS	Akronym für „Common Vulnerability Scoring System“ (Allgemeines Bewertungssystem für Sicherheitsrisiken). Ein anbieterunabhängiger offener Branchenstandard zur Bewertung des Schweregrads von Sicherheitsrisiken auf Computersystemen und zur Bestimmung der Dringlichkeit und Priorität der Reaktion. Weitere Informationen finden Sie im *ASV-Programmführer*.
Datenflussdiagramm	Ein Diagramm, aus dem hervorgeht, wie die Daten durch eine Anwendung, ein System oder ein Netzwerk fließen.
Datenbank	Ein strukturiertes Format zur Organisation und Aufrechterhaltung schnell abrufbarer Informationen. Einfache Datenbankbeispiele sind Tabellen und Tabellenkalkulationen.
Datenbankadministrator	Auch kurz als „DBA“ bezeichnet. Eine Person, die für die Verwaltung von Datenbanken verantwortlich ist.
Standardkonten	Ein in einem System, einer Anwendung oder einem Gerät vordefiniertes Konto, um den Zugriff beim Systemerststart zu gewährleisten. Unter Umständen generiert das System auch während des Installationsprozesses Standardkonten.
Standardkennwörter	Ein Kennwort von in einem System, einer Anwendung oder einem Gerät vordefinierten Systemverwaltungs-, Benutzer- und Servicekonten; es ist normalerweise einem Standardkonto zugeordnet. Standardkonten und -kennwörter sind öffentlich zugänglich und allgemein bekannt und können deshalb leicht erraten werden.
Entmagnetisieren	Auch als „Entmagnetisieren von Datenträgern“ bezeichnet. Ein Prozess oder eine Technik, bei der der Datenträger entmagnetisiert wird, sodass alle darauf gespeicherten Daten unwiderruflich gelöscht werden.
Abhängigkeit	Im Kontext des PA-DSS ist eine Abhängigkeit eine bestimmte Software- oder Hardwarekomponente (beispielsweise ein Hardware-Terminal, eine Datenbank, ein Betriebssystem, eine API, eine Codebibliothek usw.), ohne die die Zahlungsanwendung nicht die PA-DSS-Anforderungen erfüllt.
Festplattenverschlüsselung	Eine Technik oder Technologie (entweder Software oder Hardware) zur Verschlüsselung aller auf einem Gerät gespeicherten Daten (z. B. eine Festplatte oder ein Flash-Laufwerk). Alternativ wird die *Verschlüsselung auf Dateiebene* oder die *Verschlüsselung auf Datenbankspaltenebene* zur Verschlüsselung der Inhalte spezifischer Dateien oder Spalten eingesetzt.

Begriff	Definition
DMZ	Abkürzung für „demilitarisierte Zone“. Ein physisches oder logisches Teilnetzwerk, das dem internen privaten Netzwerk eines Unternehmens eine zusätzliche Sicherheitsschicht bietet. Die DMZ bietet eine zusätzliche Netzwerk-Sicherheitsschicht zwischen dem Internet und dem internen Netzwerk eines Unternehmens, damit externe Parteien nur direkte Verbindungen zu Geräten in der DMZ, anstatt dem gesamten internen Netzwerk, aufbauen können.
DNS	Akronym für „Domain Name System“ (Domänennamensystem) bzw. „Domain Name Server“ (Domänennamenserver). Ein System, in dem Informationen im Zusammenhang mit Domänennamen in einer verteilten Datenbank gespeichert werden, damit Benutzern von Netzwerken wie dem Internet Namensauflösungsdienste bereitstehen.
DSS	Akronym für „Datensicherheitsstandard“ (Data Security Standard). Siehe *PA-DSS* und *PCI DSS.*
Doppelte Kontrolle	Ein Prozess, bei dem zwei oder mehr Stellen (normalerweise Personen) eingesetzt werden, um gemeinsam vertrauliche Funktionen oder Informationen zu schützen. Beide Stellen sind gleichermaßen für den physischen Schutz sämtlicher Materialien zuständig, die in risikoreichen Transaktionen verwendet werden. Einzelnen Personen ist weder der Zugriff noch die Verwendung dieser Materialien gestattet (z. B. dem kryptographischen Schlüssel). Beim manuellen Erstellen, Übertragen, Laden, Speichern und Abrufen von Schlüsseln erfordert das Prinzip der doppelten Kontrolle, dass das Wissen zu den Schlüsseln unter den Stellen aufgeteilt wird. (Siehe auch *Geteiltes Wissen.*)
Dynamische Paketfilterung	Siehe *Statusgesteuerte Inspektion.*
ECC	Akronym für „Elliptic Curve Cryptography“ (Elliptische-Kurven-Kryptographie). Eine Methode für öffentliche Kryptographieschlüssel auf der Basis elliptischer Kurven über endlichen Körpern. Siehe *Starke Kryptographie.*
Egress-Filterung	Eine Methode zum Filtern ausgehenden Datenverkehrs, damit nur ausdrücklich zugelassener Datenverkehr das Netzwerk verlassen kann.
Verschlüsselung	Ein Prozess zum Konvertieren von Informationen in ein unleserliches Format, ausgenommen für Inhaber eines spezifischen kryptographischen Schlüssels. Durch die Verschlüsselung werden Informationen zwischen dem Ver- und Entschlüsselungsvorgang (das Gegenteil der Verschlüsselung) vor unerlaubten Freigaben geschützt. Siehe *Starke Kryptographie.*
Verschlüsselungsalgorithmus	Auch als „kryptographischer Algorithmus“ bezeichnet. Eine Sequenz mathematischer Anweisungen, um unverschlüsselten Text oder Daten in verschlüsselten Text oder Daten umzuwandeln und umgekehrt. Siehe *Starke Kryptographie.*

Begriff	Definition
Einheit	Bezeichnet ein Unternehmen, eine Organisation oder einen Betrieb, der sich einer PCI-DSS-Überprüfung unterzieht.
Prüfung der Dateiintegrität	Eine Technik oder Technologie, bei der bestimmte Dateien oder Protokolle überwacht werden, um zu ermitteln, ob sie modifiziert werden. Wenn wichtige Dateien oder Protokolle verändert werden, sollten entsprechende Warnmeldungen an das zuständige Sicherheitspersonal gesendet werden.
Verschlüsselung auf Dateiebene	Eine Technik oder Technologie (entweder Software oder Hardware) zum Verschlüsseln des gesamten Inhalts spezifischer Dateien. Alternativ siehe *Festplattenverschlüsselung* oder *Verschlüsselung auf Datenbankspaltenebene.*
FIPS	Akronym für „Federal Information Processing Standards“ (US-Bundesstandards für die Datenverarbeitung). Standards, die öffentlich von US-amerikanischen Bundesbehörden anerkannt wurden; finden auch für nicht-behördliche Einrichtungen und Unternehmen Anwendung.
Firewall	Hardware- und/oder Softwaretechnologie, die Netzwerkressourcen vor unerlaubten Zugriffen schützt. Eine Firewall lässt Datenverkehr zwischen Netzwerken mit verschiedenen Sicherheitsebenen auf Grundlage einer Reihe von Regeln und anderen Kriterien entweder zu oder lehnt diesen ab.
Forensik	Auch bezeichnet als „IT-Forensik“. Im Zusammenhang mit der Informationssicherheit der Einsatz von Untersuchungstools und Analysetechniken zur Sammlung von Hinweisen von Computerressourcen, mit denen sich die Ursache der Datensicherheitsverletzungen ermitteln lässt.
FTP	Akronym für „File Transfer Protocol“ (Datenübertragungsprotokoll). Ein Netzwerkprotokoll, das zur Übertragung von Daten von einem Computer auf einen anderen über ein öffentliches Netzwerk wie beispielsweise das Internet dient. FTP wird gemeinhin als unsicheres Protokoll angesehen, weil Kennwörter und Dateiinhalte ungeschützt und in Klartext übertragen werden. Jedoch kann FTP mit SSH oder anderen Technologien sicher implementiert werden. Siehe *S-FTP*.
GPRS	Akronym für „General Packet Radio Service“ (Allgemeiner Paket-Funkdienst). Ein mobiler Datendienst, der den Nutzern von GSM-Mobiltelefonen zur Verfügung steht. Anerkannt für seine effektive Nutzung begrenzter Bandbreiten. Besonders geeignet zum Versenden und Empfangen kleiner Datenpakete, wie etwa E-Mails und Webbrowsing.

