SICHERE KARTENZAHLUNG FÜR KLEINHÄNDLER

Gängige Zahlungssysteme

Version 1.0 | Juli 2016

PCI Security Standards Council®

Zahlungssysteme und wie man sie schützt

ARTEN VON ZAHLUNGSSYSTEMEN

Um Ihr Unternehmen gegen Zahlungsdatendiebstahl zu schützen, müssen Sie erst einmal verstehen, wie die Zahlung in Ihrem Geschäft bzw. Ihrer Filiale abläuft. Welche Geräte verwenden Sie? Welche Bank und welchen Technologieanbieter haben Sie? Und wie funktioniert das alles eigentlich im Ganzen?

Anhand der folgenden Beispiele aus dem Alltag können Sie ermitteln, welches Zahlungssystem Sie verwenden, welche Risiken damit verbunden sind und wie Sie sich schützen können.

PCI Security Standards Council®

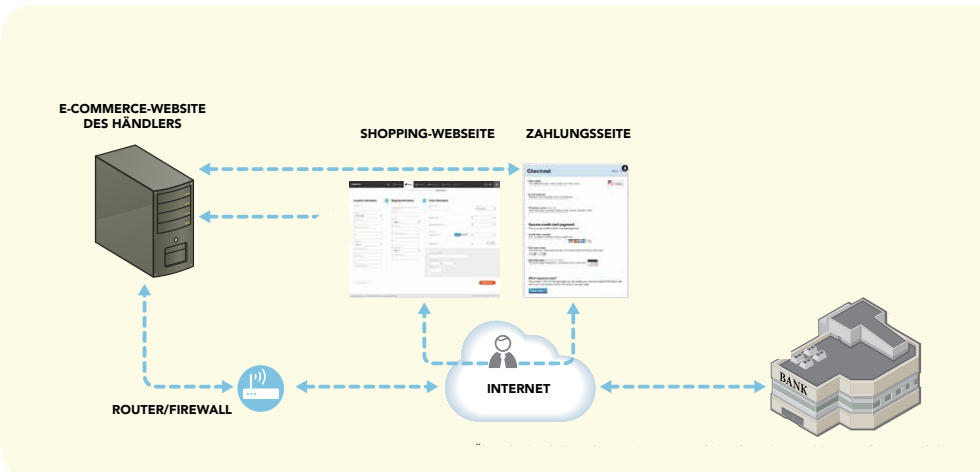
Arten von Zahlungssystemen im Überblick

Typ	Beschreibung des Zahlungssystems
1	Dial-up Zahlungsterminal. Zahlungsdaten werden über das Telefonnetz gesendet.
2	Dial-up Zahlungsterminal und internetfähige elektronische Kasse. Zahlungsdaten werden über das Telefonnetz gesendet.
3	An eine elektronische Kasse angeschlossenes Zahlungsterminal. Die elektronische Kasse sendet die Zahlungsdaten via Internet.
4	An eine elektronische Kasse angeschlossenes Zahlungsterminal mit Verschlüsselungstechnologie. Die elektronische Kasse sendet die Zahlungsdaten via Internet.
5	Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse mit Internetverbindung. Zahlungsdaten werden via Internet gesendet.
6	Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse greifen auf dieselben kartenunabhängigen Daten zu (teilintegriert). Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet.
7	Integriertes Zahlungsterminal und Zahlungs-Middleware greifen auf dieselben Kartendaten zu. Zahlungsdaten werden via Internet gesendet.
8	Kabelloses Zahlungsterminal mit Verschlüsselungstechnologie („Pay-at-Table“) mit integriertem Zahlungsterminal und Middleware. Zahlungsdaten werden via Internet gesendet.
9	An eine elektronische Kasse angeschlossenes Zahlungsterminal, das mit weiteren Geräten verbunden ist. Zahlungsdaten werden via Internet gesendet.
10	E-Commerce-Händler ohne eigene Zahlungsseite. Die Zahlungsdaten werden via Internet von einem Drittanbieter gesendet.
11	E-Commerce-Händler bietet eigene Zahlungsseite und eigene Website an. Zahlungsdaten werden vom Händler via Internet gesendet.
12	Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz gesendet.
13	Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz oder WLAN gesendet.
14	Virtuelles Zahlungsterminal mit Zugriff über den Internetbrowser des Händlers. Zahlungsdaten werden via Internet gesendet.

Wie nutzen Sie diese Ressource?

BESTIMMEN SIE, WELCHES SCHAUBILD AM EHESTEN IHREM ZAHLUNGSSYSTEM ENTSPRICHT:

- Dieser Leitfaden ist als Ergänzung zum *Leitfaden für sichere Zahlungsverfahren* gedacht und zeigt verschiedene gängige Zahlungssysteme in Form von Schaubildern – vom einfachsten zum komplexesten.
- Jedes Schaubild besteht aus vier Ansichten:
  1) Überblick
  2) Risiken: Wo sind die Kartendaten Risiken ausgesetzt?
  3) Gefahr: Wie gelangen Kriminelle an Kartendaten?
  4) Schutz: Empfehlungen zum Schutz von Kartendaten.
- Finden Sie heraus, welches Schaubild am ehesten Ihrem Zahlungssystem entspricht.



RISIKEN UND GEFAHREN ERKENNEN:

- Sobald Sie herausgefunden haben, welches Schaubild Ihr Zahlungssystem am besten widerspiegelt, entnehmen Sie den beiden Folgeschaubildern, in welchen Bereichen die Kartendaten besonders gefährdet sind und inwiefern Ihr Unternehmen anfällig für Angriffe ist.

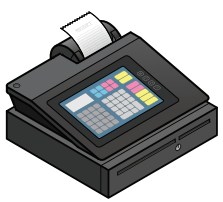
KARTENDATEN UND DAS EIGENE UNTERNEHMEN MITHILFE GRUNDLEGENDER SICHERHEITSMASSNAHMEN SCHÜTZEN:

- In der vierten Ansicht erfahren Sie schließlich, wie Sie Ihr Unternehmen schützen können.
- Als Hilfestellung finden Sie in dieser Ansicht Links zu den entsprechenden Bereichen im *Leitfaden für sichere Zahlungsverfahren*.
- Siehe auch *Fragen an Ihre Anbieter* und *Glossar zu Begrifflichkeiten aus dem Zahlungsverkehr und der Informationssicherheit*

Was bedeuten diese Begriffe?

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.

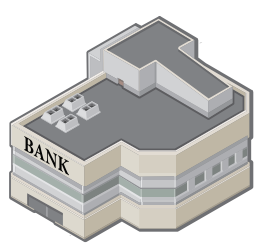
Ein **ZAHLUNGSTERMINAL** ist das Gerät, mit dem man die Kartenzahlung eines Kunden entgegennimmt, indem man die Karte durchzieht, einsteckt, einfach ans Lesegerät hält oder die Kartennummer manuell eingibt. POS-Terminal, Kreditkartenlesegerät, EC- oder Kartenterminal oder Chipkartenleser sind weitere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

TYP 1

Dial-up Zahlungsterminal. Zahlungsdaten werden über das Telefonnetz gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

TYP 1

Dial-up Zahlungsterminal. Zahlungsdaten werden über das Telefonnetz gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

An welchem Punkt sind Kartendaten gefährdet?

TYP 1

Dial-up Zahlungsterminal. Zahlungsdaten werden über das Telefonnetz gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

Wie kommen Kriminelle an Ihre Kartendaten?

Sie stehlen Belege oder Berichte, die Sie nicht sicher verwahren, die Sie verwahren, obwohl Sie sie nicht länger brauchen, oder die Sie nicht sicher entsorgen.

Sie stehlen Kartendaten mithilfe sogenannter Skimming-Geräte, die sie am Zahlungsterminal anbringen (oder darin verbauen).

Sie können auch Ihr Terminal stehlen und durch ein manipuliertes ersetzen, um an die Kartendaten zu gelangen.

TYP 1

Dial-up Zahlungsterminal. Zahlungsdaten werden über das Telefonnetz gesendet.

RISIKOPROFIL

Chip: GERING

Magnetstreifen: GERING

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Schützen Sie die Daten und verwahren Sie nur das, was Sie brauchen
- Untersuchen Sie Ihre Zahlungsterminals auf Schäden oder Auffälligkeiten
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe

*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

TYP 2

Dial-up Zahlungsterminal und internetfähige elektronische Kasse. Zahlungsdaten werden über das Telefonnetz gesendet.

RISIKOPROFIL

Chip: GERING

Magnetstreifen: GERING

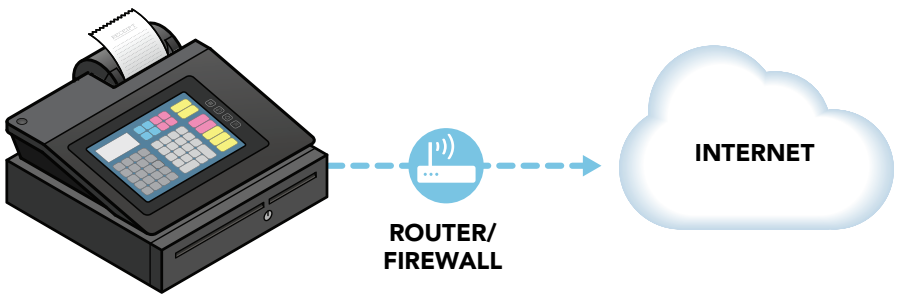
JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

ELEKTRONISCHE KASSE

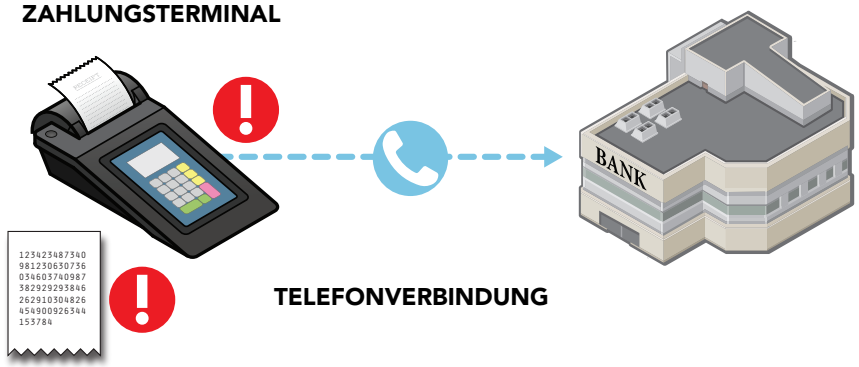
Mit dem Internet verbundene elektronische Kasse, an der jedoch keine Kartenzahlung erfolgt



ZAHLUNGSTERMINAL

Der Gesamtbetrag wird im Zahlungsterminal manuell eingegeben

Das Zahlungsterminal ist mit der Bank lediglich über eine Telefonverbindung verbunden



Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

TYP 2

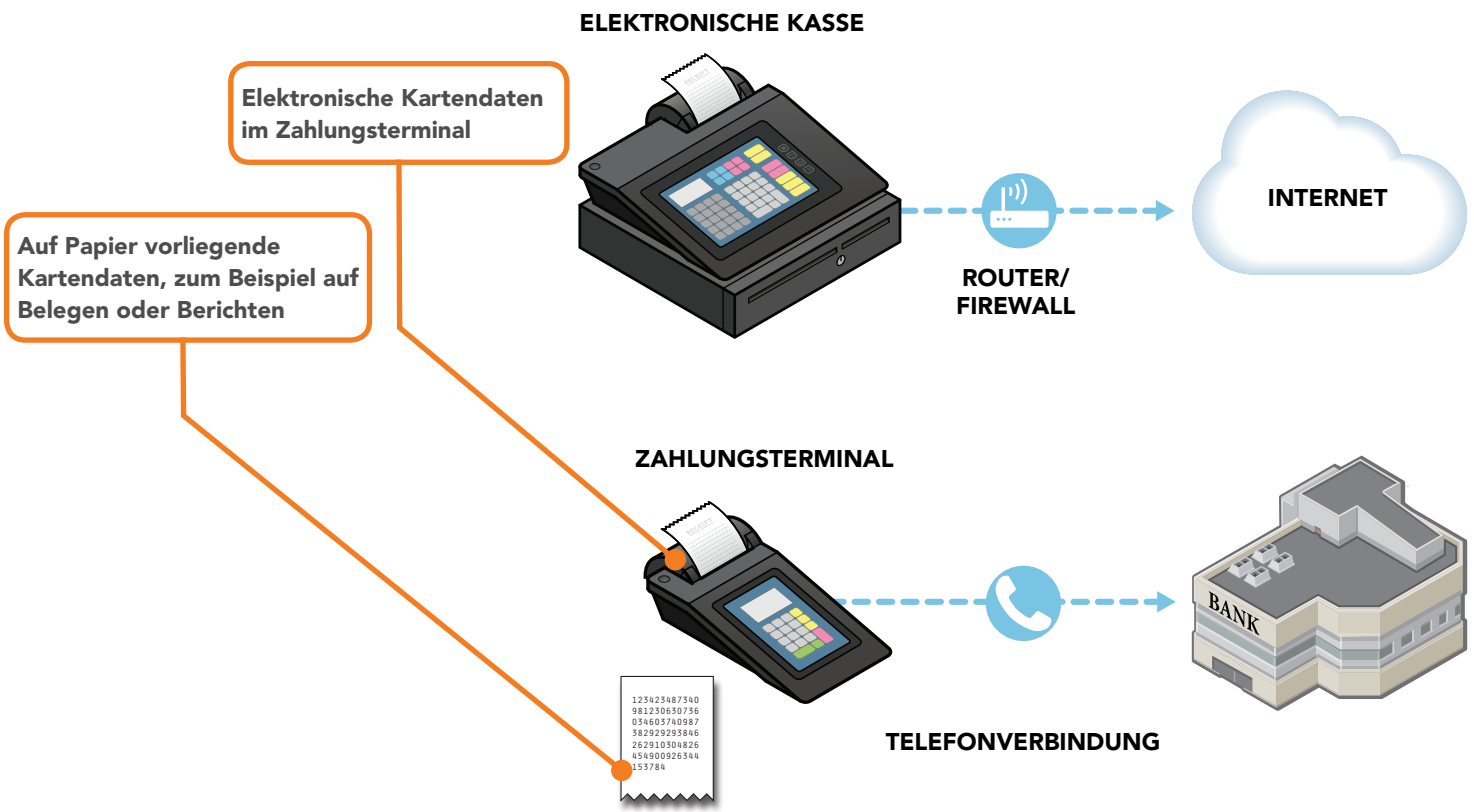
Dial-up Zahlungsterminal und internetfähige elektronische Kasse. Zahlungsdaten werden über das Telefonnetz gesendet.

RISIKOPROFIL

Chip: GERING

Magnetstreifen: GERING

An welchem Punkt sind Kartendaten gefährdet?



PCI Security Standards Council

TYP 2

Dial-up Zahlungsterminal und internetfähige elektronische Kasse. Zahlungsdaten werden über das Telefonnetz gesendet.

RISIKOPROFIL

Chip: GERING

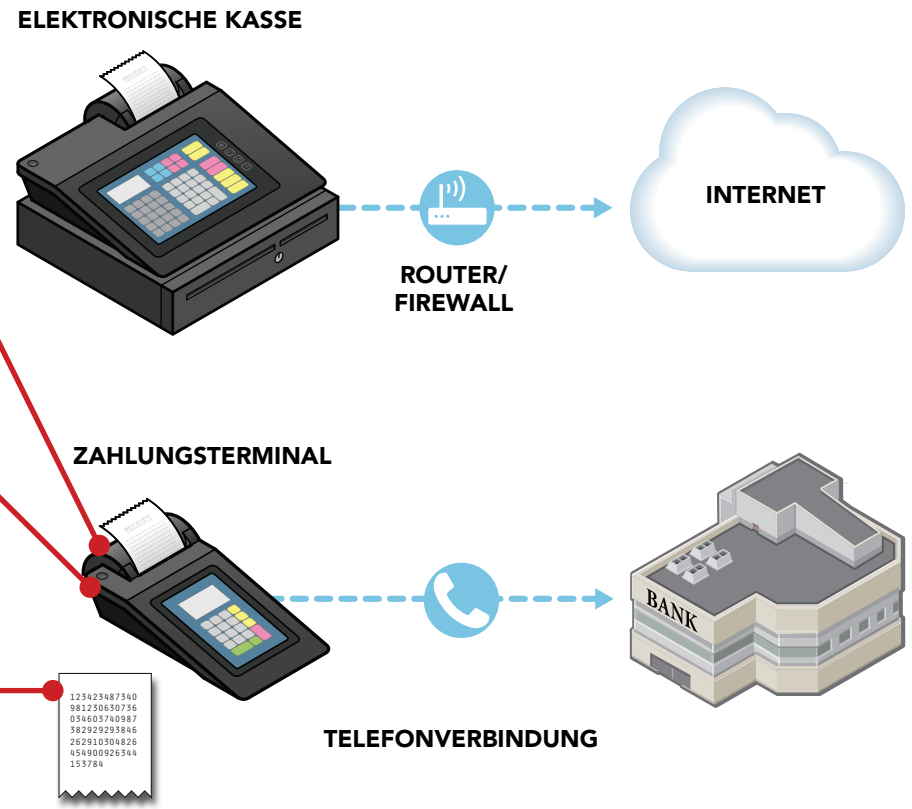
Magnetstreifen: GERING

Wie kommen Kriminelle an Ihre Kartendaten?

Sie stehlen Kartendaten mithilfe sogenannter Skimming-Geräte, die sie am Zahlungsterminal anbringen (oder darin verbauen).

Sie können auch Ihr Terminal stehlen und durch ein manipuliertes ersetzen, um an die Kartendaten zu gelangen.

Sie stehlen Belege oder Berichte, die Sie nicht sicher verwahren, die Sie verwahren, obwohl Sie sie nicht länger brauchen, oder die Sie nicht sicher entsorgen.



TYP 2

Dial-up Zahlungsterminal und internetfähige elektronische Kasse. Zahlungsdaten werden über das Telefonnetz gesendet.

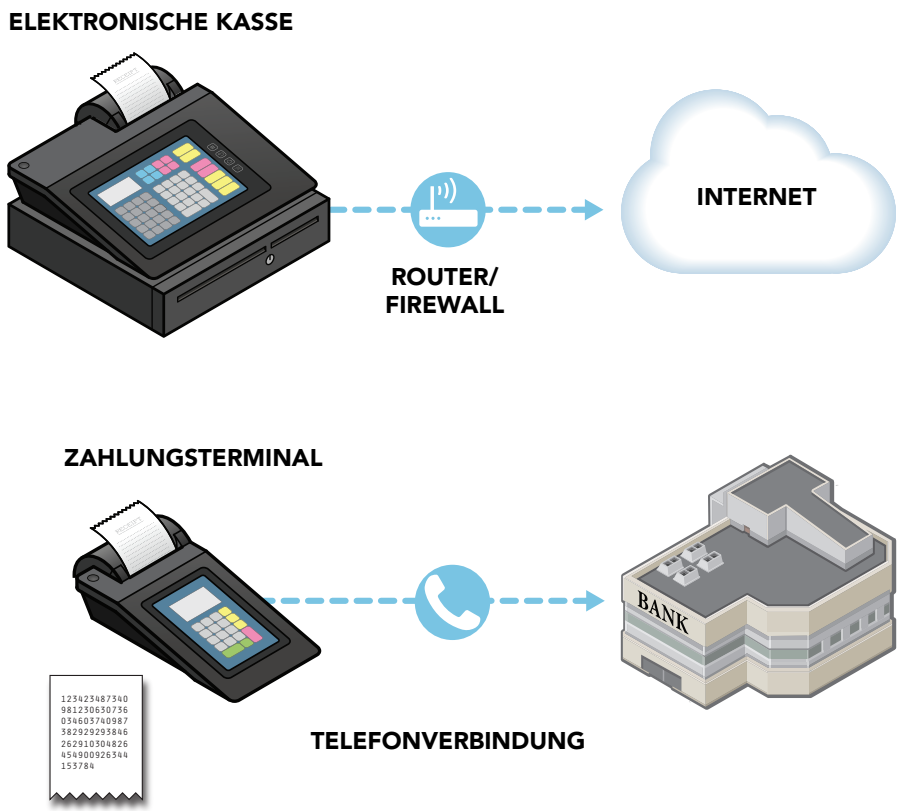
RISIKOPROFIL

Chip: GERING

Magnetstreifen: GERING

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Schützen Sie Ihre Daten und verwahren Sie nur das, was Sie brauchen
- Untersuchen Sie Ihre Zahlungsterminals auf Schäden oder Auffälligkeiten
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

TYP 3

An eine elektronische Kasse angeschlossenes Zahlungsterminal. Die elektronische Kasse sendet die Zahlungsdaten via Internet.

