

Payment Card Industry (PCI) Datensicherheitsstandard (DSS) und Datensicherheitsstandard für Zahlungsanwendungen (PA-DSS)

Glossar für Begriffe, Abkürzungen und Akronyme

Version 2.0

Oktober 2010

Begriff	Definition
AAA	Akronym für „Authentication, Authorization and Accounting“. Protokoll zur Authentifizierung eines Benutzers basierend auf dessen nachweisbarer Identität, zur Autorisierung eines Benutzers auf Grundlage seiner Benutzerrechte und 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 vertraulichen Authentifizierungsdaten. Siehe <i>Karteninhaberdaten</i> und <i>Vertrauliche Authentifizierungsdaten</i>
Kontonummer	Siehe <i>Primary Account Number (PAN)</i> .
Acquirer	Auch als „erwerbende Bank“ oder „erwerbendes Finanzinstitut“ bezeichnet. Eine Stelle, die Beziehungen zu Händlern aufnimmt oder aufrechterhält, damit diese ihre Zahlungskarten akzeptieren.
Adware	Ein schädlicher Softwaretyp der, wenn er installiert wird, den Computer dazu zwingt, automatisch Werbung anzuzeigen oder herunterzuladen.
AES	Abkürzung für „Advanced Encryption Standard“. In der symmetrischen Schlüsselkryptographie verwendete Blockchiffrierung, übernommen von NIST im November 2001 unter der Bezeichnung U.S. FIPS PUB 197 (oder „FIPS 197“). Siehe <i>Starke Kryptographie</i> .
ANSI	Akronym für „American National Standards Institute“. Eine private, gemeinnützige Organisation, die das in den USA freiwillige Standardisierungs- und Konformitätsbewertungssystem verwaltet und koordiniert.
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.
Anwendung	Hierzu zählen alle erworbenen oder benutzerspezifischen Softwareprogramme oder Programmgruppen, einschließlich sowohl interne als auch externe (z. B. Web-) Anwendungen.
Audit-Protokoll	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 <i>Audit-Protokoll</i> .
ASV	Akronym für „Approved Scanning Vendor.“ Ein vom PCI-SSC zugelassenes Unternehmen, um externe Services zum Scannen von Anfälligkeiten anzubieten.

Begriff	Definition
Authentifizierung	<p>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:</p> <ul style="list-style-type: none"> ▪ 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	<p>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.</p>
Autorisierung	<p>Zugangsberechtigung oder andere Rechte eines Benutzers, Programms oder Prozesses. Im Falle eines Netzwerks bestimmt die Autorisierung, was eine Person oder ein Programm nach der erfolgreichen Authentifizierung tun darf.</p> <p>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.</p>
Sicherheitskopie	<p>Eine zweite Datenkopie zu Archivzwecken oder um sich vor Schadensfällen oder Verlust zu schützen.</p>
Bluetooth	<p>Drahtlosprotokolle, die kurzreichweitige Kommunikationstechnologien für Datenübertragungen über kurze Distanzen einsetzen.</p>
Karteninhaber	<p>Nichtverbraucher oder Verbraucher, denen eine Zahlungskarte ausgestellt wird oder Personen, die befugt sind, die Zahlungskarte zu benutzen.</p>
Karteninhaberdaten	<p>Karteninhaberdaten bestehen mindestens aus der vollständigen PAN. Karteninhaberdaten können auch die vollständige PAN einschließlich folgende Datenelemente umfassen: Name des Karteninhabers, Verfallsdatum und/oder Servicecode</p> <p>Für weitere Datenelemente, die bei einer Zahlungstransaktion übertragen oder verarbeitet (jedoch nicht gespeichert) werden können, siehe <i>Vertrauliche Authentifizierungsdaten</i>.</p>
Karteninhaberdaten-Umgebung	<p>Personen, Prozesse und Technologien, die Karteninhaberdaten oder vertrauliche Authentifizierungsdaten, einschließlich jeglicher angeschlossener Systemkomponenten, speichern, verarbeiten oder übertragen.</p>

