

SICHERE KARTENZAHLUNG FÜR KLEINHÄNDLER

# Leitfaden für sichere Zahlungsverfahren

Version 1.0 | Juli 2016

DAS EIGENE RISIKO KENNEN.....	4
SCHÜTZEN SIE IHR UNTERNEHMEN MITHILFE FOLGENDER GRUNDLEGENDER SICHERHEITSMASSNAHMEN .....	7
WEITERFÜHRENDE QUELLEN .....	20



# **DAS EIGENE RISIKO KENNEN**

# Das eigene Risiko kennen

**Als mittelständisches Unternehmen sind Sie ein beliebtes Ziel für Datendiebe.**

Wenn es bei der Zahlungsabwicklung mit Zahlungskarten zu Datenpannen kommt, kann die Situation schnell kritisch werden. Ihre Kunden verlieren das Vertrauen in Ihre Fähigkeit, die persönlichen Daten Ihrer Kunden zu schützen. Die Kunden wenden sich von Ihnen ab und wechseln den Händler. Es drohen Strafgebühren und Gerichtsverfahren und Ihr Unternehmen verliert unter Umständen die Berechtigung, Bezahlverfahren mit Zahlungskarten anzubieten. Eine Umfrage unter 1.015 kleinen und mittleren Unternehmen ergab, dass 60 % der von einer Datenpanne betroffenen Betriebe innerhalb von sechs Monaten nach dem Vorfall schließen mussten. (NCSA)

60 %



DER MITTELSTÄNDISCHEN UNTERNEHMEN WAREN SCHON EINMAL VON EINER DATENPANNE BETROFFEN  
(HM Government)



71 %

DER HACKER GREIFEN UNTERNEHMEN MIT WENIGER ALS 100 MITARBEITERN AN  
(Verizon 2012)

20.752 \$



DIE KOSTEN, DIE FÜR MITTELSTÄNDISCHE UNTERNEHMEN AUFGRUND VON HACKERANGRIFFEN IM DURCHSCHNITT ENTSTEHEN; 2013 LAG DIE SUMME NOCH BEI 8.600 \$  
(NSBA)

69 %



DER US-AMERIKANISCHEN VERBRAUCHER SIND BESORGT, DASS IHRE ZAHLUNGSKARTENDATEN GESTOHLEN WERDEN KÖNNTEN  
(Gallup)



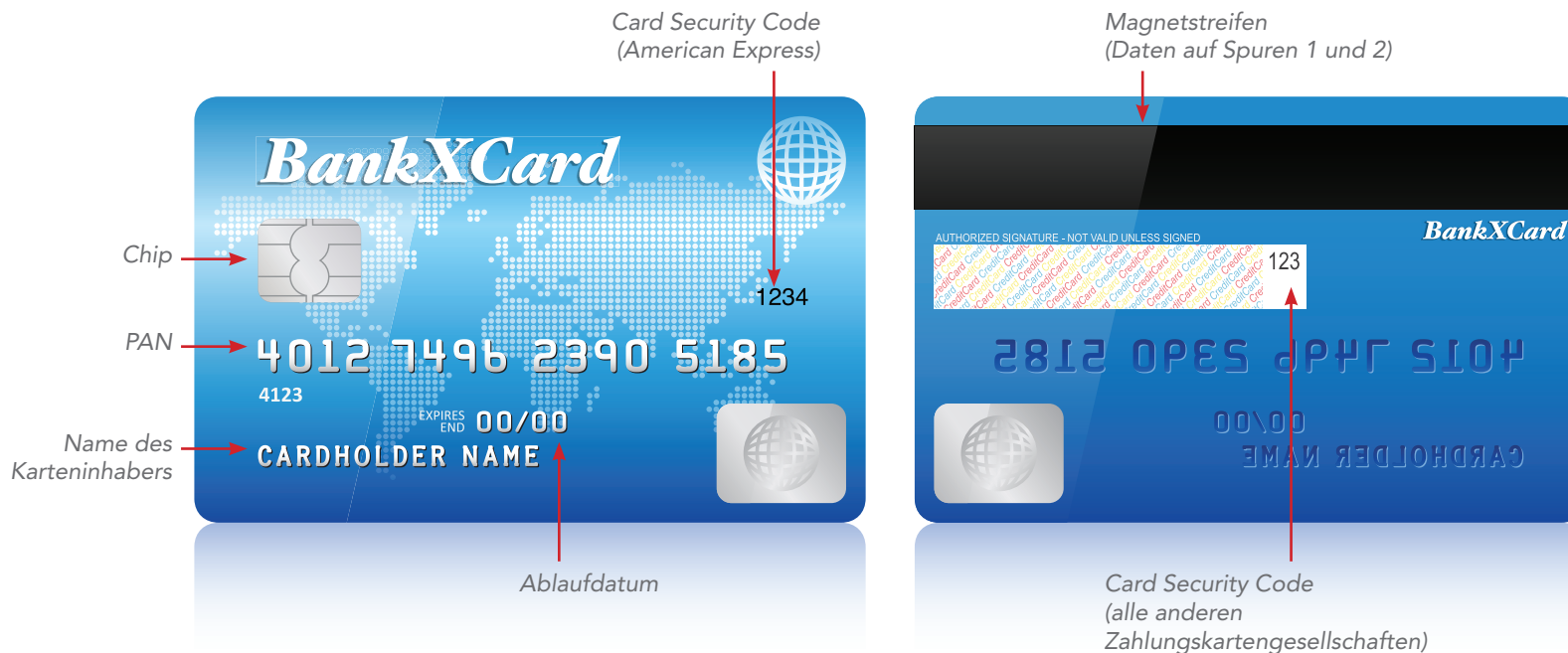
# Wo lauern Gefahren?

**DIE KARTENDATEN IHRER KUNDEN SIND FÜR KRIMINELLE WAHRE GOLDGRUBEN. LASSEN SIE NICHT ZU, DASS DIESE DATEN IN DIE FALSCHEN HÄNDE GERATEN!**

**Folgen Sie den Anweisungen in diesem Leitfaden, um sich gegen Datendiebstahl zu schützen.**

**Zu den Zahlungskartendaten zählen beispielsweise die Primary Account Number (PAN) und die drei- oder vierstellige Kartenprüfnummer. Die roten Pfeile unten verweisen auf die verschiedenen Daten, die geschützt werden müssen.**

## DIE VERSCHIEDENEN DATEN AUF EINER ZAHLUNGSKARTE



## WAS BEDEUTET „PCI DSS“?

Der „Payment Card Industry Data Security Standard“ (PCI DSS) ist ein Regelwerk für Sicherheitsanforderungen, die Kleinhändlern helfen können, die Kartendaten ihrer Kunden, die sich auf Zahlungskarten befinden, zu schützen.

Als Kleinhändler sind Sie vielleicht bereits damit vertraut, Ihre PCI DSS Konformität per Selbstbeurteilungsfragebogen (SBF) prüfen zu lassen.

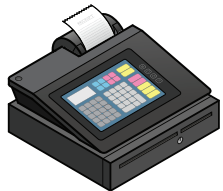
Weitere Informationen zum PCI DSS finden Sie unter „Onlinequellen“ am Ende dieses Leitfadens.

# Das eigene Zahlungssystem kennen: Die gängigsten Zahlungsbegriffe

Je nachdem, in welcher Ecke der Welt sich Ihr Unternehmen befindet, heißen Bezahlgeräte anders. Das sind die Geräte, auf die wir uns in diesem Dokument beziehen, und ihre Bezeichnungen.



