SICHERE KARTENZAHLUNG FÜR KLEINHÄNDLER

Glossar zu Begrifflichkeiten aus dem Zahlungsverkehr und der Informationssicherheit

VERSION 1.0 | JULI 2016

PCI Security Standards Council®

Einleitung

Das vorliegende *Glossar zu Begrifflichkeiten aus dem Zahlungsverkehr und der Informationssicherheit* ist eine Ergänzung zum *Leitfaden für sichere Zahlungsverfahren* als Teil der Dokumentenreihe „Sichere Kartenzahlung für Kleinhändler". Es zielt darauf ab, einschlägige Begriffe aus der Zahlungskartenbranche (PCI) und der Informationssicherheit auf verständliche Weise zu erklären.

Die Definitionen von Begriffen, die mit einem Sternchen (*) gekennzeichnet sind, basieren auf den Definitionen aus den Dokumenten *Zahlungskartenbranche (PCI) Datensicherheitsstandard (DSS)* und *Zahlungsanwendung Datensicherheitsstandard (PA-DSS): Glossar für Begriffe, Abkürzungen und Akronyme*, Version 3.2 vom April 2016.

Wir möchten Sie auch auf die anderen Dokumente *Leitfaden für sichere Zahlungsverfahren* und die Ressourcen für „Sichere Kartenzahlung für Kleinhändler" hinweisen:

QUELLE	URL
Leitfaden für sichere Zahlungsverfahren	https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Gängige Zahlungssysteme	https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Fragen an Ihre Anbieter	https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf

Hinweis:
Die aktuellste Version des Dokuments *Zahlungskartenbranche (PCI) Datensicherheitsstandard (DSS) und Zahlungsanwendung Datensicherheitsstandard (PA-DSS): Glossar für Begriffe, Abkürzungen und Akronyme* gilt als zuverlässige Quelle, auf die Sie sich zwecks der aktuellen und vollständigen PCI-DSS- und PA-DSS-Definitionen beziehen müssen.

Glossar

BEGRIFF	DEFINITION
Acquirer *	Siehe *Handelsbank* und*Zahlungsabwickler.*
Antivirus-Software *	Ein Softwareprogramm, das schädliche 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. Auch als „Antivirenprogramm“ bezeichnet.
Anwendung *	Softwareprogramm oder mehrere Programme, die auf einem PC, Smartphone, Tablet, internen Server oder Webserver ausgeführt werden.
Approved Scanning Vendor (ASV) *	Ein vom PCI Security Standards Council zugelassenes Unternehmen, das Scanning-Services durchführen kann, um Schwachstellen im System zu ermitteln. Siehe auch *ASV.*
ASV *	Akronym für „Approved Scanning Vendor“ (Zugelassener Scanning-Anbieter).
Authentifizierung *	Ein Vorgang zur Überprüfung der Identität einer Person, eines Geräts oder eines Prozesses. Die Authentifizierung erfolgt üblicherweise unter Anwendung eines oder mehrerer der folgenden Authentifizierungsfaktoren: • Etwas, das Sie kennen, etwa ein Kennwort oder eine Passphrase • Etwas, das Sie besitzen, etwa einen Hardware-Token oder eine Smartcard • Etwas, das Sie ausmacht, etwa eine biometrische Angabe
Autorisierung *	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.
Bankleitzahl (BLZ)	Die ersten sechs (oder mehr) Ziffern einer Zahlungskartennummer, anhand derer man das Finanzinstitut ermitteln kann, das dem Karteninhaber die Zahlungskarte ausgestellt hat.
Need-to-know-Prinzip	Das Prinzip besagt, dass einem Benutzer der Zugriff auf Systeme oder Daten nur auf Grundlage einer betrieblichen Notwendigkeit gewährt wird, d. h., nur in dem Rahmen, der es für die Durchführung seiner Aufgaben erforderlich macht.
Kartendaten/Kartendaten des Kunden *	Die Kartendaten umfassen mindestens die Kontonummer (PAN) und können zudem den Namen des Karteninhabers sowie das Gültigkeitsdatum der Karte beinhalten. Die PAN ist auf der Vorderseite der Karte aufgedruckt und im Magnetstreifen bzw. Chip kodiert. Auch als Karteninhaberdaten bezeichnet. Für weitere Datenelemente, die Bestandteil einer Zahlungstransaktion sein können, jedoch nach Autorisierung der Transaktion nicht gespeichert werden müssen, siehe *Vertrauliche Authentifizierungsdaten.*
Chip	Auch bekannt unter der Bezeichnung „EMV-Chip“. Der Mikroprozessor (bzw. Chip) auf einer Zahlungskarte, der für die Abwicklung von Transaktionen in Übereinstimmung mit den internationalen Vorschriften für EMV-Transaktionen benutzt wird.