Begriff	Definition
GSM	Akronym für „Global System for Mobile Communications“ (Globales System für mobile Datenübertragungen). Ein gängiger Standard für Mobiltelefone und -netze. Durch die Allgegenwärtigkeit des GSM-Standards ist das internationale Roaming zwischen Mobiltelefonanbietern zur Normalität geworden, wodurch Anwender ihre Telefone in weiten Teilen der Welt benutzen können.
Hashing	Ein Prozess, bei dem Karteninhaberdaten unleserlich gemacht werden, indem Daten in ein Message-Digest mit einer fixen Länge umgewandelt werden. . Hashing ist eine (mathematische) Funktion, bei der ein bekannter Algorithmus eine beliebig lange Nachricht als Input nimmt und anschließend einen Output mit fester Länge erzeugt (auch als „Hash-Code“ oder „Message-Digest“ bezeichnet). Eine Hash-Funktion muss folgende Eigenschaften aufweisen: (1) Es ist rechnerisch unmöglich, ausschließlich basierend auf dem Hash-Code den Ausgangswert zu ermitteln. (2) Es ist rechnerisch unmöglich, zwei verschiedene Ausgangswerte zu finden, die denselben Hash-Code ergeben. Im Zusammenhang mit dem PCI DSS muss die Hashing-Methode auf die vollständige PAN angewendet werden, damit der Hash-Code als unleserlich betrachtet werden kann. Es wird empfohlen, dass gehashte Karteninhaberdaten einen „Salt“-Wert als Input-Variable für die Hashing-Funktion beinhalten. Hierdurch lässt sich die Effektivität vorab berechneter Rainbow-Table-Angriffe reduzieren oder völlig ausschalten (siehe *Input-Variable*). Weitere Informationen finden Sie in den Branchenstandards, z. B. in den aktuellen Versionen der NIST Special Publications 800-107 und 800-106, des Federal Information Processing Standard (FIPS) 180-4 Secure Hash Standard (SHS) und dem FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (Permutationsbasierte Hash- und erweiterbare Ausgabefunktionen).
Host	Die Hauptcomputerhardware, auf der sich die Computersoftware befindet.
Hosting-Anbieter	Bieten Händlern und anderen Dienstanbietern verschiedene Dienste an. Dabei kann es sich sowohl um einfache als auch komplexe Dienste handeln: Von gemeinsam genutzten „Einkaufswagen“-Optionen und Zahlungsanwendungen bis hin zu Verbindungen zu Zahlungsgateways und -prozessoren und dem dediziertem Hosting von nur einem Kunden pro Server. Ein Hosting-Anbieter kann auch von mehreren Benutzern genutzt werden und mehrere Stellen auf ein und demselben Server hosten.

Begriff	Definition
HSM	Akronym für „Hardware-Sicherheitsmodul“ bzw. „Host-Sicherheitsmodul“. Ein physisch und logisch geschütztes Gerät, das einen sicheren Satz an kryptographischen Services für Kryptographieschlüssel-Verwaltungsfunktionen und/oder die Entschlüsselung von Kontodaten bereitstellt.
HTTP	Akronym für „Hypertext Transfer Protocol“ (Hypertext-Übertragungsprotokoll). Offenes Internetprotokoll zur Übertragung von Informationen im World Wide Web.
HTTPS	Akronym für „Hypertext Transfer Protocol over Secure Socket Layer“ (Sicheres Hypertext-Übertragungsprotokoll). Ein sicheres HTTP mit Authentifizierung und verschlüsselten Kommunikationen über das World Wide Web für die Kommunikation mit hohen Sicherheitsanforderungen, wie etwa webbasierte Anmeldungen.
Hypervisor	Eine Software oder Firmware, die für das Hosten und die Verwaltung virtueller Rechner zuständig ist. Im Zusammenhang mit dem PCI DSS schließt die Hypervisor-Systemkomponente auch den Monitor des virtuellen Rechners ein (VMM).
ID	Kennung eines bestimmten Benutzers oder einer Anwendung.
IDS	Akronym für „Intrusion Detection System“ (System zur Erkennung von Eindringversuchen). Software oder Hardware zur Identifizierung von und Warnung vor Anomalien und Eindringversuchen in Netzwerken bzw. Systemen. Es besteht aus Sensoren, die Sicherheitsereignisse generieren, einer Konsole, die Ereignisse und Warnungen überwacht und die Sensoren kontrolliert sowie einem zentralen Modul, das die von den Sensoren protokollierten Ereignisse in einer Datenbank protokolliert. Warnungen bei erkannten Sicherheitsereignissen werden anhand eines Regelsystems generiert. Siehe *IPS*
IETF	Akronym für „Internet Engineering Task Force“ (Internettechnik-Arbeitsgruppe). Große offene internationale Community von Netzwerkdesignern, Betreibern, Anbietern und Forschern, die sich mit der Entwicklung der Internet-Architektur und dem reibungslosen Betrieb des Internets beschäftigt. Für den IETF gibt es keine formelle Mitgliedschaft, die Community steht allen Interessierten offen.
IMAP	Akronym für „Internet Message Access Protocol“ (Protokoll für den Zugriff auf Internet-Nachrichten). Ein Internetprotokoll auf Anwendungsebene, über das ein E-Mail-Client auf E-Mails zugreifen kann, die sich auf einem Remote-Mailserver befinden.
Index-Token	Ein kryptographisches Token, das die PAN durch einen bestimmten Index für einen unvorhersehbaren Wert ersetzt.
Informationssicherheit	Schutz von Informationen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit.

Begriff	Definition
Informationssystem	Diskreter Satz strukturierter Datenressourcen, der zur Erfassung, Verarbeitung, Verwaltung, Verwendung, gemeinsamen Nutzung, Verbreitung oder Anordnung von Informationen verwendet wird.
Ingress-Filtering	Eine Methode zum Filtern eingehenden Datenverkehrs, damit nur ausdrücklich zugelassener Datenverkehr in das Netzwerk gelangen kann.
Injektionsschwachstellen	Ein Sicherheitsrisiko aufgrund von unsicheren Codierungstechniken, die zu einer unsachgemäßen Validierung des Inputs führen. Dies ermöglicht es Angreifern, bösartigen Code über eine Webanwendung in das zugrundeliegende System zu schleusen. Diese Klasse von Sicherheitsrisiken umfasst SQL-, LDAP- und XPath-Injektionen.
Input-Variable	Eine zufällige Zeichenfolge, die vor der Anwendung einer unidirektionalen Hash-Funktion an die Quelldaten angehängt wird. Input-Variablen können dazu beitragen, die Effektivität von Rainbow-Table-Angriffen zu senken. Siehe auch *Hashing* und *Rainbow Tables.*
Unsicheres Protokoll/Dienste/Port	Ein Protokoll, Dienst oder Port, das/der die Sicherheit aufgrund fehlender Kontrollen der Vertraulichkeit und/oder Intregrität gefährdet. Zu diesen Sicherheitsrisiken gehören Dienste, Protokolle oder Ports, die Daten und Authentifizierungsinformationen (z. B. Kennwörter/Kennsätze) in Klartext über das Internet übertragen oder die aufgrund ihrer Standardeinstellung oder bei Fehlkonfigurationen leicht ausgenutzt werden können. Zu unsicheren Diensten, Protokollen und Ports gehören unter anderem FTP, Telnet, POP3, IMAP und SNMP v1 und v2.
IP	Akronym für „Internet Protocol“ (Internetprotokoll). Ein Protokoll auf Netzwerkebene, das Adress- und einige Steuerinformationen enthält und das Routing von Daten vom Quell- zum Zielhost sowie deren Bereitstellung ermöglicht. IP ist das primäre Netzwerkprotokoll unter den Internetprotokollen. Siehe *TCP*.
IP-Adresse	Auch als „Internetprotokolladresse“ bezeichnet. Ein Zahlencode, mit dem ein bestimmter Computer (Host) im Internet eindeutig identifiziert wird.
IP-Adress-Spoofing	Angriff, bei dem der Angreifer sich unerlaubt Zugriff auf Netzwerke oder Computer verschafft. Der Eindringling sendet trügerische Mitteilungen an einen Computer mit einer IP-Adresse, die scheinbar von einem vertrauten Host stammt.
IPS	Akronym für „Intrusion Prevention System“ (System zur Verhinderung von Eindringversuchen). Zusätzlich zum IDS werden beim IPS Eindringungsversuche blockiert.