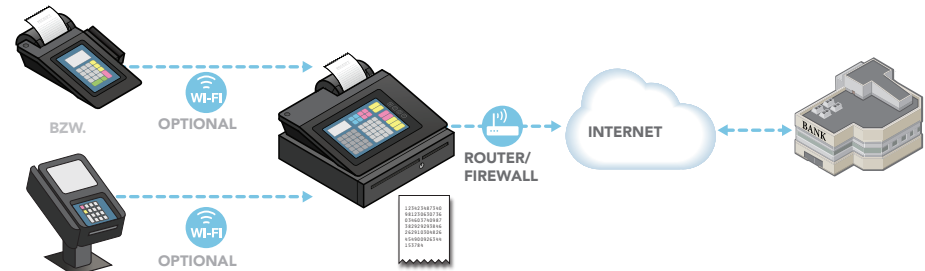
Ein **ZAHLUNGSTERMINAL** ist das Gerät, mit dem man die Kartenzahlung eines Kunden entgegennimmt, indem man die Karte durchzieht, einsteckt, einfach ans Lesegerät hält oder die Kartennummer manuell eingibt. POS-Terminal, Kreditkartenlesegerät, EC- oder Kartenterminal oder Chipkartenleser sind weitere Bezeichnungen für diese Geräte.



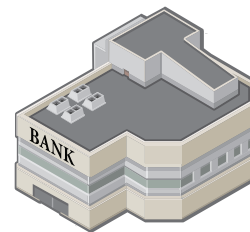
Eine **ELEKTRONISCHE KASSE** registriert und kalkuliert Transaktionen und druckt möglicherweise Kassenbelege aus, jedoch kann darüber keine Kartenzahlung erfolgen.



Ein **INTEGRIERTES ZAHLUNGSTERMINAL** ist eine Kombination aus Zahlungsterminal und elektronischer Kasse, d. h. man kann Kartenzahlungen darüber abwickeln, Transaktionen registrieren und kalkulieren und Belege ausdrucken.



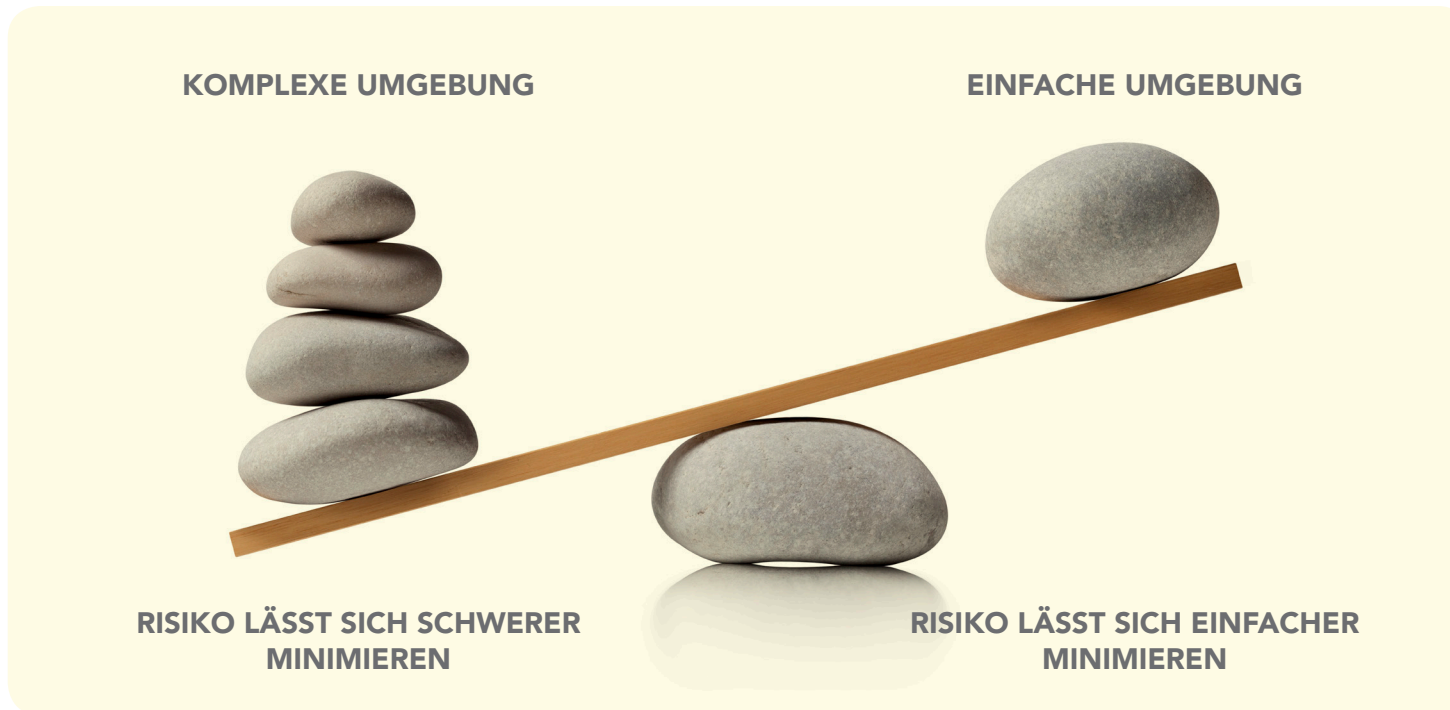
Ein **ZAHLUNGSSYSTEM** umfasst den gesamten Vorgang der Zahlungsannahme am Verkaufsort (im Geschäft oder an der digitalen Ladenzeile) und kann Zahlungsterminals, elektronische Kassen, sonstige Geräte oder Systeme, die mit dem Zahlungsterminal verbunden sind (zum Beispiel WLAN oder einen PC), Server mit E-Commerce-Komponenten wie Zahlungsseiten und die Verbindung zur Handelsbank umfassen.



**HANDELSBANKEN** sind Banken bzw. Finanzinstitute, die Debit- oder Kreditkartenzahlungen für Händler abwickeln. Eine solche Einrichtung wird auch als Acquirer, erwerbende Bank oder Zahlungsabwickler bezeichnet.

# Inwieweit ist Ihr Unternehmen gefährdet?

**Je mehr Funktionen Ihr Zahlungssystem umfasst, desto komplexer gestaltet sich seine Sicherung. Zusatzfunktionen bieten Kriminellen oftmals leichtes Spiel, die Kartendaten Ihrer Kunden zu stehlen. Überlegen Sie sich genau, ob Sie all die verfügbaren Zusatzfunktionen (z. B. WLAN oder Kameras) in Ihrem Unternehmen wirklich benötigen.**