Glossar

BEGRIFF	DEFINITION
Chip und PIN	Ein Verifizierungsverfahren, bei dem der Kunde zwecks Bezahlung einer Ware oder Dienstleistung seine PIN an einem Zahlungsterminal eingibt, das EMV-Chips lesen kann.
Chip und Unterschrift	Ein Verifizierungsverfahren, bei dem der Kunde zwecks Bezahlung einer Ware oder Dienstleistung an einem Zahlungsterminal, das EMV-Chips lesen kann, unterschreiben muss.
Anmeldeinformationen	Informationen zur Identifikation und Authentifizierung eines Benutzers, um diesem Zugriff auf ein System zu gewähren. Die Anmeldeinformationen bestehen oftmals aus dem Benutzernamen und dem Kennwort. Die Anmeldedaten können einen Fingerabdruck, einen Netzhautscan oder eine einmalig verwendbare Ziffer umfassen, die von einem mobilen „Token-Generator" erzeugt wird. Die Sicherheit ist größer, wenn für den Zugriff mehrere Anmeldedaten erforderlich sind.
Cyber-Angriff	Ein Angriff, mit dem versucht wird, in einen Computer oder ein System einzudringen. Cyber-Angriffe reichen von der Installation von Spyware auf einem PC über das Einbrechen in ein Zahlungssystem zum Stehlen von Kartendaten bis zum Versuch, essenzielle Infrastruktur wie die Stromversorgung zu zerstören.
Datensicherheitsverletzung	Eine Datensicherheitsverletzung ist ein Vorfall, bei dem möglicherweise sensible Daten von einer nicht autorisierten Partei angezeigt, gestohlen oder verwendet wurden. Datensicherheitsverletzungen können u. a. Kartendaten, geschützte Gesundheitsdaten (Personal Health Information, PHI), personenbezogene Informationen (PII), Geschäftsgeheimnisse und geistiges Eigentum betreffen.
Standardkennwörter	Ein einfaches Kennwort, das im Lieferumfang neuer Software oder Hardware enthalten ist. Standardkennwörter wie „admin" „password" oder „123456" lassen sich einfach erraten und es kann eine Online-Suche nach ihnen durchgeführt werden. Sie dienen als Platzhalter und bieten keine echte Sicherheit. Nach der Installation der neuen Software oder Hardware müssen sie zu stärkeren Kennwörtern geändert werden.
Elektronische Kasse (ECR)	Eine Gerät, das Transaktionen registriert und kalkuliert und möglicherweise Kassenbelege ausdruckt; es können jedoch keine Kartenzahlungen darüber erfolgen. Auch als „Kasse" bezeichnet.
Verschlüsselung	Prozess, bei dem mithilfe von Kryptografie Daten mathematisch in eine Form umgewandelt werden, die nur für Inhaber eines bestimmten digitalen Schlüssels nutzbar ist. Verschlüsselung schützt Daten, da sie deren Wert für Kriminelle vermindert. Siehe auch *Kryptografie*.
Firewall *	Hardware und/oder Software, die Netzwerkressourcen vor unerlaubtem Zugriff schützt. Eine Firewall lässt die Kommunikation zwischen Computern oder Netzwerken mit verschiedenen Sicherheitsgraden auf Grundlage von Regeln und anderen Kriterien entweder zu oder lehnt sie ab.
Forensic Investigator (Forensikprüfer)	PCI Forensic Investigators (PFIs) sind vom PCI Council zugelassene Unternehmen, die ermitteln, wann und wie eine Kartendaten-Sicherheitsverletzung aufgetreten ist. Sie führen mithilfe bewährter investigativer Methoden und Tools Untersuchungen in der Finanzbranche durch. Sie arbeiten außerdem mit Strafvollzugsbehörden zusammen, um Stakeholder bei evtl. resultierenden Strafverfolgungen zu unterstützen.