RISIKOPROFIL

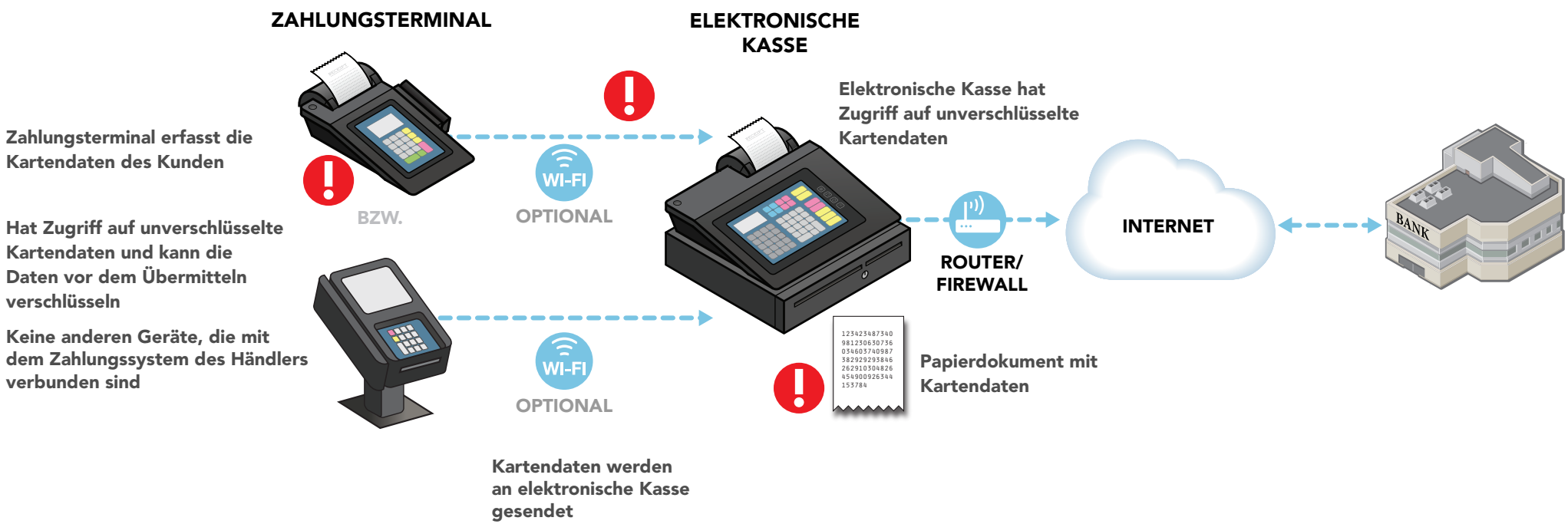
Chip: MITTEL

Magnetstreifen: HOCH

JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.



Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

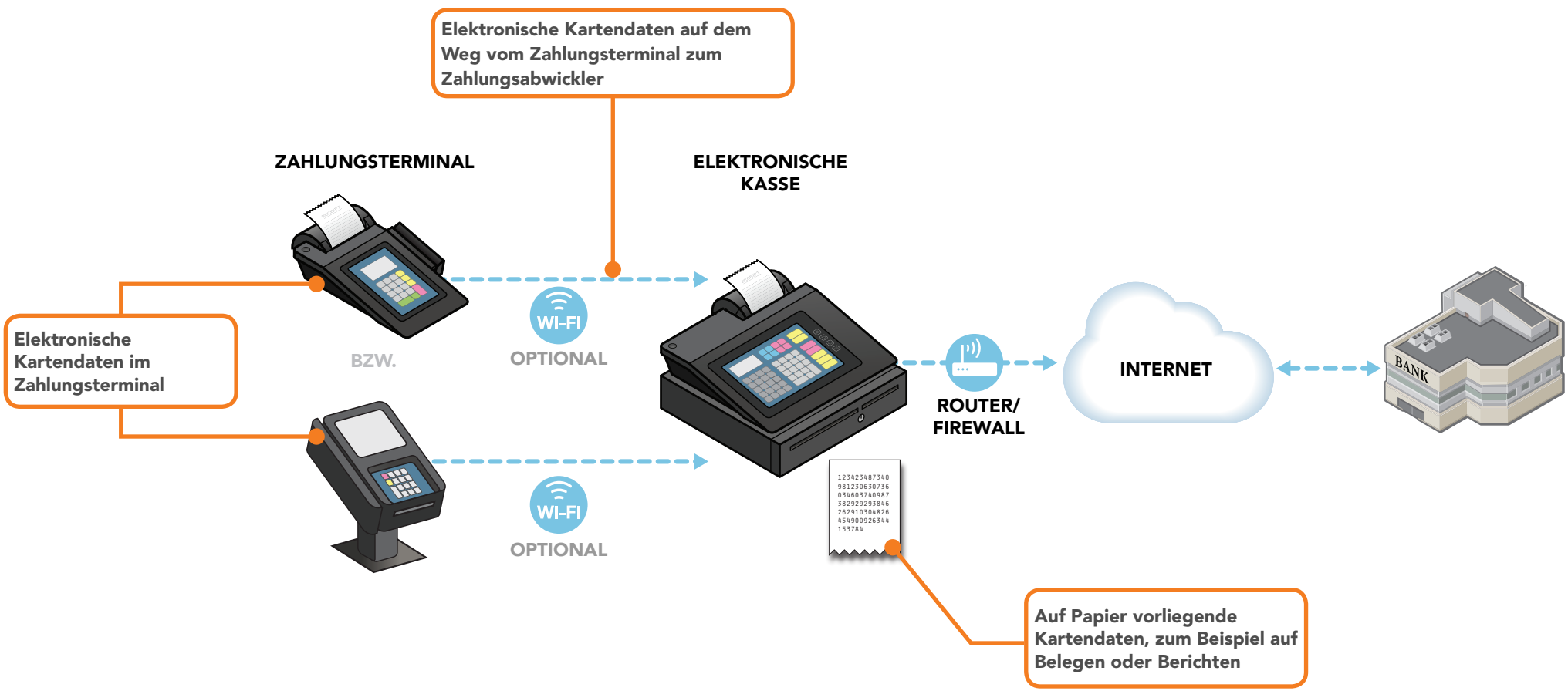
An eine elektronische Kasse angeschlossenes Zahlungsterminal. Die elektronische Kasse sendet die Zahlungsdaten via Internet.

RISIKOPROFIL

Chip: MITTEL

Magnetstreifen: HOCH

An welchem Punkt sind Kartendaten gefährdet?



An eine elektronische Kasse angeschlossenes Zahlungsterminal. Die elektronische Kasse sendet die Zahlungsdaten via Internet.

RISIKOPROFIL

Chip: MITTEL

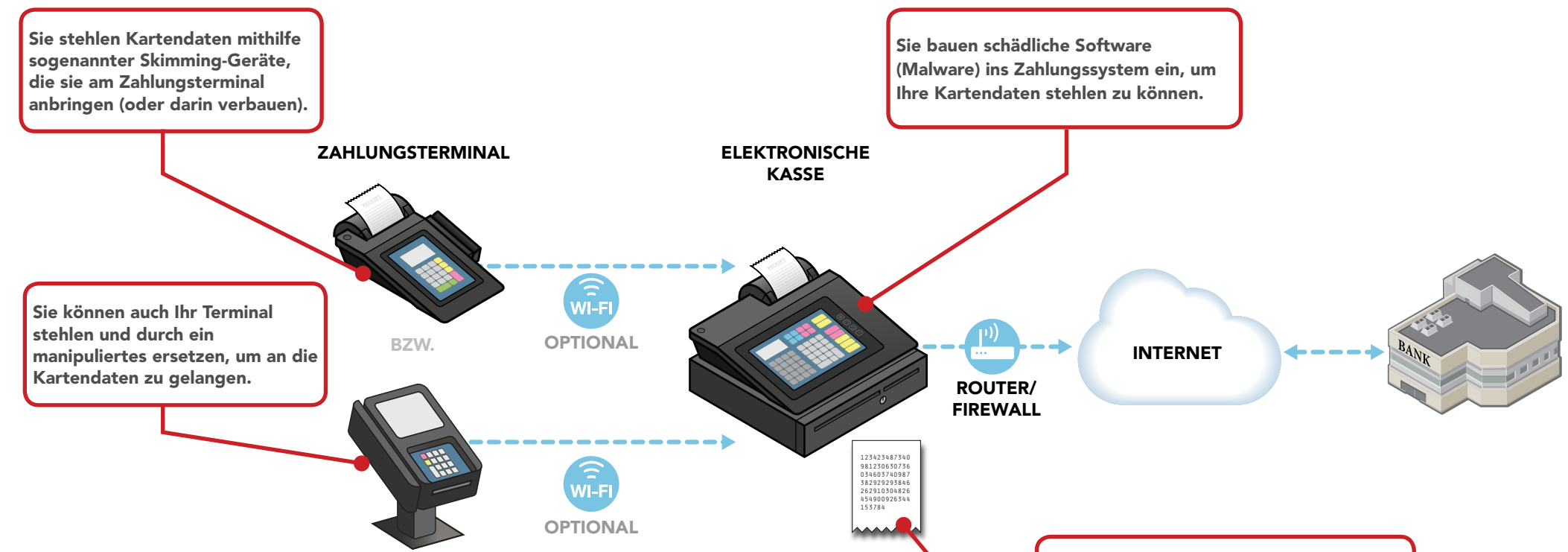
Magnetstreifen: HOCH

Wie kommen Kriminelle an Ihre Kartendaten?

Sie stehlen Kartendaten mithilfe sogenannter Skimming-Geräte, die sie am Zahlungsterminal anbringen (oder darin verbauen).

Sie können auch Ihr Terminal stehlen und durch ein manipuliertes ersetzen, um an die Kartendaten zu gelangen.

Sie bauen schädliche Software (Malware) ins Zahlungssystem ein, um Ihre Kartendaten stehlen zu können.



Sie stehlen Belege oder Berichte, die Sie nicht sicher verwahren, die Sie verwahren, obwohl Sie sie nicht länger brauchen, oder die Sie nicht sicher entsorgen.

PCI Security Standards Council

TYP 3

An eine elektronische Kasse angeschlossenes Zahlungsterminal. Die elektronische Kasse sendet die Zahlungsdaten via Internet.

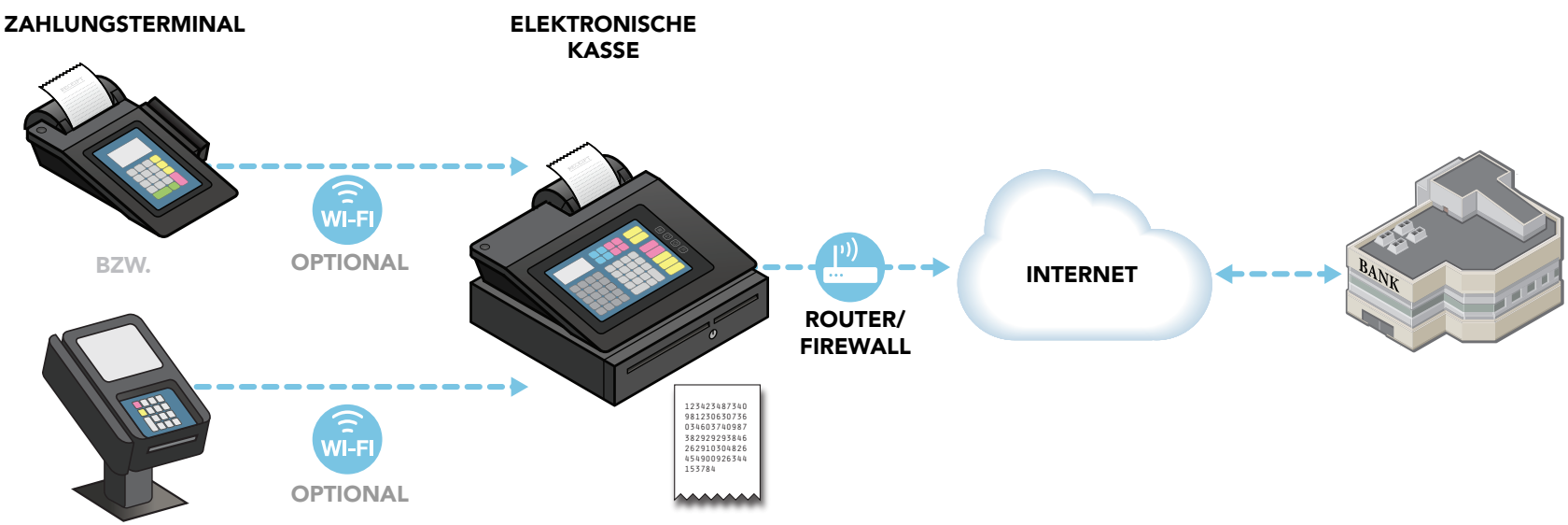
RISIKOPROFIL

Chip: MITTEL

Magnetstreifen: HOCH

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Schützen Sie die Daten und verwahren Sie nur das, was Sie brauchen
- Untersuchen Sie Ihre Zahlungsterminals auf Schäden oder Auffälligkeiten
- Installieren Sie Patches Ihres Zahlungsterminal-Anbieters
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Beschränken Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter
- Lassen Sie regelmäßig Scans auf Sicherheitsrisiken durchführen
- Verwenden Sie sichere Zahlungsterminals
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet
- Machen Sie Ihre Kartendaten nutzlos für Kriminelle



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

TYP 4

An eine elektronische Kasse angeschlossenes Zahlungsterminal mit Verschlüsselungstechnologie. Die elektronische Kasse sendet die Zahlungsdaten via Internet.

RISIKOPROFIL

Chip: MITTEL

Magnetstreifen: HOCH

JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

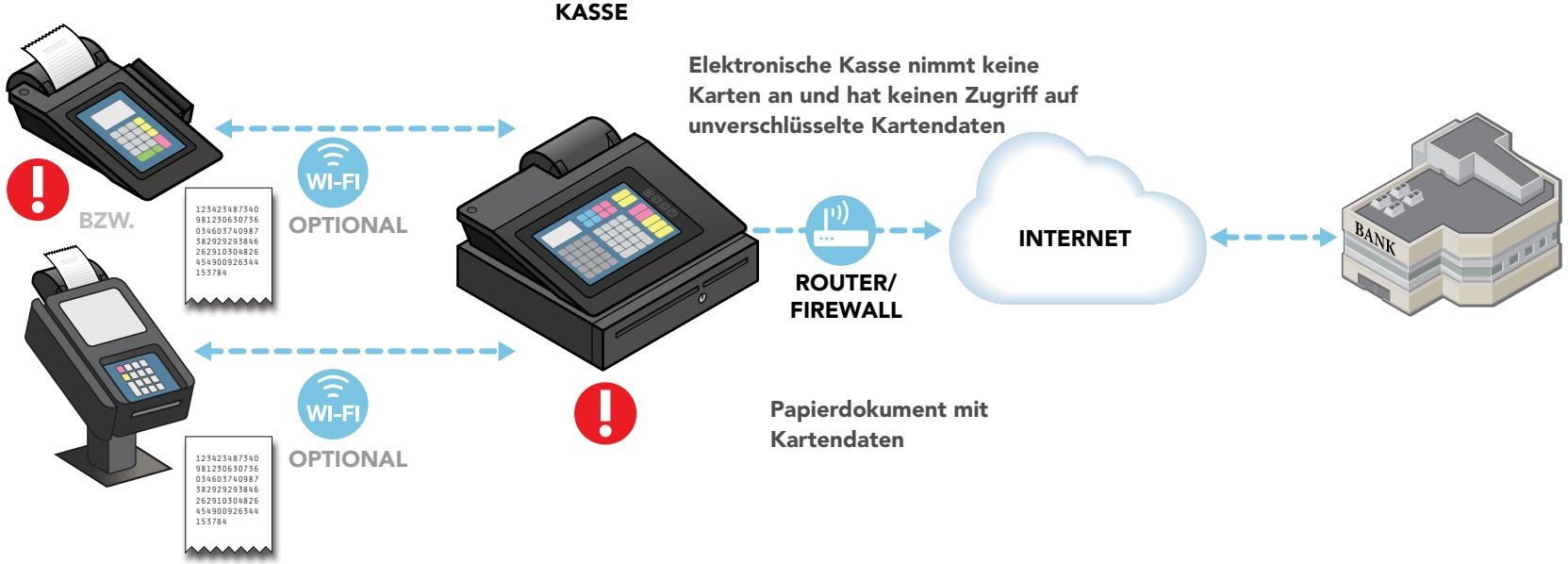
ZAHLUNGSTERMINAL

ELEKTRONISCHE KASSE

Zahlungsterminal verschlüsselt Kartendaten (z. B. mithilfe von SRED, Secure Reading and Exchange of Data von PCI)

Der Händler hat keinen Zugriff auf unverschlüsselte Daten

Keine anderen Geräte, die mit den Zahlungssystemen des Händlers verbunden sind



Elektronische Kasse nimmt keine Karten an und hat keinen Zugriff auf unverschlüsselte Kartendaten

Papierdokument mit Kartendaten

Kartendaten werden verschlüsselt an elektronische Kasse gesendet

Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

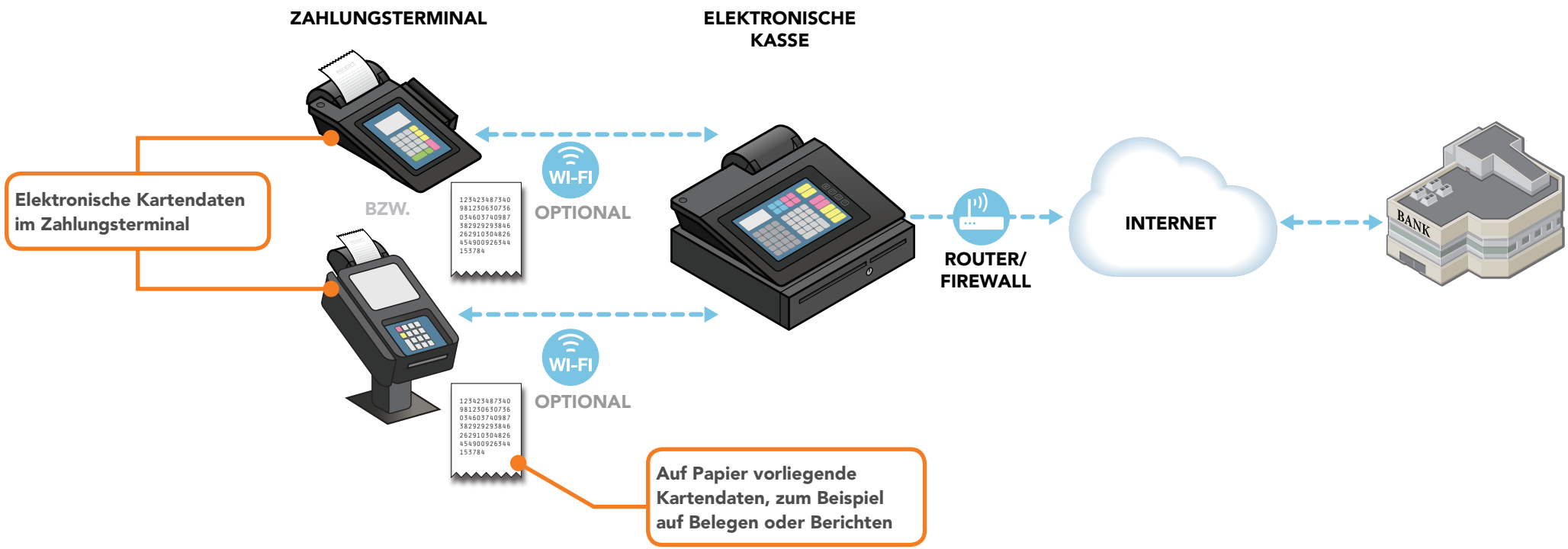
TYP 4

An eine elektronische Kasse angeschlossenes Zahlungsterminal mit Verschlüsselungstechnologie. Die elektronische Kasse sendet die Zahlungsdaten via Internet.

RISIKOPROFIL

Chip	Magnetstreifen
MITTEL	HOCH

An welchem Punkt sind Kartendaten gefährdet?



PCI Security Standards Council

TYP 4

An eine elektronische Kasse angeschlossenes Zahlungsterminal mit Verschlüsselungstechnologie. Die elektronische Kasse sendet die Zahlungsdaten via Internet.

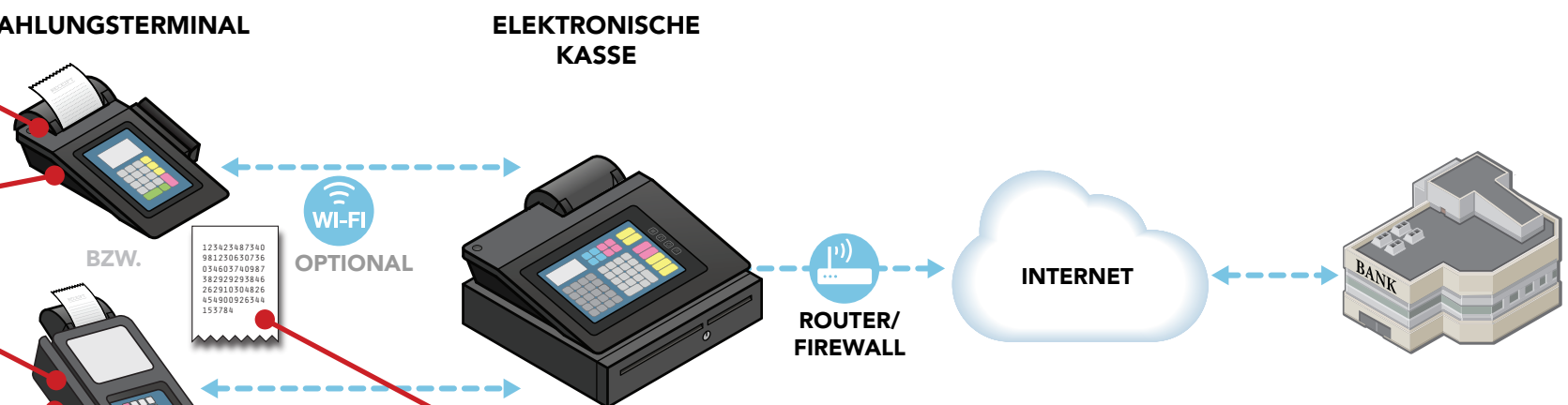
RISIKOPROFIL

Chip: MITTEL

Magnetstreifen: HOCH

Wie kommen Kriminelle an Ihre Kartendaten?