Begriff	Definition
IPSEC	Abkürzung für „Internet Protocol Security“ (Internetprotokoll-Sicherheit). Der Standard zum Schutz von IP-Kommunikation auf Netzwerkebene. Für den Schutz werden sämtliche IP-Pakete in einer Kommunikationssitzung verschlüsselt und/oder authentifiziert.
ISO	Im Kontext von Industrienormen und bewährten Verfahren ist ISO, besser bekannt als „International Organization for Standardization“, eine Nicht-Regierungsorganisation, die aus einem Netzwerk nationaler Norminstitute besteht.
Emittent	Eine Stelle, die Zahlungskarten ausstellt oder Ausstellungsservices anbietet, ermöglicht oder unterstützt, einschließlich, aber nicht beschränkt auf Banken und Ausstellungsdienste. Wird auch als „ausstellende Bank“ oder „ausstellendes Finanzinstitut“ bezeichnet.
Ausstellungsdienste	Zu den Ausstellungsdiensten gehören unter anderem die Autorisierung und Kartenpersonalisierung.
LAN	Akronym für „Local Area Network“ (Lokales Netzwerk). Eine Gruppe von Computern und/oder Geräten mit gemeinsamen Kommunikationsleitungen – oft in einem Gebäude oder in mehreren Gebäuden.
LDAP	Akronym für „Lightweight Directory Access Protocol“ (Kompaktes Verzeichniszugriffsprotokoll). Ein Repository für Authentifizierungs- und Autorisierungsdaten, das zur Abfrage und Änderung von Benutzerrechten und zur Erteilung von Zugriffsrechten auf geschützte Ressourcen verwendet wird.
Mindestberechtigung	Die Einräumung der Zugriffs- und/oder Nutzungsrechte, die zur Durchführung der tätigkeitsbezogenen Aufgaben mindestens erforderlich sind.
Protokoll	Siehe *Prüfprotokoll.*
LPAR	Abkürzung für „Logische Partition“. Ein System, bei dem die gesamten Ressourcen eines Computers (Prozessoren, Hauptspeicher und Datenspeicher) in kleinere Einheiten aufgeteilt oder partitioniert werden, die gegebenenfalls mit ihrer eigenen Kopie des Betriebssystems und der Anwendungen laufen können. Die logische Partitionierung wird normalerweise eingesetzt, wenn mehrere verschiedene Betriebssysteme und Anwendungen auf einem einzigen Gerät verwendet werden sollen. Die Partitionen können so konfiguriert werden, dass sie miteinander kommunizieren oder Ressourcen des Servers wie etwa Netzwerkschnittstellen gemeinsam nutzen.
MAC	Im Kryptographie-Kontext ein Akronym für „message authentication code“ (Code zur Nachrichtenauthentifizierung). Ein kleines Informationselement zur Authentifizierung einer Nachricht. Siehe *Starke Kryptographie.*

Begriff	Definition
MAC-Adresse	Abkürzung für „Media Access Control Address“ (Adresse zur Medienzugriffskontrolle). Eine eindeutige vom Hersteller zugewiesene Kennzeichnung von Netzwerkadaptern und Netzwerkschnittstellenkarten.
Magnetstreifendaten	Siehe *Verfolgungsdaten.*
Großrechner	Computer, die dazu dienen, sehr große Mengen an Datenein- und -ausgaben zu verarbeiten und das Durchsatzrechnen hervorzuheben. Großrechner sind in der Lage, mehrere Betriebssysteme auszuführen, und erwecken daher den Anschein aus mehreren Computern zu bestehen. Viele vorhandene Systeme verfügen über ein Großrechnerdesign.
Schädliche Software/Malware	Software oder Firmware, mit der ein Computersystem ohne Wissen oder Zustimmung des Eigentümers infiltriert bzw. beschädigt werden kann und die mit der Absicht eingesetzt wird, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder Betriebssysteme des Eigentümers zu gefährden. Eine solche Software dringt normalerweise in ein Netzwerk ein, während mehrere vom Unternehmen genehmigte Aktivitäten ausgeführt werden. Dies führt zur Ausnutzung von Sicherheitsrisiken. Dazu zählen beispielsweise Viren, Würmer, Trojaner (oder Trojanische Pferde), Spyware, Adware und Rootkits.
Maskierung	Im Rahmen des PCI DSS handelt es sich um eine Methode zum Verbergen eines Datensegments, wenn dieses angezeigt oder ausgedruckt wird. Die Maskierung wird eingesetzt, wenn es aus geschäftlichen Gründen nicht erforderlich ist, die vollständige PAN einzusehen. Die Maskierung trägt zum Schutz der PAN bei, wenn diese angezeigt oder ausgedruckt wird. Siehe Stichwort *Abkürzung*, um Informationen über den Schutz der PAN, wenn diese in Dateien, Datenbanken usw. gespeichert wird, zu erhalten.
Memory-Scraping-Angriffe	Malware-Aktivität, bei der im Hauptspeicher befindliche Daten während der Verarbeitung oder nicht ordnungsgemäß gelöschte bzw. überschriebene Daten extrahiert werden.
Händler	Im Zusammenhang mit dem PCI DSS wird ein Händler als eine Stelle definiert, die Zahlungskarten mit den Logos einer der fünf PCI-DSS-Mitglieder (American Express, Discover, JCB, MasterCard oder Visa) zur Bezahlung von Gütern und/oder Services akzeptiert. Beachten Sie, dass ein Händler, der Zahlungskarten zur Bezahlung von Gütern und/oder Services akzeptiert, auch ein Dienstanbieter sein kann, wenn die verkauften Services im Zusammenhang mit der Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten im Namen anderer Händler oder Dienstanbieter stehen. Ein ISP ist beispielsweise ein Händler, der Zahlungskarten für monatliche Abrechnungen akzeptiert, er ist jedoch auch ein Dienstanbieter, wenn er Händlern Hosting-Dienste anbietet.

Begriff	Definition
MO/TO	Akronym für „Mail-Order/Telephone-Order“ (schriftlicher/telefonischer Bestelleingang)
Überwachung	Der Einsatz von Systemen oder Prozessen zur kontinuierlichen Überwachung von Computer- und Netzwerkressourcen, um das Personal im Fall von Unterbrechungen, Warnmeldungen oder anderen vordefinierten Ereignissen zu alarmieren.
MPLS	Akronym für „Multi-Protocol Label Switching“ (Wechsel zwischen mehreren Protokollen). Ein Netzwerk- oder Telekommunikationsmechanismus, der zur Verbindung einer Gruppe von paketvermittelten Netzwerken dient.
Multi-Faktor-Authentifizierung	Eine Methode zur Authentifizierung eines Benutzers, bei der mindestens zwei Faktoren überprüft werden. Diese Faktoren umfassen etwas, das der Benutzer hat (z. B. eine Smart Card oder einen Dongle), etwas, das der Benutzer weiß (z. B. ein Kennwort, Kennsatz oder eine PIN), oder etwas, das den Benutzer identifiziert (z. B. Fingerabdrücke oder andere biometrische Daten).
NAC	Akronym für „Network Access Control“ (Netzwerkzugriffskontrolle) bzw. „Network Admission Control“ (Netzwerkzugangssteuerung). Eine Methode zur Implementierung von Sicherheitsfunktionen auf Netzwerkebene. Hierfür wird die Verfügbarkeit von Netzwerkressourcen gemäß einer festgelegten Sicherheitsrichtlinie auf Endpunktgeräte beschränkt.
NAT	Akronym für „Network Address Translation“ (Netzwerkadressübersetzung). Wird auch als Netzwerk- oder IP-Maskierung bezeichnet. Die Änderung einer in einem Netzwerk verwendeten IP-Adresse in eine in einem anderen Netzwerk verwendete Adresse. Dadurch erhalten Organisationen interne Adressen, die intern sichtbar sind, und externe Adressen, die nur extern sichtbar sind.
Netzwerk	Zwei oder mehr Computer, die zur gemeinsamen Ressourcennutzung miteinander verbunden sind.
Netzwerkadministrator	Die Person, die für die Verwaltung des Netzwerkes innerhalb einer Einheit verantwortlich ist. Zu den Verantwortlichkeiten gehören unter anderem die Netzwerksicherheit, Installationen, Upgrades, die Wartung und Aktivitätsüberwachung.
Netzwerkkomponenten	Umfassen unter anderem Firewalls, Switches, Router, Zugriffspunkte für drahtlose Netzwerke, Netzwerkgeräte und sonstige Sicherheitsvorrichtungen.
Netzwerkdiagramm	Ein Diagramm mit Systemkomponenten und Verbindungen innerhalb einer Netzwerkumgebung.