Glossar

BEGRIFF	DEFINITION
Hacker	Eine Person oder Organisation, die versucht, Sicherheitsmaßnahmen von Computersystemen zu umgehen, um ihre Kontrolle zu übernehmen und Zugriff auf sie zu erhalten. Dies erfolgt üblicherweise, um Kartendaten zu stehlen.
Hosting-Anbieter *	Bieten verschiedene Dienste für Händler und andere Dienstanbieter an, bei denen die Daten ihrer Kunden auf den Servern des Anbieters „gehostet" bzw. gespeichert werden. Typische Dienste umfassen geteilten Speicherplatz für mehrere Händler auf einem Server, die Bereitstellung eines dedizierten Servers für einen einzigen Händler oder Web-Anwendungen, wie z. B. eine Website mit „Warenkorb"-Optionen.
Integriertes Zahlungsterminal	Eine Kombination aus Zahlungsterminal und elektronischer Kasse, d. h., man kann Zahlungen darüber abwickeln, Transaktionen registrieren und kalkulieren und Belege ausdrucken.
Integrator/Wiederverkäufer	Ein Integrator/Wiederverkäufer ist ein Unternehmen, das Zahlungsterminals, Zahlungssysteme bzw. Zahlungsanwendungen für Händler implementiert, konfiguriert bzw. unterstützt. Diese Unternehmen können als Bestandteil ihrer Dienstleistung auch die Zahlungsgeräte oder -anwendungen verkaufen. Siehe auch *Qualified Integrator Reseller (QIR) (Qualifizierter Integrator/Wiederverkäufer)*.
Protokoll *	Eine Datei, die automatisch erstellt wird, wenn bestimmte vorab definierte (oft sicherheitsbezogene) Ereignisse in einem Computersystem oder Netzwerk eintreten. Die Protokolldaten umfassen Datums-/Zeitstempel, eine Beschreibung des Ereignisses und spezifische Ereignisinformationen. Diese Dateien sind hilfreich zur Behebung technischer Probleme und zur Untersuchung von Datensicherheitsverletzungen. Auch als „Prüfprotokoll" oder „Audit-Trail" bezeichnet.
Malware *	Schadsoftware, die dazu konzipiert ist, ein Computersystem zu infiltrieren, mit der Absicht, Daten zu stehlen oder Anwendungen oder das Betriebssystem zu beschädigen. Solche Software gelangt üblicherweise bei vielen geschäftskonformen Aktivitäten, wie per E-Mail oder über aufgerufene Websites, in ein Netzwerk. Zu Schadsoftware zählen beispielsweise Viren, Würmer, Trojaner (oder trojanische Pferde), Spyware, Adware und Rootkits.
Handelsbank *	Eine Bank bzw. ein Finanzinstitut, die/das Debit- oder Kreditkartenzahlungen für Händler abwickelt. Auch als „Acquirer" „erwerbende Bank", „Kartenverarbeiter" oder „Zahlungsabwickler" bezeichnet. Siehe auch *Zahlungsabwickler*.
Mobilgerät	Allgemeiner Begriff für eine Klasse kleiner, tragbarer elektronischer Verbrauchergeräte, die z. B. Smartphones und Tablets umfasst und die eine drahtlose Verbindung zu Computernetzwerken herstellen können.
Mobile Zahlungsannahme	Verwendung eines Mobilgeräts zur Annahme und Verarbeitung von Zahlungstransaktionen. Das Mobilgerät wird üblicherweise mit einem handelsüblichen Kartenlesegerät-Zubehör kombiniert.
Multi-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. eine Smart Card oder einen Dongle), etwas, das der Benutzer weiß (z. B. ein Kennwort, Kennsatz oder eine PIN), oder etwas, das den Benutzer identifiziert (z. B. Fingerabdrücke oder andere biometrische Daten).
Netzwerk *	Zwei oder mehr Computer, die zur gemeinsamen Ressourcennutzung miteinander verbunden sind.