Sie stehlen Kartendaten mithilfe sogenannter Skimming-Geräte, die sie am Zahlungsterminal anbringen (oder darin verbauen).



Sie können auch Ihr Terminal stehlen und durch ein manipuliertes ersetzen, um an die Kartendaten zu gelangen.

Sie stehlen Belege oder Berichte, die Sie nicht sicher verwahren, die Sie verwahren, obwohl Sie sie nicht länger brauchen, oder die Sie nicht sicher entsorgen.

PCI Security Standards Council

TYP 4

An eine elektronische Kasse angeschlossenes Zahlungsterminal mit Verschlüsselungstechnologie. Die elektronische Kasse sendet die Zahlungsdaten via Internet.

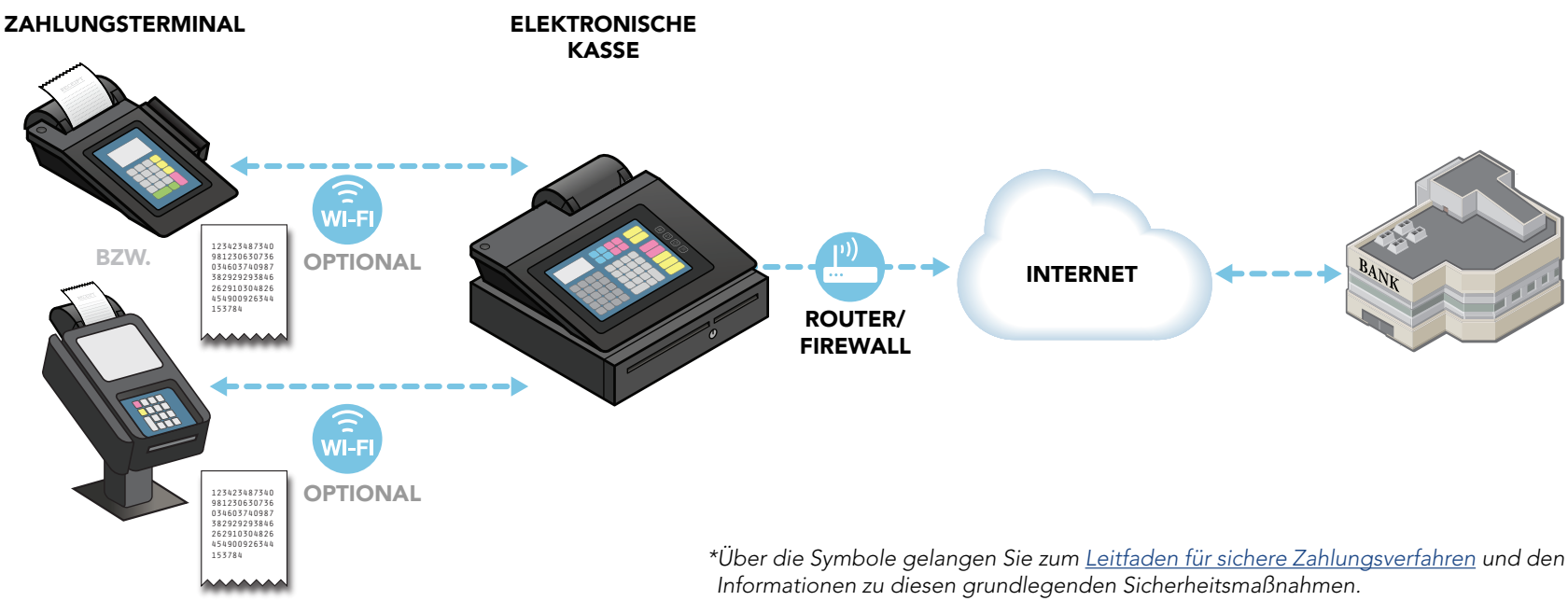
RISIKOPROFIL

Chip: MITTEL

Magnetstreifen: HOCH

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Verwenden Sie sichere Zahlungsterminals
- Schützen Sie die Daten und verwahren Sie nur das, was Sie brauchen
- Sichern Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet
- Untersuchen Sie Ihre Zahlungsterminals auf Schäden oder Auffälligkeiten
- Beschränken Sie den Remote-Zugriff für Anbieter – geben Sie Hackern keine Chance
- Installieren Sie Patches Ihres Zahlungsterminal-Anbieters
- Lassen Sie regelmäßig Scans auf Sicherheitsrisiken durchführen



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

TYP 5

Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse mit Internetverbindung. Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

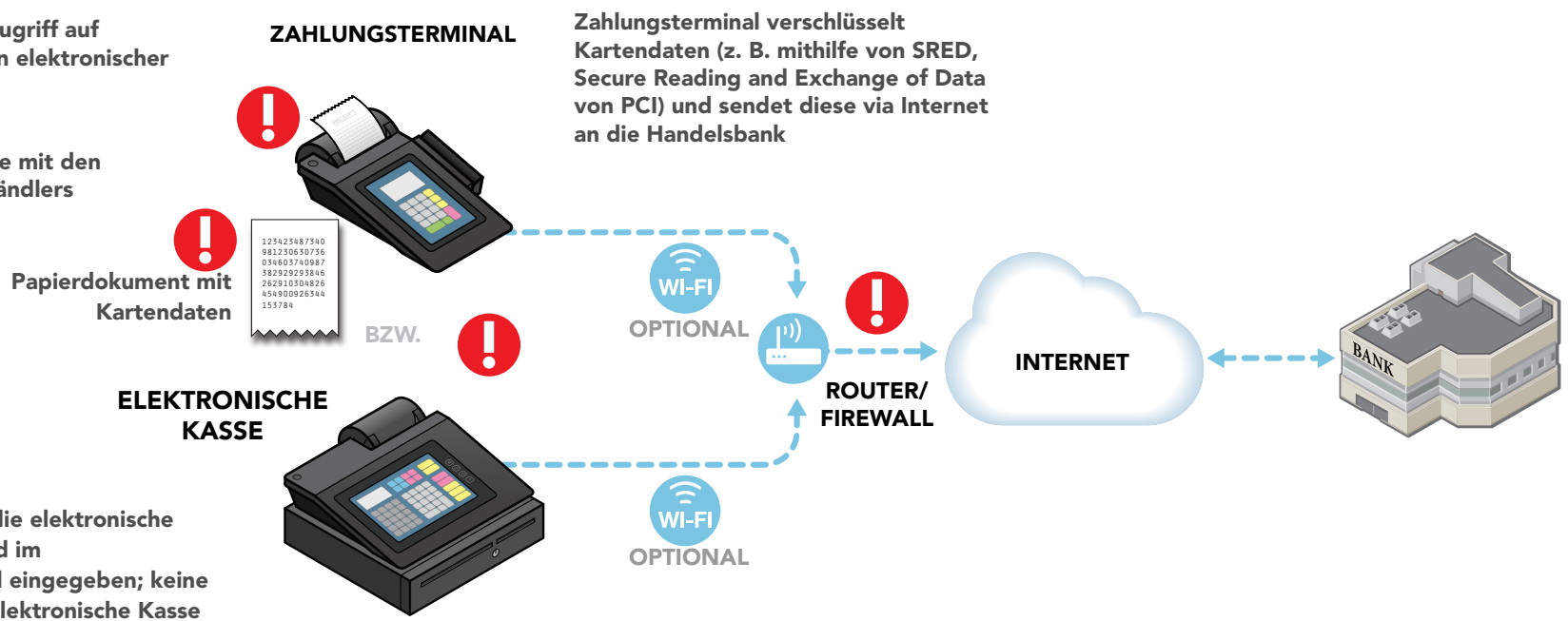
JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

Der Händler hat keinen Zugriff auf unverschlüsselte Daten (in elektronischer Form)

Keine anderen Geräte, die mit den Zahlungssystemen des Händlers verbunden sind



Der Gesamtbetrag, den die elektronische Kasse berechnet hat, wird im Zahlungsterminal manuell eingegeben; keine Kartenzahlung über die elektronische Kasse möglich

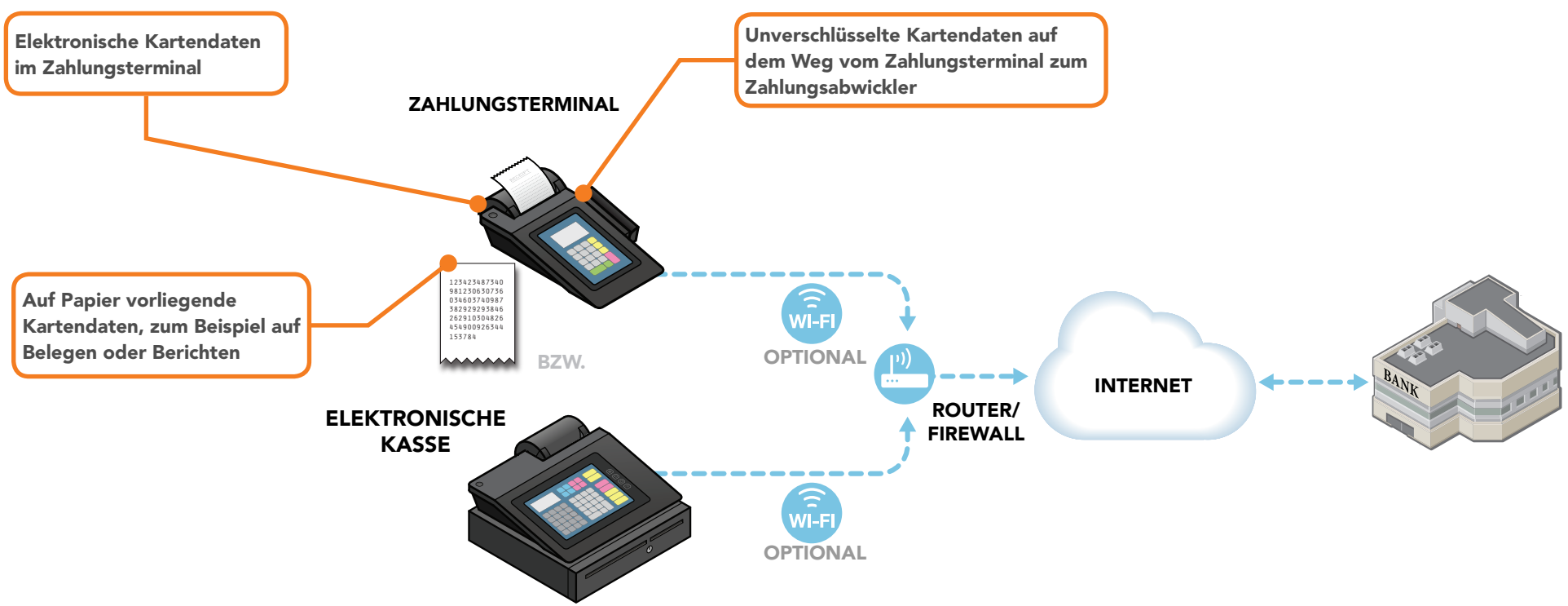
Die Risiken für den Kartendatendiebstahl werden durch ein ! gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse mit Internetverbindung. Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

An welchem Punkt sind Kartendaten gefährdet?

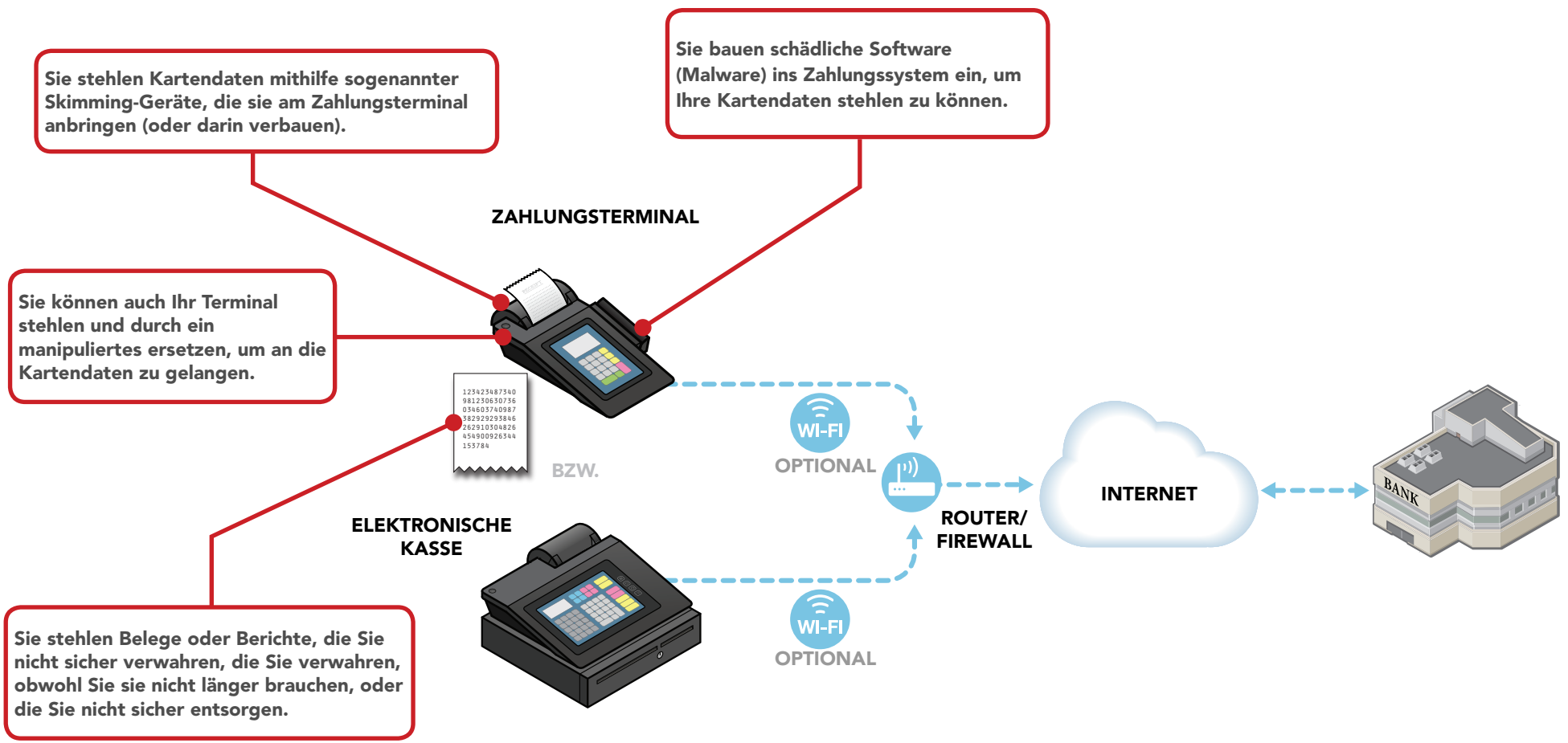


Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse mit Internetverbindung. Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

Wie kommen Kriminelle an Ihre Kartendaten?



TYP 5

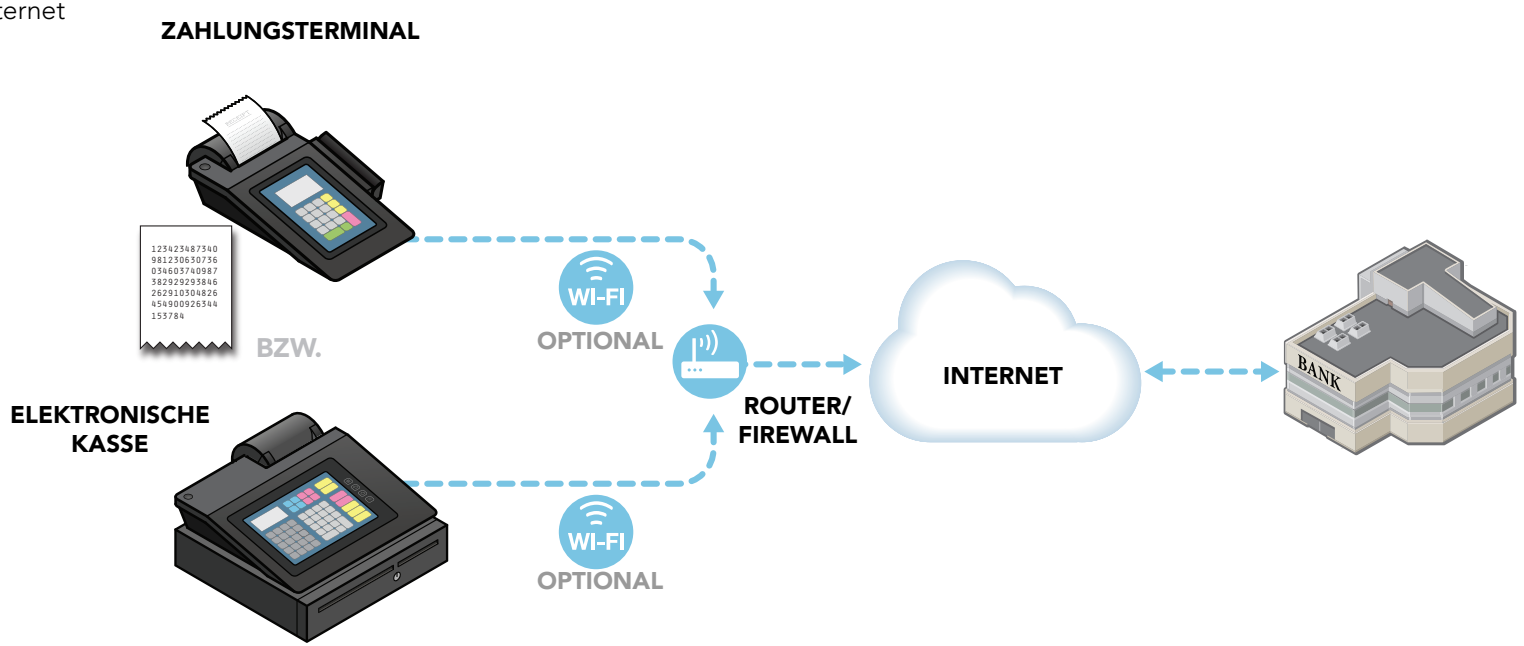
Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse mit Internetverbindung. Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Schützen Sie die Daten und verwahren Sie nur das, was Sie brauchen
- Untersuchen Sie Ihre Zahlungsterminals auf Schäden oder Auffälligkeiten
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Sichern Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter
- Beschränken Sie den Remote-Zugriff für Anbieter – geben Sie Hackern keine Chance
- Lassen Sie regelmäßig Scans auf Sicherheitsrisiken durchführen
- Verwenden Sie sichere Zahlungsterminals
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

TYP 6

Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse greifen auf dieselben kartenunabhängigen Daten zu (teilintegriert). Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet.

RISIKOPROFIL

Chip: GERING

Magnetstreifen: MITTEL

JA
Das IST mein System.
Weitere Details ansehen.

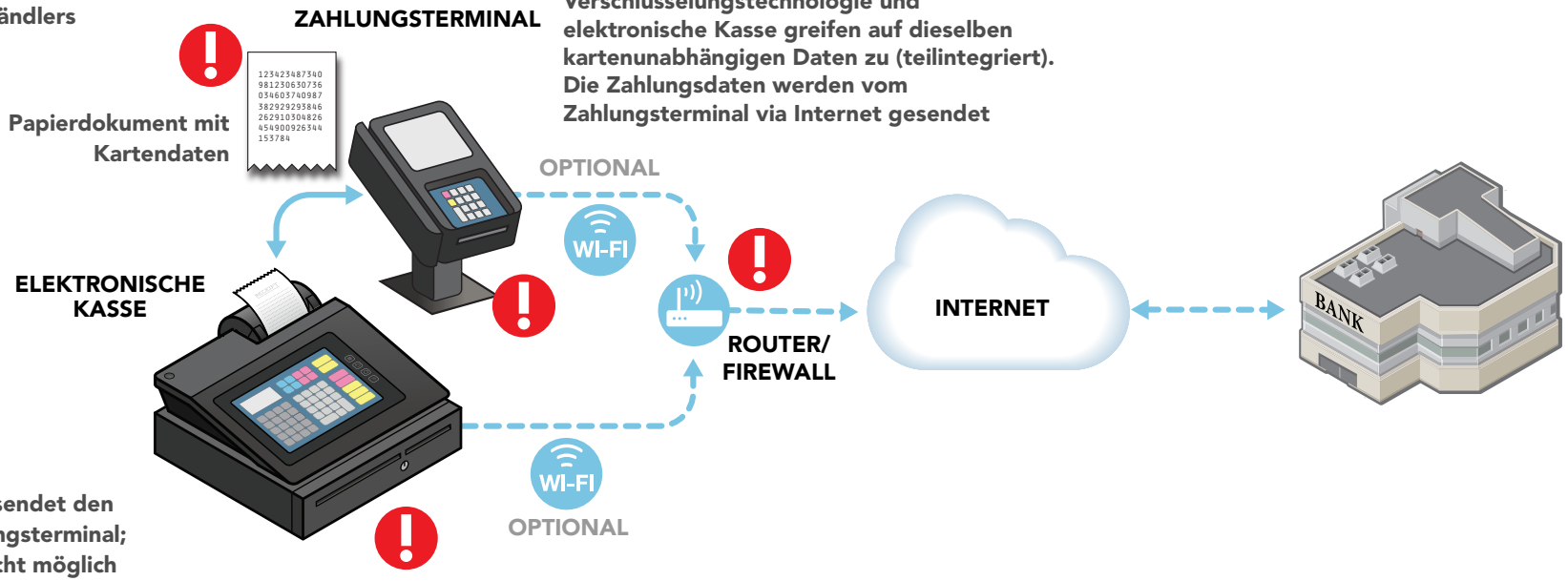
NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

Es werden keine Kartendaten zwischen der elektronischen Kasse und dem Zahlungsterminal ausgetauscht

Keine anderen Geräte, die mit den Zahlungssystemen des Händlers verbunden sind

Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse greifen auf dieselben kartenunabhängigen Daten zu (teilintegriert). Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet



Die elektronische Kasse sendet den Gesamtbetrag ans Zahlungsterminal; Kartenzahlung ist hier nicht möglich

Die Risiken für den Kartendatendiebstahl werden durch ein ! gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse greifen auf dieselben kartenunabhängigen Daten zu (teilintegriert). Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet.