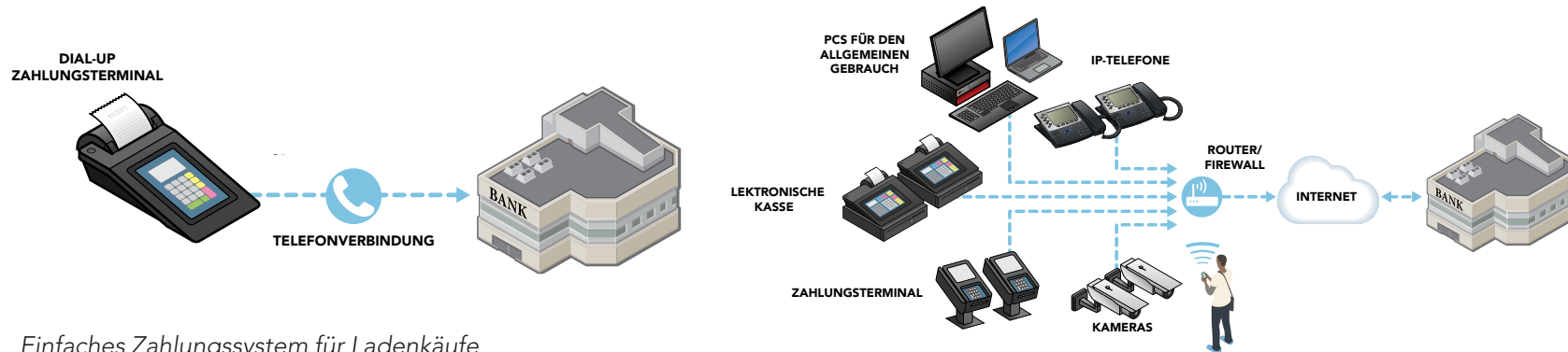


Wie verkaufen Sie Ihre Waren oder Dienstleistungen? Es gibt folgende drei Hauptverkaufswege:

1. Der Kunde kommt in Ihre Verkaufsstelle und kauft mir seiner Karte ein.
2. Der Kunde besucht Ihre Website und zahlt online.
3. Der Kunde ruft in Ihrer Verkaufsstelle an und gibt seine Karteninformationen am Telefon an oder versendet diese per Post oder Fax.

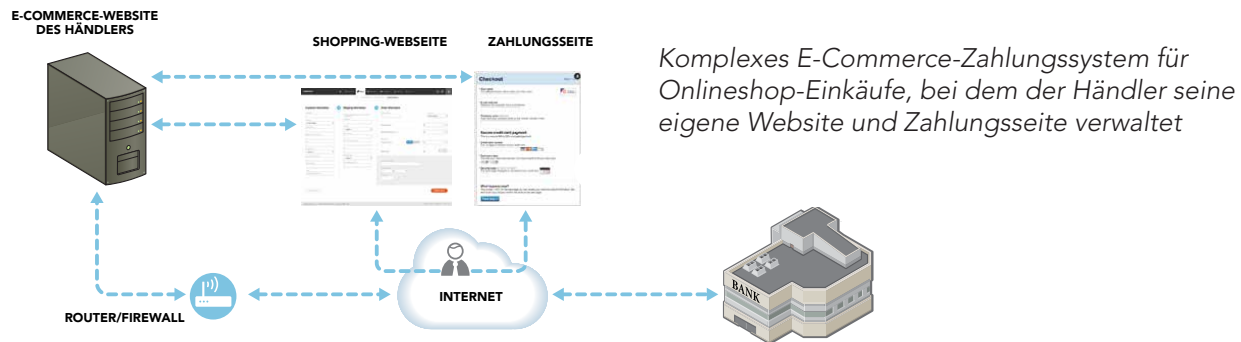
# Das eigene Risiko kennen: Arten von Zahlungssystemen

Ihr Sicherheitsrisiko hängt stark davon ab, wie komplex Ihr Zahlungssystem ist. Das gilt sowohl für den persönlichen Zahlungsverkehr vor Ort als auch online.



Einfaches Zahlungssystem für Ladenkäufe

Komplexes Zahlungssystem für Ladenkäufe mit WLAN, Kameras, Smartphones und weiteren zugehörigen Systemen



Komplexes E-Commerce-Zahlungssystem für Onlineshop-Einkäufe, bei dem der Händler seine eigene Website und Zahlungsseite verwaltet

















































Mithilfe des Leitfadens Gängige Zahlungssysteme können Sie ermitteln, welches Zahlungssystem Sie verwenden, welche Risiken das System birgt und welche Sicherheitstipps als Einstiegspunkt für Gespräche mit Ihrer Handelsbank und Ihren Vertriebspartnern empfohlen werden.



**SCHÜTZEN SIE IHR  
UNTERNEHMEN  
MIT HILFE FOLGENDER  
GRUNDLEGENDER  
SICHERHEITSMASSNAHMEN**

# Wie schützen Sie Ihr Unternehmen?

**Die gute Nachricht: Mithilfe der folgenden grundlegenden Sicherheitsmaßnahmen können Sie noch heute damit beginnen, Ihr Unternehmen zu schützen.**

So schützen Sie Ihr Unternehmen vor Datenpannen		Kostenaufwand	Komplexität	Risikominderung
	Verwenden Sie sichere Kennwörter und ändern Sie Standardkennwörter			
	Schützen Sie Ihre Kartendaten und speichern Sie nur das, was Sie brauchen			
	Prüfen Sie Kartenlesegeräte auf Manipulationsversuche			
	Installieren Sie Patches Ihrer Anbieter			
	Arbeiten Sie mit vertrauenswürdigen Geschäftspartnern zusammen und halten Sie deren Kontaktdaten bereit			
	Sichern Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter			
	Geben Sie Hackern keine Chance, auf Ihre Systeme zuzugreifen			
	Verwenden Sie Antivirus-Software			
	Prüfen Sie Ihre Systeme auf Schwachstellen und beheben Sie Probleme			
	Verwenden Sie sichere Kartenlesegeräte und -lösungen			
	Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet			
	Der beste Schutz: Machen Sie Ihre Daten nutzlos für Kriminelle			

*Diese grundlegenden Sicherheitsmaßnahmen sind nach Komplexität und Kostenaufwand sortiert (von geringer Komplexität und geringem Kostenaufwand zu hoher Komplexität und hohem Kostenaufwand). Die Größenordnung der Risikominderung, die sich mit den einzelnen Maßnahmen für Klein Händler ergibt, wird in der Spalte „Risikominderung“ angegeben.*



# Verwenden Sie sichere Kennwörter und ändern Sie Standardkennwörter

Kostenaufwand	
Komplexität	
Risikominderung	

Ihre Kennwörter sind für die Computer- und Kartendatensicherheit von entscheidender Bedeutung. So, wie ein Schloss an Ihrer Tür Ihr physisches Eigentum schützt, schützen Kennwörter Ihre Geschäftsdaten. Beachten Sie, dass neu gekaufte Computergeräte und -software (einschließlich Ihres Kartenlesegeräts) oftmals ein (voreingestelltes) Standardkennwort wie z. B. „password“ oder „admin“ aufweisen. Diese Kennwörter sind Hackern bekannt und werden häufig für Angriffe auf Kleinhändler genutzt.

Ca.  
**80 %** der Datenpannen gehen auf erratene oder gestohlene Passwörter zurück

Verizon PCI 2015

## ÄNDERN SIE IHRE KENNWÖRTER REGELMÄSSIG.

Behandeln Sie Ihre Kennwörter wie Ihre Zahnbürste. Lassen Sie sie von niemand anderem verwenden und legen Sie sich alle drei Monate ein neues zu.

**HOLEN SIE SICH HILFE.** Bitten Sie Ihre (Dienst-)Anbieter um Informationen zu Standardkennwörtern und darüber, wie man diese ändert. Und dann nichts wie Kennwörter ändern!

**ÜBERLEGEN SIE SICH KENNWÖRTER, DIE SCHWER ZU ERRATEN SIND.** Die häufigsten Kennwörter sind „password“ und „123456“. Hacker testen Kennwörter, die leicht zu erraten sind, weil die Hälfte aller Menschen solche Kennwörter verwendet. Ein sicheres Kennwort besteht aus mindestens sieben Zeichen sowie aus einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. !@#\$\$&\*). Auch eine Wortverbindung kann ein sicheres Kennwort sein (und lässt sich vielleicht auch leichter merken), z. B. „B1gMac&PommeS“.

