



Payment Card Industry (PCI)- Datensicherheitsstandard (DSS) und Payment Application (PA)- Datensicherheitsstandard (PA-DSS)

Glossar für Begriffe, Abkürzungen und Akronyme

Version 1.2

Oktober 2008

Begriff	Definition
AAA	Akronym für „authentication, authorization, and accounting“. Dieses Protokoll dient der Benutzerauthentifizierung basierend auf den verifizierbaren Identitätsdaten, der Benutzerautorisierung entsprechend der zugewiesenen Benutzerrechte und der Berechnung der Netzwerkressourcen, die von einem Benutzer verbraucht werden.
Abkürzung	Methode, mit der die vollständige PAN unlesbar gemacht wird, indem ein Segment der PAN-Daten dauerhaft entfernt wird.
Acquirer	Auch als „akquirierende Bank“ oder „akquirierende Finanzinstitution“ bezeichnet. Der Acquirer begründet und pflegt Beziehungen mit Händlern im Sinne der Verbreitung von Zahlungskarten.
Adware	Schadprogramm, das nach einer Installation den Computer zwingt, automatisch Werbung anzuzeigen oder herunterzuladen.
AES	Abkürzung für „Advanced Encryption Standard“. Das symmetrische Kryptosystem mit Blockchiffren wurde im November 2001 vom NIST (National Institute of Standards and Technology) als U.S FIPS PUB 197 (oder kurz „FIPS 197“) bekannt gegeben. Siehe <i>Starke Kryptographie</i> .
Anfälligkeit	Eine Systemschwachstelle, die von böswilligen Personen ausgenutzt werden, um das System anzugreifen und die Integrität zu verletzen.
ANSI	Akronym für „American National Standards Institute“. Eine private, gemeinnützige Organisation, die das freiwillige Standardisierungs- und Konformitätsbewertungssystem der USA verwaltet und koordiniert.
Antivirensoftware	Programm oder Software zur Erkennung und Beseitigung von bzw. zum Schutz vor diversen Arten von bösartiger Software (auch „Malware“ oder „Schadprogramme“ genannt), z. B. Viren, Würmer, Trojaner (oder trojanische Pferde), Spyware, Adware und Rootkits.
Anwendung	Die Gesamtheit sämtlicher gekaufter oder individuell zusammengestellter Softwareprogramme oder Programmgruppen, inklusive interner und externer (z. B. Web-) Anwendungen.
ASV	Akronym für „Approved Scanning Vendor“. Ein Unternehmen, das vom PCI SSC geprüft wurde und externe Dienste für Anfälligkeitsscans anbieten darf.
Aufgabentrennung	Verfahren, bei dem einzelne Funktionsschritte auf verschiedene Personen aufgeteilt werden, sodass keine Einzelperson den kompletten Prozess unterwandern kann.
Authentifizierung	Der Prozess der Überprüfung der Identität von Personen, Geräten oder Prozessen.
Autorisierung	Das Gewähren von Zugriff oder anderen Rechten für Benutzer, Programme oder Prozesse. In einem Netzwerk bestimmt die Autorisierung, was eine Person oder ein Programm nach erfolgreicher Authentifizierung tun darf. Im Zusammenhang mit Zahlungskartentransaktionen ist die Autorisierung der Punkt, an dem ein Händler die Berechtigung erhält, eine Zahlungskarte für eine bestimmte Transaktion zu verwenden.
Backup	Eine Sicherungskopie von Daten für Archivierungszwecke oder zum Schutz vor Schaden oder Verlust.

Begriff	Definition
Bedrohung	Eine Bedingung oder Aktivität, die dazu führen kann, dass Informationen oder Ressourcen zur Informationsverarbeitung absichtlich oder versehentlich verloren gehen, geändert, offengelegt, dauerhaft gesperrt oder in anderer Weise zum Schaden eines Unternehmens betroffen werden.
Betriebssystem/BS	Die Software eines Computersystems, die für die Verwaltung und Koordinierung sämtlicher Aktivitäten sowie die Freigabe von Computerressourcen verantwortlich ist. Zu den Betriebssystemen gehören z. B. Microsoft Windows, Mac OS, Linux und Unix.
Bluetooth	Ein Protokoll für die drahtlose Kommunikation im Nahbereich zur einfacheren Datenübertragung zwischen zwei Geräten über kurze Entfernungen.
CIS	Akronym für „Center for Internet Security“ (Zentrum für Internetsicherheit). Ein gemeinnütziges Unternehmen, das anderen Organisationen dabei hilft, die Risiken im Geschäft und im E-Commerce, die durch nicht angemessene technische Sicherheitskontrollen auftreten können, zu minimieren.
Datenbank	Ein strukturiertes Format zur Organisation und Pflege leicht abzurufender Informationen. In ihrer einfachsten Form sind Datenbanken zum Beispiel Tabellen und Kalkulationsbögen.
Datenbankadministrator	Auch als „DBA“ bezeichnet. Die Person, die für die Verwaltung und Administration von Datenbanken zuständig ist.
Datenhygiene	Löschen sensibler Daten aus einer Datei, einem Gerät oder einem System oder Ändern von Daten, sodass sie bei einem böswilligen Zugriff nutzlos sind.
Datenträgerverschlüsselung	Technik oder Technologie (Software oder Hardware) zu Verschlüsselung sämtlicher auf einem Gerät (z. B. einer Festplatte oder einem Flash-Laufwerk) gespeicherten Daten. Alternativ wird die <i>Verschlüsselung auf Dateiebene</i> oder <i>Datenbankverschlüsselung auf Spaltenebene</i> genutzt, um Inhalte spezifischer Dateien oder Spalten zu verschlüsseln.
Dienstanbieter	Ein Unternehmen, bei dem es sich nicht um eine Marke für Zahlungsanwendungen handelt, das direkt in die Verarbeitung, Speicherung oder Übertragung von Karteninhaberdaten involviert ist. Hierzu gehören auch Unternehmen, die Dienste anbieten, mit denen die Sicherheit von Karteninhaberdaten kontrolliert wird bzw. die einen Einfluss auf die Sicherheit haben könnten. Dienstanbieter sind z. B. Anbieter von verwalteten Firewalls, IDS- und anderen Diensten, sowie Hosting-Anbieter und andere Unternehmen. Unternehmen wie etwa Telekommunikationsfirmen, die nur Kommunikationsverbindungen ohne Zugriff auf die Anwendungsebene der Kommunikationsverbindung anbieten, gehören nicht hierzu.
DMZ	Abkürzung für „demilitarized zone“ (entmilitarisierte Zone). Ein physisches oder logisches Sub-Netzwerk oder ein Computer-Host, der eine zusätzliche Sicherheitsebene für das interne Privatnetzwerk eines Unternehmens bereitstellt. Die DMZ fügt eine zusätzliche Netzwerksicherheitsebene zwischen dem Internet und dem internen Netzwerk eines Unternehmens ein, sodass externe Parteien nur direkt auf Geräte in der DMZ und nicht auf das gesamte interne Netzwerk zugreifen können.
DNS	Akronym für „Domain Name System“ oder „Domain Name Server“. Ein System, das Informationen für bestimmte Domännennamen in einer über verschiedene Netzwerke wie das Internet verteilte Datenbank speichert.
Drahtlosnetzwerke	Netzwerke, die Computer ohne physische Kabelverbindung miteinander verbinden.