Begriff	Definition
Netzwerksicherheitsscan	Ein Prozess, bei dem mithilfe eines manuellen oder automatischen Tools über eine Remoteverbindung die Systeme einer Stelle auf Sicherheitsrisiken überprüft werden. Bei den Sicherheitsscans werden interne und externe Systeme überprüft und Berichte über Dienste, die im Kontakt mit dem Netzwerk stehen, erstellt. Sicherheitsrisiken in Betriebssystemen, Diensten und Geräten, die von Hackern für Angriffe verwendet werden können, werden durch Scans ermittelt.
Netzwerksegmentierung	Wird auch als „Segmentierung“ bzw. „Isolierung“ bezeichnet. *Die Netzwerksegmentierung isoliert Systemkomponenten, die Karteninhaberdaten speichern, verarbeiten oder von Systemen übertragen, die dies nicht tun.* Eine angemessene Netzwerksegmentierung kann den Umfang der Karteninhaberdaten-Umgebung und somit den Umfang der PCI-DSS-Bewertung reduzieren. Siehe den Abschnitt Netzwerksegmentierung in *PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren* für eine Anleitung über die Nutzung der Netzwerksegmentierung. Die Netzwerksegmentierung ist keine PCI-DSS-Anforderung.
Netzwerk-Sniffing	Auch als „Paket-Sniffing“ oder „Sniffing“ bezeichnet. Eine Technik, bei der die Netzwerkkommunikation passiv überwacht wird bzw. Daten zur Kommunikation erfasst und Protokolle decodiert sowie Inhalte auf interessante Informationen hin durchsucht werden.
NIST	Akronym für „National Institute of Standards and Technology“ (Nationales Institut für Normen und Technik). Eine dem Technikreferat des US-Handelsministeriums unterstellte Bundesbehörde ohne Aufsichtsbefugnisse.
NMAP	Eine Software für Sicherheitsscans, die Netzwerke abbildet und offene Ports in Netzwerkressourcen erkennt.
Nichtkonsolen-Zugriff	Der logische Zugriff auf eine Systemkomponente, der über eine Netzwerkschnittstelle und nicht über eine direkte physische Verbindung zur Systemkomponente stattfindet. Der Nichtkonsolen-Zugriff umfasst den Zugriff aus lokalen/internen Netzwerken sowie aus externen Netzwerken bzw. Remote-Netzwerken.
Benutzer, die keine Kunden sind	Alle Personen, außer Karteninhabern, die auf Systemkomponenten zugreifen, u. a. Mitarbeiter, Administratoren und Dritte.
NTP	Akronym für „Network Time Protocol“ (Netzwerkzeitprotokoll). Protokoll zur Synchronisation der Uhren von Computersystemen, Netzwerkgeräten und anderen Systemkomponenten.
NVD	Akronym für „National Vulnerability Database“ (Nationale Datenbank der Sicherheitsrisiken). Die Zusammenstellung der Daten zum auf Standards basierenden Management von Sicherheitsrisiken durch US-Behörden. Die NVD umfasst Datenbanken mit Sicherheits-Checklisten, Sicherheitsrisiken in Software, Fehlkonfigurationen, Produktnamen und Kennzahlen für die Auswirkung von Risiken.

Begriff	Definition
OCTAVE®	Akronym für „Operationally Critical Threat, Asset, and Vulnerability Evaluation“ (Bewertung wichtiger Bedrohungen, Ressourcen und Risiken). Ein Paket aus Tools, Techniken und Methoden für die strategische Bewertung und Planung der risikobasierten Informationssicherheit.
Seriengefertigt	Beschreibt Produkte, die in Form von Lagerbeständen aufbewahrt werden und weder kundenspezifisch noch für einen bestimmten Benutzer- oder Anwendertyp entwickelt wurden und die schnell zur Verfügung gestellt werden können.
Betriebssystem/OS	Die Software eines Computersystems, die für die Verwaltung und Koordination aller Aktivitäten, einschließlich der Verteilung von Computerressourcen verantwortlich ist. Beispiele für Betriebssysteme sind unter anderen Microsoft Windows, Mac OS, Linux und Unix.
Organisatorische Unabhängigkeit	Eine Organisationsstruktur, bei der es keine Interessenkonflikte zwischen der für die Durchführung der Aktivität zuständigen Person/Abteilung und der für die Bewertung dieser Aktivität zuständigen Person/Abteilung gibt. So müssen Personen, die Bewertungen durchführen, organisatorisch vom Management der zu bewertenden Umgebung getrennt sein.
OWASP	Akronym für „Open Web Application Security Project“ (Sicherheitsprojekt für offene Webanwendungen). Eine gemeinnützige Organisation mit Schwerpunkt auf der Verbesserung der Sicherheit von Anwendungssoftware. OWASP führt eine Liste mit nennenswerten Sicherheitsrisiken in Webanwendungen. (Siehe http://www.owasp.org).
PA-DSS	Akronym für „Payment Application Datensicherheitsstandard“ (Zahlungsanwendung Datensicherheitsstandard).
PA-QSA	Akronym für „Payment Application Qualified Security Assessor“ (Akkreditierte Sicherheitsgutachter für Zahlungsanwendungen). PA-QSAs erhalten von PCI SSC eine Qualifizierung zur Beurteilung der Zahlungsanwendungen im Hinblick auf die PA-DSS-Anforderungen. Details zu den Anforderungen an PA-QSA-Unternehmen und -Mitarbeiter finden Sie im *PA-DSS-Programmleitfaden* und unter *PA-QSA-Qualifikationen*.
Pad	In der Kryptografie ist der One-Time-PAD ein Verschlüsselungsalgorithmus mit einer Kombination aus Text und einem Zufallsschlüssel oder „PAD“, der die gleiche Länge wie der Klartext hat und nur einmal verwendet wird. Wenn der Schlüssel außerdem wirklich zufallsgeneriert ist, niemals wieder verwendet und streng vertraulich behandelt wird, ist der One-Time-PAD nicht zu entschlüsseln.

Begriff	Definition
PAN	Akronym für „Primary Account Number“ (Primäre Kontonummer). Sie wird auch als Kontonummer bezeichnet. Die Zahlungskartennummer (normalerweise eine Kredit- oder Debitkarte), die den Kartenaussteller und das jeweilige Karteninhaberkonto eindeutig identifiziert.
Parametrisierte Abfragen	Eine Methode zur Strukturierung von SQL-Abfragen, um Außerkraftsetzungsversuche zu begrenzen und folglich Injection-Angriffe zu vermeiden.
Kennwort/Kennsatz	Eine Zeichenfolge, die als Authentifizierung des Benutzers dient.
PAT	Akronym für „Port Address Translation“ (Übersetzung der Portadresse), auch bezeichnet als „Network Address Port Translation“ (Übersetzung der Netzwerkportadresse). Ein Untertyp der *NAT*, bei dem auch Portnummern übersetzt werden.
Patch	Ein Update für eine vorhandene Software, um zusätzliche Funktionalitäten zu installieren oder Fehler zu korrigieren.
Zahlungsanwendung	Im Kontext des PA-DSS eine Softwareanwendung, mit der Karteninhaberdaten im Rahmen der Autorisierung bzw. Abrechnung gespeichert, verarbeitet oder übertragen werden, wenn die Zahlungsanwendung an Dritte verkauft, verteilt oder lizenziert wird. Weitere Details finden Sie im *PA-DSS-Programmleitfaden*.
Zahlungskarten	Jegliche Zahlungskarten oder -geräte, die zum Zwecke des PCI DSS das Logo der Gründungsmitglieder des PCI SSC abbilden. Dazu zählen American Express, Discover Financial Services, JCB International, MasterCard Worldwide und Visa Inc.
Zahlungsabwickler	Manchmal auch als „Zahlungs-Gateway“ oder „Payment Service Provider (PSP)“ (Zahlungs-Serviceprovider) bezeichnet. Organisation, die von einem Händler oder einer anderen Organisation beauftragt wird, die Transaktion mit Zahlungskarten stellvertretend abzuwickeln. Auch wenn Zahlungsabwickler typischerweise Acquirer-Leistungen bereitstellen, werden diese nicht als Acquirer erachtet, sofern sie nicht von einer Zahlungskartenmarke als solcher definiert sind. Siehe auch *Acquirer.*
PCI	Akronym für „Payment Card Industry“ (Zahlungskartenbranche).
PCI DSS	Akronym für „Payment Card Industry Data Security Standard“ (Zahlungskartenbranche Datensicherheitsstandard).
PDA	Akronym für „Personal Data Assistant“ (Persönlicher Datenassistent) bzw. „Personal Digital Assistant“ (Persönlicher digitaler Assistent). Mobile Geräte mit Telefon-, E-Mail- oder Browserfunktion.
PED	PIN Entry Device