**KENNWÖRTER DÜRFEN NICHT VON MEHREREN VERWENDET WERDEN.** Bestehen Sie darauf, dass jeder Mitarbeiter seine eigenen Anmeldedaten und Kennwörter hat. Kennwörter werden nicht gemeinsam genutzt!

Weitere Informationen zur Kennwortsicherheit finden Sie auf der Website des PCI Council:

### INFOGRAFIK



It's Time to Change Your Password (Zeit, Ihr Kennwort zu ändern)



### VIDEO

Learn Password Security in 2 Minutes (Kennwortsicherheit in 2 Minuten)

Typische Standardkennwörter, die geändert werden MÜSSEN:

[kein Passwort]

[Produkt-/Anbietername]

1234 oder 4321

zugriff

admin

anonym

datenbank

gast

manager

pass

password

root

sa

geheim

sysadmin

benutzer





# Schützen Sie Ihre Kartendaten und speichern Sie nur das, was Sie brauchen

Kostenaufwand	
Komplexität	
Risikominderung	

**Kartendaten können nur geschützt werden, wenn Sie wissen, wo sich diese Daten befinden.**

**Wie geht man dabei am besten vor?**

Mit Tokenisierung erzielt man Ähnliches wie mit Verschlüsselung, Tokenisierung funktioniert allerdings anders. Hierbei werden Kartendaten durch bedeutungslose Daten („Token“) ersetzt, die für einen Hacker wertlos sind.

**FRAGEN SIE EINEN EXPERTEN.** Erkundigen Sie sich beim Anbieter Ihres Kartenlesegeräts oder bei Ihrer Handelsbank, wo die Daten von Ihrem System gespeichert werden und ob Sie die Zahlungsabwicklung vereinfachen können. Fragen Sie außerdem nach, wie Sie bestimmte Transaktionen (z. B. regelmäßige Zahlungen) so durchführen können, ohne dass die Kartenprüfnummer gespeichert wird.


**LAGERN SIE DEN ZAHLUNGSVERKEHR AUS.** Das beste Mittel gegen Datenpannen ist, Kartendaten gar nicht erst zu speichern. Ziehen Sie in Betracht, Ihren Zahlungsverkehr an einen PCI DSS-konformen Dienstanbieter auszulagern. Unter „Onlinequellen“ auf Seite 22 finden Sie eine Liste konformer Dienstanbieter.

## **SPEICHERN SIE KEINE KARTENDATEN, DIE NICHT BENÖTIGT WERDEN.**

Vernichten Sie auf sichere Weise sämtliche Kartendaten, die Sie nicht benötigen. Falls Sie Unterlagen mit sensiblen Kartendaten aufbewahren müssen, schwärzen Sie die Daten mit einem dicken, schwarzen Filzstift, bis die Daten nicht mehr lesbar sind, und bewahren Sie die Unterlagen in einer abgesperrten Schublade oder einem Safe auf, zu dem nur wenige Personen Zugang haben.

**GRENZEN SIE DAS RISIKO EIN.** Statt Zahlungsdetails per E-Mail zu empfangen, bitten Sie Ihre Kunden, diese Daten per Telefon, Fax oder Post bereitzustellen.

## **VERWENDEN SIE TOKEN ODER VERSCHLÜSSELUNGEN.**

Fragen Sie bei Ihrer Handelsbank nach, ob Sie die Kartendaten WIRKLICH speichern müssen. Falls ja, bitten Sie Ihre Handelsbank oder Ihren Dienstanbieter um Informationen zu Verschlüsselung bzw. Tokenisierung, damit Kartendaten selbst bei Diebstahl nutzlos werden. (Weitere Informationen finden Sie unter „“ auf Seite 19.)

## **EINFÜHRUNG IN DIE VERSCHLÜSSELUNG**

*In der Kryptografie werden mathematische Formeln verwendet, um Klartext in Geheimentext zu verwandeln, den Personen ohne bestimmte Kenntnisse („Schlüssel“) nicht lesen können. Kryptografie kommt gleichermaßen bei gespeicherten Daten wie auch bei Daten, die über ein Netzwerk übermittelt werden, zum Einsatz.*

**VERSCHLÜSSELUNG**  
verwandelt Klartext in Geheimentext.

**ENTSCHLÜSSELUNG**  
verwandelt Geheimentext zurück in Klartext.

**Beispiel:**

Das ist ein Text, der geheim bleiben soll.

**VERSCHLÜSSELUNGSSCHLÜSSEL**

5a0 (k\$hQ%...

**ENTSCHLÜSSELUNGSSCHLÜSSEL**

Das ist ein Text, der geheim bleiben soll.





# Prüfen Sie Kartenlesegeräte auf Manipulationsversuche

Kostenaufwand



Komplexität



Risikominderung



Mithilfe von Skimming-Geräten werden die Kartendaten Ihrer Kunden beim Auslesen am Kartenlesegerät ausgespäht. Es ist unerlässlich, dass Sie und Ihre Mitarbeiter wissen, wie man ein Skimming-Gerät erkennt. Sie müssen Ihre Kartenlesegeräte regelmäßig prüfen, um sicherzustellen, dass sie nicht manipuliert wurden. Führen Sie Protokoll über die geprüften Lesegeräte und notieren Sie dabei, wann und durch wen die Prüfung stattfand und ob dabei etwas festgestellt wurde.

Weitere Informationen finden Sie unter PCI Council's guide: Skimming Prevention – Overview of Best Practices for Merchants (Leitfaden des PCI Council: Vermeidung von Skimming-Angriffen – Überblick über die Best Practices für Händler)

Seien Sie wachsam und gehen Sie wie folgt vor:

**FÜHREN SIE EINE LISTE** aller Kartenlesegeräte und machen Sie Fotos von diesen (Vorderseite, Rückseite, Kabel und Verbindungen), damit Sie wissen, wie die Geräte aussehen müssen.

**ACHTEN SIE AUF TYPISCHE MANIPULATIONSZEICHEN**, z. B. gebrochene Siegel an Abdeckblenden oder Schrauben, ungewöhnliche/andere Verkabelung sowie neue Geräte oder Funktionen, die Ihnen nicht bekannt sind. Im unten genannten Leitfaden des Council finden Sie weitere Informationen hierzu.

**SCHÜTZEN SIE IHRE LESEGERÄTE.** Bewahren Sie die Geräte außerhalb der Reichweite Unbefugter auf und schützen Sie das Display vor fremden Blicken. Stellen Sie vor Ladenschluss stets sicher, dass sämtliche Lesegeräte, die die Zahlungskarten oder persönlichen Identifikationsnummern (PINs) Ihrer Kunden auslesen, sicher verwahrt sind.

**KONTROLLIEREN SIE ETWAIGE REPARATUREN.** Lassen Sie Reparaturen an Ihren Kartenlesegeräten ausschließlich von autorisiertem Fachpersonal durchführen und auch nur dann, wenn Sie diese Personen erwarten. Weisen Sie Ihre Mitarbeiter entsprechend an.

**MELDEN** Sie dem Anbieter Ihres Kartenlesegeräts oder Ihrer Handelsbank umgehend, wenn Ihnen irgendetwas Ungewöhnliches auffällt!