Begriff	Definition
DSS	Akronym für „Data Security Standard“ (Datensicherheitsstandard), wie auch in „PCI-DSS“.
Duale Kontrolle	Vorgehensweise, bei der zwei oder mehr separate Stellen (üblicherweise Personen) zusammen arbeiten, um sensible Funktionen oder Informationen zu schützen. Beide Stellen sind gleichermaßen für den physischen Schutz der in anfällige Transaktionen involvierten Materialien verantwortlich. Es wird keiner Einzelperson gestattet, auf die Materialien (z. B. einen kryptographischen Schlüssel) zuzugreifen oder diese zu nutzen. Für die manuelle Erzeugung von Schlüsseln, die Übertragung, das Laden, die Speicherung und das Abrufen erfordert die duale Kontrolle eine Aufteilung der Kenntnis des Schlüssels unter den Stellen. (Siehe auch <i>Geteiltes Wissen</i> .)
Dynamische Paketfilterung	Siehe <i>Statusgesteuerte Inspektion</i> .
ECC	Akronym für „Elliptic Curve Cryptography“. Ein Ansatz für die Kryptographie öffentlicher Schlüssel basierend auf elliptischen Kurven über endlichen Körpern. Siehe <i>Starke Kryptographie</i> .
Egress Filtering	Methode zum Filtern von aus einem internen Netzwerk über einen Router ausgehendem Datenverkehr, damit nicht autorisierte Daten niemals das interne Netzwerk verlassen.
Elektronische Wechselmedien	Medien, auf denen digitale Daten gespeichert werden und die leicht entfernt und/oder von einem Computersystem zum anderen transportiert werden können. Hierzu gehören CD-ROM, DVD-ROM, USB-Flashlaufwerke und mobile Festplatten.
Entmagnetisierung	Auch als „Datenträgerentmagnetisierung“ bezeichnet. Die Verfahrensweise oder Technik, mit der ein Datenträger entmagnetisiert wird, wodurch sämtliche darauf gespeicherten Daten unwiederbringlich zerstört werden.
Erneute Schlüsselvergabe	Prozess der Änderung kryptographischer Schlüssel zur Begrenzung der Datenmenge, die mit demselben Schlüssel verschlüsselt werden können.
FIPS	Akronym für „Federal Information Processing Standards“. Normen, die öffentlich durch die US-Regierung anerkannt sind, und auch durch Nichtregierungsbehörden und Subunternehmer genutzt werden.
Firewall	Eine Hardware- und/oder Softwaretechnologie, die die Netzwerkressourcen vor nicht autorisierten Zugriffen schützt. Eine Firewall gestattet oder verhindert, dass Datenverkehr zwischen Netzwerken fließen kann. Hierfür kommen unterschiedliche Sicherheitsebenen basierend auf einer Reihe von Regeln und weiteren Kriterien zum Einsatz.
Forensik	Auch als „Computerforensik“ bezeichnet. Da sich der Begriff hier auf Informationssicherheit bezieht, meint Forensik die Anwendung von Ermittlungstools und Analysetechniken zum Sammeln von Hinweisen auf einer Computerressource, um den Grund von Datenschutzverletzungen festzustellen.
FTP	Akronym für „File Transfer Protocol“. Ein Netzwerkprotokoll, das zur Übertragung von Daten von einem Computer auf einen anderen über ein öffentliches Netzwerk wie das Internet genutzt wird. FTP wird weithin als unsicheres Protokoll angesehen, da Kennwörter und Dateinhalte ungeschützt als unverschlüsselter Text gesendet werden. FTP lässt sich aber sicher mit der SSH- oder anderen Technologien implementieren.