Glossar

BEGRIFF	DEFINITION
Betriebssystem *	Die Software eines Computersystems, die für die Verwaltung und Koordination aller Aktivitäten, einschließlich der Verteilung von Computerressourcen, verantwortlich ist. Zum Beispiel Microsoft Windows, Apple OSX, iOS, Android, Linux und UNIX.
P2PE	Akronym für den Standard „Point-to-Point-Encryption" des PCI Council. Weitere Informationen finden Sie unter *www.pcisecuritystandards.org*.
PA-DSS *	Akronym für den „Payment Application Data Security Standard" (Zahlungsanwendung Datensicherheitsstandard) des PCI Council. Weitere Informationen finden Sie unter *www.pcisecuritystandards.org*.
Kennwort *	Ein Wort, ein Ausdruck oder eine Zeichenfolge, die zur Authentifizierung eines Benutzers dient. In Kombination mit dem Benutzernamen dient das Kennwort dazu, die Identität des Benutzers für den Zugriff auf Computerressourcen zu belegen.
Patch *	Ein Update für eine vorhandene Software, das die Funktionalität erweitert oder einen Fehler („Bug") korrigiert.
Zahlungsanwendung *	In Bezug auf PA-DSS: eine Softwareanwendung, die im Zuge der Autorisierung oder Verrechnung von Zahlungstransaktionen Karteninhaberdaten speichert, verarbeitet oder überträgt.
Anbieter der Zahlungsanwendung	Eine Einheit, die eine Zahlungsanwendung verkauft, vertreibt oder lizenziert – entweder an POS-Integratoren/ Wiederverkäufer zur Integration in Händlerzahlungssysteme oder direkt an Händler zur eigenen Installation und Nutzung.
Zahlungs-Middleware	Ein allgemeiner Begriff für Software, die zwei oder mehr möglicherweise nicht verwandte Zahlungsanwendungen verbindet. Sie kann z. B. Kartendaten zwischen einer Anwendung auf einem Zahlungsterminal und anderen Händlersystemen übertragen, die Kartendaten an einem Abwickler senden.
Zahlungsabwickler *	Eine Einheit, die von Händlern beauftragt wird, Zahlungskartentransaktionen in ihrem Auftrag abzuwickeln. Auch wenn Zahlungsabwickler typischerweise Acquirer-Leistungen bereitstellen, werden diese nicht als Acquirer (Handelsbanken) erachtet, sofern sie nicht von einer Zahlungskartenmarke als solcher definiert sind. Auch als „Zahlungs-Gateway" oder „Zahlungs-Dienstanbieter" (PSP) bezeichnet. Siehe auch *Handelsbank*.
Zahlungssystem	Umfasst den gesamten Vorgang der Zahlungsannahme am Händlerverkaufsort (im Geschäft oder an der digitalen Ladenzeile) und kann Zahlungsterminals, elektronische Kassen, sonstige Geräte oder Systeme, die mit dem Zahlungsterminal verbunden sind (zum Beispiel WLAN oder einen PC), Server mit E-Commerce-Komponenten wie Zahlungsseiten und die Verbindung zu einer Handelsbank umfassen.
Zahlungssystem-Anbieter	Ein Anbieter, der eine umfassende Zahlungslösung an einen Händler verkauft, lizenziert oder vertreibt. Die Lösung umfasst die Hardware und Software, die zur Zahlungsabwicklung im Geschäft erforderlich ist, und stellt ein Verfahren zur Verbindung mit einem Zahlungsabwickler bereit.
Zahlungsterminal	Hardwaregerät, mit dem man Kartenzahlungen von Kunden annimmt, indem man die Karte durchzieht, einsteckt oder einfach ans Lesegerät hält. Auch als „Point-of-Sale-Terminal" (POS-Terminal), „Kreditkartenlesegerät" oder „PDQ-Terminal" bezeichnet.