# Installieren Sie Patches Ihrer Anbieter

Kostenaufwand	
Komplexität	
Risikominderung	

**Beim Schreiben von Softwarecode können Programmieren Fehler unterlaufen, die zu sogenannten Sicherheitslücken, Bugs oder Schwachstellen führen. Hacker nutzen diese Fehler, um Ihren Computer anzugreifen und Kontodaten zu stehlen. Schützen Sie Ihre Systeme, indem Sie vom Anbieter bereitgestellte „Patches“ installieren, um Codierungsfehler zu beheben. Eine zeitnahe Installation von Sicherheits-Patches ist unerlässlich!**

**ERKUNDIGEN SIE SICH** bei Ihrem (Dienst-)Anbieter, wie Sie über neue Sicherheits-Patches benachrichtigt werden, und stellen Sie sicher, dass Sie diese Benachrichtigungen erhalten und lesen.

## **WELCHE ANBIETER SENDEN IHNEN PATCHES?**

Patches können von verschiedenen Anbietern kommen, z. B. dem Anbieter Ihres Kartenlesegeräts, Ihrer Zahlungsanwendungen, sonstiger Zahlungssysteme (Ladenkassen, Registrierkassen, PCs usw.), Ihrer Betriebssysteme (Android, Windows, iOS usw.), Ihrer Anwendungssoftware (einschließlich Ihres Webbrowsers) sowie Ihrer Unternehmenssoftware.

**STELLEN SIE SICHER**, dass Ihre Anbieter Ihre Kartenlesegeräte, Betriebssysteme usw. aktualisieren, damit die neuesten Sicherheits-Patches unterstützt werden können. Haken Sie gegebenenfalls nach.

**E-COMMERCE-HÄNDLER.** Auch für Sie ist es absolut wichtig, Patches so bald wie möglich zu installieren. Halten Sie die Augen nach Patches von Ihrem Dienstanbieter offen. Erkundigen Sie sich bei Ihrem E-Commerce-Hosting-Anbieter, ob (und wie oft) er für Ihr System Patches bereitstellt. Stellen Sie sicher, dass Ihr Anbieter das Betriebssystem, die E-Commerce-Plattform bzw. die Web-Anwendung aktualisiert, damit die neuesten Patches unterstützt werden.

**BEFOLGEN** Sie die Anweisungen Ihres (Dienst-)Anbieters und installieren Sie die Patches so bald wie möglich.



# Arbeiten Sie mit vertrauenswürdigen Geschäftspartnern zusammen und halten Sie deren Kontaktdaten bereit

Kostenaufwand	
Komplexität	
Risikominderung	

Sie beziehen zahlungsbezogene Dienstleistungen, Geräte und Anwendungen von externen Anbietern. Sie arbeiten möglicherweise auch mit Dienstanbietern zusammen, die Ihre Zahlungssysteme unterstützen oder verwalten oder denen Sie Zugriff auf Kartendaten gewähren. Ganz gleich, ob Ihnen diese Anbieter als „Abwickler“, „Drittanbieter“ oder „Dienstanbieter“ geläufig sind. Sie alle haben Einfluss auf Ihre Fähigkeit, Ihre Kartendaten zu schützen. Deshalb ist es unerlässlich, dass Sie diese Anbieter kennen und wissen, welche Sicherheitsfragen sie diesen Stellen müssen.

**SIE MÜSSEN WISSEN, AN WEN SIE SICH WENDEN KÖNNEN.** Welche ist Ihre Handelsbank? Wer hilft Ihnen noch mit der Zahlungsabwicklung? Von wem haben Sie Ihre Zahlungsgeräte/-software gekauft und wer hat Sie für Sie eingerichtet/installiert? Wer sind Ihre Dienstanbieter?

**FÜHREN SIE EINE LISTE.** Sie wissen nun, an wen Sie sich wenden müssen. Halten Sie Unternehmens- und Kontaktnamen, Telefonnummern, Webadressen und weitere Kontaktdaten bereit, sodass Sie diese im Notfall schnell zur Hand haben.

**PRÜFEN SIE IHRE DIENSTANBIETER AUF IHRE SICHERHEIT.** Erfüllt Ihr Dienstanbieter die PCI DSS Anforderungen? Für E-Commerce-Händler ist es ebenfalls wichtig, dass der Zahlungsdienstleister PCI DSS-konform ist! Unter „Onlinequellen“ auf Seite 22 finden Sie eine Liste konformer Dienstleister.

**STELLEN SIE FRAGEN.** Sobald Sie Ihre externen Anbieter kennen und wissen, was diese für Sie tun, informieren Sie sich bei den Anbietern, wie sie Ihre Kartendaten schützen. Weitere Informationen zu den Fragen, die Sie stellen sollten, finden Sie im Dokument [Fragen an Ihre Anbieter](#).

**INFORMIEREN SIE SICH ÜBER DIE GÄNGIGEN ANBIETER.** In der Leiste rechts finden Sie eine Übersicht der gängigen Arten von (Dienst-)Anbietern, mit denen Sie möglicherweise zusammenarbeiten.

## GÄNGIGE ANBIETER

Weitere Informationen zu den folgenden gängigen Anbietern finden Sie in der Tabelle im Dokument [Fragen an Ihre Anbieter](#).

Kartenlesegerät-Anbieter

Zahlungsanwendungs-Anbieter

Installierer von Zahlungssystemen (sogenannte Integratoren/Wiederverkäufer)

Dienstleister, die Zahlungsabwicklungen, E-Commerce-Hosting oder -Abwicklungen durchführen

Dienstleister, die Ihnen helfen, die PCI DSS Anforderung(en) zu erfüllen (z. B. durch die Bereitstellung einer Firewall oder von Antivirus-Services)

Software-as-a-Service-Anbieter



# Sichern Sie den Zugriff auf Ihre Daten durch eigene Mitarbeiter

Kostenaufwand



Komplexität



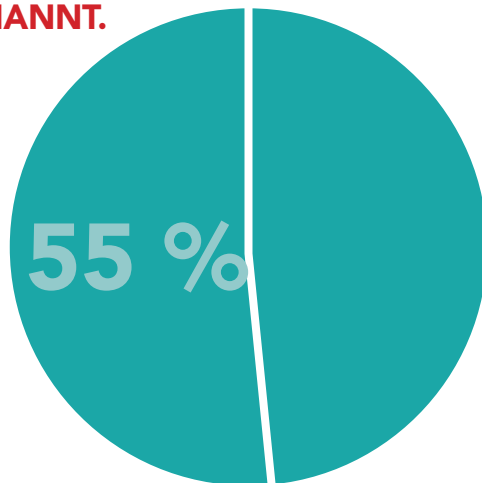
Risikominderung



„Missbräuchliche Verwendung von Berechtigungen“ bedeutet, dass eine Person ...

... die Zugriffsdaten und Berechtigungen von jemand anderem verwendet, um auf Systeme oder Daten zuzugreifen, für die die Person keine Zugriffsberechtigungen hat.

**DIE MISSBRÄUCLICHE VERWENDUNG VON BERECHTIGUNGEN IST DER HÄUFIGSTE GRUND FÜR DATENPANNEN UND WIRD IN 55 % DER GEMELDETEN VORFÄLLE ALS URSACHE GENANNT.**



Verizon 2015

## ZUGRIFFSKONTROLLE HAT OBERSTE PRIORITÄT.

Richten Sie Ihr System so ein, dass Zugriff ausschließlich auf Basis des sogenannten Need-to-know-Prinzips gewährt wird. Sie als Inhaber haben Zugriff auf alles. Für die meisten Mitarbeiter reicht es jedoch aus, Zugriff nur auf bestimmte Daten, Anwendungen und Funktionen zu haben.