Begriff	Definition
Geteiltes Wissen	Dies meint, dass das Wissen über einen kryptographischen Schlüssel auf zwei oder mehrere Parteien aufgeteilt wird, die die Komponenten der jeweils anderen Parteien nicht kennen.
GPRS	Akronym für „General Packet Radio Service“. Ein mobiler Datendienst für Nutzer von GSM-Mobiltelefonen. GPRS ist für die effiziente Nutzung begrenzter Bandbreiten bekannt und eignet sich besonders für das Senden und Empfangen kleiner Datenmengen wie z. B. E-Mails und für Web-Browsing.
GSM	Akronym für „Global System for Mobile Communications“. Verbreiteter Standard für Mobiltelefone und Netzwerke. Die Allgegenwärtigkeit des GSM-Standards ermöglicht das internationale Roaming zwischen Mobilfunkanbietern, sodass Kunden ihre Telefone in vielen Teilen der Welt nutzen können.
Händler	Im Sinne des PCI-DSS wird als Händler jede Stelle bezeichnet, die Zahlungskarten der fünf PCI-SSC-Mitglieder (American Express, Discover, JCB, MasterCard oder Visa) für die Zahlung von Waren und/oder Dienstleistungen akzeptiert. Es ist zu beachten, dass ein Händler, der Zahlungskarten für die Zahlung von Waren und/oder Dienstleistungen annimmt, auch ein Dienstleister sein kann, wenn die verkauften Dienstleistungen zur Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten im Auftrag anderer Händler oder Dienstleister führt. Ein ISP ist beispielsweise ein Händler, der Zahlungskarten für die monatliche Abrechnung akzeptiert, er ist aber auch ein Dienstleister, wenn er Händler als Kunden hostet.
Hashing	Der Prozess der Unlesbarmachung von Karteninhaberdaten mithilfe einer Konvertierung der Daten in eine Nachrichtenzusammenfassung mit fester Länge über <i>starke Kryptographie</i> .
Host	Der Hauptcomputer (Hardware), auf dem sich die Computersoftware befindet.
Hosting-Anbieter	Bietet Händlern und anderen Dienstleister verschiedene Services an. Diese können einfach oder komplex sein, von der Bereitstellung gemeinsam genutzten Speicherplatzes auf einem Server bis hin zu einer ganzen Reihe von „Warenkorb“-Optionen, von Zahlungsanwendungen hin zu Verbindungen mit Zahlungs-Gateways und -Prozessoren sowie für das Hosting dedizierter Server für jeweils nur einen Kunden. Ein Hosting-Anbieter kann auch ein gemeinsam genutzter Hosting-Anbieter sein, der mehrere Unternehmen auf einem einzigen Server hostet.
HTTP	Akronym für „Hypertext Transfer Protocol“. Ein offenes Internetprotokoll für die Übertragung oder Bereitstellung von Informationen im World Wide Web.
HTTPS	Akronym für „Hypertext Transfer Protocol Secure“. Ein sicheres HTTP, das Authentifizierungs- und Verschlüsselungsmethoden für die Kommunikation im Internet bietet und für sensible Daten wie webbasierte Anmeldeinformationen entwickelt wurde.
ID	Der Bezeichner (Name) eines bestimmten Benutzers oder einer Anwendung.

Begriff	Definition
IDS	Akronym für „Intrusion Detection System“. Software oder Hardware zur Erkennung von Eindringversuchen in Netzwerken oder Systemen und zur Alarmierung. Das System besteht aus Sensoren, die Sicherheitsereignisse erzeugen, einer Konsole zur Überwachung von Ereignissen und Alarmen und zur Sensorensteuerung sowie eine zentrale Engine, die von Sensoren protokollierte Ereignisse in einer Datenbank aufzeichnet. Mithilfe eines Regelsystems werden Alarme als Reaktion auf erkannte Sicherheitsereignisse erzeugt.
IETF	Akronym für „Internet Engineering Task Force“. Eine große, offene, internationale Gemeinschaft von Netzwerkentwicklern, Betreibern, Anbietern und Forschern, die sich mit der Weiterentwicklung der Internetarchitektur und einer Betriebsoptimierung im Internet beschäftigen. Die IETF erfordert keine offizielle Mitgliedschaft und steht allen interessierten Personen offen.
Index-Token	Ein kryptographischer Token, durch den die PAN anhand eines bestimmten Index durch einen unvorhersehbaren Wert ersetzt wird.
Informationssicherheit	Der Schutz von Informationen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit.
Informationssystem	Eine eigene Reihe strukturierter Datenressourcen, die zur Erhebung, Verarbeitung, Pflege, (gemeinsamen) Nutzung, Weitergabe oder Löschung von Informationen organisiert werden.
Ingress Filtering	Methode zum Filtern von Datenverkehr, der über einen Router in ein internes Netzwerk geht. Bei eingehenden Paketen wird geprüft, ob diese tatsächlich von den angegebenen Netzwerken stammen.
IP	Akronym für „Internet Protocol“. Protokoll auf Netzwerkebene, das Adressinformationen und einige Steuerungsinformationen zur Paketweiterleitung enthält. IP ist das Hauptprotokoll auf Netzwerkebene in der Reihe der Internetprotokolle.
IP Address Spoofing	Eine Angriffstechnik, die von böswilligen Personen genutzt wird, um nicht autorisierten Zugriff auf Computer zu erlangen. Der Angreifer sendet betrügerische Nachrichten an einen Computer und verwendet dafür eine IP-Adresse, die Anzeigt, dass die Nachricht von einem vertrauenswürdigen Host stammt.
IP-Adresse	Auch als „Internet Protocol Address“ bezeichnet. Ein numerischer Code, der einen bestimmten Computer eindeutig im Internet ausweist.
IPS	Akronym für „Intrusion Prevention System“. Neben dem IDS bietet das IPS eine zusätzliche Maßnahme zum Blockieren von Eindringversuchen.
IPSEC	Akronym für „Internet Protocol Security“. Standard für die Sicherung von IP-Kommunikation durch Verschlüsselung und/oder Authentifizierung aller IP-Pakete. IPSEC bietet Sicherheit auf der Netzwerkebene.
ISO	Besser bekannt als „Internationale Organisation für Normung“. Eine Nichtregierungsorganisation bestehend aus einem Netzwerk der nationalen Institute für Normung aus über 150 Ländern mit einem Mitglied pro Land und einem Zentralsekretariat in Genf, das mit der Koordination des Systems betraut ist.
Kartenumittent	Auch als „emittierende Bank“ oder „emittierende Finanzinstitution“ bezeichnet. Stelle, die Zahlungskarten direkt an Verbraucher und Nichtverbraucher ausgibt.