Begriff	Definition
Kartenverifizierungscode oder -wert	<p>Auch bekannt als Kartenvalidierungscode oder -wert oder Kartenprüfnummer.</p> <p>Bezieht sich entweder auf: (1) Magnetstreifendaten oder (2) aufgedruckte Sicherheitsmerkmale.</p> <p>(1) Ein Datenelement auf dem Magnetstreifen einer Karte, die einen sicheren Verschlüsselungsprozess anwendet, um die Integrität der Daten auf dem Magnetstreifen zu gewährleisten, und die jegliche Art von Manipulationen oder Fälschungen preisgibt. Je nach Kreditkartenunternehmen wird dies als CAV, CVC, CVV oder CSC bezeichnet. In der folgenden Liste werden die Begriffe für sämtliche Kreditkartenunternehmen aufgeführt:</p> <ul style="list-style-type: none"> ▪ CAV – Card Authentication Value (JCB-Zahlungskarten) ▪ CVC – Card Validation Code (MasterCard-Zahlungskarten) ▪ CVV – Card Verification Value (Visa und Discover-Zahlungskarten) ▪ CSC – Card Security Code (American Express) <p>(2) Bei Discover, JCB, MasterCard und Visa-Zahlungskarten ist der zweite Typ des Kartenverifizierungswerts oder -codes der rechte dreistellige Wert, der in dem Unterschriftsfeld 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 werden die Begriffe für sämtliche Kreditkartenunternehmen aufgeführt:</p> <ul style="list-style-type: none"> ▪ CID – Card Identification Number (American Express und Discover-Zahlungskarten) ▪ CAV2 – Card Authentication Value 2 (JCB-Zahlungskarten) ▪ CVC2 – Card Validation Code 2 (MasterCard-Zahlungskarten) ▪ CVV2 – Card Verification Value 2 (Visa und Discover-Zahlungskarten)
CERT	<p>Akronym für das „Computer Emergency Response Team“ der Carnegie Mellon University. Das CERT-Programm entwickelt und fördert die Nutzung angemessener Technologie- und Systemverwaltungspraktiken, um Angriffen auf vernetzte Systeme zu widerstehen und somit eventuelle Schäden einzudämmen und die Kontinuität wichtiger Systeme zu gewährleisten.</p>
CIS	<p>Akronym für „Center for Internet Security.“ Ein gemeinnütziges Unternehmen, das Organisationen hilft, das Risiko von Geschäfts- und E-Commerce-Unterbrechungen durch unangemessene technische Sicherheitskontrollen zu reduzieren.</p>
Verschlüsselung auf Datenbankspaltenebene	<p>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 <i>Datenträgerverschlüsselung</i> oder <i>Verschlüsselung auf Dateiebene</i>.</p>

Begriff	Definition
Kompensationskontrollen	<p>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:</p> <ol style="list-style-type: none"> (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) Dem zusätzlichen Risiko, das durch die Nichteinhaltung der PCI-DSS-Anforderung entsteht, angemessen sein. <p>Siehe „Kompensationskontrollen“ in Anhang B und C in <i>PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren</i> für eine Anleitung über die Nutzung von Kompensationskontrollen.</p>
Sicherheitsverletzung	<p>Auch als „Verletzung der Datensicherheit“ bezeichnet. Ein Zugriff auf ein System, bei dem eine vermeintliche unbefugte Enthüllung von Daten bzw. ein Datendiebstahl, Modifikationen an oder die Vernichtung von Karteninhaberdaten erfolgte.</p>
Konsole	<p>Bildschirm und Tastatur, die den Zugriff auf und die Steuerung eines Servers, Großrechners oder eines anderen Systemtyps in einer vernetzten Umgebung ermöglichen.</p>
Verbraucher	<p>Eine Person, die Güter oder Services oder beides einkauft.</p>
Kryptographie	<p>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.</p>
Schlüssellebensdauer	<p>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. <i>NIST Special Publication 800-57</i>).</p>
Datenbank	<p>Ein strukturiertes Format zur Organisation und Aufrechterhaltung schnell abrufbarer Informationen. Einfache Datenbankbeispiele sind Tabellen und Tabellenkalkulationen.</p>
Datenbankadministrator	<p>Auch als „DBA“ bezeichnet. Eine Person, die für die Verwaltung von Datenbanken verantwortlich ist.</p>
Standardkonten	<p>Ein in einem System, einer Anwendung oder einem Gerät vordefiniertes Konto, um den Zugriff beim Systemerstart zu gewährleisten. Unter Umständen generiert das System auch während des Installationsprozesses Standardkonten.</p>