RISIKOPROFIL

Chip: GERING

Magnetstreifen: MITTEL

An welchem Punkt sind Kartendaten gefährdet?

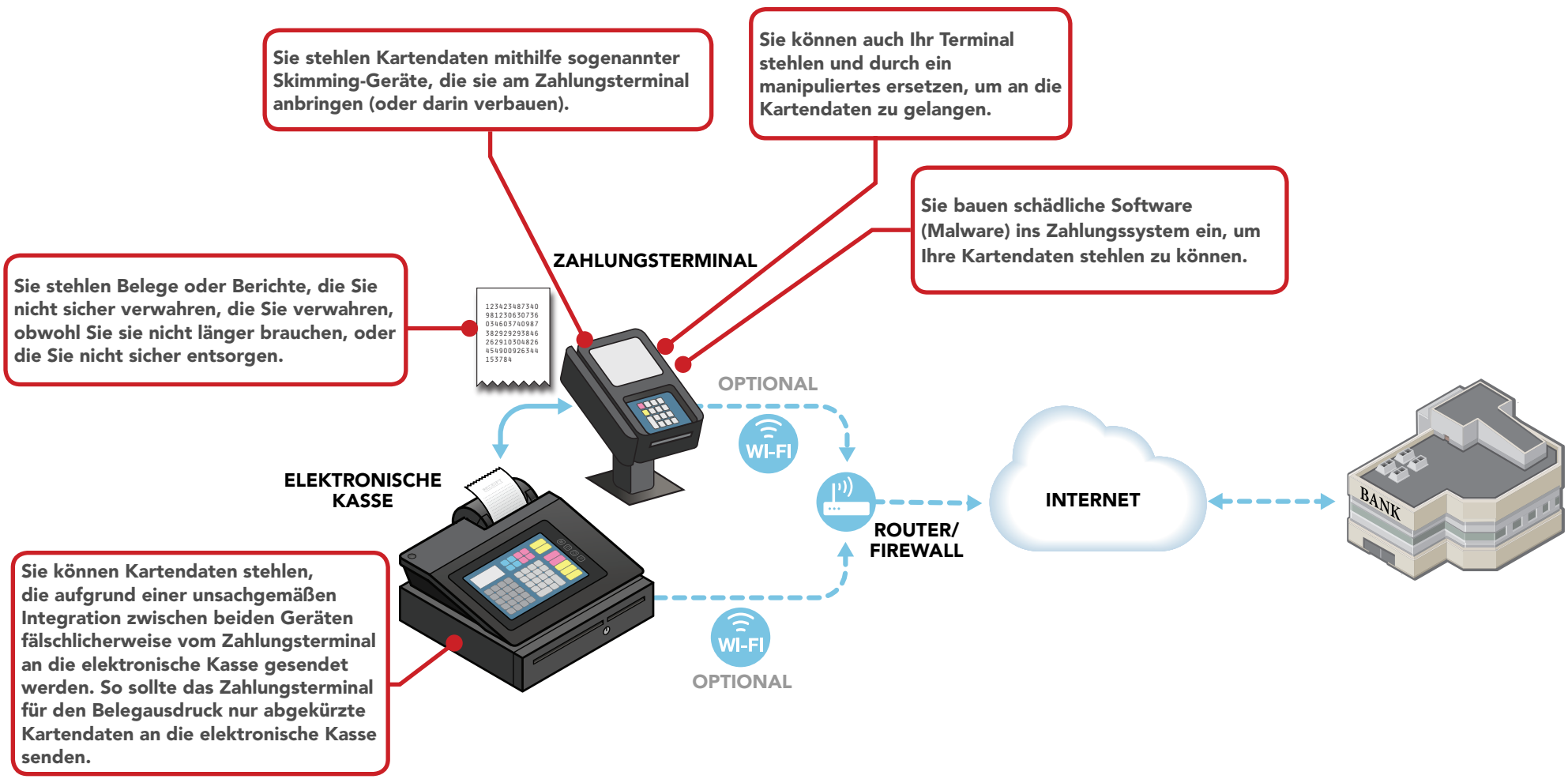
Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse greifen auf dieselben kartenunabhängigen Daten zu (teilintegriert). Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet.

RISIKOPROFIL

Chip: GERING

Magnetstreifen: MITTEL

Wie kommen Kriminelle an Ihre Kartendaten?



PCI Security Standards Council

Zahlungsterminal mit Verschlüsselungstechnologie und elektronische Kasse greifen auf dieselben kartenunabhängigen Daten zu (teilintegriert). Die Zahlungsdaten werden vom Zahlungsterminal via Internet gesendet.

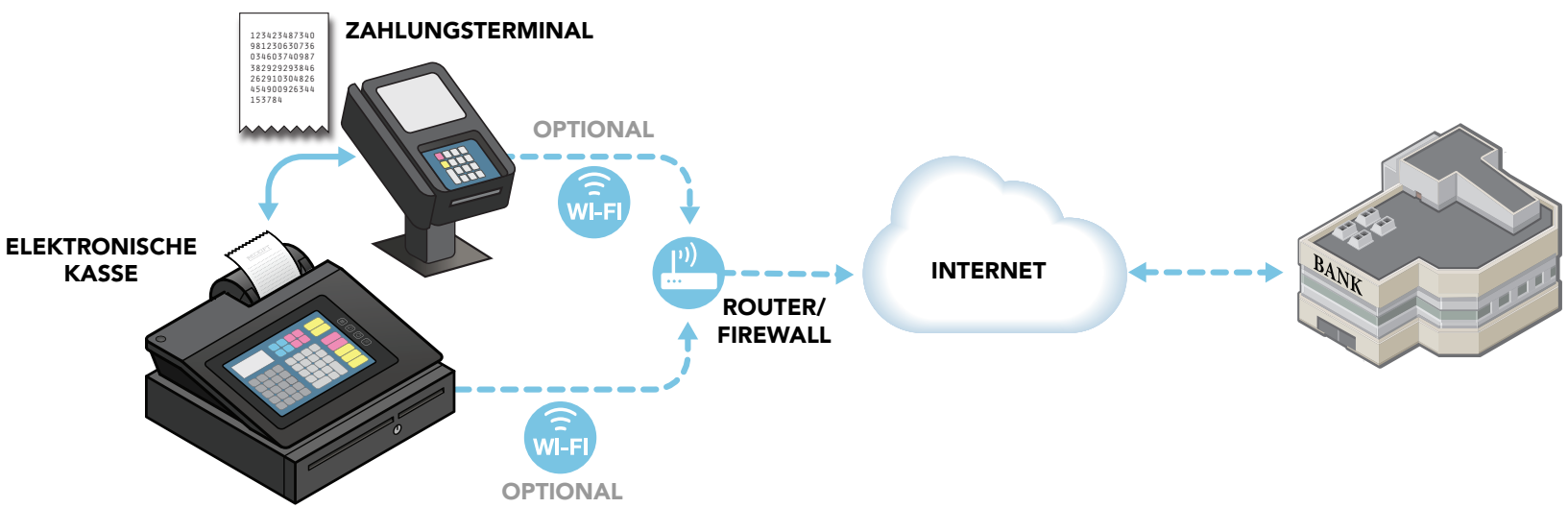
RISIKOPROFIL

Chip: GERING

Magnetstreifen: MITTEL

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Schützen Sie die Daten und verwahren Sie nur das, was Sie brauchen
- Untersuchen Sie Ihre Zahlungsterminals auf Schäden oder Auffälligkeiten
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Sichern Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter
- Beschränken Sie den Remote-Zugriff für Anbieter – geben Sie Hackern keine Chance
- Lassen Sie regelmäßig Scans auf Sicherheitsrisiken durchführen
- Verwenden Sie sichere Zahlungsterminals
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

TYP 7

Integriertes Zahlungsterminal und Middleware greifen auf dieselben Kartendaten zu. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

Chip

Magnetstreifen

HOCH

JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

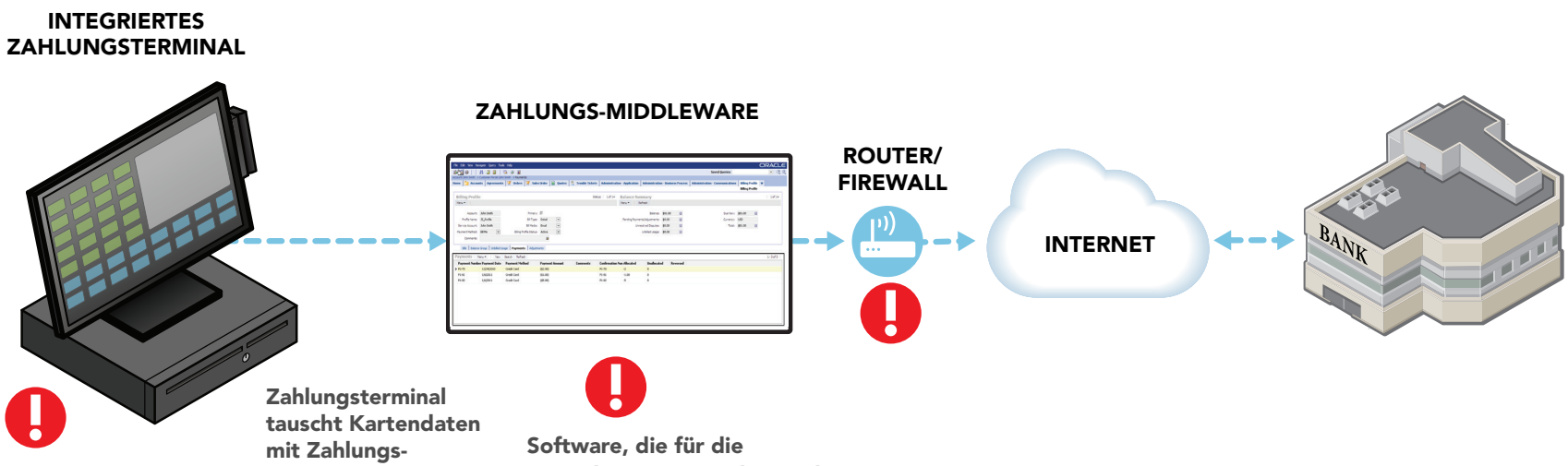
ZURÜCK
zum vorherigen Schaubild.

Kombination aus elektronischer Kasse und Zahlungsterminal

Karte wird von einem Mitarbeiter durchgezogen; Schaubild für Chipkarten nicht zutreffend

Kein zusätzliches PIN Entry Device

Keine anderen Geräte, die mit dem Zahlungssystem des Händlers verbunden sind



Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

PCI Security Standards Council

Integriertes Zahlungsterminal und Middleware greifen auf dieselben Kartendaten zu. Zahlungsdaten werden via Internet gesendet.

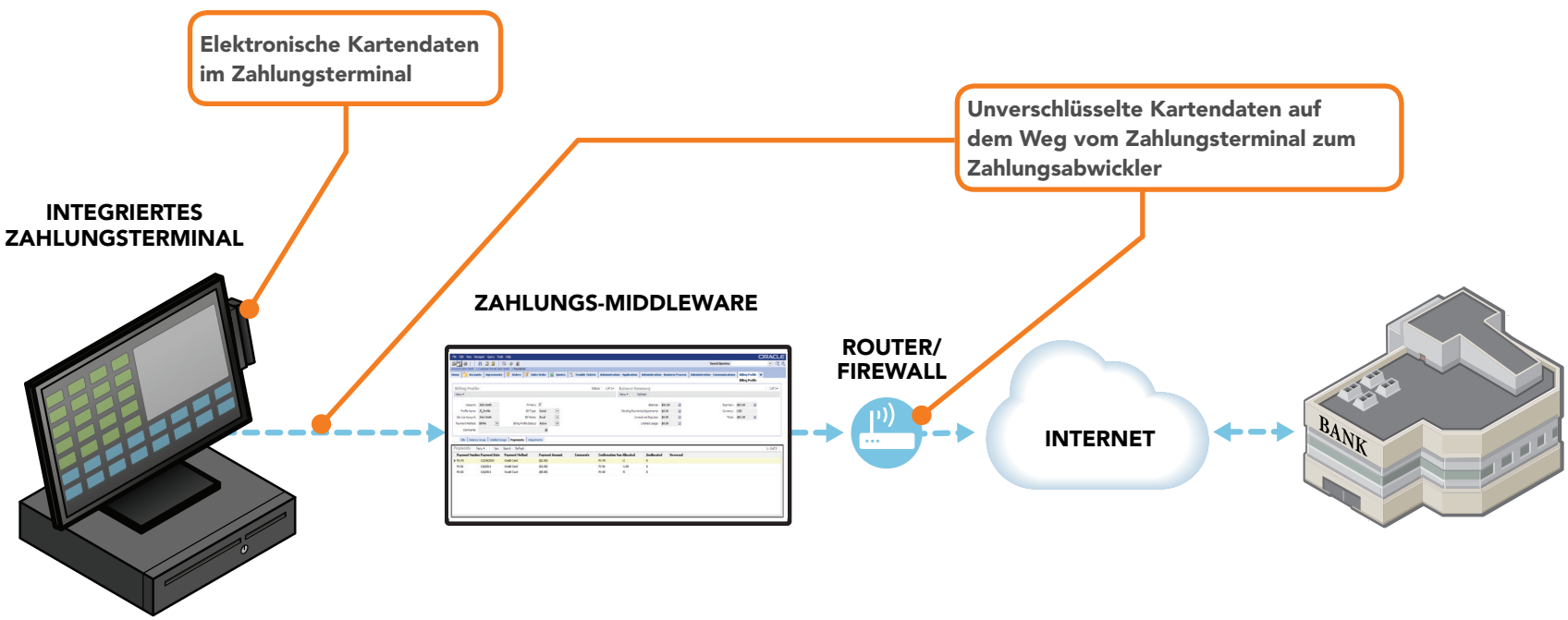
RISIKOPROFIL

Chip

Magnetstreifen

HOCH

An welchem Punkt sind Kartendaten gefährdet?



Integriertes Zahlungsterminal und Middleware greifen auf dieselben Kartendaten zu. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

Chip

Magnetstreifen

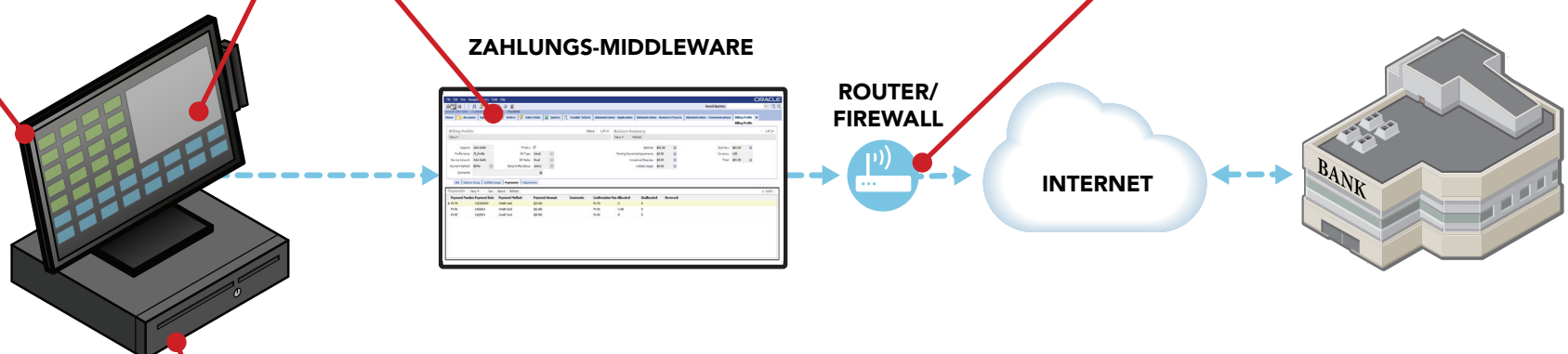
HOCH

Wie kommen Kriminelle an Ihre Kartendaten?

Sie stehlen Kartendaten mithilfe sogenannter Skimming-Geräte, die sie am Zahlungsterminal anbringen (oder darin verbauen).

Sie bauen schädliche Software (Malware) ins Zahlungssystem ein, um Ihre Kartendaten stehlen zu können.

Sie können auch über dieselbe Remote-Zugriff-Software, die Ihr Anbieter für den Support Ihres Zahlungssystems nutzt, auf die Kartendaten Ihrer Kunden zugreifen und diese stehlen.



Sie können auch Ihr Terminal stehlen und durch ein manipuliertes ersetzen, um an die Kartendaten zu gelangen.

TYP 7

Integriertes Zahlungsterminal und Middleware greifen auf dieselben Kartendaten zu. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

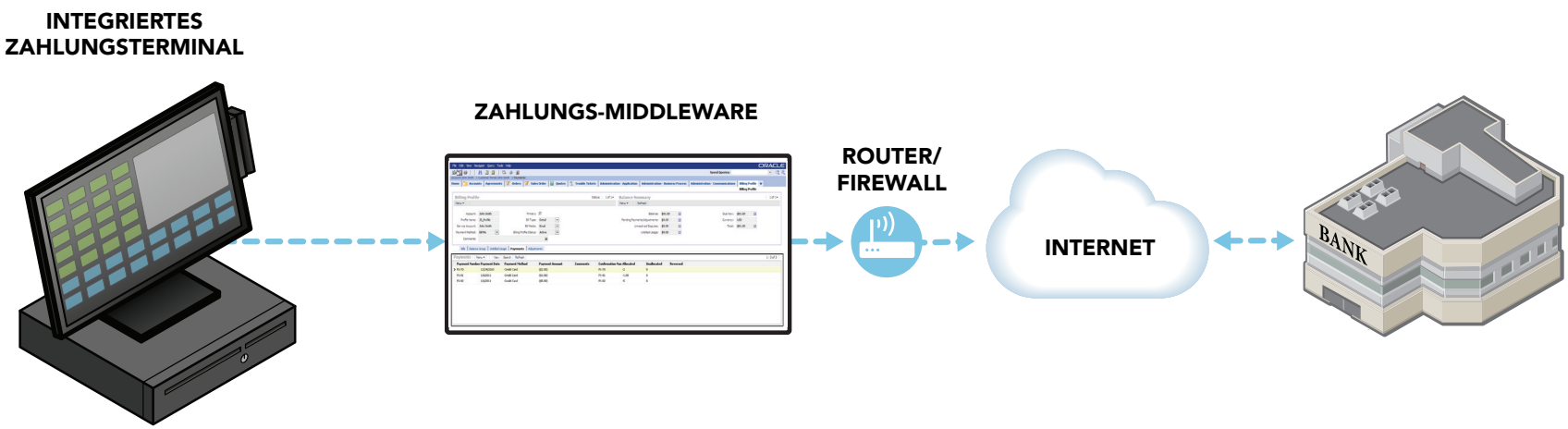
Chip

Magnetstreifen

HOCH

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Schützen Sie die Daten und verwahren Sie nur das, was Sie brauchen
- Untersuchen Sie Ihre Zahlungsterminals auf Schäden oder Auffälligkeiten
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Sichern Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter
- Beschränken Sie den Remote-Zugriff für Anbieter – geben Sie Hackern keine Chance
- Verwenden Sie Antivirus-Software
- Lassen Sie regelmäßig Scans auf Sicherheitsrisiken durchführen
- Verwenden Sie sichere Zahlungsterminals
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet
- Machen Sie Ihre Kartendaten nutzlos für Kriminelle



Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

TYP 8

Kabelloses Zahlungsterminal mit Verschlüsselungstechnologie („Pay-at-Table“) mit integriertem Zahlungsterminal und Middleware. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

Chip: GERING

Magnetstreifen: MITTEL

JA
Das IST mein System.
Weitere Details ansehen.