Begriff	Definition
Kennwort/Kennsatz	Eine Zeichenfolge zur Authentifizierung des Benutzers.
Kompensationskontrollen	<p>Kompensationskontrollen können in Fällen, in denen eine Stelle eine explizite Anforderung aufgrund von legitimen technischen oder dokumentierten geschäftlichen Einschränkungen nicht exakt erfüllen kann, in Erwägung gezogen werden. Voraussetzung hierfür ist jedoch, dass der mit der Nichterfüllung verbundene Risikozuwachs durch die Implementierung von Kontrollen an anderer Stelle kompensiert wird. Kompensationskontrollen müssen:</p> <ol style="list-style-type: none"> <li data-bbox="516 537 1393 590">(1) In Absicht und Anspruch den ursprünglichen PCI-DSS-Anforderungen entsprechen <li data-bbox="516 604 1338 657">(2) Ein vergleichbares Schutzniveau wie die ursprüngliche PCI-DSS-Anforderung bereitstellen <li data-bbox="516 672 1393 724">(3) Mindestens so weitreichend wie andere PCI-DSS-Anforderungen sein (nicht nur konform mit weiteren PCI-DSS-Anforderungen) <li data-bbox="516 739 1393 791">(4) Dem zusätzlichen Risiko, das durch die Nichteinhaltung der PCI-DSS-Anforderung entsteht, angemessen sein <p>Siehe auch die Anhänge B und C für Kompensationskontrollen in <i>PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren</i> für Anweisungen zur Verwendung von Kompensationskontrollen.</p>
Konformitätsbericht	Auch als „Report on Compliance“, kurz „ROC“ bezeichnet. Ein Bericht mit detaillierten Informationen zum Konformitätsstatus einer Stelle entsprechend dem PCI-DSS.
Konsole	Einheit aus Bildschirm und Tastatur für den Zugriff und die Steuerung des Servers oder Mainframe-Computers in einer Netzwerkumgebung.
Kontonummer	Siehe <i>Primary Account Number (PAN)</i> .
Kryptographie	Disziplin der Mathematik und Computerwissenschaft, die sich mit Informationssicherheit, speziell mit Verschlüsselung und Authentifizierung beschäftigt. In Anwendungen und Netzwerksicherheit ist Kryptographie ein Tool für die Zugriffskontrolle und die Sicherung der Vertraulichkeit und Integrität von Informationen.
LAN	Akronym für „Local Area Network“. Computernetzwerk für einen kleinen Bereich, oft ein Gebäude oder eine Gruppe von Gebäuden.
LDAP	Akronym für „Lightweight Direct Access Protocol“. Ein Datenspeicher zur Authentifizierung und Autorisierung, der zur Abfrage und Bearbeitung von Benutzerberechtigungen und zum Gewähren von Zugriff auf geschützte Ressourcen genutzt wird.
LPAR	Abkürzung für „Logical Partition“. Ein System zur Unterteilung oder „Partitionierung“ der Ressourcen eines Computers – Prozessoren, Arbeitsspeicher und Massenspeicher – in kleinere Einheiten, die mit einer eigenen Kopie des Betriebssystems und der Anwendungen ausgeführt werden. Die logische Partitionierung wird üblicherweise genutzt, um die Nutzung verschiedener Betriebssysteme und Anwendungen auf einem einzigen Gerät zu ermöglichen. Die Partitionen können bei Bedarf für eine Kommunikation untereinander oder die gemeinsame Nutzung bestimmter Serverressourcen, etwa der Netzwerkschnittstellen, konfiguriert werden.
MAC	Akronym für „Message Authentication Code“. In der Kryptographie bezeichnet diese eine kleine Menge von Informationen, die zur Authentifizierung einer Nachricht genutzt wird. Siehe <i>Starke Kryptographie</i> .

Begriff	Definition
MAC-Adresse	Abkürzung für „Media Access Controll-Adresse“. Ein eindeutiger Wert, der Netzwerkadaptern und Netzwerkschnittstellenkarten durch den Hersteller zugewiesen wird.
Magnetstreifendaten	Auch als „Verfolgungsdaten“ bezeichnet. Im Magnetstreifen oder auf dem Chip verschlüsselte Daten, die bei der Autorisierung während einer Transaktion verwendet werden. Hierbei kann es sich um das Magnetstreifen-Image auf einem Chip oder um die Daten auf Spur 1 und/oder Spur 2 des Magnetstreifens handeln. Stellen dürfen nach der Transaktionsautorisierung keine vollständigen Magnetstreifendaten speichern.
Mainframe	Computer, die zur Handhabung großer Dateneingabe- und -ausgabemengen entwickelt wurden und eine Durchsatz-Datenbearbeitung ermöglichen. Mainframes können mehrere Betriebssysteme ausführen und somit scheinbar als mehrere Computer operieren. Viele ältere Systeme sind als Mainframes entwickelt.
Masking	Methode zur Tarnung von Datensegmenten bei der Anzeige. Masking wird genutzt, wenn es nicht erforderlich ist, die gesamte PAN anzuzeigen.
MPLS	Akronym für „Multi Protocol Label Switching“. Netzwerk- oder Telekommunikationsmechanismus zur Verbindung einer Gruppe von PSN (Packet-Switched Networks).
NAT	Akronym für „Network Address Translation“. Auch bekannt als Netzwerk- oder IP-Maskierung. Die Änderung einer IP-Adresse, die innerhalb eines Netzwerks verwendet wird, in eine andere IP-Adresse, die in einem anderen Netzwerk bekannt ist.
Netzwerk	Zwei oder mehr Computer, die zur gemeinsamen Nutzung von Ressourcen miteinander verbunden sind.
Netzwerkkomponenten	Netzwerkkomponenten umfassen unter anderem Firewalls, Switches, Router, Zugriffspunkte für drahtlose Netzwerke, Netzwerkgeräte und andere Sicherheitsgeräte.
Netzwerksegmentierung	Methode zur Reduzierung des Umfangs einer PCI-DSS-Bewertung durch Reduzieren der Größe der Karteninhaberdatenumgebung. Um dies zu erreichen, sollten Systeme, die keine Karteninhaberdaten speichern, verarbeiten oder übertragen können, von den Systemen, die dies können, über Netzwerksteuerungen getrennt werden. Weitere Informationen zur Nutzung der Netzwerksegmentierung stehen im Abschnitt „Netzwerksegmentierung“ im Dokument <i>PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren</i> zur Verfügung.
Netzwerksicherheitsscan	Prozess zur Remote-Prüfung von Systemen einer Stelle auf Anfälligkeiten mithilfe manuell bedienbarer oder automatischer Tools. Zu Sicherheitsscans gehören die Nachforschungen in internen und externen Systemen und die Berichterstellung zu Diensten, die im Netzwerk anfällig sind. Bei Scans können Anfälligkeiten von Betriebssystemen, Diensten und Geräten gefunden werden, die von böswilligen Personen ausgenutzt werden könnten.
Nicht vertrauenswürdige Netzwerk	Ein Netzwerk, das außerhalb der unternehmenseigenen Netzwerke liegt und damit nicht vom Unternehmen kontrolliert oder verwaltet werden kann.
Nichtverbraucherbenutzer	Personen, ausgenommen Karteninhaber, die auf Systemkomponenten zugreifen, darunter Mitarbeiter, Administratoren und dritte Parteien.