Begriff	Definition
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.
Entmagnetisierung	Auch als „Entmagnetisierung von Datenträgern“ bezeichnet. Ein Prozess oder eine Technik, bei der der Datenträger entmagnetisiert wird, sodass alle darauf gespeicherten Daten unwiderruflich vernichtet werden.
Datenträgerverschlüsselung	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 <i>Verschlüsselung auf Dateiebene</i> oder die <i>Verschlüsselung auf Datenbankspaltenebene</i> zur Verschlüsselung der Inhalte spezifischer Dateien oder Spalten eingesetzt.
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“ oder „Domain Name Server“. Ein System, das Informationen im Zusammenhang mit Domainnamen in einer auf Netzwerken wie etwa dem Internet dezentralisierten Datenbank speichert.
DSS	Akronym für „Data Security Standard“, auch bezeichnet als „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 <i>Geteiltes Wissen</i> .)
Dynamische Paketfilterung	Siehe <i>Statusgesteuerte Inspektion</i> .
ECC	Akronym für „Elliptic Curve Cryptography.“ Eine öffentliche Schlüsselkryptographie basierend auf elliptischen Kurven auf endlichen Körpern. Siehe <i>Starke Kryptographie</i> .
Egress-Filterung	Eine Methode zum Filtern ausgehenden Datenverkehrs, damit nur ausdrücklich zugelassener Datenverkehr das Netzwerk verlassen kann.

Begriff	Definition
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 <i>Starke Kryptographie</i> .
Verschlüsselungsalgorithmus	Eine Sequenz mathematischer Anweisungen, um unverschlüsselten Text oder Daten in verschlüsselten Text oder Daten umzuwandeln und umgekehrt. Siehe <i>Starke Kryptographie</i> .
Einheit	Bezeichnet ein Unternehmen, eine Organisation oder einen Betrieb, der sich einer PCI-DSS-Überprüfung unterzieht.
Datei-Integritätsüberwachung	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 <i>Datenträgerverschlüsselung</i> oder <i>Verschlüsselung auf Datenbankspaltenebene</i> .
FIPS	Akronym für „Federal Information Processing Standards“. Standards, die öffentlich von den 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.
Ursachenanalyse	Auch bezeichnet als „IT-Forensik“. Im Zusammenhang mit der Informationssicherheit der Einsatz von Untersuchungstools und Analysetechniken zur Sammlung von Hinweisen von Computerressourcen, um die Ursache der Datensicherheitsverletzungen zu ermitteln.
FTP	Akronym für „File Transfer Protocol“. 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.
GPRS	Akronym für „General Packet Radio Service“. Ein für Benutzer von GSM-Mobiltelefonen verfügbarer mobiler Datendienst. Anerkannt für seine effektive Nutzung begrenzter Bandbreiten. Besonders geeignet zum Versenden und Empfangen kleiner Datenpakete, wie etwa E-Mails und Webbrowsering.

Begriff	Definition
GSM	Akronym für „Global System for Mobile Communications.“ Ein verbreiteter Standard für Mobiltelefone und Netzwerke. 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	<p>Ein Prozess, bei dem Karteninhaberdaten unleserlich gemacht werden, indem Daten mittels einer <i>starken Kryptographie in ein Message-Digest mit einer fixen Länge umgewandelt werden</i>. Hashing ist eine (mathematische) Funktion, bei der ein bekannter Algorithmus eine beliebig lange Nachricht als Input nimmt und anschließend eine fixe Länge ausgibt (auch „Hash-Code“ oder „Message-Digest“ genannt). Eine Hash-Funktion muss folgende Eigenschaften aufweisen:</p> <ol style="list-style-type: none"> (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. <p>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 für die Hashing-Funktion beinhalten (siehe <i>Salt</i>).</p>
Host	Die Hauptcomputerhardware, auf der sich die Computersoftware befindet.
Hosting-Anbieter	Bieten Händlern und anderen Diensteanbietern 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 dedizierten 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.
HTTP	Akronym für „Hypertext Transfer Protocol“. Offenes Internetprotokoll zur Übertragung von Informationen im World Wide Web.
HTTPS	Akronym für „Hypertext Transfer Protocol over Secure Socket Layer“. Ein sicheres HTTP mit Authentifizierung und verschlüsselten Kommunikationen über das World Wide Web für Kommunikationen 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.