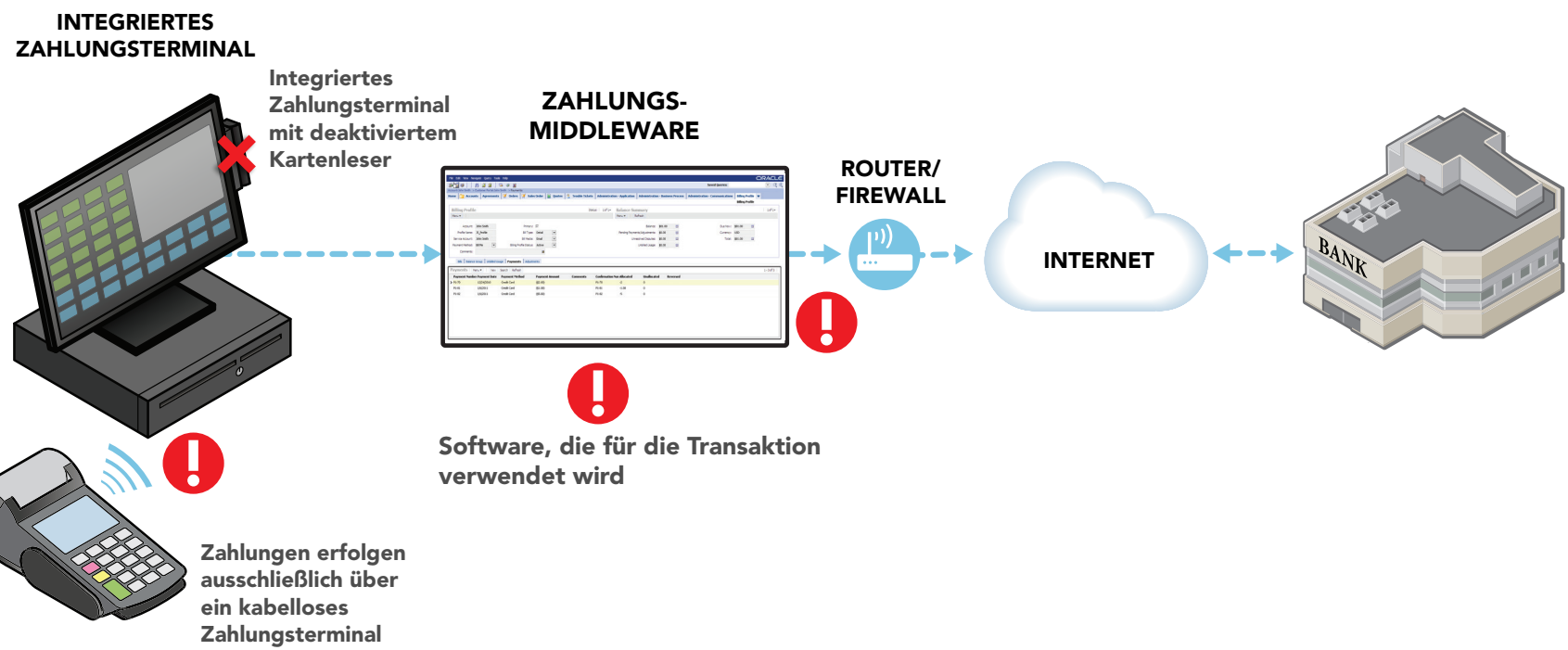
NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

Verschlüsselte Kartendaten, die mit dem Zahlungsterminal und der Middleware ausgetauscht werden

Keine anderen Geräte, die mit den Zahlungssystemen des Händlers verbunden sind

Kabelloses Zahlungsterminal verschlüsselt Kartendaten (z. B. mithilfe von SRED, Secure Reading and Exchange of Data von PCI)



Die Risiken für den Kartendatendiebstahl werden durch ein ! gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

PCI Security Standards Council

TYP 8

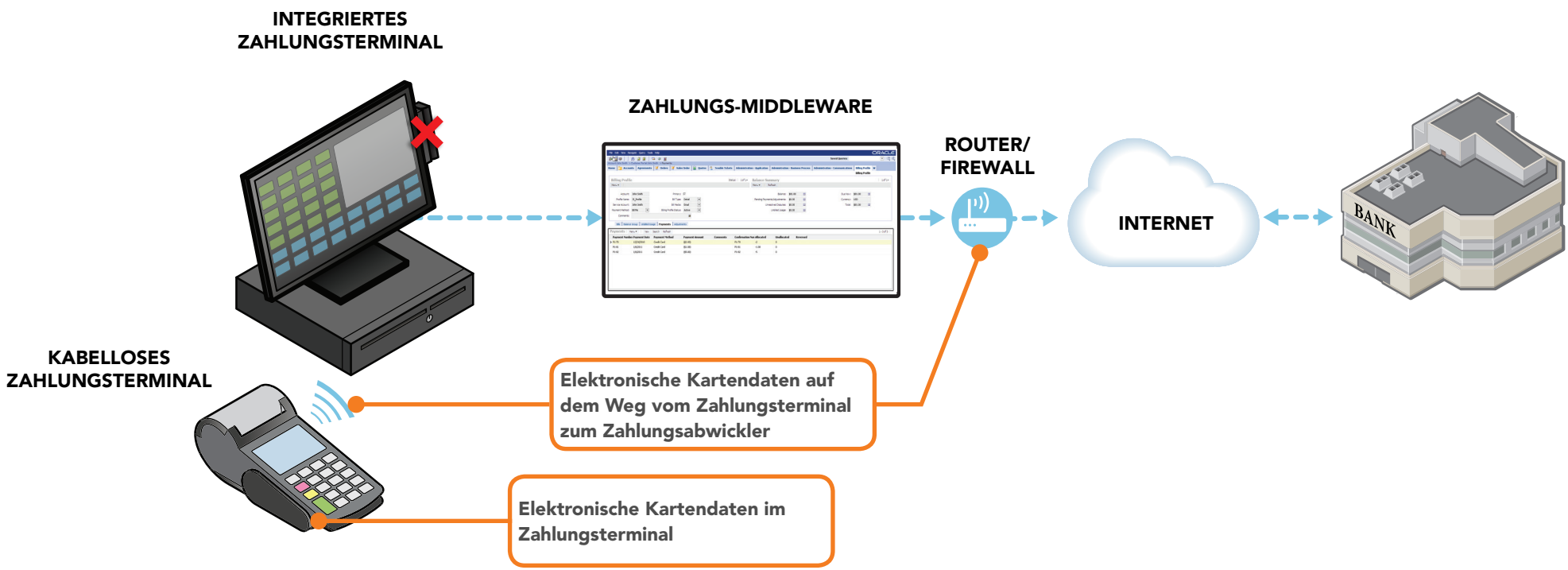
Kabelloses Zahlungsterminal mit Verschlüsselungstechnologie („Pay-at-Table“) mit integriertem Zahlungsterminal und Middleware. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

Chip: GERING

Magnetstreifen: MITTEL

An welchem Punkt sind Kartendaten gefährdet?



PCI Security Standards Council

TYP 8

Kabelloses Zahlungsterminal mit Verschlüsselungstechnologie („Pay-at-Table“) mit integriertem Zahlungsterminal und Middleware. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

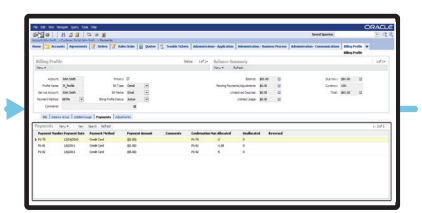
Chip: GERING

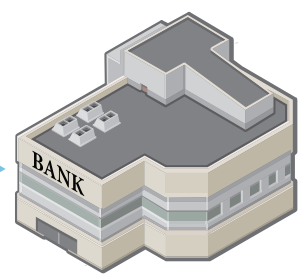
Magnetstreifen: MITTEL

Wie kommen Kriminelle an Ihre Kartendaten?

Sie bauen schädliche Software (Malware) ins Zahlungssystem ein, um Ihre Kartendaten stehlen zu können.

Sie stehlen Kartendaten mithilfe sogenannter Skimming-Geräte, die sie am Zahlungsterminal anbringen (oder darin verbauen).





Sie können auch Ihr Terminal stehlen und durch ein manipuliertes ersetzen, um an die Kartendaten zu gelangen.

Sie können auch über dieselbe Remote-Zugriff-Software, die Ihr Anbieter für den Support Ihres Zahlungssystems nutzt, auf die Kartendaten zugreifen und diese stehlen.

PCI Security Standards Council

TYP 8

Kabelloses Zahlungsterminal mit Verschlüsselungstechnologie („Pay-at-Table“) mit integriertem Zahlungsterminal und Middleware. Zahlungsdaten werden via Internet gesendet.

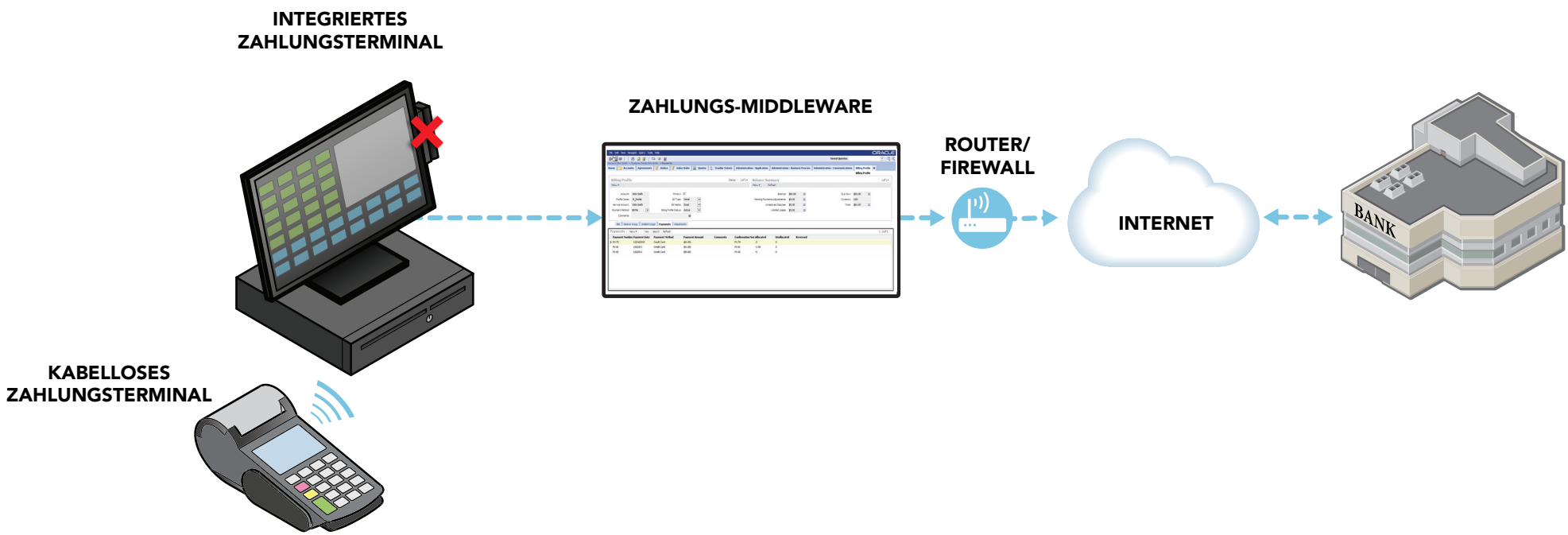
RISIKOPROFIL

Chip: GERING

Magnetstreifen: MITTEL

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Schützen Sie die Daten und verwahren Sie nur das, was Sie brauchen
- Untersuchen Sie Ihre Zahlungsterminals auf Schäden oder Auffälligkeiten
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Sichern Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter
- Beschränken Sie den Remote-Zugriff für Anbieter – geben Sie Hackern keine Chance
- Verwenden Sie Antivirus-Software
- Lassen Sie regelmäßig Scans auf Sicherheitsrisiken durchführen
- Verwenden Sie sichere Zahlungsterminals
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet
- Machen Sie Ihre Kartendaten nutzlos für Kriminelle



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

TYP 9

An eine elektronische Kasse angeschlossenes Zahlungsterminal, das mit weiteren Geräten verbunden ist. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

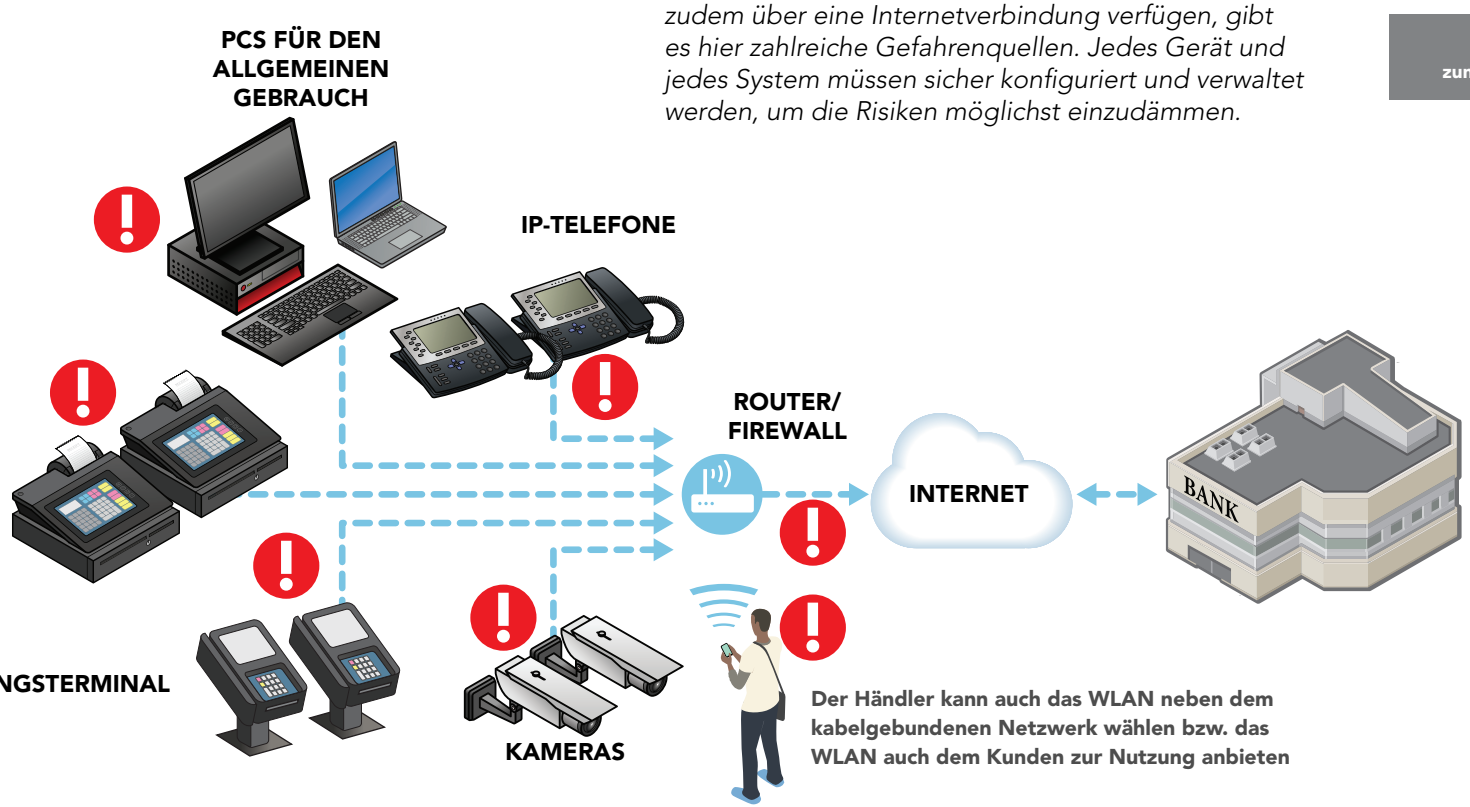
HOCH

JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

Da hier weitere Geräte am selben Netzwerk angeschlossen sind wie das Zahlungsterminal und sie zudem über eine Internetverbindung verfügen, gibt es hier zahlreiche Gefahrenquellen. Jedes Gerät und jedes System müssen sicher konfiguriert und verwaltet werden, um die Risiken möglichst einzudämmen.



Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

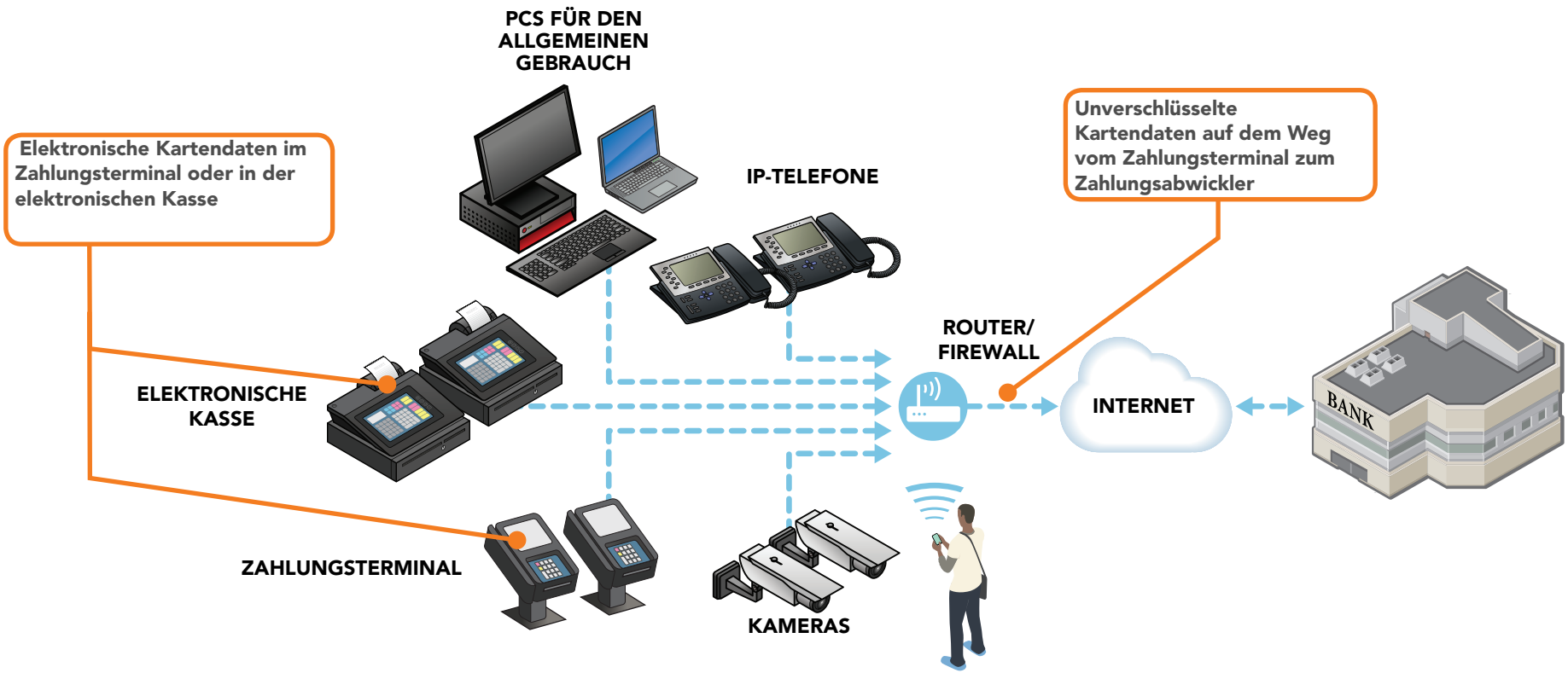
TYP 9

An eine elektronische Kasse angeschlossenes Zahlungsterminal, das mit weiteren Geräten verbunden ist. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

HOCH

An welchem Punkt sind Kartendaten gefährdet?