Begriff	Definition
NIST	Akronym für „National Institute of Standards and Technology“. Nicht-regulative Behörde innerhalb der Technologieadministration des US-Handelsministeriums. Ziel des NIST ist das Vorantreiben von Innovationen und industrieller Wettbewerbsfähigkeit in den USA durch Fortschritte bei Messwissenschaft, -standards und -technologie zur Verbesserung der wirtschaftlichen Sicherheit und der Lebensqualität.
NMAP	Software für Sicherheitsscans, mit der Netzwerke „kartographiert“ und offene Ports in Netzwerkressourcen gefunden werden können.
NTP	Akronym für „Network Time Protocol“. Protokoll zur Synchronisierung der Uhren von Computersystemen in PSN (Packet-Switched Networks) mit variabler Latenz.
Öffentliches Netzwerk	Ein durch einen Telekommunikationsanbieter eingerichtetes und betriebenes Netzwerk für die öffentliche Bereitstellung von Datenübertragungsdiensten. Daten in öffentlichen Netzwerken können während der Übertragung abgefangen, modifiziert und/oder zweckentfremdet werden. Zu den vom PCI-DSS abgedeckten öffentlichen Netzwerken gehören das Internet sowie Drahtlos- und Mobiltechnologien.
OWASP	Akronym für „Open Web Application Security Project“. Eine 2004 gegründete gemeinnützige Organisation, die sich der Verbesserung der Sicherheit von Anwendungssoftware widmet. OWASP hat die OWASP Top Ten veröffentlicht, eine Liste der größten Anfälligkeiten von Webanwendungen. (Siehe http://www.owasp.org).
Pad	In der Kryptographie wird ein Verschlüsselungsalgorithmus, bei dem Text mit einem Zufallsschlüssel oder „Pad“ verschlüsselt wird, der genauso lang wie der Text ist und nur einmal verwendet wird, als „One-Time-Pad“ bezeichnet. Wenn der Schlüssel wirklich zufällig ist, nie wiederverwendet wird und absoluter Geheimhaltung unterliegt, kann das One-Time-Pad nicht geknackt werden.
PAN	Akronym für „Primary Account Number“, auch als „Kontonummer“ bezeichnet. Die eindeutige Nummer einer Zahlungskarte (üblicherweise Kredit- oder Debitkarten), mit der der Emittent und das jeweilige Karteninhaberkonto identifiziert werden.
PA-QSA	Akronym für „Payment Application Qualified Security Assessor“. Ein vom PCI SSC bestätigtes Unternehmen, das zur Durchführung von Bewertungen von Zahlungsanwendungen anhand des PA-DSS berechtigt ist.
PAT	Akronym für „Port Address Translation“ auch als „Network Address Port Translation“ bezeichnet. NAT, bei der auch die Portnummern übersetzt werden.
Patch	Aktualisierung bestehender Software um weitere Funktionen oder zur Fehlerbehebung.
PCI	Die Zahlungskartenbranche („Payment Card Industry“).
PDA	Akronym für „Personal Data Assistant“ oder „Personal Digital Assistant“. Mobile Handheld-Geräte mit Funktionen wie Mobiltelefonie, E-Mail oder Webbrowser.

Begriff	Definition
Penetrationstest	Bei Penetrationstests wird versucht, Schwachstellen auszunutzen, um zu prüfen, ob eine nicht autorisierter Zugriff oder sonstige böswillige Aktivitäten möglich sind. Penetrationstests umfassen die Netzwerk- und Anwendungsebene und berücksichtigen Steuerelemente und Prozesse rund um die Netzwerke und Anwendungen. Der Test muss von außerhalb des Netzwerks versuchen, in das Netzwerk einzudringen, und er muss innerhalb des Netzwerks durchgeführt werden.
PIN	Akronym für „Personal Identification Number“. Ein geheimes numerisches Kennwort, das nur dem Benutzer und einem System zur Benutzerauthentifizierung bekannt ist. Der Benutzer erhält nur Zugriff, wenn die eingegebene PIN mit der PIN im System übereinstimmt. Ein typisches Anwendungsgebiet für PINs sind Geldautomaten. Weiterhin werden PINs in EMV-Chipkarten genutzt, bei denen die PIN die Unterschrift des Karteninhabers ersetzt.
POS	Akronym für „Point of Sale“. Hardware und/oder Software, die zur Verarbeitung von Zahlungskartentransaktionen an Händlerstandorten genutzt wird.
Privates Netzwerk	Von einem Unternehmen eingerichtetes Netzwerk, das privaten IP-Adressraum nutzt. Private Netzwerke sind normalerweise als LANs eingerichtet. Der Zugriff auf private Netzwerke von öffentlichen Netzwerken aus sollte ordnungsgemäß mit Firewalls und Routern geschützt sein.
Protokoll	Die beschlossene Methode zur Kommunikation innerhalb von Netzwerken. Eine Spezifikation, in der Regeln und Verfahrensweisen beschrieben werden, die von Computerprodukten bei der Durchführung von Aktivitäten in einem Netzwerk befolgt werden sollten.
Prüfprotokoll	Auch als „Audit-Trail“ oder Prüfverfahren bezeichnet. Die chronologische Aufzeichnung der Systemaktivitäten. Mit dem bereitgestellten Protokoll können Umgebungs- und Aktivitätsabläufe im Rahmen oder mit dem Zweck einer Operation, Verfahrensweise oder eines Ereignisses innerhalb einer Transaktion vom Start bis zu den Endergebnissen rekonstruiert, überprüft und untersucht werden.
PVV	Akronym für „PIN Verification Value“. Ein freiwillig eingesetzter Prüfwert, der verschlüsselt auf dem Magnetstreifen einer Zahlungskarte liegt.
QSA	Akronym für „Qualified Security Assessor“. Ein vom PCI SSC bestätigtes Unternehmen, das zur Durchführung von Vor-Ort-Bewertungen anhand des PCI-DSS berechtigt ist.
RADIUS	Abkürzung für „Remote Authentication and Dial-In User Service“. Ein System zur Authentifizierung und Abrechnung. Das System prüft, ob an den RADIUS-Server übermittelte Informationen wie Benutzername und Kennwort korrekt sind und autorisiert dann den Systemzugriff.
RBAC	Akronym für „Role-based Access Control“. Die Kontrolle zur Einschränkung des Zugriffs durch bestimmte autorisierte Benutzer, basierend auf ihrer jeweiligen Verantwortlichkeit.
Remote-Zugriff	Zugriff auf Computernetzwerke von einem entfernten Standort, üblicherweise von außerhalb des Netzwerks, aus. Ein Beispiel für eine Remote-Zugriffstechnologie ist VPN.