Begriff	Definition
IDS	Akronym für „Intrusion Detection System“. Wird zur Identifizierung und Warnung vor Angriffsversuchen auf Netzwerke oder Systeme verwendet. 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. Es verwendet ein Regelsystem, um bei erkannten Sicherheitsereignissen Warnungen zu generieren.
IETF	Akronym für „Internet Engineering Task Force“. 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.
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.
Informationssystem	Diskreter Satz strukturierter Datenressourcen, der zur Erfassung, Verarbeitung, Verwaltung, Verwendung, gemeinsamen Nutzung, Verbreitung oder Anordnung von Informationen verwendet wird.
Ingress-Filterung	Eine Methode zum Filtern eingehenden Datenverkehrs, damit nur ausdrücklich zugelassener Datenverkehr in das Netzwerk gelangen kann.
Unsicheres Protokoll/Dienste/Port	Ein Protokoll, Dienst oder Port, das/der die Sicherheit aufgrund fehlender Kontrollen der Vertraulichkeit und/oder Integrität gefährdet. Zu diesen Sicherheitsrisiken gehören Dienste, Protokolle oder Ports, die Daten und Authentifizierungsinformationen übertragen (z. B. Kennwörter/Kensätze in Klartext über das Internet) oder die aufgrund ihrer Standardeinstellung oder bei Fehlkonfigurationen leicht ausgenutzt werden können. Beispiele für unsichere Dienste, Protokolle oder Ports sind unter anderem FTP, Telnet, POP3, IMAP und SNMP.
IP	Akronym für „Internet Protocol“. Ein Netzwerkprotokoll, das Adress- und einige Steuerungsinformationen enthält, mit deren Hilfe Pakete weitergeleitet werden können. IP ist das primäre Netzwerkprotokoll unter den Internetprotokollen.
IP-Adresse	Auch als „Internetprotokolladresse“ bezeichnet. Ein numerischer Code, der zur eindeutigen Identifizierung eines Computers im Internet dient.
IP-Adress-Spoofing	Von Eindringlingen verwendetes Verfahren, um sich unbefugten Zugriff auf Computer zu verschaffen. 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“. Zusätzlich zum IDS werden beim IPS Eindringungsversuche blockiert.

Begriff	Definition
IPSEC	Abkürzung für „Internet Protocol Security“. Standard zur Sicherung von IP-Kommunikation durch Verschlüsselung und/oder Authentifizierung aller IP-Pakete. IPSEC bietet Sicherheit auf Netzwerkebene.
ISO	Besser bekannt unter „International Organization for Standardization“. Eine internationale Nichtregierungsorganisation von Normungsinstituten aus über 150 Ländern mit einem Vertreter pro Land. Die Zentrale der Organisation befindet sich in Genf, von wo aus das System koordiniert wird.
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.
Schlüssel	In der Kryptografie ist ein Schlüssel ein Algorithmuswert, der auf unverschlüsselten Text angewendet wird, um diesen zu verschlüsseln. Die Länge des Schlüssels bestimmt in der Regel, wie schwierig die Entschlüsselung des Textes der jeweiligen Mitteilung ist. Siehe <i>Starke Kryptographie</i> .
Schlüsselverwaltung	In der Kryptographie beschreibt dies eine Reihe von Prozessen und Mechanismen, die die Erstellung und Pflege von Schlüsseln unterstützen und nach Bedarf ältere Schlüssel durch neue ersetzen.
LAN	Akronym für „Local Area Network“. Ein Computer- und/oder Gerätenetzwerk – oft in einem Gebäude oder in mehreren Gebäuden.
LDAP	Akronym für „Lightweight Directory Access Protocol“. Ein Repository für Authentifizierungs- und Autorisierungsdaten, das zur Abfrage und Änderung von Benutzerrechten und zur Erteilung von Zugriffsrechten auf geschützte Ressourcen verwendet wird.
Protokoll	Siehe <i>Audit-Protokoll</i> .
LPAR	Abkürzung für „Logical 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	Akronym für „Message Authentication Code“. Eine kleine Menge an Informationen, die in der Kryptographie zur Authentifizierung einer Nachricht dient. Siehe <i>Starke Kryptographie</i> .