Glossar

BEGRIFF	DEFINITION
PCI *	Akronym für „Payment Card Industry" (Zahlungskartenbranche).
PCI DSS *	Akronym für den „Payment Card Industry Data Security Standard" (Datensicherheitsstandard der Zahlungskartenbranche) des PCI Council. Weitere Informationen finden Sie unter *www.pcisecuritystandards.org.*
PCI DSS-konform	Die kontinuierliche Einhaltung aller geltenden Anforderungen des aktuellen PCI DSS im Standardbetrieb (Business-As-Usual). Die Konformität wird zu einem bestimmten Zeitpunkt bewertet und geprüft; es ist jedoch die Aufgabe jedes Händlers, die Anforderungen kontinuierlich zu erfüllen, um hohe Sicherheit zu ermöglichen. Handelsbanken bzw. Zahlungsmarken können Anforderungen für die offizielle, jährliche Validierung der PCI DSS Konformität festgelegt haben.
PCI-DSS-validiert	Erbringen des Nachweises, dass alle geltenden PCI DSS Anforderungen zu einem bestimmten Zeitpunkt erfüllt sind. Je nach den jeweiligen Anforderungen der Handelsbank oder Zahlungsmarke kann die Validierung über den betreffenden PCI DSS Selbstbeurteilungs-Fragebogen oder durch einen Konformitätsbericht erreicht werden, der aus einer Vor-Ort-Bewertung resultiert.
PCI-geprüfte Zahlungsanwendung	Softwareanwendung, die gemäß dem PCI Zahlungsanwendung Datensicherheitsstandard (PA-DSS) validiert wurde und auf der Website des PCI Council aufgeführt ist.
PCI-zugelassenes Zahlungsterminal	Zahlungsterminal, das gemäß dem PCI Standard „PIN Transaktionssicherheit" (PTS) zugelassen ist und auf der Website des PCI Council aufgeführt ist.
PCI-notierte P2PE-Lösung (Point-to-Point Encryption, Punkt-zu-Punkt-Verschlüsselung)	Verschlüsselungslösung, die gemäß dem PCI P2PE-Standard validiert wurde und auf der Website des PCI Council aufgeführt ist.
PED *	Akronym für „PIN Entry Device" (PIN-Eingabegerät). Ziffernblock, über den der Kunde seine PIN eingibt. Auch als „PIN-Pad" bezeichnet.
PIN *	Akronym für „persönliche Identifizierungsnummer". Eine eindeutige Nummer, die nur der Benutzer kennt, und ein System zur Authentifizierung des Benutzers im System. PINs werden üblicherweise zum Geldabheben an Geldautomaten oder für EMV-Chipkarten verwendet, um die Unterschrift des Karteninhabers zu ersetzen. PINs helfen, zu ermitteln, ob ein Karteninhaber zur Nutzung der Karte autorisiert ist, und eine nicht autorisierte Verwendung zu verhindern, wenn die Karte gestohlen wurde.
Primäre Kontonummer (PAN) *	Eindeutige Nummer für Kredit- und Debitkarten, die das Konto des Karteninhabers kennzeichnet.
Missbräuchliche Verwendung	Die missbräuchliche Verwendung von Zugangsberechtigungen für Computersysteme. Dazu zählt beispielsweise, wenn ein Systemadministrator zu böswilligen Zwecken auf Kartendaten zugreift, oder jemand zu böswilligen Zwecken die höheren Zugangsberechtigungen eines Administrators stiehlt oder nutzt.
PTS *	Akronym für den „PIN Transaction Security Standard" des PCI Council. PTS beschreibt eine Reihe modularer Bewertungsanforderungen für PIN-fähige POI-Terminals. Weitere Informationen finden Sie unter www.pcisecuritystandards.org.
QIR *	Akronym für „Qualified Integrator or Reseller" (qualifizierter Integrator oder Wiederverkäufer). Weitere Informationen finden Sie unter *www.pcisecuritystandards.org.*