Begriff	Definition
Penetrationstest	Bei Penetrationstests werden potenzielle Sicherheitsrisiken von Systemen ermittelt. Dazu wird versucht, die Sicherheitsfunktionen der Systemkomponenten zu umgehen. Penetrationstests müssen die Netzwerk- und Anwendungsebene umfassen sowie Steuerelemente und Prozesse rund um die Netzwerke und Anwendungen berücksichtigen. Die Versuche müssen sowohl von außerhalb als auch von innerhalb des Netzwerks erfolgen.
Persönliche Firewall-Software	Eine auf einem Computer installierte Software-Firewall.
Personenbezogene Informationen	Informationen, die dazu dienen, eine Person zu identifizieren, insbesondere Name, Anschrift, Sozialversicherungsnummer, biometrische Daten, Geburtsdatum usw.
Mitarbeiter	Voll- und Teilzeitmitarbeiter, temporäre Mitarbeiter, Subunternehmer und Berater, die am Standort der jeweiligen Stelle „ansässig“ sind oder anderweitig Zugriff auf die Karteninhaberdaten-Umgebung haben.
PIN	Akronym für „persönliche Identifizierungsnummer“. Es handelt sich um ein geheimes numerisches Kennwort, das nur der Benutzer kennt, und ein System zur Authentifizierung des Benutzers im System. Dem Benutzer wird nur Zugriff gewährt, wenn die vom Benutzer eingegebene PIN mit der PIN im System übereinstimmt. PINs werden üblicherweise an Bankautomaten für Geldabhebungen benutzt. Eine andere Art von PIN wird in EMV-Chipkarten benutzt, in denen die PIN die Unterschrift des Karteninhabers ersetzt.
PIN-Block	Ein Datenblock zum Verbergen der PIN während der Verarbeitung. Das PIN-Blockformat bestimmt den Inhalt des PIN-Blocks und wie er verarbeitet wird, um die PIN abzurufen. Der PIN-Block besteht aus der PIN, der PIN-Länge und unter Umständen aus einem Teilsatz der PAN.
POI	Akronym für „Point of Interaction“, der Ausgangspunkt, von dem Daten einer Karte gelesen werden. Ein POI, eine elektronische Akzeptanzumgebung, bestehend aus Hardware und Software, die in einem Akzeptanzgerät gehostet ist und die es dem Karteninhaber gestattet, Kartentransaktionen durchzuführen. Das POI kann von Personal bedient oder personalfrei sein. POI-Transaktionen sind normalerweise auf Karten mit integrierten Schaltungen (Chip) und/oder mit Magnetstreifen basierte Zahlungstransaktionen.
Richtlinie	Unternehmensweite Regeln in Bezug auf die zulässige Nutzung von Computerressourcen, Sicherheitspraktiken und eine Anleitung bei der Entwicklung von Betriebsverfahren.
POP3	Akronym für „Post Office Protocol v3“ (Postprotokoll, Version 3). Protokoll auf Anwendungsebene, das von E-Mail-Clients zum Abrufen von E-Mails von einem Remote-Server über eine TCP/IP-Verbindung verwendet wird.

Begriff	Definition
Port	Logischer (virtueller) Verbindungspunkt für ein bestimmtes Kommunikationsprotokoll, der die netzwerkübergreifende Kommunikation erleichtert.
POS	Akronym für „Point of Sale“ (Verkaufspunkt). Eine Hardware und/oder Software, die zur Verarbeitung von Zahlungskartentransaktionen an Handelsstellen verwendet wird.
Privates Netzwerk	Ein von einem Unternehmen eingerichtetes Netzwerk, das einen privaten IP-Adressbereich verwendet. Private Netzwerke werden häufig in Form lokaler Netzwerke eingerichtet. Der private Netzwerkzugang über öffentliche Netzwerke sollte mithilfe von Firewalls und Routern geschützt werden. Siehe auch *Öffentliches Netzwerk*.
Privilegierter Nutzer	Alle Benutzerkonten, denen nicht nur grundlegende Zugriffsrechte eingeräumt werden. Diese Konten verfügen in der Regel über mehr Rechte als ein Standard-Benutzerkonto. Welche Rechte den einzelnen Konten jedoch eingeräumt werden, hängt sehr stark von der Organisation, der Funktion bzw. Rolle und der verwendeten Technik ab.
Verfahren	Beschreibende Schilderung einer Richtlinie. Ein Verfahren beschreibt die Umsetzung und Durchführung einer Richtlinie.
Protokoll	Vereinbartes Kommunikationsverfahren innerhalb von Netzwerken. Eine Spezifikation, die die Regeln und Verfahren beschreibt, die von Computerprodukten bei Aktivitäten in einem Netzwerk befolgt werden sollten.
Proxyserver	Ein Server, der als Vermittler zwischen einem internen Netzwerk und dem Internet dient. Eine Funktion des Proxyservers besteht beispielsweise darin, Verbindungen zwischen internen und externen Verbindungen zu beenden oder zu vermitteln, sodass jede Verbindung ausschließlich mit dem Proxyserver kommuniziert.
PTS	Akronym für „PIN Transaction Security“ (PIN-Transaktionssicherheit). PTS beschreibt eine Reihe modularer Bewertungsanforderungen, die vom PCI Security Standards Council für PIN-fähige POI-Terminals verwaltet werden. Bitte besuchen Sie www.pcisecuritystandards.org.
Öffentliches Netzwerk	Ein von einem dritten Telekommunikationsanbieter oder einem anerkannten Privatunternehmen eingerichtetes und betriebenes Netzwerk, das dem Zweck dient, Datenübertragungsdienste für die Öffentlichkeit bereitzustellen. Die Daten müssen für die Übertragung über öffentliche Netzwerke verschlüsselt werden, da Hacker sie mühelos abfangen, ändern und umleiten können. Beispiele für öffentliche Netzwerke sind das Internet, GPRS und GSM. Siehe auch *Privates Netzwerk*.
PVV	Akronym für “PIN Verification Value” (PIN-Verifizierungswert). Ein verschlüsselter Wert auf dem Magnetstreifen einer Zahlungskarte.

Begriff	Definition
QIR	Akronym für „Qualified Integrator or Reseller“ (Qualifizierter Integrator oder Wiederverkäufer). Weitere Informationen hierzu finden Sie auf der PCI-SSC-Website im *QIR-Programmleitfaden*.
QSA	Akronym für „Qualified Security Assessor“ (Qualifizierter Sicherheitsprüfer). QSAs werden durch PCI SSC für die Durchführung von PCI-DSS-Vor-Ort-Beurteilungen qualifiziert. Details zu den Anforderungen an QSA-Unternehmen und -Mitarbeiter finden Sie unter *QSA-Qualifikationsanforderungen*
RADIUS	Abkürzung für „Remote Authentication Dial-In User Service“ (Authentifizierungsdienst für sich einwählende Benutzer). Authentifizierungs- und Accounting-System. Überprüft die Richtigkeit von an den RADIUS-Server geleiteten Benutzernamen und Kennwörtern und autorisiert anschließend den Zugriff auf das System. Diese Authentifizierungsmethode kann mit einem Token, einer Smartcard usw. verwendet werden, um eine Multi-Faktor-Authentifizierung einzusetzen.
Rainbow-Table-Angriff	Methode eines Datenangriffs, bei der mittels einer vorab berechneten Hash-String-Tabelle (Message-Digest mit fixer Länge) die Original-Datenquelle identifiziert wird, insbesondere zum Knacken von Kennwörtern oder Karteninhaberdaten-Hashes.
Erneute Schlüsselvergabe	Ein Vorgang, bei dem kryptographische Schlüssel gewechselt werden. Regelmäßige erneute Schlüsselvergaben beschränken die von einem einzigen Schlüssel verschlüsselte Datenmenge.
Remote-Zugriff	Zugriff auf Computer-Netzwerke von einem Standort außerhalb des Netzwerks. Verbindungen für den Remote-Zugriff gehen entweder von dem internen unternehmenseigenen Netzwerk oder von einem externen Standort außerhalb des Unternehmensnetzwerks aus. Eine Technologie, die Remote-Zugriff unterstützt, ist beispielsweise *VPN*.
Externe Laborumgebung	Ein Labor, das nicht vom PA-QSA unterhalten wird.
Elektronische Wechselmedien	Datenträger, die digitalisierte Daten speichern und die leicht entfernt und/oder von einem Computersystem zum anderen transportiert werden können. Beispiele für elektronische Wechselmedien sind unter anderen CD-ROM, DVD-ROM, USB-Flash-Laufwerke und externe Festplatten.
Wiederverkäufer/Integratoren	Eine Stelle, die Zahlungsanwendungen vertreibt und/oder integriert, sie jedoch nicht entwickelt.
RFC 1918	Der Standard der Internet Engineering Task Force (IETF), in dem die Nutzung und die entsprechenden Adressbereiche für private (nicht weiterleitbare) Netzwerke definiert werden.