Begriff	Definition
MAC-Adresse	Abkürzung für „Media Access Control-Adresse“. Ein einmaliger Identifikationswert, den Hersteller Netzwerkadaptern und Netzwerkschnittstellenkarten zuweisen.
Magnetstreifendaten	Auch als „Spurdaten“ 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.
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	Eine Software, die entwickelt wurde, um ohne das Wissen oder die Zustimmung des Benutzers in ein Computersystem einzudringen oder dieses zu beschädigen. Eine solche Software dringt normalerweise in ein Netzwerk ein, während mehrere vom Unternehmen genehmigte Aktivitäten ausgeführt werden. Dies führt zur Ausnutzung von Sicherheitslücken. 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 <i>Abkürzung</i> , um Informationen über den Schutz der PAN, wenn diese in Dateien, Datenbanken usw. gespeichert wird, zu erhalten.
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 Serviceanbieter sein kann, wenn die verkauften Services im Zusammenhang mit der Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten im Namen anderer Händler oder Serviceanbieter stehen. Ein ISP ist beispielsweise ein Händler, der Zahlungskarten für monatliche Abrechnungen akzeptiert, er ist jedoch auch ein Dienstleister, wenn er Händlern Hosting-Dienste anbietet.
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.

Begriff	Definition
MPLS	Akronym für „Multi Protocol Label Switching“. Ein Netzwerk- oder Telekommunikationsmechanismus, der zur Verbindung einer Gruppe von paketvermittelten Netzwerken dient.
NAT	Akronym für „Network Address Translation“. Wird auch als Netzwerkmaskierung oder IP-Maskierung bezeichnet. Änderung einer in einem Netzwerk verwendeten IP-Adresse in eine andere IP-Adresse, die in einem anderen Netzwerk bekannt ist.
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.
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	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 <i>PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren</i> für eine Anleitung über die Nutzung der Netzwerksegmentierung. Die Netzwerksegmentierung ist keine PCI-DSS-Anforderung. Siehe <i>Systemkomponenten</i> .
NIST	Akronym für „National Institute of Standards and Technology“. Nicht-regulative Behörde der technologischen Administration des US-Handelsministeriums. Ziel dieser Behörde ist es, die Innovation und industrielle Wettbewerbsfähigkeit der USA durch Unterstützung von Messwissenschaft, Standards und Technologie zu fördern und so die wirtschaftliche Stabilität und den Lebensstandard zu verbessern.
NMAP	Eine Software für Sicherheitsscans, die Netzwerke abbildet und offene Ports in Netzwerkressourcen erkennt.
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“. Protokoll zur Synchronisation der Uhren von Computersystemen, Netzwerkgeräten und anderen Systemkomponenten.

Begriff	Definition
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.
OWASP	Akronym für „Open Web Application Security Project“. Eine gemeinnützige Organisation, die sich der Verbesserung der Sicherheit von Anwendungssoftware verschrieben hat. OWASP führt eine Liste mit nennenswerten Sicherheitslücken in Webanwendungen. (Siehe http://www.owasp.org).
PA-QSA	Akronym für „Payment Application Qualified Security Assessor“. Ein vom PCI-SSC zugelassenes Unternehmen, um Bewertungen von Zahlungsanwendungen bezüglich ihrer Konformität mit dem PA-DSS durchzuführen.
PAN	Akronym für „Primary Account Number“. Sie wird auch als Kontonummer bezeichnet. Die Zahlungskartenummer (normalerweise eine Kredit- oder Debitkarte), die den Kartenaussteller und das jeweilige Karteninhaberkonto identifiziert.
Kennwort/Kennsatz	Eine Zeichenfolge, die als Authentifizierung des Benutzers dient.
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.
Parametrisierte Abfragen	Eine Methode zur Strukturierung von SQL-Abfragen, um Außerkräftsetzungsversuche zu begrenzen und folglich Injection-Angriffe zu vermeiden.
PAT	Akronym für „Port Address Translation“, auch bezeichnet als „Network Address Port Translation“. Ein Untertyp der NAT, bei dem auch Portnummern umgeschrieben werden.
Patch	Ein Update für eine vorhandene Software, um zusätzliche Funktionalitäten zu installieren oder Fehler zu korrigieren.
Zahlungsanwendung	Anwendungen, die im Zuge der Autorisierung oder Verrechnung Karteninhaberdaten speichern, verarbeiten oder übertragen.
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.
PCI	Akronym für „Payment Card Industry.“