**SCHRÄNKEN SIE DIE ZUGRIFFSRECHTE EIN** und gewähren Sie nur denjenigen Mitarbeitern Zugriff auf Zahlungssysteme und unverschlüsselte Kartendaten, die darauf angewiesen sind. Zugriff sollte außerdem nur auf die Daten, Anwendungen und Funktionen gewährt werden, die die Mitarbeiter für ihre tägliche Arbeit wirklich benötigen.

**FÜHREN SIE PROTOKOLL.** Machen Sie sich Notizen über sämtliche „Besucher hinter dem Tresen“. Notieren Sie Name, Grund des Besuchs und Name des Mitarbeiters, der dem Besucher Zutritt gewährt hat. Bewahren Sie die Aufzeichnungen mindestens ein Jahr auf.

## GERÄTE MÜSSEN SICHER ENTSORGT WERDEN.

Erkundigen Sie sich bei Ihrem Zahlungssystem-Anbieter oder Dienstleister, wie Sie Kartendaten sicher löschen können, bevor Sie Zahlungsgeräte weiterverkaufen oder entsorgen (damit die Daten nicht wiederhergestellt werden können).

**GEBEN SIE DIESE INFORMATIONEN WEITER.** Geben Sie diesen Leitfaden Ihren Mitarbeitern und Geschäftspartnern, damit alle Beteiligten wissen, was von ihnen erwartet wird.

*Ziehen Sie in Betracht, Mitarbeiter zur Annahme von Zahlungen zu berechtigen, aber nicht zur Abwicklung von Rückgaben – oder zur Annahme neuer Buchungen/Bestellungen, aber nicht zum Zugriff auf Zahlungskartendaten, die mit bereits getätigten Buchungen/Bestellungen in Verbindung stehen. Manche Mitarbeiter sollten überhaupt keine Zugriffsberechtigungen haben.*



# Geben Sie Hackern keine Chance, auf Ihre Systeme zuzugreifen

Kostenaufwand	
Komplexität	
Risikominderung	

## HACKER SIND KRIMINELLE

Einer der einfachsten Wege für Hacker, in Ihr System einzudringen, bietet sich mit den Menschen, denen Sie vertrauen. Sie müssen wissen, wie Ihre Anbieter auf Ihr System zugreifen, um sicherzustellen, dass keine Sicherheitslücken für Hacker entstehen.

Bei der Multi-Faktor-Authentifizierung werden ein Benutzername und ein Kennwort sowie mindestens ein weiterer Faktor (z. B. eine Smartcard, ein Dongle\* oder eine einmalige Kennung) verwendet.

\*Ein kleines Gerät, das man an den Computer anschließt, um Zugriff auf WLAN, Softwarefunktionen usw. zu gewähren.

**INFORMIEREN SIE SICH.** Fragen Sie Ihren Zahlungssystem-Anbieter oder Diensteanbieter, ob dieser Remote-Zugriff verwendet, um Ihrem Unternehmen Support zu bieten oder auf Daten zuzugreifen.

**FRAGEN SIE NACH, WIE SICH DER REMOTE-ZUGRIFF EINSCHRÄNKEN LÄSST.** Viele Programme für den Remote-Zugriff sind standardmäßig immer aktiv. Senken Sie Ihr Risiko: Erkundigen Sie sich bei Ihrem Anbieter, wie der Remote-Zugriff deaktiviert werden kann, wenn er nicht benötigt wird, und wie Sie ihn wieder aktivieren können, wenn Ihr (Dienst-)Anbieter dies ausdrücklich verlangt.

**DEAKTIVIEREN SIE DEN REMOTE-ZUGRIFF, WENN ER NICHT BENÖTIGT WIRD.**

**VERWENDEN SIE EINE SICHERE AUTHENTIFIZIERUNG.** Wenn Sie Remote-Zugriff gewähren müssen, verlangen Sie Multi-Faktor-Authentifizierung und starke Kryptografie.

**STELLEN SIE SICHER, DASS IHRE DIENSTANBIETER EINDEUTIGE ANMELDEDATEN VERWENDEN.** Jeder der Anbieter muss Anmeldedaten für den Remote-Zugriff verwenden, die nur für Ihr Unternehmen gelten; dieselben Anmeldedaten dürfen nicht für mehrere Kunden verwendet werden.

**BITTEN SIE UM HILFE.** Bitten Sie Ihren (Dienst-)Anbieter um Hilfe bei der Deaktivierung des Remote-Zugriffs oder bei der Einrichtung von Multi-Faktor-Authentifizierung (sofern Ihr (Dienst-)Anbieter Remote-Zugriff benötigt). Weitere Informationen zu den Fragen, die Sie Ihrem Anbieter stellen sollten, finden Sie im Dokument [Fragen an Ihre Anbieter](#).

*Wenn Ihr Anbieter Support oder Fehlerbehebung für Ihr Kartenlesegerät von seinem Standort aus (statt an Ihrem Standort) bietet, nutzt er hierfür das Internet und Software für Remote-Zugriff.*

*Zu den gängigen Produkten, die Anbieter auf Geräten installieren und für den Remote-Support einsetzen, gehören VNC und LogMeIn.*



# Verwenden Sie Antivirus-Software

Kostenaufwand	
Komplexität	
Risikominderung	

Systeme und Software sind extrem flexibel und bieten zahlreiche Funktionen. Hacker schreiben Viren und andere Schadcodes, um diese Funktionen und eventuelle Codierungsfehler auszunutzen und so in Ihre Systeme einzudringen und Kartendaten zu stehlen. Mithilfe aktueller Antivirussoftware (auch Antischadsoftware genannt) können Sie Ihre Systeme schützen.

**INSTALLIEREN SIE ANTIVIRUSSOFTWARE, UM IHR ZAHLUNGSSYSTEM ZU SCHÜTZEN.** Antivirussoftware ist im Elektronikfachhandel erhältlich und einfach zu installieren.

**LEGEN SIE FEST, DASS DIE SOFTWARE AUTOMATISCH AKTUALISIERT WIRD,** damit Sie stets die aktuelle Version nutzen und optimal geschützt sind.

**INFORMIEREN SIE SICH.** Bitten Sie Ihren Fachhändler um Empfehlungen für Antivirus-/Antischadsoftware.

**FÜHREN SIE REGELMÄSSIG SCANS DURCH.** Führen Sie regelmäßig vollständige Systemscans durch. Ihre Systeme könnten nämlich mit neuer Schadsoftware infiziert worden sein, die in Umlauf gebracht wurde, bevor Ihre Antivirussoftware diese überhaupt entdecken konnte.





# Prüfen Sie Ihre Systeme auf Schwachstellen und beheben Sie Probleme

Kostenaufwand	
Komplexität	
Risikominderung	

Jeden Tag werden neue Schwachstellen, Sicherheitslücken und Bugs entdeckt. Es ist wichtig, dass Sie Ihre internetfähigen Systeme regelmäßig testen lassen, um neue Risiken zu ermitteln und diese möglichst frühzeitig in Angriff zu nehmen. Ihre internetfähigen Systeme (zu denen viele Zahlungssysteme gehören) sind am anfälligsten, da diese von Kriminellen angegriffen und ausgespäht werden können.

*Die ASVs des PCI Council führen externe Schwachstellen-Scans durch und erstellen entsprechende Berichte. Weitere Informationen finden Sie unter [List of PCI-Approved Scanning Vendors](#) (Liste der PCI-zugelassenen Scanning-Anbieter)*

**INFORMIEREN SIE SICH.** Erkundigen Sie sich bei Ihrer Handelsbank, ob man dort Partnerschaften mit von PCI zugelassenen Scanning-Anbietern (Approved Scanning Vendors, ASVs) pflegt. Fragen Sie auch bei Ihren (Dienst-)Anbietern nach.