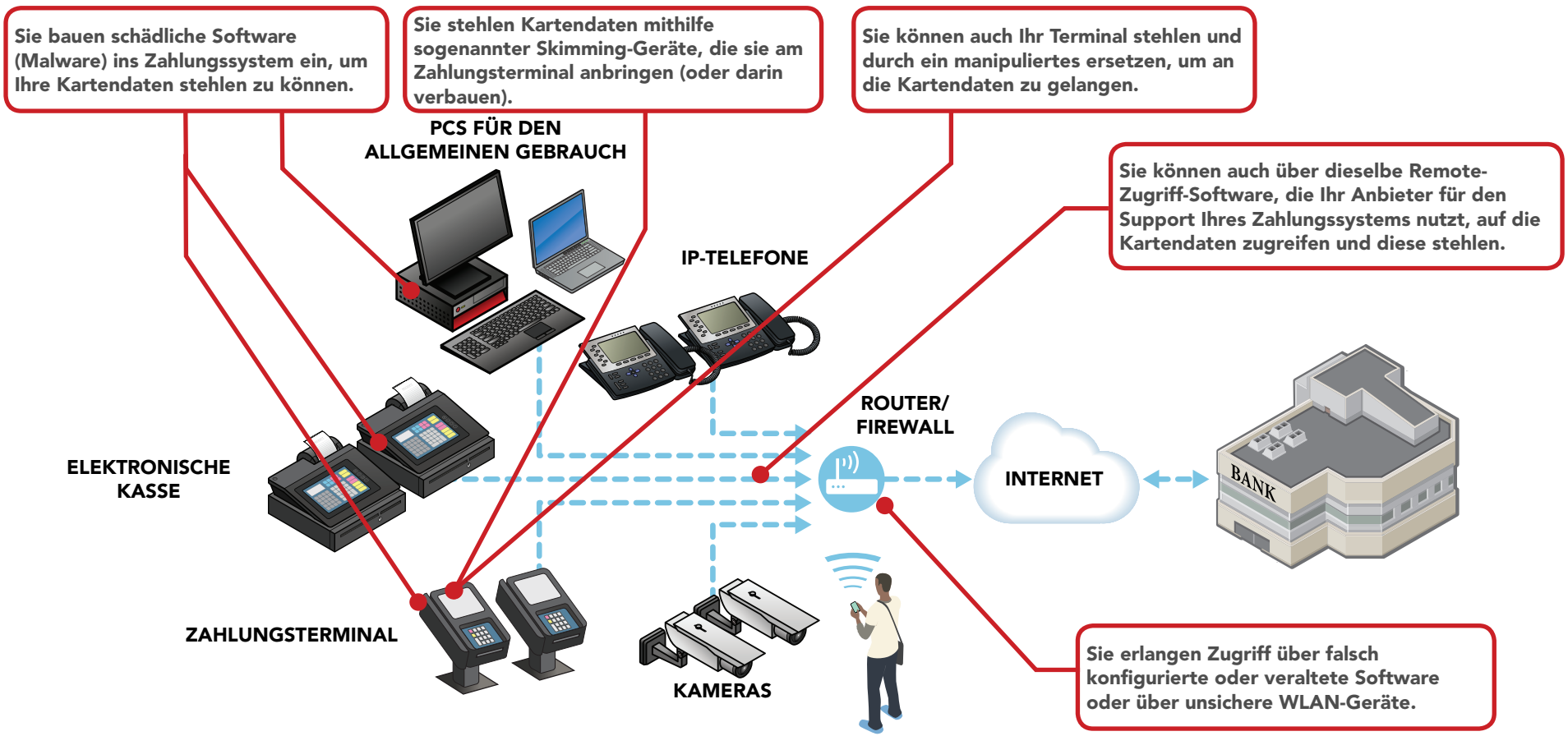


An eine elektronische Kasse angeschlossenes Zahlungsterminal, das mit weiteren Geräten verbunden ist. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

HOCH

Wie kommen Kriminelle an Ihre Kartendaten?



PCI Security Standards Council®

TYP 9

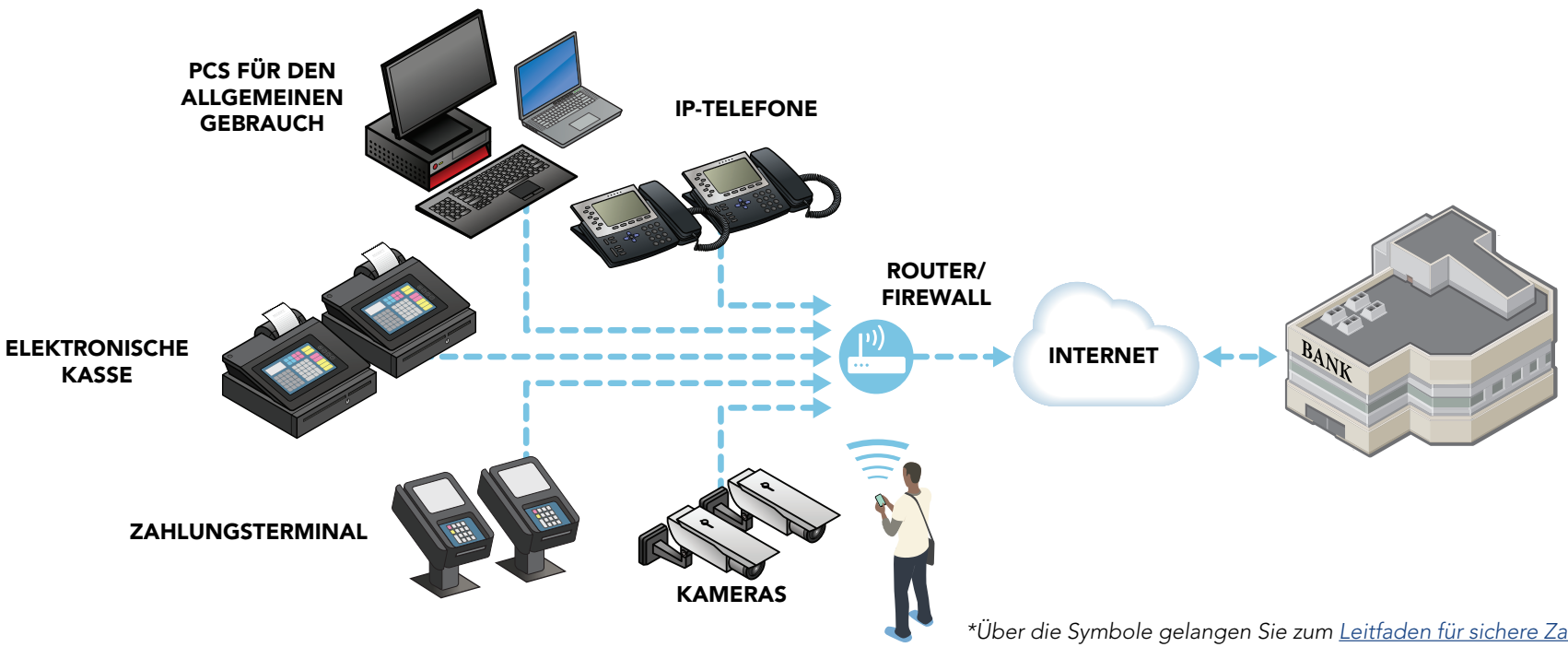
An eine elektronische Kasse angeschlossenes Zahlungsterminal, das mit weiteren Geräten verbunden ist. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

HOCH

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Sichern Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter
- Verwenden Sie sichere Zahlungsterminals
- Schützen Sie die Daten und verwahren Sie nur das, was Sie brauchen
- Beschränken Sie den Remote-Zugriff für Anbieter – geben Sie Hackern keine Chance
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet
- Untersuchen Sie Ihre Zahlungsterminals auf Schäden oder Auffälligkeiten
- Verwenden Sie Antivirus-Software
- Machen Sie Ihre Kartendaten nutzlos für Kriminelle
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Lassen Sie regelmäßig Scans auf Sicherheitsrisiken durchführen



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

Sichere Kartenzahlung für Kleinhändler: Gängige Zahlungssysteme

TYP 10

E-Commerce-Händler ohne eigene Zahlungsseite. Die Zahlungsdaten werden via Internet von einem Drittanbieter gesendet.

RISIKOPROFIL

GERING

JA
Das IST mein System.
Weitere Details ansehen.

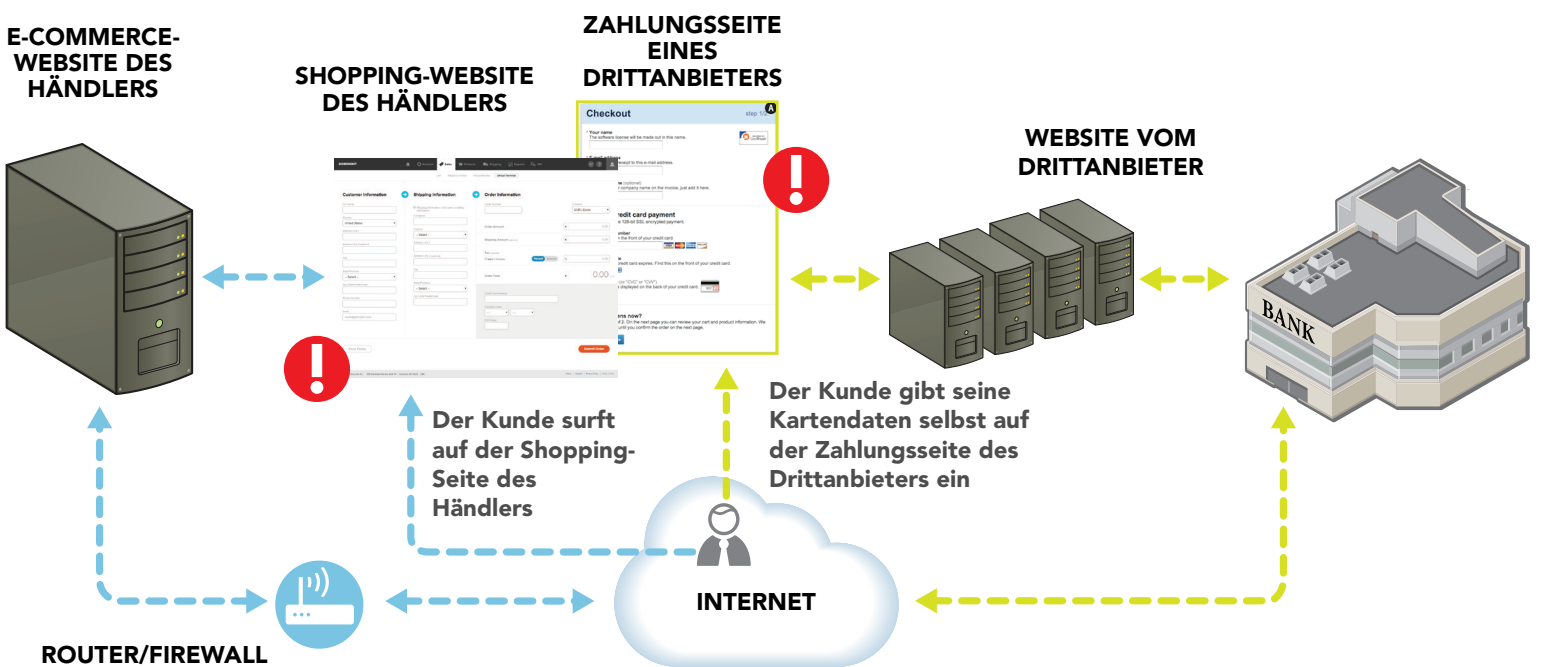
NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

Der Händler betreibt eine eigene Website, hat jedoch keinen Zugriff auf die Zahlungsseite

Der Händler bietet nur Produktinformationen (Shopping-Seiten etc.), die auf seiner Website verfügbar sind, hat jedoch keinen Zugriff auf Kartendaten

Die gesamte Zahlungsseite des Händlers wird an einen PCI-DSS-konformen Drittanbieter outgesourct



Die Shopping-Seiten können vom Händler oder vom Hosting-Anbieter des Händlers bereitgestellt werden

Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

PCI Security Standards Council

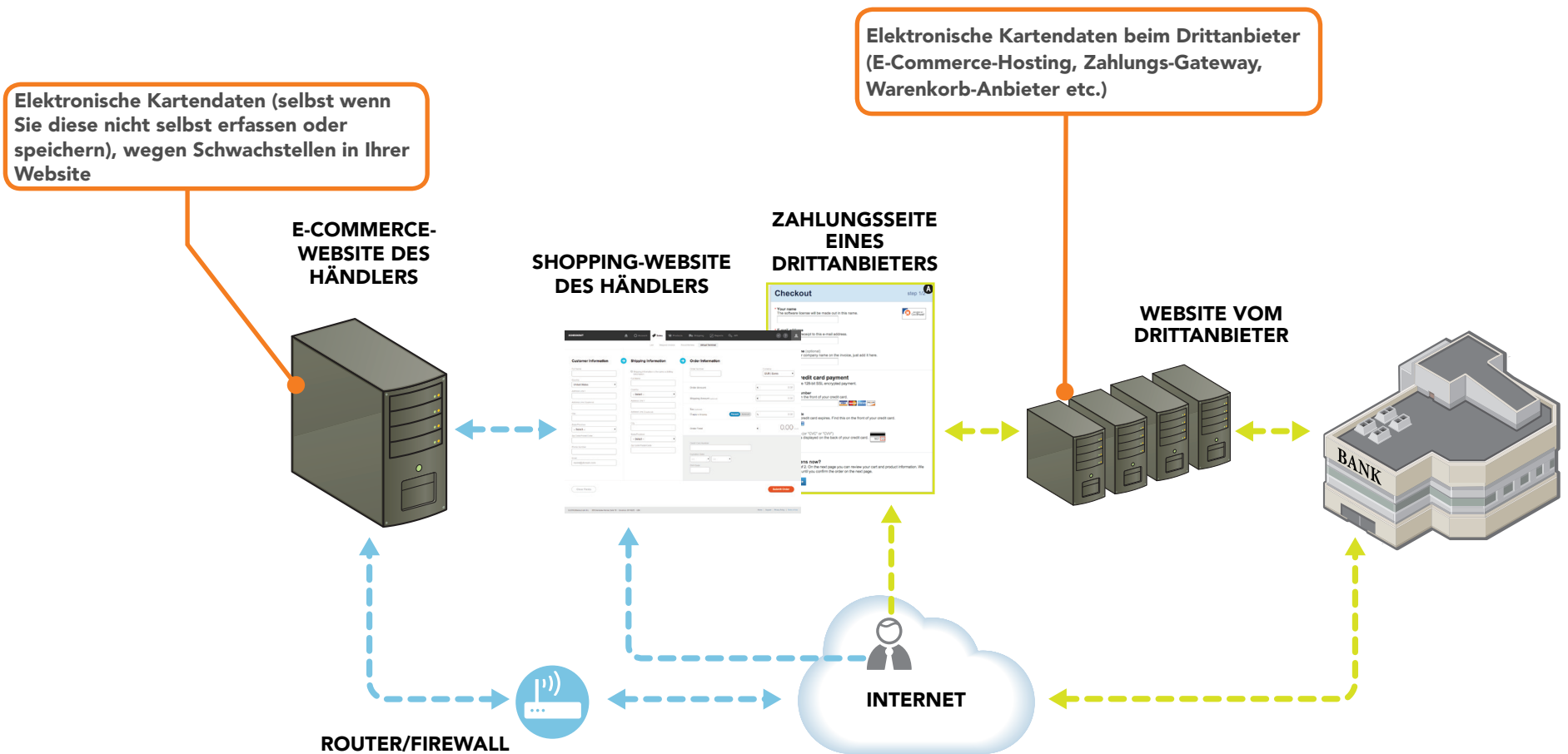
TYP 10

E-Commerce-Händler ohne eigene Zahlungsseite. Die Zahlungsdaten werden via Internet von einem Drittanbieter gesendet.

RISIKOPROFIL

GERING

An welchem Punkt sind Kartendaten gefährdet?



TYP 10

E-Commerce-Händler ohne eigene Zahlungsseite. Die Zahlungsdaten werden via Internet von einem Drittanbieter gesendet.

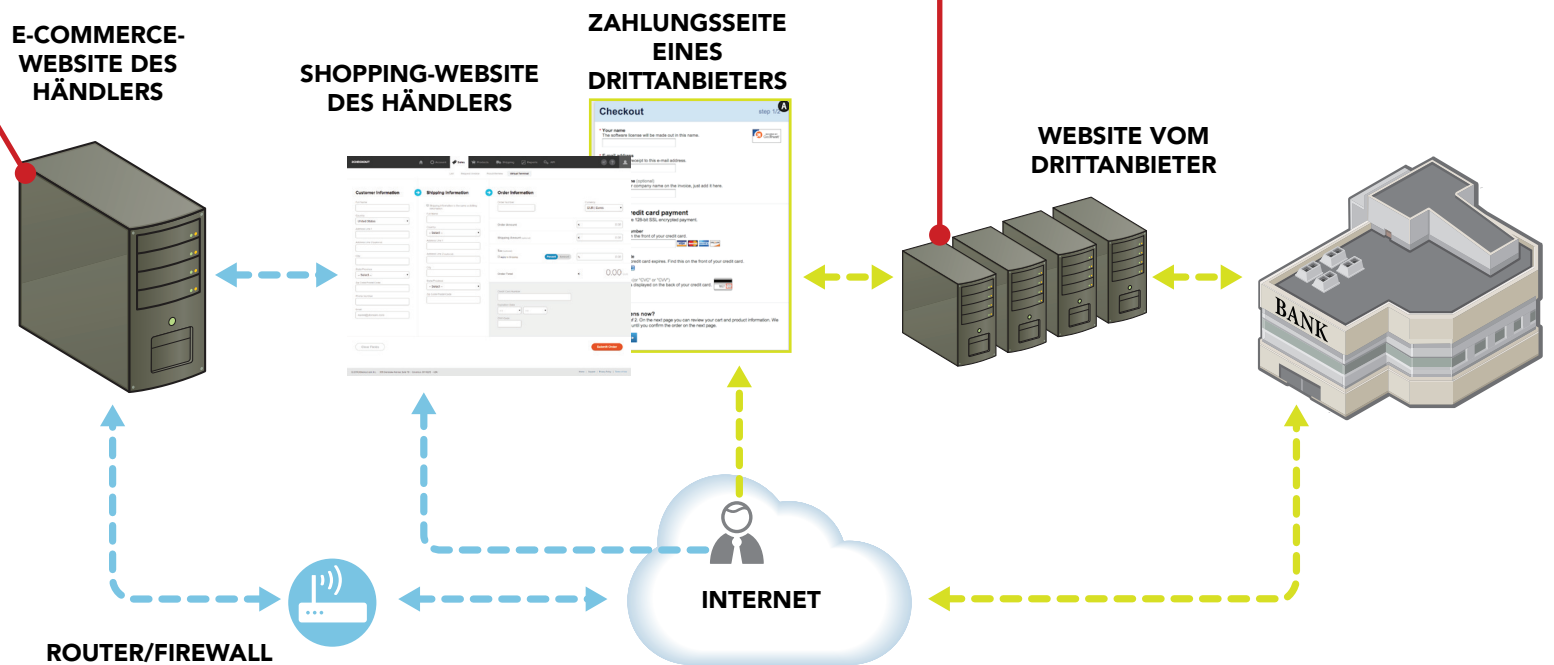
RISIKOPROFIL

GERING

Wie kommen Kriminelle an Ihre Kartendaten?

Sie nutzen Schwachstellen, um Ihre Website anzugreifen, und fangen Kartendaten ab, wenn die Kunden diese an Ihren ausgelagerten E-Commerce-Anbieter senden.

Sie können Kartendaten von ausgelagerten Anbietern mithilfe zahlreicher Methoden stehlen (Schadsoftware installieren, falsch konfigurierte Software nutzen etc.).



TYP 10

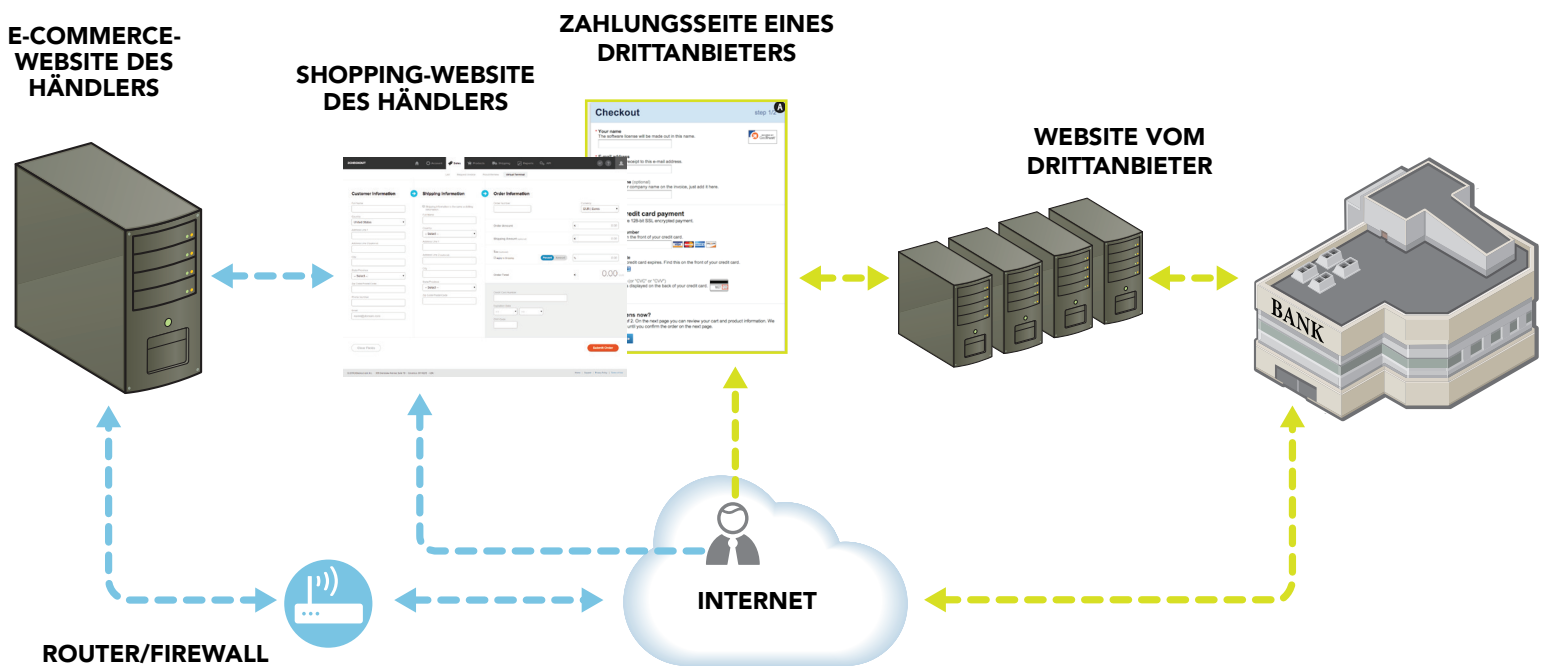
E-Commerce-Händler ohne eigene Zahlungsseite. Die Zahlungsdaten werden via Internet von einem Drittanbieter gesendet.