Begriff	Definition
PDA	Akronym für „Personal Data Assistant“ oder „Personal Digital Assistant“. Mobile Handgeräte mit Mobiltelefon-, E-Mail- oder Webbrowserfunktionen.
PED	PIN Entry Device
Penetrationstest	Bei Penetrationstests wird versucht, Schwachstellen ausnutzen, um zu ermitteln, ob unbefugte Zugriffe oder andere böswillige Aktivitäten möglich sind. Der Penetrationstest muss die Netzwerk- und Anwendungsebene umfassen sowie Steuerelemente und Prozesse rund um die Netzwerke und Anwendungen berücksichtigen. Der Test muss von außerhalb des Netzwerks versuchen, in das Netzwerk einzudringen, und er muss innerhalb des Netzwerks durchgeführt werden.
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.
Personenbezogene Informationen	Informationen, die dazu dienen, eine Person zu identifizieren, einschließlich, aber nicht beschränkt auf Name, Anschrift, Sozialversicherungs- und Telefonnummer usw.
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.
POS	Akronym für „Point of Sale“. Eine Hardware und/oder Software, die zur Verarbeitung von Zahlungskartentransaktionen an Handelsstellen verwendet wird.

Begriff	Definition
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.
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.
PTS	Akronym für „PIN Transaction Security“. 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 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, die dem PCI-DSS-Standard entsprechen, sind das Internet, GPRS und GSM.
PVV	Akronym für „PIN Verification Value“. Ein verschlüsselter Wert auf dem Magnetstreifen einer Zahlungskarte.
QSA	Akronym für „Qualified Security Assessor“. Ein vom PCI-SSC zugelassenes Unternehmen, um vor Ort Bewertungen bezüglich der Konformität mit dem PCI-DSS durchzuführen.
RADIUS	Abkürzung für „Remote Authentication Dial-In User Service“. 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 Zwei-Faktor-Authentifizierung einzusetzen.
RBAC	Akronym für „Role-Based Access Control“. Eine Steuerung zur Beschränkung des Zugriffs auf Benutzer, die aufgrund ihrer beruflichen Verantwortlichkeiten einen Informationsbedarf haben.
Remote-Zugriff	Der Zugriff auf Computernetzwerke von einem externen Standort, üblicherweise von außerhalb des Netzwerks. Eine Technologie, die Remote-Zugriff unterstützt, ist beispielsweise <i>VPN</i> .
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.

Begriff	Definition
Konformitätsbericht	Auch als „ROC“ (aus dem Englischen „Report on Compliance“) bezeichnet. Ein detaillierter Bericht, in dem der Konformitätsstatus einer Stelle mit dem PCI-DSS dokumentiert wird.
Validierungsbericht	Auch als „ROV“ (aus dem Englischen „Report on Validation“) bezeichnet. Ein detaillierter Bericht, in dem die Konformität einer Zahlungsanwendung mit dem PCI-DSS dokumentiert wird.
Erneute Schlüsselvergabe	Ein Vorgang, bei dem kryptographische Schlüssel gewechselt werden. Regelmäßige erneute Schlüsselvergaben beschränken die von einem einzigen Schlüssel verschlüsselte Datenmenge.
Externe Laborumgebung	Ein Labor, das nicht vom PA-QSA unterhalten wird.
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.
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.
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.
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.
Salt	Eine zufällige Zeichenfolge, die mit anderen Daten verkettet wird, bevor sie von einer Hash-Funktion verarbeitet wird. Siehe auch <i>Hash</i> .
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 .)

Begriff	Definition
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“. 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.
Sicher mit Wipe löschen	Auch „sicheres Löschen“ genannt. Ein Programm zum permanenten Löschen bestimmter Dateien von einem Computersystem.
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 unter anderen SSL/TLS, IPSEC, SSH, usw.
SBF	Akronym für „Self-Assessment Questionnaire“. Ein Tool einer beliebigen Einheit, um die eigene Konformität mit dem PCI-DSS zu überprüfen.
Zugangsbeschränkte Bereiche	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 Kassbereich im Einzelhandel).
Vertrauliche Authentifizierungsdaten	Sicherheitsinformationen (Kartenprüfcodes/-werte, vollständige Spurdaten, 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, 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.