Begriff	Definition
Richtlinie	Unternehmensweite Regeln zur Verwendung von Computerressourcen, zu Sicherheitspraktiken und für Hilfestellung bei der Entwicklung von Betriebsverfahrensweisen.
Risikoanalyse/-bewertung	Prozess zur Identifizierung wertvoller Systemressourcen sowie von Bedrohungen. Basierend auf der geschätzten Häufigkeit und den voraussichtlichen Kosten von Bedrohungen wird der potenzielle Verlust kalkuliert. Optional werden Empfehlungen zur Zuweisung von Ressourcen für Gegenmaßnahmen gegeben, um die Gefährdung zu minimieren.
Rootkit	Ein Schadprogramm, das nach nicht autorisierter Installation seine Präsenz verschleiern kann und die administrative Kontrolle über ein Computersystem übernehmen kann.
Router	Eine Hard- oder Software zur Verbindung von zwei oder mehr Netzwerken. Sortiert und interpretiert Adressen und durchgehende Daten und ordnet diese entsprechend zu. Software-Router werden gelegentlich auch als Gateways bezeichnet.
RSA	Algorithmus für die Kryptographie öffentlicher Schlüssel, beschrieben 1977 von Ron Rivest, Adi Shamir und Len Adleman vom Massachusetts Institute of Technology (MIT). Die Buchstaben RSA stehen für die Initialen der Vornamen dieser Wissenschaftler.
SANS	Akronym für „SysAdmin, Audit, Networking and Security“, ein Institut, das Schulungen zur Computersicherheit und professionelle Zertifizierungen anbietet. (Siehe www.sans.org .)
SBF	Akronym für „Selbstbeurteilungs-Fragebogen.“ Ein Tool, mit dem eine beliebige Stelle ihre PCI-DSS-Konformität validieren kann.
Schadprogramme/ Malware	Software zum Infiltrieren oder Beschädigen eines Computersystems ohne das Wissen oder die Zustimmung des Eigentümers. Diese Programme dringen üblicherweise zusammen mit geschäftlich bestätigten Aktivitäten in Netzwerke ein und nutzen Schwachstellen im System aus. Als Beispiele seien Viren, Würmer, Trojaner (auch „Trojanische Pferde“ genannt), Spyware, Adware und Rootkits genannt.
Schlüssel	In der Kryptographie ist ein Schlüssel ein Wert, der die Ausgabe eines Verschlüsselungsalgorithmus bei der Umwandlung von unverschlüsseltem in verschlüsselten Text festlegt. Die Länge des Schlüssels bestimmt im Allgemeinen, wie schwierig es ist, den Text in einer gegebenen Nachricht zu entschlüsseln. Siehe <i>Starke Kryptographie</i> .
SDLC	Akronym für „System Development Life Cycle“. Die Entwicklungsphasen für eine Software oder ein Computersystem, von der Planung über Analyse, Design, und Tests bis hin zur Implementierung.
Secure Wipe	Auch als „sicheres Lösungsverfahren“ bezeichnet. Ein Dienstprogramm, das spezifische Dateien permanent von einem Computersystem löscht.
Sensibler Bereich	Rechenzentren, Serverräume und andere Bereiche, in denen sich Systeme befinden, auf denen Karteninhaberdaten gespeichert, verarbeitet oder übertragen werden. Nicht hierzu zählen die Bereiche, in denen lediglich Point-of-Sale-Terminals vorhanden sind (z. B. der Kassenbereich im Einzelhandel).
Server	Ein Computer, der Dienste für andere Computer bereitstellt, wie die Verarbeitung von Kommunikation, Datenspeicherung oder Zugriff auf eine Druckanlage. Zu Servern gehören unter anderem Web-, Datenbank-, Anwendungs-, Authentifizierungs-, DNS-, Mail-, Proxy- und NTP-Server.