Begriff	Definition
Risikoanalyse/Risikobewertung	Vorgang, bei dem wertvolle Systemressourcen und Bedrohungen systematisch identifiziert und Verlustpotenziale basierend auf geschätzten Vorkommenshäufigkeiten und -kosten quantifiziert werden. Auf Wunsch kann dieser Vorgang auch Empfehlungen zur Zuweisung von Ressourcen für Gegenmaßnahmen umfassen, um das Risiko einer systemweiten Gefährdung zu minimieren.
Risikobewertung	Ein festgelegtes Messkriterium, das auf der Risikobeurteilung und Risikoanalyse zu einer bestimmten Stelle basiert.
ROC	Akronym für „Report on Compliance“ (Konformitätsbericht). In diesem Bericht werden die Ergebnisse der PSI-DSS-Beurteilung einer Stelle detailliert dokumentiert.
Rootkit	Eine schädliche Software, die, wenn sie ohne Zustimmung installiert wird, ihre Existenz verbergen kann und in der Lage ist, die administrative Kontrolle über ein Computersystem zu erlangen.
Router	Hardware oder Software, die eine Verbindung zu einem oder mehreren Netzwerken herstellen. Dient als Sortierer und Interpreter und leitet Informationsabschnitte anhand von Adressen an ihre jeweiligen Zielorte. Softwarerouter werden manchmal auch als Gateways bezeichnet.
ROV	Akronym für „Report on Validation“ (Validierungsbericht). In diesem Bericht werden die Ergebnisse der PA-DSS-Beurteilung zu Zwecken des PA-DSS-Programms detailliert dokumentiert.
RSA	Algorithmus für die Verschlüsselung öffentlicher Schlüssel, der 1977 von Ron Rivest, Adi Shamir und Len Adleman vom Massachusetts Institute of Technology (MIT) beschrieben wurde. Der Name des Algorithmus (RSA) ergibt sich aus den Anfangsbuchstaben ihrer Nachnamen.
S-FTP	Akronym für Secure-FTP. S-FTP kann Authentifizierungsinformationen und Dateien während der Übertragung verschlüsseln. Siehe *FTP.*
Stichprobenkontrolle	Der Prozess, bei dem ein Querschnitt einer Gruppe genommen wird, der repräsentativ für die gesamte Gruppe ist. Stichprobenkontrollen können von Bewertern eingesetzt werden, um den Testaufwand zu reduzieren, wenn bereits bestätigt wurde, dass eine Stelle standardisierte und zentralisierte PCI-DSS-Sicherheits- und Betriebsprozesse und -kontrollen implementiert hat. Die Stichprobenkontrolle ist keine PCI-DSS-Anforderung.
SANS	Akronym für „SysAdmin, Audit, Networking and Security“. Ein Institut, das Schulungen und professionelle Zertifizierungen zum Thema Computersicherheit anbietet. (Siehe www.sans.org.)
SBF	Akronym für „Selbstbeurteilungsfragebogen“. Berichtstool, mit dem die Ergebnisse der Selbstbeurteilung im Rahmen der PCI-DSS-Beurteilung einer Stelle dokumentiert werden.

Begriff	Definition
Schema	Formale Beschreibung der Datenbankkonstruktion, einschließlich Organisation der Datenelemente.
Scoping	Ein Prozess zur Identifizierung aller Computerkomponenten, Personen und Prozesse, die in einer PCI-DSS-Bewertung berücksichtigt werden müssen. Der erste Schritt in einer PCI-DSS-Bewertung liegt in der eingehenden Bestimmung des Umfangs der Prüfung.
SDLC	Akronym für „System Development Life Cycle“ oder „Software Development Life Cycle“ (System- bzw. Softwareentwicklungszyklus). Entwicklungsphasen einer Software oder eines Computersystems, einschließlich Planung, Analyse, Design, Testphase und Implementierung.
Sicheres Codieren	Der Prozess, bei dem manipulations- und/oder angriffssichere Anwendungen erstellt und implementiert werden.
Sicheres kryptographisches System	Hardware, Software und Firmware, die kryptographische Prozesse implementiert (einschließlich kryptographischer Algorithmen und Schlüsselgenerierung) und innerhalb festgelegter kryptographischer Grenzen enthalten ist. Beispiele für sichere kryptographische Systeme sind gemäß PCI PTS validierte Host-/Hardwaresicherheitsmodule (HSMs) und Point-of-Interaction-Geräte (POIs).
Secure Wipe (sicheres Löschverfahren)	Auch „Secure Delete“ genannt. Eine Methode zum Überschreiben von Daten, die sich auf einer Festplatte oder einem anderen digitalen Medium befinden, mit dem Ergebnis, dass die Daten unwiderruflich gelöscht sind.
Sicherheitsereignis	Ein Vorkommnis, das nach Auffassung des Unternehmens/der Organisation potenzielle Sicherheitsauswirkungen auf ein System oder seine Umgebung hat. Im Zusammenhang mit PCI DSS weisen Sicherheitsereignisse auf verdächtige oder anomale Aktivitäten hin.
Sicherheitsbeauftragter	Hauptverantwortlicher für sicherheitsrelevante Angelegenheiten einer Einheit.
Sicherheitsrichtlinie	Eine Reihe von Gesetzen, Regeln und Praktiken, die die Verwaltung, den Schutz und die Verteilung von vertraulichen Informationen innerhalb eines Unternehmens regeln.
Sicherheitsprotokolle	Netzwerkkommunikationsprotokolle, die zur Sicherung von Datenübertragungen dienen. Sicherheitsprotokolle sind z. B. TLS, IPSEC, SSH und HTTPS.
Sensibler Bereich	Jegliche Art von Rechenzentren, Serverräumen und anderen Bereichen, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Hierzu zählen nicht die Bereiche, in denen lediglich Point-of-Sale-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).

Begriff	Definition
Vertrauliche Authentifizierungsdaten	Sicherheitsinformationen (insbesondere Kartenprüfcodes/-werte, vollständige Spurdaten (vom Magnetstreifen oder Chip), PINs und PIN-Blöcke), die zur Authentifizierung von Karteninhabern und/oder Autorisierung von Transaktionen mit Zahlungskarten verwendet werden.
Aufgabentrennung	Aufteilung von Aufgaben in einer Funktion auf verschiedene Einzelpersonen, sodass keine dieser Personen allein den Prozess sabotieren kann.
Server	Ein Computer, der anderen Computern Dienste zur Verfügung stellt, z. B. Kommunikationsverarbeitung, Dateispeicherung oder Zugriff auf eine Druckeinrichtung. Zu den Servertypen gehören u. a. Web-, Datenbank-, Anwendungs-, Authentifizierungs-, DNS-, Mail-, Proxy- und NTP-Server.
Servicecode	Ein drei- oder vierstelliger Wert auf dem Magnetstreifen hinter dem Ablaufdatum der Zahlungskarte auf den Spurdaten. Er erfüllt gleichzeitig mehrere Zwecke, wie etwa die Definition von Serviceattributen, die Differenzierung zwischen internationalem und nationalem Datenaustausch oder die Identifizierung von Nutzungsbeschränkungen.
Dienstanbieter	Ein Unternehmen o. Ä., das keine Kreditkartengesellschaft ist und direkt an der Verarbeitung, Speicherung, Übertragung und Vermittlung von Karteninhaberdaten für ein anderes Unternehmen beteiligt ist. Dazu gehören auch Unternehmen, die Dienste anbieten, die die Sicherheit von Karteninhaberdaten kontrollieren oder sich darauf auswirken können. Beispiele umfassen Managed Service-Anbieter, die verwaltete Firewalls, IDS und andere Dienste anbieten, sowie Hosting-Anbieter und andere Entitäten. Bietet ein Unternehmen eine Dienstleistung an, die *ausschließlich* aus der Bereitstellung des Zugriffs auf ein öffentliches Netzwerk besteht – etwa ein Telekommunikationsunternehmen, das nur die Kommunikationsverbindung bereitstellt – gilt das Unternehmen im Zusammenhang mit dieser Dienstleistung nicht als Dienstanbieter (möglicherweise jedoch im Zusammenhang mit anderen Dienstleistungen).
Session Token	Im Zusammenhang mit dem Websession-Management bezeichnet ein Session Token (auch als „Session Identifier“ oder „Session ID“ bezeichnet) ein einzigartiges Identifikationsmerkmal (wie z. B. ein „Cookie“), das verwendet wird, um eine bestimmte Sitzung zwischen einem Webbrowser und einem Webserver nachzuverfolgen.
SHA-1/SHA-2	Akronym für „Secure Hash Algorithm“ (Sicherer Hash-Algorithmus). Ein Satz miteinander verwandter kryptografischer Hash-Funktionen, einschließlich SHA-1 und SHA-2. Siehe *Starke Kryptographie.*