Begriff	Definition
Dienstleister	Eine Geschäftsentität, die keine Kreditkartengesellschaft ist, die direkt an der Verarbeitung, Speicherung, Übertragung und Vermittlung von Karteninhaberdaten 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. Entitäten wie Telekommunikationsunternehmen, die nur Kommunikationsverbindungen ohne Zugriff auf die Anwendungsebene der Kommunikationsverbindungen bereitstellen, gehören nicht zu dieser Gruppe.
SHA-1/SHA-2	Akronym für „Secure Hash Algorithm“. Ein Satz miteinander verwandter kryptografischer Hash-Funktionen, einschließlich SHA-1 und SHA-2. Siehe <i>Starke Kryptographie</i> .
Smartcard	Auch als „Chipkarte“ oder „IC-Karte (Integrated-Circuit)“ 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“. Unterstützt die Überwachung von Geräten in einem Netzwerk auf jegliche Zustände, die die Aufmerksamkeit eines Administrators erfordern.
Geteiltes Wissen	Zwei oder mehr Stellen verfügen über Teile eines Schlüssels, 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“. 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 entwerfen und/oder sich über den Computer, der die Datenbank hostet, Zugriff auf die Hostcomputer einer Organisation verschaffen.
SSH	Akronym für „Secure Shell“. Eine Protokollsuite, die Verschlüsselungsfunktionen für Netzwerkdienste wie Remoteanmeldung oder Remotedatenübertragung bietet.
SSL	Akronym für „Secure Sockets Layer“. Ein etablierter Branchenstandard, der den Kanal zwischen einem Webbrowser und einem Webserver verschlüsselt und die Vertraulichkeit und Zuverlässigkeit der über diesen Kanal übertragenen Daten gewährleistet.

Begriff	Definition
Statusgesteuerte Inspektion	Auch „dynamische Paketfilterung“ genannt. Eine Firewallfunktion für erweiterte Sicherheit, indem Kommunikationspakete nachverfolgt werden. Nur eingehende Pakete mit einer passenden Antwort („etablierten Verbindungen“) können die Firewall passieren.
Starke Kryptographie	Eine auf industrieerprobten und akzeptierten Algorithmen basierte Kryptographie, zusammen mit starken Schlüssellängen und angemessenen Schlüsselverwaltungspraktiken. Die Kryptographie ist eine Datenschutzmethode, bei der sowohl Verschlüsselungs- (reversibel) als auch Hashing-Verfahren (nicht reversibel, oder unidirektional) eingesetzt werden. Beispiele für industrieerprobte und akzeptierte Standards und Algorithmen zur Verschlüsselung sind unter anderen AES (128 Bits und mehr), TDES (mindestens doppelt lange Schlüssel), RSA (1024 Bits und mehr), ECC (160 Bits und mehr) und ElGamal (1024 Bits und mehr). Für ausführlichere Informationen siehe NIST Special Publication 800-57 (http://csrc.nist.gov/publications/).
SysAdmin	Abkürzung für „Systemadministrator“. Eine Person mit erweiterten Rechten, die für die Verwaltung eines Computersystems oder Netzwerkes verantwortlich ist.
Systemkomponenten	Jegliche Netzwerkkomponenten, Server 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, einschließlich, aber nicht beschränkt auf ausführbare Anwendungsdateien und Konfigurationsdateien, Systemkonfigurationsdateien, Static und Shared Libraries & DLLs, ausführbare Systemdateien, Gerätetreiber und Gerätekonfigurationsdateien sowie zusätzliche 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 Zwei-Faktor-Authentifizierung einzusetzen.
TCP	Akronym für „Transmission Control Protocol“. Eine grundlegende Kommunikationssprache oder -protokoll des Internets.
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 <i>Starke Kryptographie</i> .
TELNET	Abkürzung für „Telephone Network Protocol“. Wird in der Regel zur Bereitstellung von benutzerorientierten Befehlszeilen-Anmeldesitzungen für Geräte in einem Netzwerk verwendet. Benutzerinformationen werden in Klartext übermittelt.