Begriff	Definition
Servicecode	Ein drei- oder vierstelliger Wert auf dem Magnetstreifen, der auf den Spurdaten auf das Ablaufdatum der Zahlungskarte folgt. Dieser Code wird für diverse Punkte genutzt, beispielsweise für die Definition von Serviceattributen, der Unterscheidung zwischen internationalem und nationalem Austausch oder die Identifizierung von Nutzungseinschränkungen.
SHA-1/SHA-2	Akronym für „Secure Hash Algorithm“. Eine Reihe miteinander verwandter kryptographischer Hash-Funktionen inklusive SHA-1 und SHA-2. Siehe auch <i>Starke Kryptographie</i> .
Sicherheitsbeauftragter	Die hauptverantwortliche Person für sicherheitsbezogene Themen in einem Unternehmen.
Sicherheitsrichtlinie	Reihe von Gesetzen, Regeln und Praktiken hinsichtlich Verwaltung, Schutz und Weitergabe sensibler Informationen in einem Unternehmen.
Smartcard	Auch als „Chipkarte“ oder „IC-Card“ (Integrated Circuit Card) bezeichnet. Eine Zahlungskarte mit integrierten Stromkreisen. Die Stromkreise, auch als „Chip“ bezeichnet, enthalten Zahlungskartendaten, darunter Daten wie bei Magnetstreifen.
SNMP	Akronym für „Simple Network Management Protocol“. Dieses Protokoll unterstützt die Überwachung von Netzwerkgeräten hinsichtlich sämtlicher Bedingungen, die einer besonderen Aufmerksamkeit des Administrators bedürfen.
Spyware	Ein Schadprogramm, das nach einer Installation Daten abfängt oder eine teilweise Kontrolle über den Computer des Benutzers ohne dessen Zustimmung übernehmen.
SQL	Akronym für „Structured Query Language“. Eine Computersprache zum Erstellen, Bearbeiten und Abrufen von Daten aus relationalen Datenbankverwaltungssystemen.
SQL-Injektion	Ein Angriff auf eine datenbankbetriebene Website. Eine böswillige Person führt nicht autorisierte SQL-Befehle aus, indem sie unsicheren Code auf einem mit dem Internet verbundenen System ausnutzt. SQL-Injektionsangriffe werden genutzt, um Informationen aus einer Datenbank zu stehlen, deren Daten normalerweise nicht verfügbar sind, und/oder Zugriff auf die Host-Computer eines Unternehmens über den Computer, der die Datenbank hostet, zu gewinnen.
SSH	Abkürzung für „Secure Shell“. Eine Protokoll-Suite für die Verschlüsselung von Netzwerkdiensten wie z. B. Remote-Anmeldung oder Remote-Dateiübertragung.
SSL	Akronym für „Secure Sockets Layer“. Gängiger Branchenstandard zur Verschlüsselung des Kanals zwischen einem Webbrowser und einem Webserver, um den Schutz und die Zuverlässigkeit von Daten, die über diesen Kanal übertragen werden, sicherzustellen.
Standardkennwort	Kennwort, das für die Systemverwaltung oder Servicekonten eines Systems, einer Anwendung oder eines Gerät festgelegt wurde, für gewöhnlich im Zusammenhang mit einem Standardkonto. Standardkonten und -kennwörter werden veröffentlicht und sind bekannt, können daher also leicht erraten werden.
Standardkonten	Für ein System, eine Anwendung oder ein Gerät festgelegte Anmeldekonto, die einen ersten Zugriff ermöglichen, wenn das System zum ersten Mal eingerichtet wird.

Begriff	Definition
Starke Kryptographie	<p>Eine Kryptographie basierend auf branchenweit getesteten und anerkannten Algorithmen, mit ausreichenden Schlüssellängen und robusten Schlüsselverwaltungsverfahren. Kryptographie ist eine Methode zum Schutz von Daten. Sie beinhaltet sowohl Verschlüsselung (die umkehrbar ist) und Hashing (das nicht umkehrbar ist). SHA-1 ist ein Beispiel für einen von der Branche getesteten und akzeptierten Hashing-Algorithmus. Zu den branchenweit getesteten und akzeptierten Standards- und Algorithmen für die Verschlüsselung gehören AES (128 Bit und höher), TDES (Schlüssel von mindestens doppelter Länge), RSA (1024 Bit und höher), ECC (160 Bit und höher) und ElGamal (1024 Bit und höher).</p> <p>Weitere Informationen finden Sie in der NIST-Sonderveröffentlichung 800-57 (http://csrc.nist.gov/publications/).</p>
Statusgesteuerte Inspektion	<p>Auch als „Dynamic Packet Filtering“ bezeichnet. Eine Firewall-Fähigkeit, die mithilfe der Nachverfolgung von Kommunikationspaketen eine erhöhte Sicherheit bereitstellt. Nur eingehende Pakete mit entsprechender Reaktion („etablierte Verbindungen“) können die Firewall passieren.</p>
SysAdmin	<p>Abkürzung für „Systemadministrator“. Eine Person mit weitreichenden Berechtigungen, die für die Verwaltung eines Computersystems oder -netzwerks verantwortlich ist.</p>
Systemkomponenten	<p>Alle Netzwerkkomponenten, Server oder Anwendungen, die in der Karteninhaberdaten-Umgebung enthalten oder damit verbunden sind.</p>
TACACS	<p>Akronym für „Terminal Access Controller Access Control System“. Ein Protokoll zur Remote-Authentifizierung, das häufig in Netzwerken genutzt wird und zwischen einem Server für Remote-Zugriff und einem Authentifizierungsserver kommuniziert, um Zugriffsberechtigungen für Benutzer im Netzwerk festzulegen.</p>
TCP	<p>Akronym für „Transmission Control Protocol“. Eine grundlegende Sprach bzw. ein grundlegendes Protokoll für die Kommunikation im Internet.</p>
TDES	<p>Akronym für „Triple Data Encryption Standard“ auch bekannt als „3DES“ oder „Triple DES“. Blockchiffre bestehend aus der dreimal verwendeten DES-Chiffre. Siehe <i>Starke Kryptographie</i>.</p>
TELNET	<p>Abkürzung für „Telephone Network Protocol“. Üblicherweise wird dieses Protokoll genutzt, um einen benutzerorientierte Befehlszeilenzugriff auf Netzwerkgeräte zu gewähren. Die Anmeldedaten werden in Form von Text übertragen.</p>
TLS	<p>Akronym für „Transport Layer Security“. Entwickelt mit dem Ziel einer Datengeheimhaltung und Aufrechterhaltung der Datenintegrität zwischen zwei Kommunikationsanwendungen. TLS ist der Nachfolger von SSL.</p>
Token	<p>Eine Hard- oder Software dynamischen Zwei-Faktor-Authentifizierung.</p>
Transaktionsdaten	<p>Daten von elektronischen Zahlungskartentransaktionen.</p>
Trojaner	<p>Auch als „trojanisches Pferd“ bezeichnet. Ein Schadprogramm, das dem Benutzer nach einer Installation gestattet, weiter normal zu arbeiten, und gleichzeitig bössartige Funktionen am Computersystem ausübt, ohne dass der Benutzer davon etwas merkt.</p>
Überwachung	<p>Die Nutzung von Systemen oder Prozessen, die ständig Computer- oder Netzwerkressourcen überwachen, um Personal im Fall von Ausfällen, Alarmen oder anderen vorher festgelegten Ereignissen zu warnen.</p>