**SPRECHEN SIE MIT EINEM PCI ASV.** Diese Anbieter können für Sie Tools bereitstellen, die Ihr Netzwerk automatisch auf Schwachstellen prüfen und einen Bericht erstellen, falls Sie beispielsweise ein Patch installieren müssen. Weitere Informationen zu Scanning-Anbietern finden Sie in der unten genannten Liste des PCI Council.

**SUCHEN SIE NACH EINEM PASSENDEN SCAN-PROGRAMM.** Wenden Sie sich an mehrere PCI ASVs, um einen Anbieter zu finden, der das passende Programm für Ihr mittelständisches Unternehmen hat.


**NEHMEN SIE SCHWACHSTELLEN IN ANGRIFF.** Bitten Sie Ihren ASV um Hilfe bei der Behebung von Problemen, die bei den Scans gefunden wurden.



# Verwenden Sie sichere Kartenlesegeräte und -lösungen

Kostenaufwand	
Komplexität	
Risikominderung	

Eine gute Möglichkeit, um Ihr Unternehmen besser zu schützen, ist der Einsatz von Zahlungslösungen und geschultem Fachpersonal. Lesen Sie, wie Sie sichere Produkte finden und sicherstellen, dass diese sicher eingerichtet sind.

Weitere Informationen zu PCI Kartenlesegeräten anderen sicheren Kartenlesegeräten, die Kartendaten verschlüsseln, finden Sie unter  auf Seite 19.

**VERWENDEN SIE SICHERE KARTENLESE- UND PIN-EINGABEGERÄTE.** Der PCI Council genehmigt Kartenlesegeräte, die PIN-Daten schützen. Achten Sie darauf, dass Ihr Gerät auf der [List of PCI Approved PTS Devices](#) (Liste PCI-zugelassener PTS-Geräte) steht, die Geräte umfasst, die die beste Sicherheit bieten, und EMV-Chips unterstützt.

**VERWENDEN SIE SICHERE SOFTWARE.** Achten Sie darauf, dass Ihre Zahlungssoftware auf der [List of PCI Validated Payment Applications](#) (Liste der PCI-geprüften Zahlungsanwendungen) steht.

**SETZEN SIE QUALIFIZIERTES FACHPERSONAL EIN.** Sorgen Sie dafür, dass die Person, die Ihre PA-DSS-geprüfte Anwendung installiert, diesen Vorgang ordnungsgemäß und sicher durchführt. Suchen Sie in der [List of PCI QIRs](#) (Liste der PCI QIRs) nach Unternehmen, die vom PCI Council qualifiziert wurden. Bitten Sie Ihre Handelsbank bei der Entscheidung um Hilfe.

**LESEN SIE SICH DIE LISTE DER FRAGEN AN IHREN ANBIETER DURCH.** Weitere Informationen zu den Fragen, die Sie Ihren (Dienst-)Anbietern stellen sollten, finden Sie im Dokument [Fragen an Ihre Anbieter](#).

*Ihre Kunden geben die persönlichen Identifizierungsnummern (PINs) für Ihre Zahlungskarten in Ihr Kartenlese- oder PIN-Eingabegerät ein. Es ist wichtig, sichere Geräte zu verwenden, um die PIN-Daten Ihrer Kunden zu schützen.*





# Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet

Kostenaufwand	
Komplexität	
Risikominderung	

**Das Internet ist ein wahres Paradies für Datendiebe, um Angriffe zu starten und die Kartendaten Ihrer Kunden zu stehlen. Aus diesem Grund benötigen sämtliche internetbasierten Systeme, die Sie zur Kartenzahlung nutzen, zusätzlichen Schutz.**

**VERWENDEN SIE IHRE GERÄTE ISOLIERT VONEINANDER.** Nutzen Sie das Gerät, mit dem Sie Zahlungen abwickeln, nicht für andere Zwecke. Verwenden Sie also etwa das Gerät oder den Computer, mit dem Sie Zahlungstransaktionen durchführen, nicht, um damit im Internet zu surfen, E-Mails zu lesen oder sich in sozialen Medien aufzuhalten. Falls erforderlich, verwenden Sie einen anderen Computer und nicht das Gerät, das Sie für Zahlungen verwenden (beispielsweise wenn Sie Ihren Webauftritt in den sozialen Medien aktualisieren möchten).

**SCHÜTZEN SIE IHR „VIRTUELLES TERMINAL“.** Wenn Sie Kundenzahlungen über ein virtuelles Terminal eingeben (also eine Webseite, auf die Sie per Computer oder Tablet zugreifen), senken Sie Ihr Risiko – verbinden Sie das Gerät also nicht mit einem externen Kartenlesegerät.

**SCHÜTZEN SIE IHR WLAN.** Wenn Ihre Verkaufsstelle kostenloses WLAN für Kunden anbietet, sorgen Sie dafür, dass Sie für Ihr Zahlungssystem ein anderes Netzwerk verwenden (dieses Verfahren nennt sich „Netzwerksegmentierung“). Bitten Sie Ihren Netzwerktechniker um Hilfe bei der sicheren Konfigurierung Ihres WLAN.

**VERWENDEN SIE EINE FIREWALL.** Eine ordnungsgemäß konfigurierte Firewall dient zum Schutz vor Hackern und Schadsoftware, die auf Ihre Computer und Daten zugreifen wollen. Erkundigen Sie sich bei Ihrem Kartenlesegerät-Anbieter oder Diensteanbieter, um sicherzustellen, dass Sie über eine Firewall verfügen, und bitten Sie um Hilfe bei der ordnungsgemäßen Konfigurierung.

**VERWENDEN SIE EINE PERSÖNLICHE FIREWALL-SOFTWARE ODER ANDERE GLEICHWERTIGE SOFTWARE,** wenn Zahlungssysteme nicht von Ihrer Unternehmens-Firewall geschützt werden (beispielsweise wenn eine Verbindung zu einem öffentlichen WLAN besteht).



# Der beste Schutz: Machen Sie Ihre Daten nutzlos für Kriminelle

Kostenaufwand	
Komplexität	
Risikominderung	

Ihre Daten sind bei ihrer Übertragung an Ihre Handelsbank ebenso potenziell gefährdet wie auf Ihren Computern und Geräten. Die beste Möglichkeit, Ihre Daten zu schützen, ist, die Daten – selbst bei Diebstahl – durch Verschlüsselung bzw. Tokenisierung nutzlos zu machen und komplett zu löschen, wenn Sie nicht mehr benötigt werden. Die Umsetzung dieser Maßnahme gestaltet sich zwar vergleichsweise komplex, langfristig gesehen aber kann sie den sicherheitstechnischen Verwaltungsaufwand deutlich vereinfachen.

**ERKUNDIGEN SIE SICH BEI IHREM ZAHLUNGSSYSTEM- ODER DIENSTANBIETER,** ob Ihr Kartenlesegerät Verschlüsselungs- bzw. Tokenisierungstechnologie nutzt.

**VERWENDEN SIE PCI GERÄTE, DIE KARTENDATEN VERSCHLÜSSELN.** Der PCI Council genehmigt Kartenlesegeräte, die PIN-Daten schützen (siehe auf Seite 17) sowie sichere Kartenlesegeräte, die Kartendaten zusätzlich verschlüsseln. Siehe [List of PCI Approved PTS Devices](#) (Liste PCI-zugelassener PTS-Geräte).