Glossar

BEGRIFF	DEFINITION
Qualified Security Assessor (QSA) *	Ein Unternehmen, das vom PCI Security Standards Council zugelassen ist, die Einhaltung der PCI DSS Anforderungen durch eine Einheit zu überprüfen.
Regelmäßige Zahlung	Ein Abrechnungsverfahren, bei dem Händler ihren Kunden regelmäßig Rechnungen stellen, z. B. für monatliche Mitgliedschaften oder Abonnements. Eine sichere Methode hierfür ist die Tokenisierung der Kartendaten durch den Acquirer/Abwickler. Dadurch ist ihr Schutz sichergestellt und der Händler wird in Bezug auf seine Verantwortung entlastet.
Remote-Zugriff *	Zugriff auf ein Computernetzwerk von einem Standort außerhalb des Netzwerks. Verbindungen für den Remote-Zugriff gehen entweder von dem internen unternehmenseigenen Netzwerk oder von einem externen Standort aus. Eine Technologie, die Remote-Zugriff unterstützt, ist beispielsweise ein virtuelles privates Netzwerk (VPN). Remote-Zugriff kann entweder intern (z. B. IT-Support) oder extern (z. B. Dienstanbieter, Drittanbieter, Integratoren/Wiederverkäufer) erfolgen.
Wiederverkäufer/Integrator *	Eine Stelle, die Zahlungsanwendungen vertreibt und/oder integriert, sie jedoch nicht entwickelt.
Router *	Hardware oder Software, die zwei oder mehr interne oder externe Computernetzwerke verbindet, um Daten durch ein Netzwerk zu leiten und sicherzustellen, dass die Daten ordnungsgemäß zwischen den Netzwerken fließen. Der Router kann auch die Sicherheit erhöhen, indem er nur zulässigen Datenverkehr durchlässt und unzulässigen Datenverkehr verweigert.
Sicherer Kartenleser (SCR)	Ein PTS-zugelassenes Gerät, das mit einem Mobiltelefon oder Tablet verbunden wird, um Zahlungskarten auf sichere Weise anzunehmen. PCI PTS-zulässige SCRs schützen und verschlüsseln die Kartendaten per SRED. Siehe auch *SRED*.
Sicherheitscode *	Eine drei- bzw. vierstellige Zahl auf dem Unterschriftenfeld auf der Vorder- bzw. Rückseite der Zahlungskarte Der Code ist speziell einer einzelnen Karte zugeordnet und dient als zusätzliche Prüfmethode, um sicherzustellen, dass die Karte im Besitz des legitimen Karteninhabers ist (üblicherweise bei Transaktionen, bei denen die Karte nicht vorliegt). Auch als „Kartensicherheitscode" bezeichnet.
Selbstbeurteilungs-Fragebogen (SBF) *	PCI DSS Validierungstool, mit dem die Ergebnisse der Selbstbeurteilung im Rahmen der PCI-DSS-Beurteilung einer Einheit dokumentiert werden.
Vertrauliche Authentifizierungsdaten *	Sicherheitsbezogene Informationen, die zur Authentifizierung von Karteninhabern bzw. zur Autorisierung von Zahlungskartentransaktionen verwendet werden und im Magnetstreifen oder Chip der Karte gespeichert sind.
Dienstanbieter *	Eine Geschäftseinheit, die verschiedene Dienste für Händler bereitstellt. Üblicherweise speichern, verarbeiten oder übertragen diese Einheiten im Auftrag einer anderen Einheit (z. B. eines Händlers) Kartendaten ODER es handelt sich um Anbieter von Managed Services für Firewalls, die Erkennung von Eindringversuchen oder Hosting sowie von anderen IT-Services. Auch als „Anbieter" bezeichnet.
Skimming	Der Diebstahl von Kartendaten direkt von der Zahlungskarte des Kunden oder der Zahlungsinfrastruktur am Händlerstandort, z. B. über ein betrügerisches Hand-Kartenlesegerät oder über Modifikationen am Zahlungsterminal des Händlers. Der Zweck ist Betrug, die Bedrohung ist ernst zu nehmen und sie kann jeden Händler treffen.