Begriff	Definition
Überwachung der Dateiintegrität	Technik oder Technologie, mit der bestimmte Dateien oder Protokolle überwacht werden, um festzustellen, ob sie manipuliert wurden. Wenn wichtige Dateien oder Protokolle geändert werden, werden Alarme an das zuständige Sicherheitspersonal ausgegeben.
Unsicheres/r Protokoll/Dienst/Port	Ein Protokoll, Dienst oder Port, das bzw. der Sicherheitsprobleme aufgrund fehlender Vertraulichkeits- und/oder Integritätskontrollen verursacht. Zu diesen Sicherheitsproblemen gehören Dienste, Protokolle oder Ports, die Daten und Authentifizierungsinformationen übertragen (z. B. Kennwörter/Kennsätze unverschlüsselt über das Internet) oder in ihrer Standard- bzw. einer fehlerhaften Konfiguration ein leichtes Ziel für Angriffe bieten. Ein Beispiel hierfür ist FTP.
Validierungsbericht	Auch als „Report on Validation“, kurz „ROV“ bezeichnet. Ein Bericht mit detaillierten Informationen zur Konformität einer Zahlungsanwendung mit dem PCI PA-DSS.
Verfahren	Der beschreibende Teil einer Richtlinie. Hier wird erläutert, wie eine Richtlinie umgesetzt bzw. implementiert wird.
Verschlüsselung	Der Prozess der Umwandlung von Informationen in eine Form, die nur für die Inhaber eines spezifischen kryptographischen Schlüssels verständlich ist. Mit der Verschlüsselung werden Informationen für die Dauer zwischen dem Verschlüsselungs- und Entschlüsselungsprozess (der Umkehrung der Verschlüsselung) vor nicht autorisierten Zugriffen geschützt.
Verschlüsselung auf Dateiebene	Technik oder Technologie (Software oder Hardware) zur Verschlüsselung des gesamten Inhalts spezifischer Dateien. Für Alternativen siehe auch <i>Datenträgerverschlüsselung</i> oder <i>Datenbankverschlüsselung auf Spaltenebene</i> .
Verschlüsselungsalgorithmus	Eine Sequenz mathematischer Anweisungen, die zur Umwandlung nicht verschlüsselter Textpassagen oder Daten in verschlüsselte Textpassagen und Daten und umgekehrt verwendet wird.
Vertrauenswürdige Netzwerk	Ein Netzwerk eines Unternehmens, das vollständig vom Unternehmen kontrolliert oder verwaltet wird.
Vertrauliche Authentifizierungsdaten	Sicherheitsrelevante Informationen (Kartvalidierungscodes/-werte, vollständige Magnetstreifendaten, PINs und PIN-Blöcke), die zur Authentifizierung von Karteninhaberdaten genutzt werden und im Textformat oder einer anderen ungeschützten Form dargestellt werden.
VLAN	Abkürzung für „Virtual LAN“ oder „Virtual Local Area Network.“ Logisches LAN, das über den Umfang eines einzelnen, traditionellen physischen LANs hinausgeht.
Vom Regal	Beschreibung von Produkten, die sich auf Lager befinden und nicht speziell für einen Kunden angepasst oder entwickelt wurden, sondern direkt genutzt werden können.
VPN	Akronym für „Virtual Private Network“. Ein Computernetzwerk, bei dem einige Verbindungen innerhalb eines größeren Netzwerks, z. B. dem Internet, virtuell sind und nicht über physische Kabelverbindungen erfolgen. Die Endpunkte des virtuellen Netzwerks werden in einem solchen Fall über das größere Netzwerk getunnelt. Während eine allgemeine Anwendung aus sicheren Verbindungen über das öffentliche Internet besteht, kann ein VPN starke Sicherheitsfunktionen wie die Authentifizierung oder die Verschlüsselung von Inhalten enthalten.

Begriff	Definition
WAN	Akronym für „Wide Area Network“. Computernetzwerk für einen großen Bereich, oft ein regionales oder unternehmensweites Computersystem.
Webserver	Ein Computer, der ein Programm enthält, das HTTP-Anfragen von Webclients akzeptiert und HTTP-Antworten (für gewöhnlich Webseiten) bereitstellt.
WEP	Akronym für „Wired Equivalent Privacy“. Ein schwacher Algorithmus zur Verschlüsselung von Drahtlosnetzwerken. Branchenexperten haben diverse ernstzunehmende Schwachstellen festgestellt, die das Cracken einer WEP-Verbindung mit frei verfügbarer Software binnen Minuten möglich machen. Siehe auch <i>WPA</i> .
Wireless Access Point	Auch als „AP“. Ein Gerät, das Geräten für drahtlose Kommunikation gestattet, eine Verbindung mit einem Drahtlosnetzwerk herzustellen. Üblicherweise verbunden mit einem kabelgebundenen Netzwerk kann ein WAP Daten zwischen kabellosen und kabelgebundenen Geräten im Netzwerk übertragen.
WLAN	Akronym für „Wireless Local Area Network“. Ein LAN, in dem zwei oder mehr Computer oder Geräte ohne Kabel miteinander verbunden sind.
WPA/WPA2	Akronym für „WiFi Protected Access“. Ein Sicherheitsprotokoll zum Schutz von Drahtlosnetzwerken. WPA ist der Nachfolger von WEP und soll erhöhte Sicherheitseigenschaften bieten. Als Nachfolgenergeneration zu WPA wurde bereits WPA2 veröffentlicht.
Zahlungskarten	Im Hinblick auf den PCI-DSS jede Zahlungskarte bzw. jedes Gerät mit dem Logo eines der Gründungsmitglieder des PCI-SSC (American Express, Discover Financial Services, JCB International, MasterCard Worldwide oder Visa, Inc).
Zugriffskontrolle	Mechanismen, die die Verfügbarkeit von Informationen oder Ressourcen zur Informationsverarbeitung nur für autorisierte Personen oder Anwendungen bereitstellen.
Zwei-Faktor-Authentifizierung	Methode zur Benutzerauthentifizierung, bei der zwei oder mehr Faktoren überprüft werden. Zu diesen Faktoren gehört eine Benutzerkomponente (z. B. ein Hardware- oder Softwaretoken), eine dem Benutzer bekannte Information (z. B. ein Kennwort oder -satz oder eine PIN) oder Informationen zum Benutzer bzw. seiner Tätigkeit (z. B. Fingerabdrücke oder andere biometrische Daten).