Begriff	Definition
Smartcard	Auch als „Chipkarte“ oder „IC-Karte“ (Karte mit integriertem Chip) bezeichnet. Ein Zahlungskartentyp mit integrierten Schaltungen. Die Schaltungen, auch „Chips“ genannt, enthalten Zahlungskarteninformationen, einschließlich, aber nicht beschränkt auf Magnetstreifendaten-ähnliche Informationen.
SNMP	Akronym für „Simple Network Management Protocol“ (einfaches Netzwerkverwaltungsprotokoll). Unterstützt die Überwachung von Geräten in einem Netzwerk auf jegliche Zustände, die die Aufmerksamkeit eines Administrators erfordern.
Geteiltes Wissen	Methode, bei der zwei oder mehr Stellen über Teile eines Schlüssels verfügen, die nur zusammen den kryptografischen Schlüssel ergeben.
Spyware	Eine Art von schädlicher Software, die, sobald sie installiert ist, ohne das Wissen des Benutzers dessen Computer abhört oder teilweise die Kontrolle über ihn übernimmt.
SQL	Akronym für „Structured Query Language“ (strukturierte Abrufsprache). Eine Computersprache, die zum Erstellen, Modifizieren und Abrufen von Daten aus relationellen Datenbankverwaltungssystemen verwendet wird.
SQL-Injektion	Eine Angriffsmethode auf datenbankgestützte Websites. Dabei nutzt der Angreifer einen unsicheren Code auf einem mit dem Internet verbundenen System aus, um nicht autorisierte SQL-Befehle auszuführen. Bei Angriffen mit SQL-Injection können Eindringlinge normalerweise unzugängliche Informationen aus einer Datenbank entwenden und/oder sich über den Computer, der die Datenbank hostet, Zugriff auf die Hostcomputer einer Organisation verschaffen.
SSH	Abkürzung für „Secure Shell“. Eine Protokollsuite, die Verschlüsselungsfunktionen für Netzwerkdienste wie Remoteanmeldung oder Remotedatenübertragung bietet.
SSL	Akronym für „Secure Sockets Layer“. Industriestandard zur Verschlüsselung des Kanals zwischen Webbrowser und Webserver. Jetzt abgelöst von TLS. Siehe *TLS.*
Statusgesteuerte Inspektion	Auch als „dynamische Paketfilterung“ bezeichnet. Eine Firewallfunktion, die für erweiterte Sicherheit sorgt, indem sie den Status der Netzwerkverbindungen nachverfolgt. Da die Firewall berechtigte Pakete für diverse Verbindungen unterscheidet, werden nur Pakete zugelassen, die einer „etablierten“ Verbindung entsprechen. Alle anderen werden zurückgewiesen.

Begriff	Definition
Siehe Starke Kryptographie.	Eine auf industrieerprobten und akzeptierten Algorithmen basierte Kryptografie, zusammen mit Schlüssellängen, die eine effektive Schlüssellänge von mindestens 112 Bit bereitstellen, und angemessenen Schlüsselverwaltungspraktiken. Die Kryptografie ist eine Datenschutzmethode, bei der sowohl Verschlüsselungs- (reversibel) als auch Hashing-Verfahren (unidirektional, d. h. nicht reversibel) eingesetzt werden. Siehe *Hashing.* Zum Veröffentlichungszeitpunkt zählten zu den industrieerprobten und akzeptierten Standards und Algorithmen unter anderem AES (128 Bits und mehr), TDES (dreifache Schlüssellänge), RSA (2048 Bits und mehr), ECC (224 Bits und mehr) und DSA/D-H (2048/224 Bits und mehr). Weitere Informationen zur Stärke von kryptografischen Schlüsseln und zu entsprechenden Algorithmen sind in der aktuellen Version der NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/) zu finden. ***Hinweis:*** *Die obenstehenden Beispiele sind für die dauerhafte Speicherung von Karteninhaberdaten geeignet. Die minimalen Kryptografieanforderungen für transaktionsbasierte Abläufe (wie in PCI PIN und PTS definiert) sind flexibler, weil weitere Kontrollen vorhanden sind, die das Gefährdungsniveau herabsenken.* *Es wird empfohlen, für alle neuen Implementierungen eine effektive Schlüssellänge von mindestens 128 Bits zu verwenden.*
SysAdmin	Abkürzung für „Systemadministrator“. Eine Person mit erweiterten Rechten, die für die Verwaltung eines Computersystems oder Netzwerkes verantwortlich ist.
Systemkomponenten	Alle Netzwerkgeräte, Server, Rechengeräte oder Anwendungen, die Teil der Karteninhaberdaten-Umgebung sind oder an diese angeschlossen sind.
Objekt auf Systemebene	Sämtliche auf einer Systemkomponente befindlichen Elemente, die für ihren Betrieb erforderlich sind, insbesondere Datenbanktabellen, gespeicherte Verfahren, ausführbare Anwendungsdateien und Konfigurationsdateien, Systemkonfigurationsdateien, Static und Shared Libraries und DLLs, ausführbare Systemdateien, Gerätetreiber und Gerätekonfigurationsdateien sowie Komponenten von Drittanbietern.
TACACS	Akronym für „Terminal Access Controller Access Control System“. Ein Remote-Authentifizierungsprotokoll, das häufig in Netzwerken verwendet wird, die mit einem Remote-Zugriffs-Server und einem Authentifizierungsserver kommunizieren, um die Zugriffsberechtigungen der Benutzer auf das Netzwerk zu ermitteln. Diese Authentifizierungsmethode kann mit einem Token, einer Smartcard usw. verwendet werden, um eine Multi-Faktor-Authentifizierung einzusetzen.

Begriff	Definition
TCP	Akronym für „Transmission Control Protocol“ (Übertragungssteuerungsprotokoll). Eines der wesentlichen Transportschichtprotokolle der Internet Protocol (IP)-Suite sowie grundlegende Kommunikationssprache oder -protokoll des Internets. Siehe *IP*.
TDES	Akronym für „Triple Data Encryption Standard“, wird auch als „3DES“ oder „Triple-DES“ bezeichnet. Eine Blockcodierung, die aus der DES-Codierung durch dreimalige Verwendung gebildet wird. Siehe *Starke Kryptographie.*
TELNET	Abkürzung für „Telephone Network Protocol“ (Telefonnetzprotokoll). Wird in der Regel zur Bereitstellung von benutzerorientierten Befehlszeilen-Anmeldesitzungen für Geräte in einem Netzwerk verwendet. Benutzerinformationen werden in Klartext übermittelt.
Bedrohung	Zustand, durch den Informationen oder Informationsverarbeitungsressourcen absichtlich oder versehentlich verloren gehen bzw. geändert, verfügbar gemacht oder unzugänglich gemacht oder auf andere für das Unternehmen schädigende Weise beeinträchtigt werden.
TLS	Akronym für „Transport Layer Security“ (Transportschichtsicherheit). Wurde mit dem Ziel entwickelt, Datensicherheit und -integrität zwischen zwei kommunizierenden Anwendungen zu gewährleisten. TLS ist der Nachfolger von SSL.
Token	Im Zusammenhang mit Authentifizierung und Zugriffskontrolle handelt es sich bei einem Token um einen per Hardware oder Software bereitgestellten Wert, der zur Durchführung einer dynamischen oder auf mehreren Faktoren basierenden Authentifizierung mit einem Authentifizierungsserver oder VPN arbeitet. Siehe *RADIUS, TACACS* und *VPN.* Siehe auch *Session Token*.
Spurdaten	Auch als „Full-Track-Daten“, „Magnetstreifendaten“ oder „Verfolgungsdaten“ bezeichnet. Im Magnetstreifen oder in einem Chip verschlüsselte Daten, die bei Zahlungstransaktionen zur Authentifizierung und/oder Autorisierung verwendet werden. Dabei kann es sich um das Magnetstreifenabbild auf einem Chip oder um die Daten auf der Spur 1 und/oder Spur 2 handeln, die Teil des Magnetstreifens sind.
Transaktionsdaten	Auf elektronische Transaktionen mit Zahlungskarten bezogene Daten.
Trojaner	Auch – korrekterweise – als „Trojanisches Pferd“ bezeichnet. Eine Art schädlicher Software, die, wenn sie installiert wird, es einem Benutzer ermöglicht, eine normale Funktion auszuführen, während der Trojaner ohne das Wissen des Benutzers auf dem Computersystem schädliche Funktionen ausführt.