Begriff	Definition
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“. Wurde mit dem Ziel entwickelt, Datensicherheit und -integrität zwischen zwei kommunizierenden Anwendungen zu gewährleisten. TLS ist der Nachfolger von SSL.
Token	Ein von einer Hardware oder Software ausgegebener Wert, der normalerweise mit einem Authentifizierungsserver oder VPN funktioniert, um eine dynamische oder Zwei-Faktor-Authentifizierung zu ermöglichen. Siehe <i>RADIUS</i> , <i>TACACS</i> und <i>VPN</i> .
Transaktionsdaten	Auf elektronische Transaktionen mit Zahlungskarten bezogene Daten.
Trojaner	Auch „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.
Abkürzung	Eine Methode, mit der die vollständige PAN unleserlich gemacht werden kann, indem ein Segment aus den PAN-Daten dauerhaft entfernt wird. Die Abkürzung trägt zum Schutz der PAN bei, wenn diese in Dateien, Datenbanken usw. <u>gespeichert</u> wird. Siehe Stichwort <i>Maskierung</i> , um Informationen über den Schutz der PAN, wenn diese auf Bildschirmen, Belegen usw. <u>angezeigt</u> wird, zu erhalten.
Vertrauenswürdige Netzwerk	Ein Netzwerk einer Organisation, das sich innerhalb der Kontroll- oder Verwaltungsmöglichkeiten dieser Organisation befindet.
Zwei-Faktor-Authentifizierung	Eine Methode zur Authentifizierung eines Benutzers, bei der zwei oder mehrere Faktoren überprüft werden. Diese Faktoren umfassen etwas, das der Benutzer hat (z. B. ein Hardware- oder Software-Token), etwas, das der Benutzer weiß (z. B. ein Kennwort, Kennsatz oder ein PIN), und etwas, das der Benutzer ist (z. B. Fingerabdrücke oder andere biometrische Daten).
Nicht vertrauenswürdige Netzwerk	Ein Netzwerk, das außerhalb der Netzwerke liegt, die zu einer Organisation gehören und das außerhalb der Kontroll- oder Verwaltungsmöglichkeiten der Organisation liegt.
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.

Begriff	Definition
Virtueller Hypervisor	Siehe <i>Hypervisor</i> .
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.
Virtueller Rechner	Eine unabhängige Betriebsumgebung, die sich wie ein separater Computer verhält. Der virtuelle Rechner wird auch „Guest“ bezeichnet und läuft auf einem Hypervisor.
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.
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.
Virtual-Terminal	Ein virtuelles Terminal ist ein Webbrowser-basierter Zugriffspunkt auf die Website eines Acquirers, eines Verarbeitungsunternehmens oder einen Drittanbieters zur Autorisierung von Transaktionen mit Zahlungskarten; auf dieser Website gibt ein Händler manuell Karteninhaberdaten über einen sicher verbundenen Webbrowser ein. Anders als bei physischen Terminals, lesen virtuelle Terminals keine Daten direkt von Zahlungskarten. Da die Transaktionen mit Zahlungskarten manuell eingegeben werden, werden in Händlerumgebungen mit niedrigen Transaktionsvolumen virtuelle Terminals häufig anstatt physischer Terminals eingesetzt.
VLAN	Abkürzung für „Virtual LAN“ oder „Virtual Local Area Network“. Ein logisches lokales Netzwerk, mit einer weit größeren Reichweite als herkömmliche lokale Netzwerke.
VPN	Akronym für „Virtual Private Network“. 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.
WAN	Akronym für „Wide Area Network“. Ein Computernetzwerk, das einen großen Bereich abdeckt, oft auch ein regionales oder unternehmensweites Computersystem.

Begriff	Definition
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“. Ein schwacher Algorithmus zur Verschlüsselung drahtloser Netzwerke. Branchenexperten haben schwerwiegende Schwächen entdeckt, durch die eine WEP-Verbindung innerhalb von Minuten mithilfe gängiger Software geknackt werden kann. Siehe <i>WPA</i> .
Drahtloser Zugriffspunkt	Auch bezeichnet als „AP“, Akronym aus dem Englischen für Access Point. 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“. 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.