Glossar

BEGRIFF	DEFINITION
Skimming-Gerät	Ein Gerät, das häufig an einem offiziellen Kartenlesegerät angebracht wird und mit dem Zahlungskarteninformationen auf illegale Weise erfasst und/oder gespeichert werden. Auch als „Karten-Skimmer" bezeichnet.
Kleiner Händler	Ein Unternehmen, das typischerweise über einen Standort oder evtl. ein paar Standorte verfügt, mit begrenztem oder gar keinem IT-Budget und üblicherweise ohne eigene IT-Mitarbeiter.
SRED	Ein Akronym für das sichere Lesen und Austauschen von Daten. Eine Reihe von PCI PTS Anforderungen, die Kartendaten in Zahlungsterminals schützen und verschlüsseln sollen. Eine PCI Council-notierte P2PE-Lösung muss ein PTS-zulässiges und notiertes Zahlungsterminal mit SRED-Aktivierung und aktiv durchgeführter Kartendatenverschlüsselung nutzen.
Eigenständiges Terminal	Ein Zahlungsterminal, das nicht auf die Verbindung mit anderen Geräten in der Händlerumgebung angewiesen ist und keine anderen Funktionen erfüllt. Die einzige Betriebsanforderung ist eine Verbindung mit dem Abwickler, entweder über das Internet oder eine Telefonleitung. Wenn das Terminal eine Verbindung mit einer computergestützten elektronischen Kasse erfordert oder multifunktional ist (wie ein Mobilgerät), ist es kein eigenständiges Terminal.
Sichere Authentifizierung.	Dient dazu, die Identität eines Benutzers oder Geräts zu überprüfen, um die Sicherheit des geschützten Systems sicherzustellen. Der Begriff „sichere Authentifizierung" wird oft synonym mit „Multi-Faktor-Authentifizierung" (MFA) verwendet.
Kasse	Siehe *Elektronische Kasse*.
Tokenisierung	Ein Prozess, bei dem die primäre Kontonummer (PAN) durch einen als „Token" bezeichneten Wert ersetzt wird. Tokens können anstelle der Original-PAN verwendet werden, um Funktionen durchzuführen, wenn die Karte nicht vorliegt – z. B. bei Nichtigkeit, Erstattungen oder regelmäßigen Zahlungen. Tokens bieten auch mehr Sicherheit im Diebstahlsfall, weil sie nicht nutzbar und für Kriminelle deshalb wertlos sind.
Nicht verschlüsselte Daten	Daten, die lesbar sind, ohne sie erst entschlüsseln zu müssen. Auch als „Klartext" bezeichnet.
Anbieter	Eine Geschäftseinheit, die einem Händler ein Produkt oder einen Dienst bereitstellt, das/der für den Geschäftsablauf erforderlich ist. Wenn Dienste angeboten werden, kann der Anbieter als Dienstanbieter angesehen werden und er benötigt möglicherweise Zugriff auf physische Standorte oder Computersysteme in der Händlerumgebung, was die Sicherheit der Kartendaten beeinträchtigen kann. Siehe auch *Dienstanbieter*.
Virtuelles Zahlungsterminal *	Webbrowser-basierter Zugriff auf eine Acquirer, Abwickler- oder Dritt-Dienstanbieter-Website, um Zahlungskartentransaktionen zu autorisieren. Anders als physische Terminals lesen virtuelle Zahlungsterminals Daten nicht direkt von Zahlungskarten. Der Händler gibt Zahlungskartendaten manuell über den sicher verbundenen Webbrowser ein. Da die Transaktionen mit Zahlungskarten manuell eingegeben werden, werden in Händlerumgebungen mit niedrigen Transaktionsvolumen virtuelle Zahlungsterminals häufig anstatt physischer Terminals eingesetzt.
Virtuelles privates Netzwerk (VPN) *	Das VPN besteht aus virtuellen Verbindungen in einem größeren Netzwerk, wie beispielsweise dem Internet, anstelle direkter Verbindungen mit physischen Kabeln. Die Endpunkte des VPN-„Tunnels" durch das größere Netzwerk zur Erstellung einer privaten, sicheren Verbindung.

Glossar

Virus	Schadsoftware, die in Software- oder Datendateien auf einem „infizierten" Computer Kopien von sich selbst erstellt. Nach der Replizierung führen Viren manchmal Schadprogramme aus und löschen beispielsweise sämtliche Daten auf einem Computer. Viren können inaktiv „ruhen" und das Schadprogramm erst zu einem späteren Zeitpunkt ausführen. Manchmal werden aber auch keine Schadprogramme ausgeführt. Viren, die sich selbst replizieren, indem sie sich als E-Mail-Anhang oder als Teil einer Netzwerknachricht präsentieren, werden „Würmer" genannt.
Schwachstelle *	Ein Fehler oder eine Sicherheitslücke, die, sollte sie vorsätzlich oder unwissentlich ausgenutzt werden, das System gefährden kann.
Schwachstellenscan	Ein Softwaretool, das potenzielle Schwachstellen auf einem Computer oder Netzwerk erkennt und klassifiziert. Scans werden für gewöhnlich von der IT-Abteilung eines Unternehmens oder von einem Sicherheitsdienstanbieter (wie etwa einem Approved Scanning Vendor) durchgeführt. Siehe auch *Approved Scanning Vendor (ASV)*.
WLAN *	Ein drahtloses Netzwerk, das Computer kabellos miteinander verbindet.
Kabelloses Zahlungsterminal	Zahlungsterminal, das mithilfe von Drahtlostechnologie eine Verbindung zum Internet herstellt.