RISIKOPROFIL

GERING

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Installieren Sie Patches Ihrer Anbieter
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

TYP 11

E-Commerce-Händler bietet eigene Zahlungsseite und eigene Website an. Zahlungsdaten werden vom Händler via Internet gesendet.

RISIKOPROFIL

HOCH

JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

Der Händler betreibt die Website, einschließlich der Zahlungsseite (oder bestimmter Teile der Zahlungsseite)

Die Shopping-Seiten und Zahlungsseiten können vom Händler oder vom Hosting-Anbieter des Händlers bereitgestellt werden

Beim Betreiben einer eigenen E-Commerce-Website gibt es sehr viele Dinge zu beachten. Jedes System muss ordnungsgemäß konfiguriert und verwaltet werden, um die Risiken möglichst einzudämmen.

Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

E-Commerce-Händler bietet eigene Zahlungsseite und eigene Website an. Zahlungsdaten werden vom Händler via Internet gesendet.

RISIKOPROFIL

HOCH

An welchem Punkt sind Kartendaten gefährdet?

TYP 11

E-Commerce-Händler bietet eigene Zahlungsseite und eigene Website an. Zahlungsdaten werden vom Händler via Internet gesendet.

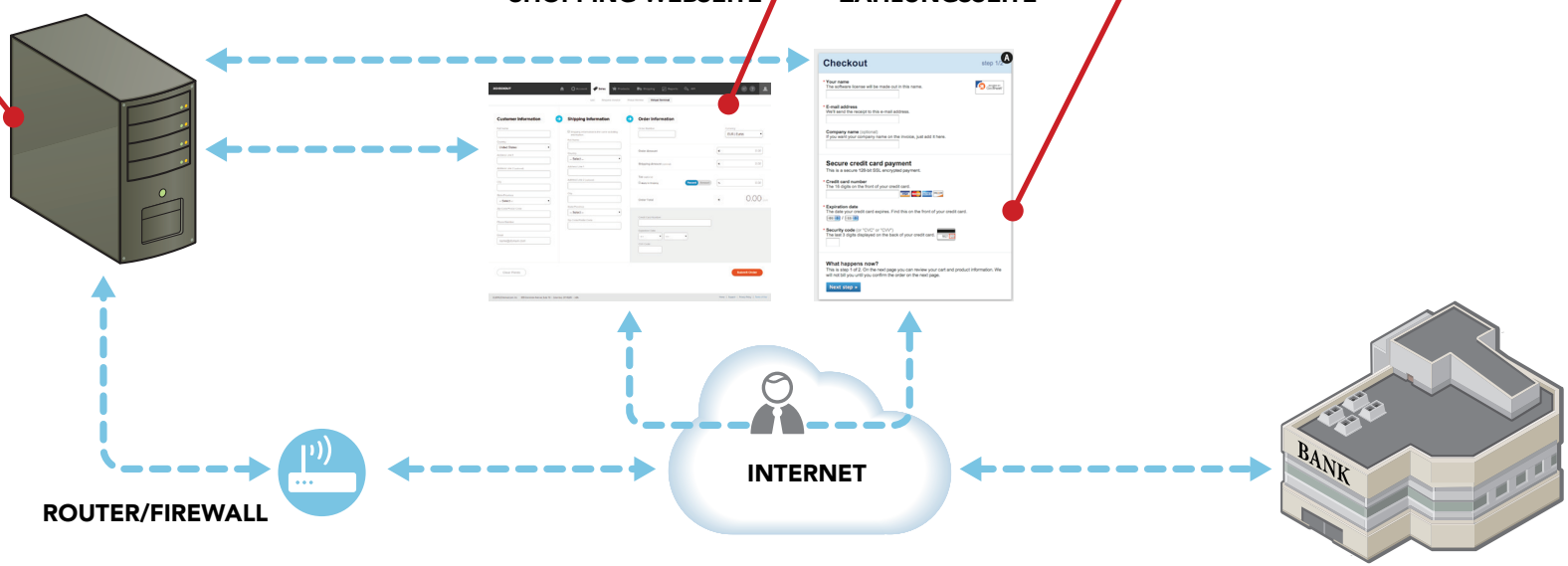
RISIKOPROFIL

HOCH

Wie kommen Kriminelle an Ihre Kartendaten?

Sie nutzen Schwachstellen, um Ihre Website anzugreifen. Die SQL-Injektion ist eine der häufigen Methoden, mit der Daten von Webseiten gestohlen werden.

Sie können Kartendaten von ausgelagerten Anbietern mithilfe zahlreicher Methoden stehlen (Schadsoftware installieren, falsch konfigurierte Software nutzen etc.).



TYP 11

E-Commerce-Händler bietet eigene Zahlungsseite und eigene Website an. Zahlungsdaten werden vom Händler via Internet gesendet.

RISIKOPROFIL

HOCH

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Sichern Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter
- Verwenden Sie sichere Zahlungsterminals
- Schützen Sie die Daten und verwahren Sie nur das, was Sie brauchen
- Beschränken Sie den Remote-Zugriff für Anbieter – geben Sie Hackern keine Chance
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet
- Installieren Sie Patches Ihres Zahlungsterminal-Anbieters
- Verwenden Sie Antivirus-Software
- Machen Sie Ihre Kartendaten nutzlos für Kriminelle
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Lassen Sie regelmäßig Scans auf Sicherheitsrisiken durchführen

*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

TYP 12

Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

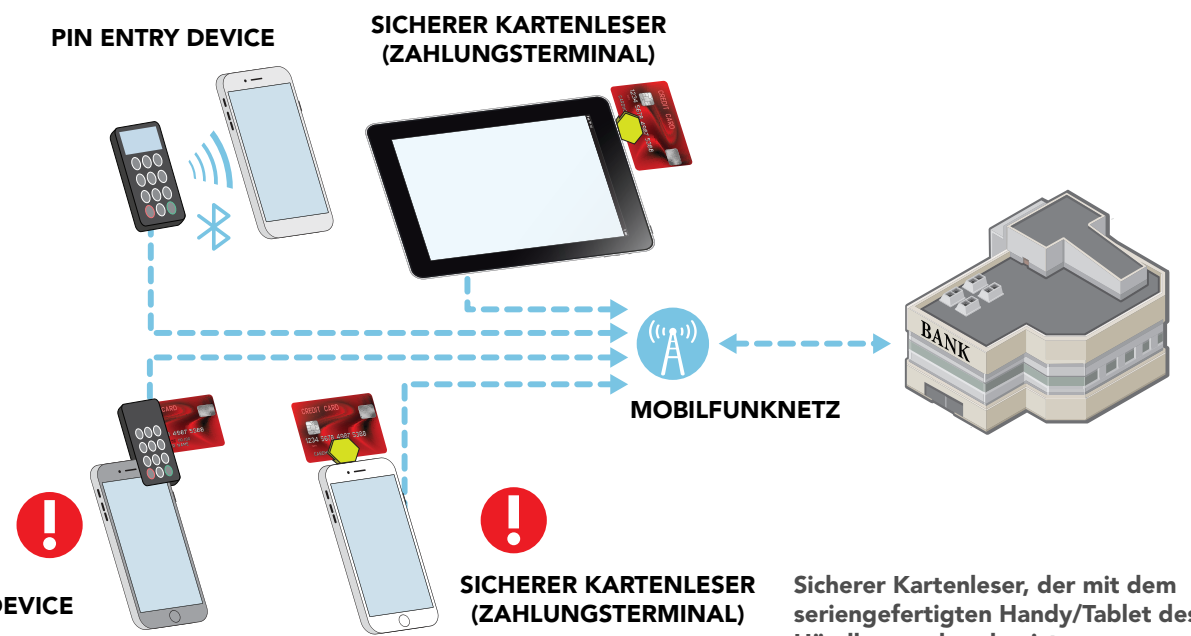
Zum Lesen von Magnetstreifenkarten, zur Eingabe der PIN und zum Lesen von Chipkartendaten werden unterschiedliche Geräte verwendet

Das mobile Zahlungsterminal ist mit dem Internet übers Mobilfunknetz verbunden und greift nicht auf WLAN zu

Für Händler an abweichenden Standorten (Flohmarkt, Messe etc.).

Kartendaten und PIN werden vom sicheren Kartenlesegerät und dem PIN Entry Device verschlüsselt, bevor sie ans Handy/Tablet geschickt werden; das Handy/Tablet hat nur Zugriff auf verschlüsselte Kartendaten

Der Händler kann die Kartendaten nicht manuell eingeben



Sicherer Kartenleser, der mit dem seriengefertigten Handy/Tablet des Händlers verbunden ist

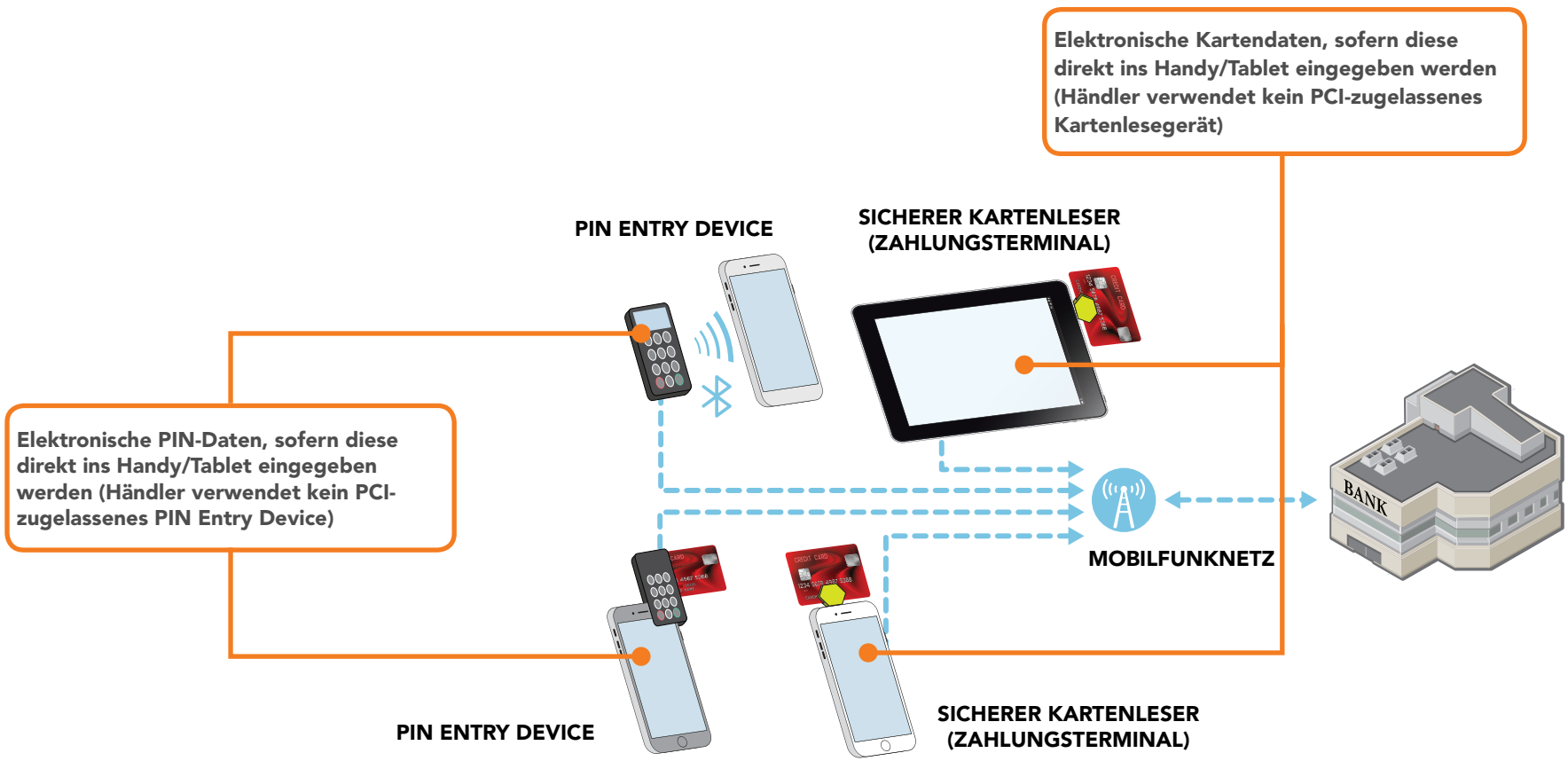
Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

An welchem Punkt sind Kartendaten gefährdet?



Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz gesendet.

RISIKOPROFIL

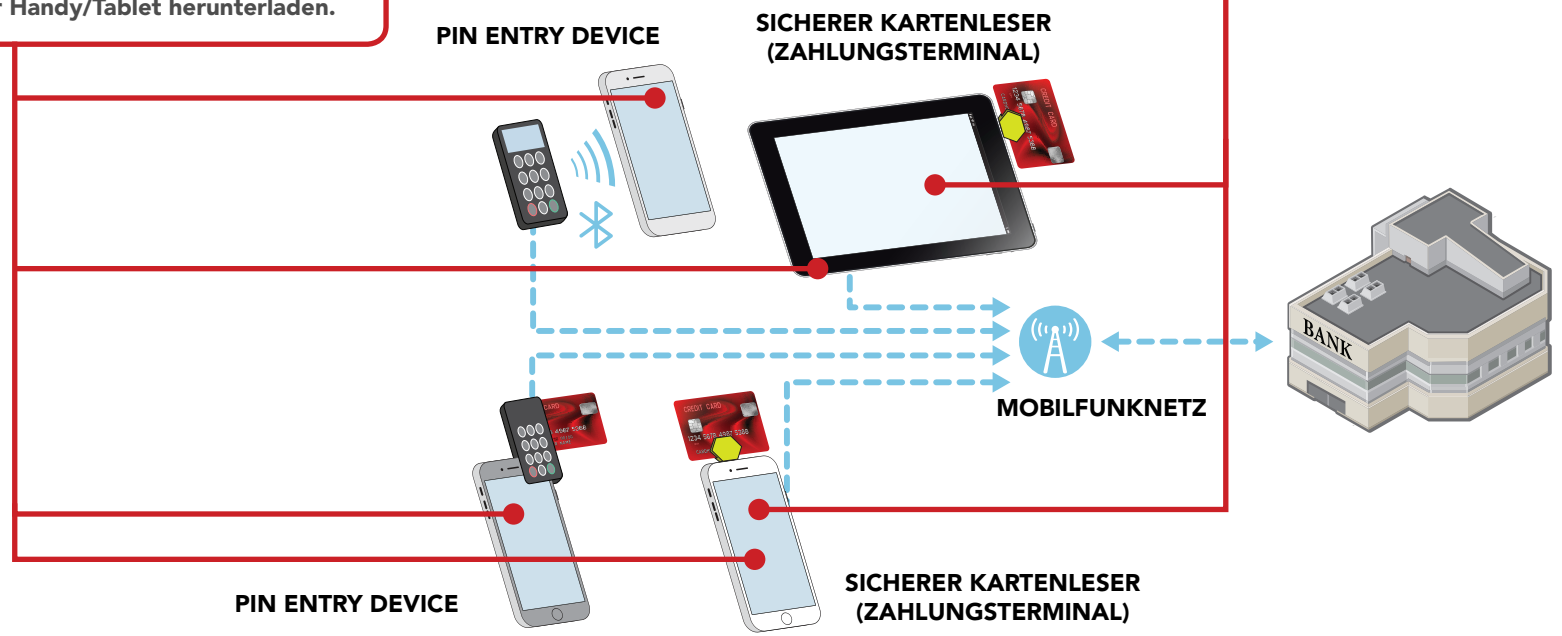
Chip	Magnetstreifen
GERING	GERING

Wie kommen Kriminelle an Ihre Kartendaten?

Sie können sich ins Handy/Tablet hacken und Schadsoftware installieren, mit der sie Karten- oder PIN-Daten vom Handy oder Tablet stehlen können.

Sie verwenden Apps im App Store, mit denen sie Karten- oder PIN-Daten stehlen können, wenn Sie diese App auf Ihr Handy/Tablet herunterladen.

Kriminelle können einen sicheren Kartenleser gegen einen austauschen, den sie entsprechend manipuliert haben.



PCI Security Standards Council

TYP 12

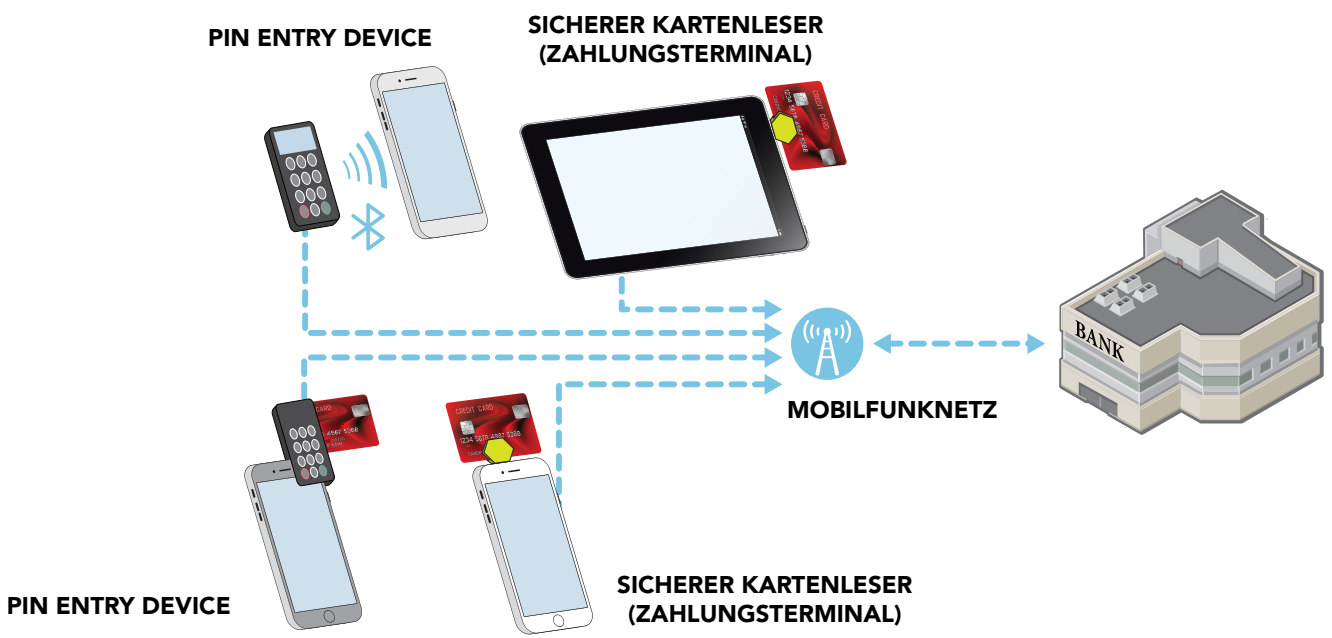
Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
GERING	GERING

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Untersuchen Sie Ihre sicheren Kartenleser und PIN Entry Devices auf Schäden oder Auffälligkeiten
- Installieren Sie Patches Ihrer Anbieter
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Verwenden Sie Antivirus-Software
- Verwenden Sie sichere Kartenlesegeräte und PIN Entry Devices
- Machen Sie Ihre Kartendaten nutzlos für Kriminelle



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

TYP 13

Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz oder WLAN gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
MITTEL	MITTEL

JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Nächstes Schaubild zeigen.

ZURÜCK
zum vorherigen Schaubild.

Ist über das Mobilfunknetz bzw. WLAN mit dem Internet verbunden

Für Händler an abweichenden Standorten (Flohmarkt, Messe etc.)