**VERWENDEN SIE SICHERE PCI VERSCHLÜSSELUNGSLÖSUNGEN.** Erkundigen Sie sich, ob die Verschlüsselung auf Ihrem Kartenlesegerät per Point-to-Point-Verschlüsselungslösung erfolgt und auf der [List of PCI P2PE Validated Solutions](#) (Liste PCI P2PE-validierter Lösungen) des PCI Council steht.

**ERWÄGEN SIE EIN UPGRADE FÜR IHRE LÖSUNG.** Senken Sie Ihr Risiko – ziehen Sie in Betracht, sich ein neues Kartenlesegerät zuzulegen, das sowohl Verschlüsselung als auch Tokenisierung nutzt, um die Kartendaten für Hacker nutzlos zu machen.

**SIND SIE HÄNDLER UND STELLEN SIE AUF EMV-CHIP-GERÄTE UM?** Dann ist das die beste Gelegenheit, in ein Gerät zu investieren, das EMV unterstützt und außerdem zusätzliche Sicherheit durch Verschlüsselung und Tokenisierung bietet.

**STELLEN SIE FRAGEN.** Weitere Informationen zu Fragen, die Sie Ihrem (Dienst-)Anbieter stellen sollten, finden Sie im Dokument [Fragen an Ihre Anbieter](#).

*PCI-zugelassene, sichere Kartenlesegeräte, die Kartendaten verschlüsseln, verwenden sogenannte SRED(Secure Reading and Exchange of Data)-Technologie. Erkundigen Sie sich bei Ihrem Anbieter, ob Ihr Kartenlesegerät mithilfe von SRED verschlüsselt.*



# WEITERFÜHRENDE QUELLEN

# Onlinequellen

## Listen des PCI Council

Quelle	Link	URL
List of Validated Payment Applications (Liste geprüfter Zahlungsanwendungen)	<a href="#"><i>PCI Council's Validated Payment Applications (Vom PCI Council geprüfte Zahlungsanwendungen)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement">https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement</a>
List of Approved PTS Devices (Liste zugelassener PTS-Geräte)	<a href="#"><i>PCI Council's Approved PTS Devices (Vom PCI Council zugelassene PTS-Geräte)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices">https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices</a>
List of Approved Scanning Vendors (Liste zugelassener Scanning-Anbieter)	<a href="#"><i>PCI Council's Approved Scanning Vendors (Vom PCI Council zugelassene Scanning-Anbieter)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors">https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors</a>
List of Qualified Integrators / Resellers (Liste qualifizierter Integratoren/Wiederverkäufer)	<a href="#"><i>PCI Council's Qualified Integrators Resellers (Vom PCI Council qualifizierte Integratoren/Wiederverkäufer)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers">https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers</a>
List of P2PE Validated Solutions (Liste P2PE-validierter Lösungen)	<a href="#"><i>PCI Council's P2PE Validated Solutions (Vom PCI Council validierte P2PE-Lösungen)</i></a>	<a href="https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions">https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions</a>

## Listen von Zahlungskartengesellschaften

Quelle	Link	URL
Lists of Compliant Service Providers (Listen konformer Dienstanbieter)	<a href="#"><i>MasterCard List of Compliant Service Providers (Liste konformer Dienstanbieter von MasterCard)</i></a>	<a href="https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html">https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html</a>
	<a href="#"><i>Visa's Global Registry of Service Providers (Globales Dienstanbieterverzeichnis von Visa)</i></a>	<a href="http://www.visa.com/splisting/">http://www.visa.com/splisting/</a>
	<a href="#"><i>Visa Europe Registered Member Agents (Registrierte Mitgliedsbeauftragte von Visa Europe)</i></a>	<a href="https://www.visaeurope.com/receiving-payments/security/downloads-and-resources">https://www.visaeurope.com/receiving-payments/security/downloads-and-resources</a>

## PCI DSS und zugehörige Anleitungen

Quelle	Link	URL
More about PCI DSS (Weitere Informationen zu PCI DSS)	<a href="#"><i>How to Secure with PCI DSS (Sicherheit mit PCI DSS)</i></a>	<a href="https://www.pcisecuritystandards.org/pci_security/how">https://www.pcisecuritystandards.org/pci_security/how</a>
PCI DSS Self-Assessment Questionnaires (PCI DSS Selbstbeurteilungs-Fragebögen)	<a href="#"><i>Self-Assessment Questionnaires (Selbstbeurteilungs-Fragebögen)</i></a>	<a href="https://www.pcisecuritystandards.org/pci_security/completing_self_assessment">https://www.pcisecuritystandards.org/pci_security/completing_self_assessment</a>
Guide: Skimming Prevention: Overview of Best Practices for Merchants (Leitfaden: Vermeidung von Skimming-Angriffen: Überblick über die Best Practices für Händler)	<a href="#"><i>Skimming Prevention: Overview of Best Practices for Merchants (Vermeidung von Skimming-Angriffen: Überblick über die Best Practices für Händler)</i></a>	<a href="https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf">https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf</a>

# Onlinequellen

## Infografiken und Videos

Quelle	Link	URL
Infografik: It's Time to Change Your Password (Zeit, Ihr Kennwort zu ändern)	<a href="#"><u>It's Time to Change Your Password (Zeit, Ihr Kennwort zu ändern)</u></a>	<a href="https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf"><u>https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf</u></a>
Infografik: Fight Cybercrime by Making Stolen Data Worthless to Thieves (Internetkriminalität bekämpfen: gestohlene Daten für Diebe unbrauchbar machen)	<a href="#"><u>Fight Cybercrime by Making Stolen Data Worthless to Thieves (Internetkriminalität bekämpfen: gestohlene Daten für Diebe unbrauchbar machen)</u></a>	<a href="https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf"><u>https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf</u></a>
Video: Learn Password Security in 2 Minutes (Kennwortsicherheit in 2 Minuten)	<a href="#"><u>Learn Password Security in 2 Minutes (Kennwortsicherheit in 2 Minuten)</u></a>	<a href="https://www.youtube.com/watch?v=FsrOXgZKa7U"><u>https://www.youtube.com/watch?v=FsrOXgZKa7U</u></a>

## Onlinequellen von PCI: sichere Kartenzahlung für Kleinhändler

Quelle	Link	URL
Gängige Zahlungssysteme	<a href="#"><u>Gängige Zahlungssysteme</u></a>	<a href="https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf"><u>https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf</u></a>
Kleinhändler-Fragen an ihre Anbieter	<a href="#"><u>Kleinhändler-Fragen an ihre Anbieter</u></a>	<a href="https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf"><u>https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf</u></a>
Kleinhändler-Glossar	<a href="#"><u>Kleinhändler-Glossar</u></a>	<a href="https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf"><u>https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf</u></a>

# Quellen

Gallup – Gallup Umfrage, Oktober 2015

HM Government – *Small Businesses: What You Need to Know about Cyber Security* (Mittelständische Unternehmen: Was Sie über Internetsicherheit wissen müssen, Vereinigtes Königreich 2014)

NCSA – *National Cyber Security Alliance survey* (Umfrage der National Cyber Security Alliance), 2012

NSBA – National Small Business Administration, *2014 Year End Economic Report* (Wirtschaftsbericht zum Jahresende 2014)

Verizon 2012 – *Verizon 2012 Data Breach Investigations Report* (Datenpannen-Untersuchungsbericht 2012 von Verizon)

Verizon 2015 – *Verizon 2015 Data Breach Investigations Report* (Datenpannen-Untersuchungsbericht 2015 von Verizon)

Verizon PCI 2015 – *Verizon 2015 PCI Compliance Report* (PCI Konformitätsbericht 2015 von Verizon)