Begriff	Definition
Abkürzung	Eine Methode, mit der die vollständige PAN unleserlich gemacht werden kann, indem ein Segment aus den PAN-Daten dauerhaft entfernt wird. Abkürzung bezieht sich auf den Schutz der PAN, wenn diese in Dateien, Datenbanken, usw. *gespeichert* wird. Siehe *Maskierung* zum Schutz der PAN, wenn diese auf Bildschirmen, Papierbelegen, usw. *angezeigt* wird.
Vertrauenswürdiges Netzwerk	Ein Netzwerk einer Organisation, das sich innerhalb der Kontroll- oder Verwaltungsmöglichkeiten dieser Organisation befindet.
Nicht vertrauenswürdiges Netzwerk	Ein Netzwerk, das außerhalb der Netzwerke liegt, die zu einer Organisation gehören und das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Organisation liegt.
URL	Akronym für „Uniform Resource Locator“ (Einheitlicher Quellenanzeiger).Eine formatierte Textzeichenfolge, die von Webbrowsern, E-Mail-Clients und sonstiger Software zur Identifizierung einer Netzwerkressource im Internet verwendet wird.
Versionierungsmethode	Ein Prozess, bei dem Versionsschemata zugewiesen werden, um einen bestimmten Zustand einer Anwendung oder Software eindeutig zu identifizieren. Diese Schemata entsprechen einem Versionsnummernformat, einer Versionsnummernnutzung und allen Wildcard-Elementen gemäß Definition durch den Softwareanbieter. Versionsnummern werden allgemein in aufsteigender Reihenfolge zugewiesen und entsprechen einer bestimmten Änderung innerhalb der Software.
Virtuelle Appliance (VA)	Eine VA übernimmt das Konzept eines vorkonfigurierten Geräts zur Ausführung bestimmter Funktionen und um das Gerät als ein Workload auszuführen. Oft wird ein vorhandenes Netzwerkgerät virtualisiert, um als eine virtuelle Appliance, wie etwa ein Router, Switch oder eine Firewall zu laufen.
Virtueller Hypervisor	Siehe *Hypervisor***.**
Virtueller Rechner	Eine unabhängige Betriebsumgebung, die sich wie ein separater Computer verhält. Der virtuelle Rechner wird auch „Guest“ bezeichnet und läuft auf einem Hypervisor.
Virtual-Machine-Monitor (VMM)	Der VMM ist Teil des Hypervisors und eine Software, die die Hardware-Abstraktion für virtuelle Rechner durchsetzt. Er verwaltet den Prozessor, den Speicher und andere Systemressourcen, um jedem Guest-Betriebssystem die benötigten Ressourcen bereitzustellen.

Begriff	Definition
Virtuelles Zahlungsterminal	Ein virtuelles Zahlungsterminal ist ein Webbrowser-basierter Zugriffspunkt auf die Website eines Acquirers, eines Verarbeitungsunternehmens oder eines Drittanbieters zur Autorisierung von Transaktionen mit Zahlungskarten; auf dieser Website gibt ein Händler manuell Karteninhaberdaten über einen sicher verbundenen Webbrowser ein. Anders als physische Terminals lesen virtuelle Zahlungsterminals Daten nicht direkt von Zahlungskarten. Da die Transaktionen mit Zahlungskarten manuell eingegeben werden, werden in Händlerumgebungen mit niedrigen Transaktionsvolumen virtuelle Zahlungsterminals häufig anstatt physischer Terminals eingesetzt.
Virtual Switch oder virtueller Router	Ein virtual Switch oder ein virtueller Router ist eine logische Einheit, die Daten auf Netzwerk-Infrastruktur-Ebene mit Routing- und Switching-Funktionalitäten versieht. Ein virtual Switch ist ein zentraler Bestandteil einer virtualisierten Server-Plattform, wie etwa einem Hypervisor-Treiber, Modul oder Plugin.
Virtualisierung	Die Virtualisierung bezieht sich auf die logische Abstraktion von Rechnerressourcen, um sie von den physischen Einschränkungen loszulösen. Eine häufige Abstraktion ist die Einrichtung von virtuellen Rechnern oder VMs, bei der der Inhalt eines physischen Rechners integriert wird und die es ermöglicht, auf verschiedener physischer Hardware und/oder mit anderen virtuellen Rechnern auf derselben physischen Hardware zu arbeiten. Neben den VMs kann die Virtualisierung auch auf viele andere Computerressourcen, einschließlich Anwendungen, Desktops, Netzwerke und Speicher angewendet werden.
VLAN	Abkürzung für „Virtual LAN" oder „Virtual Local Area Network" (virtuelles lokales Netzwerk) Ein logisches lokales Netzwerk mit einer weit größeren Reichweite als herkömmliche lokale Netzwerke.
VPN	Akronym für „Virtual Private Network" (virtuelles privates Netzwerk) Ein Computernetzwerk, in dem einige Verbindungen anstatt direkter Kabelverbindungen virtuelle Verbindungen in einem größeren Netzwerk sind, wie beispielsweise das Internet. Die Endpunkte des virtuellen Netzwerks werden in diesem Fall durch das größere Netzwerk getunnelt. Während gewöhnliche Anwendungen aus sicheren Kommunikationen über das öffentliche Internet bestehen, muss ein VPN nicht immer über solche starken Sicherheitsmerkmale, wie etwa Authentifizierung oder Inhaltsverschlüsselung, verfügen. Ein VPN kann mit einem Token, einer Smartcard usw. verwendet werden, um eine Zwei-Faktor-Authentifizierung einzusetzen.
Schwachstelle	Ein Fehler oder eine Sicherheitslücke, die, sollte sie vorsätzlich oder unwissentlich ausgenutzt werden, das System gefährden kann.

Begriff	Definition
WAN	Akronym für „Wide Area Network“ (Weitverkehrsnetz). Ein Computernetzwerk, das einen großen Bereich abdeckt, oft auch ein regionales oder unternehmensweites Computersystem.
Web-Anwendung	Eine Anwendung, auf die normalerweise über einen Webbrowser oder Webdienste zugegriffen wird. Web-Anwendungen können über das Internet oder ein privates, internes Netzwerk verfügbar sein.
Webserver	Ein Computer mit einem Programm, das HTTP-Anfragen von Web-Clients zulässt und die HTTP-Antworten ausgibt (normalerweise Webseiten).
WEP	Akronym für „Wired Equivalent Privacy“. Schwacher Algorithmus zur Verschlüsselung drahtloser Netzwerke. Branchenexperten haben gravierende Schwächen entdeckt, durch die eine WEP-Verbindung innerhalb von Minuten mithilfe gängiger Software geknackt werden kann. Siehe *WPA.*
Platzhalter	Ein Zeichen, das gegen einen definierten Teilsatz möglicher Zeichen im Versionsschema einer Anwendung ausgetauscht werden kann. Im Zusammenhang mit PA-DSS können Platzhalter optional zur Darstellung einer nicht sicherheitsrelevanten Änderung verwendet werden. Ein Platzhalter ist das einzige variable Element des Versionsschemas des Anbieters und er wird als Hinweis darauf verwendet, dass in jeder Version, die durch das Platzhalterelement dargestellt wird, nur kleine Änderungen ohne Auswirkungen auf die Sicherheit vorgenommen wurden.
Drahtloser Zugriffspunkt	Auch als „AP“ bezeichnet. Akronym aus dem Englischen für Access Point (Zugriffspunkt). Eine Einrichtung, die es drahtlosen Kommunikationsgeräten ermöglicht, eine Verbindung zu einem drahtlosen Netzwerk herzustellen. Wenn diese wie üblich an ein Kabelnetzwerk angeschlossen ist, kann sie Daten zwischen drahtlosen und verkabelten Geräten im Netzwerk übertragen.
Drahtlose Netzwerke	Ein Netzwerk, das Computer ohne Drähte miteinander verbindet.
WLAN	Akronym für „Wireless Local Area Network“ (drahtloses lokales Netzwerk). Ein lokales Netzwerk, das zwei oder mehr Computer oder Geräte kabellos miteinander verbindet.
WPA/WPA2	Akronym für „WiFi Protected Access“. Sicherheitsprotokoll zur Sicherung drahtloser Netzwerke. WPA ist der Nachfolger von WEP. Auch WPA2 wurde als nächste Generation von WPA veröffentlicht.