Kartendaten und PIN werden vom sicheren Kartenlesegerät und dem PIN Entry Device verschlüsselt, bevor sie ans Handy/Tablet geschickt werden; das Handy/Tablet hat nur Zugriff auf verschlüsselte Kartendaten

Der Händler kann die Kartendaten nicht manuell eingeben

Zum Lesen von Magnetstreifenkarten, zur Eingabe der PIN und zum Lesen von Chipkartendaten werden unterschiedliche Geräte verwendet

Sicherer Kartenleser, der mit dem seriengefertigten Handy/Tablet des Händlers verbunden ist

Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

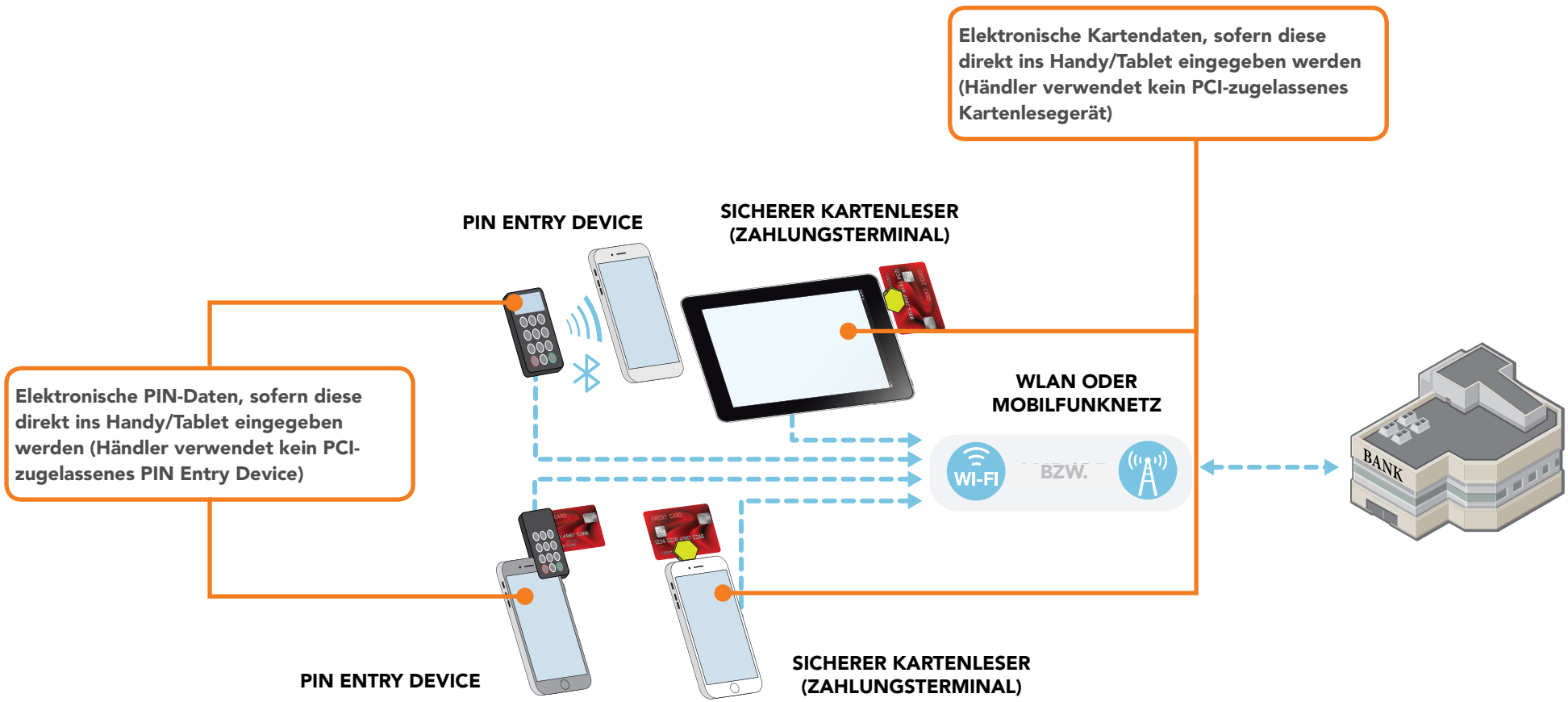
TYP 13

Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz oder WLAN gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
MITTEL	MITTEL

An welchem Punkt sind Kartendaten gefährdet?



PCI Security Standards Council

Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz oder WLAN gesendet.

RISIKOPROFIL

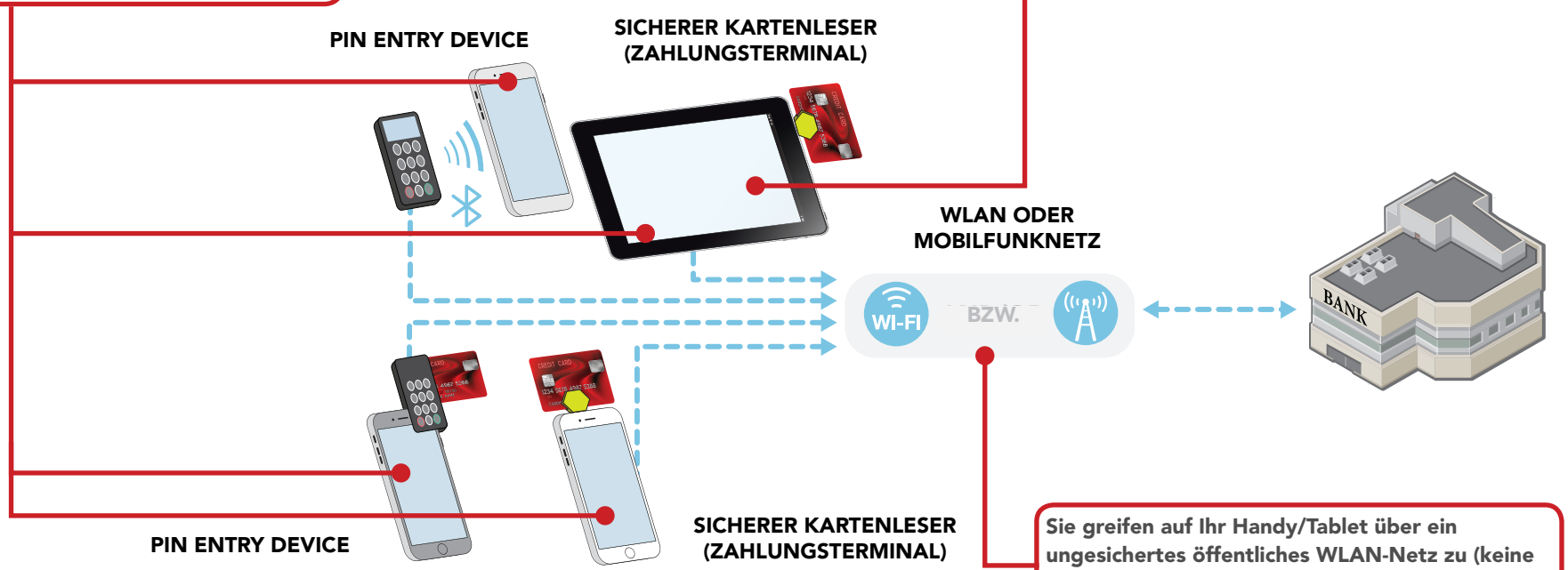
Chip	Magnetstreifen
MITTEL	MITTEL

Wie kommen Kriminelle an Ihre Kartendaten?

Sie können sich ins Handy/Tablet hacken und Schadsoftware installieren, mit der sie Karten- oder PIN-Daten vom Handy oder Tablet stehlen können.

Sie verwenden Apps im App Store, mit denen sie Karten- oder PIN-Daten stehlen können, wenn Sie diese App auf Ihr Handy/Tablet herunterladen.

Kriminelle können einen sicheren Kartenleser gegen einen austauschen, den sie entsprechend manipuliert haben.



Sie greifen auf Ihr Handy/Tablet über ein ungesichertes öffentliches WLAN-Netz zu (keine Firewall bzw. unbekannter Sicherheitsgrad), um Karten- oder PIN-Daten zu stehlen.

PCI Security Standards Council

TYP 13

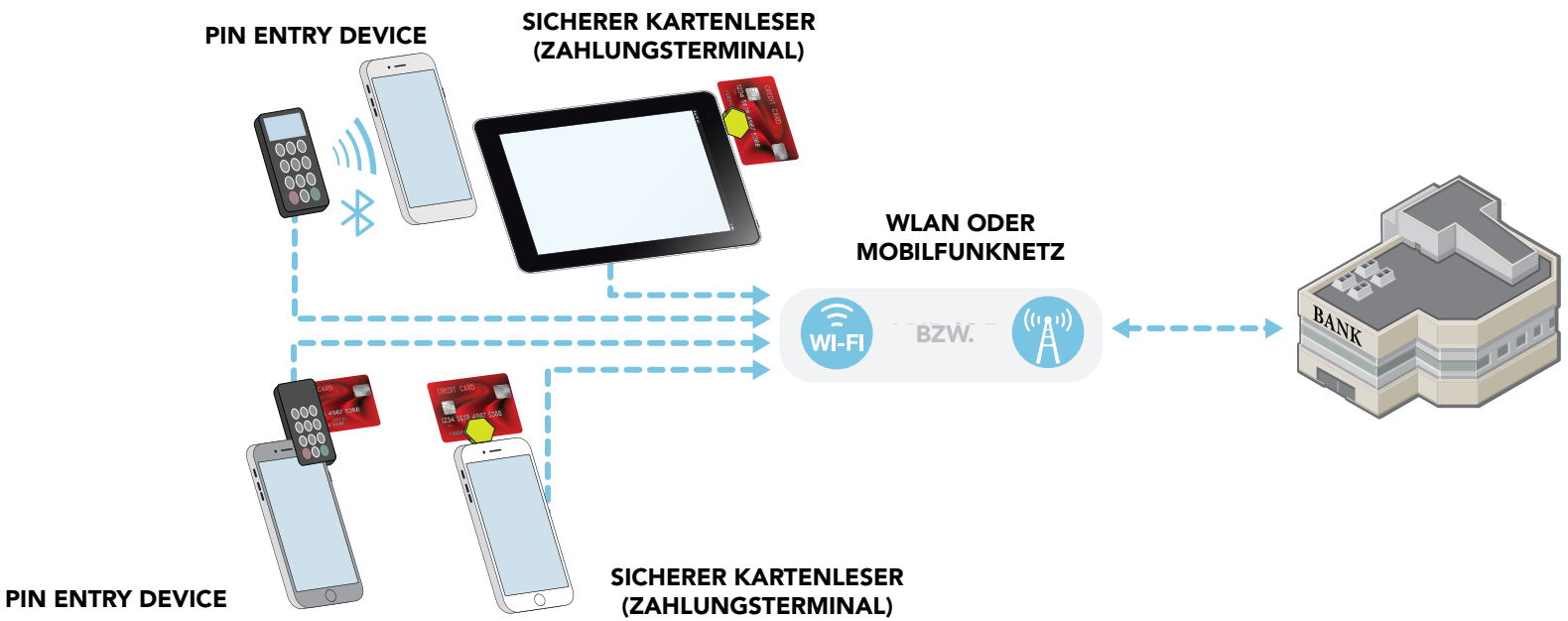
Kartenleser mit sicherer Verschlüsselungstechnologie und mobiles Zahlungsterminal. Zahlungsdaten werden ausschließlich übers Mobilfunknetz oder WLAN gesendet.

RISIKOPROFIL

Chip	Magnetstreifen
MITTEL	MITTEL

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Sichern Sie den Zugriff auf Ihre Kartendaten durch eigene Mitarbeiter
- Schützen Sie Ihr Unternehmen vor Gefahren aus dem Internet
- Untersuchen Sie Ihre sicheren Kartenleser und PIN Entry Devices auf Schäden oder Auffälligkeiten
- Beschränken Sie den Remote-Zugriff für Anbieter – geben Sie Hackern keine Chance
- Machen Sie Ihre Kartendaten nutzlos für Kriminelle
- Installieren Sie Patches Ihres Zahlungsterminal-Anbieters
- Verwenden Sie Antivirus-Software
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Verwenden Sie sichere Kartenlesegeräte und PIN Entry Devices



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

TYP 14

Virtuelles Zahlungsterminal mit Zugriff über den Internetbrowser des Händlers. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

GERING

JA
Das IST mein System.
Weitere Details ansehen.

NEIN
Das ist NICHT mein System.
Zurück zum Anfang.

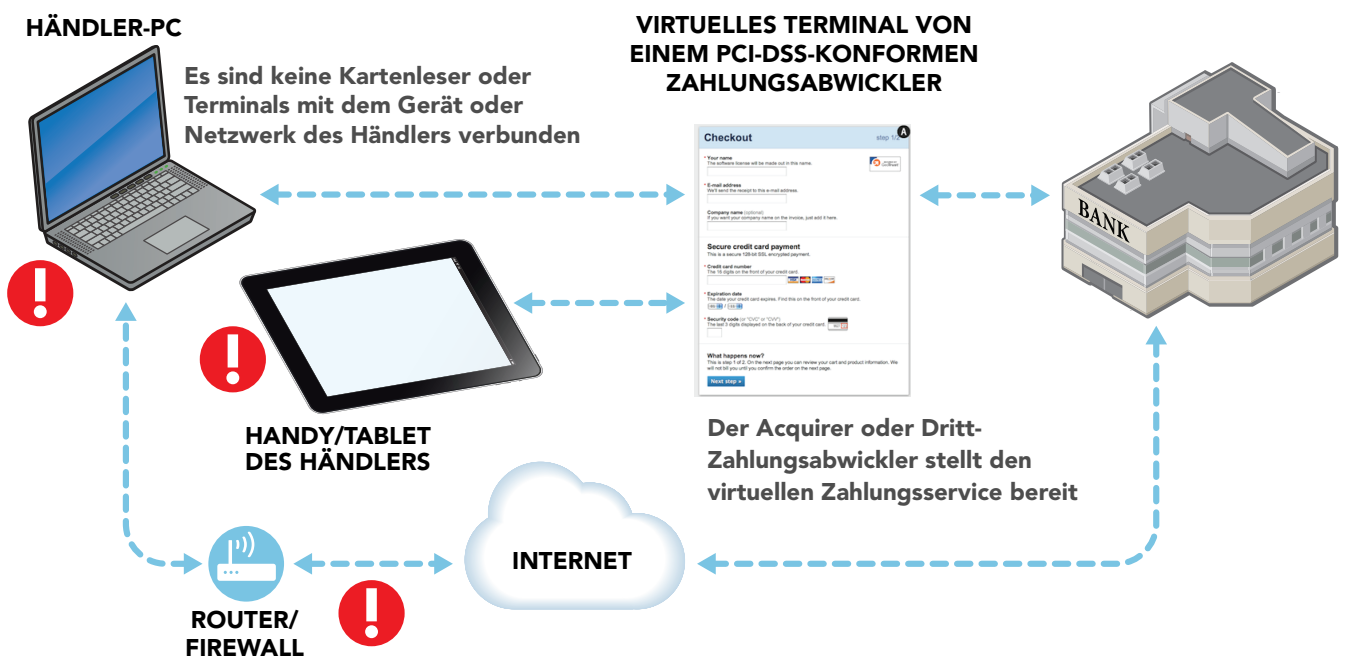
ZURÜCK
zum vorherigen Schaubild.

Beachten Sie, dass das Risiko des Datenklaus höher ist, wenn die mobile Zahlung über ein ungesichertes öffentliches WLAN-Netz erfolgt, da Kriminelle über dieses Netzwerk Ihre Daten stehlen können.

Ein „virtuelles Terminal" ist eine Webseite, auf die ein Händler zum Beispiel mithilfe eines Computers oder Tablets zugreifen kann

Der Händler gibt die Kartendaten über den Webbrowser manuell ins virtuelle Terminal ein

Für Händler ohne herkömmliches Zahlungsterminal. Sie geben die Transaktionen manuell ein und haben für gewöhnlich ein geringes Zahlungsvolumen (zum Beispiel beim Vertrieb von Zuhause)



Die Risiken für den Kartendatendiebstahl werden durch ein ❗ gekennzeichnet. Die Risiken werden auf der nächsten Seite erläutert.

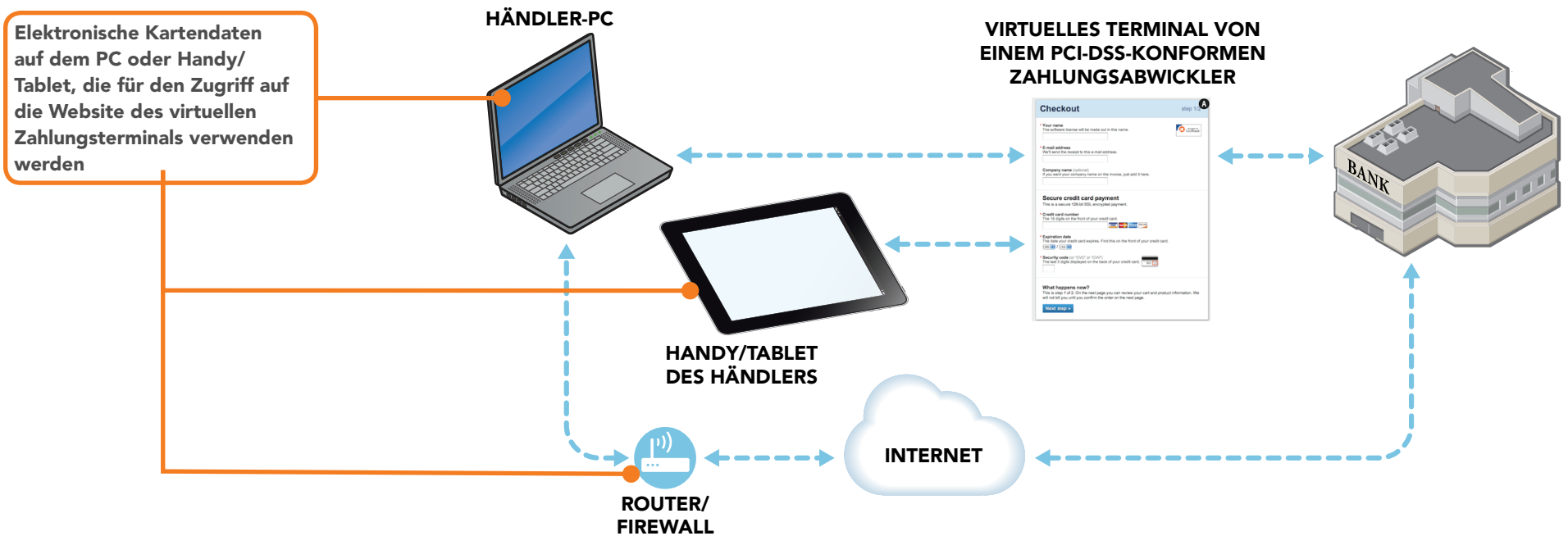
PCI Security Standards Council

Virtuelles Zahlungsterminal mit Zugriff über den Internetbrowser des Händlers. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

GERING

An welchem Punkt sind Kartendaten gefährdet?



TYP 14

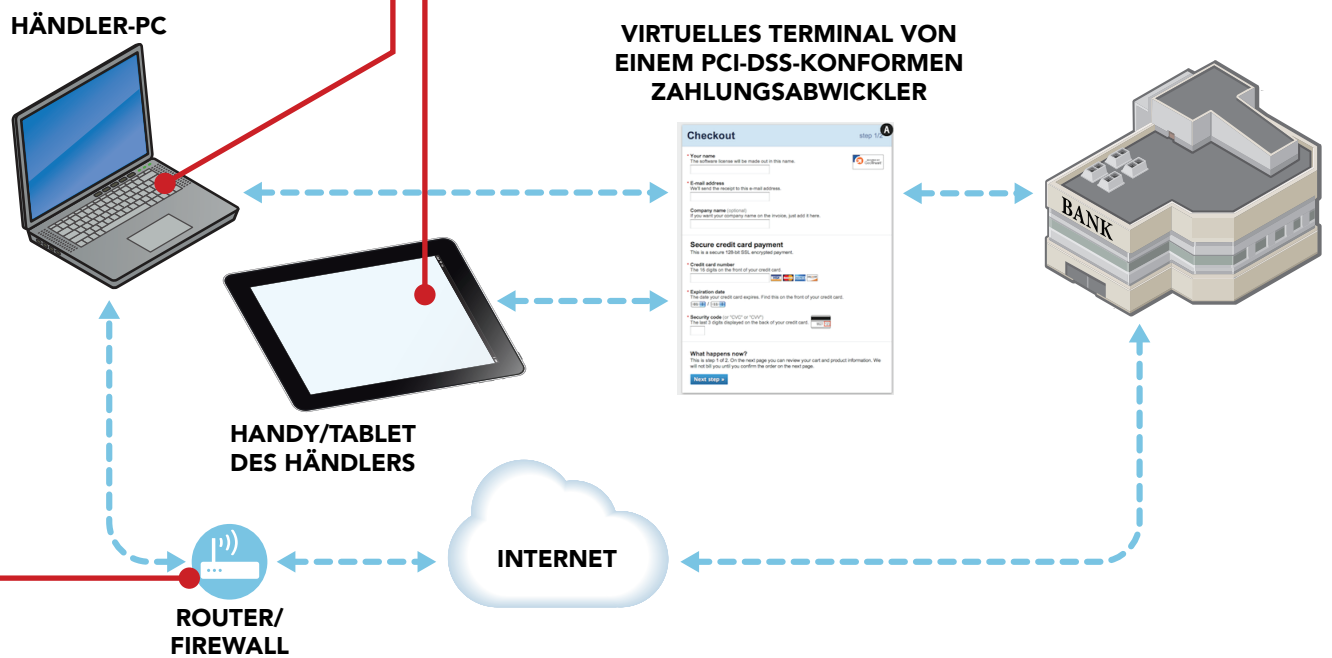
Virtuelles Zahlungsterminal mit Zugriff über den Internetbrowser des Händlers. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

GERING

Wie kommen Kriminelle an Ihre Kartendaten?

Sie hacken sich in den PC oder ins Handy/Tablet und installieren dort Schadsoftware, mit der sie Kartendaten stehlen können, sobald diese im virtuellen Terminal eingegeben werden.



Sie greifen auf Ihr Handy/Tablet über ein ungesichertes öffentliches WLAN-Netz zu (keine Firewall bzw. unbekannter Sicherheitsgrad), um Karten- oder PIN-Daten zu stehlen.

PCI Security Standards Council

TYP 14

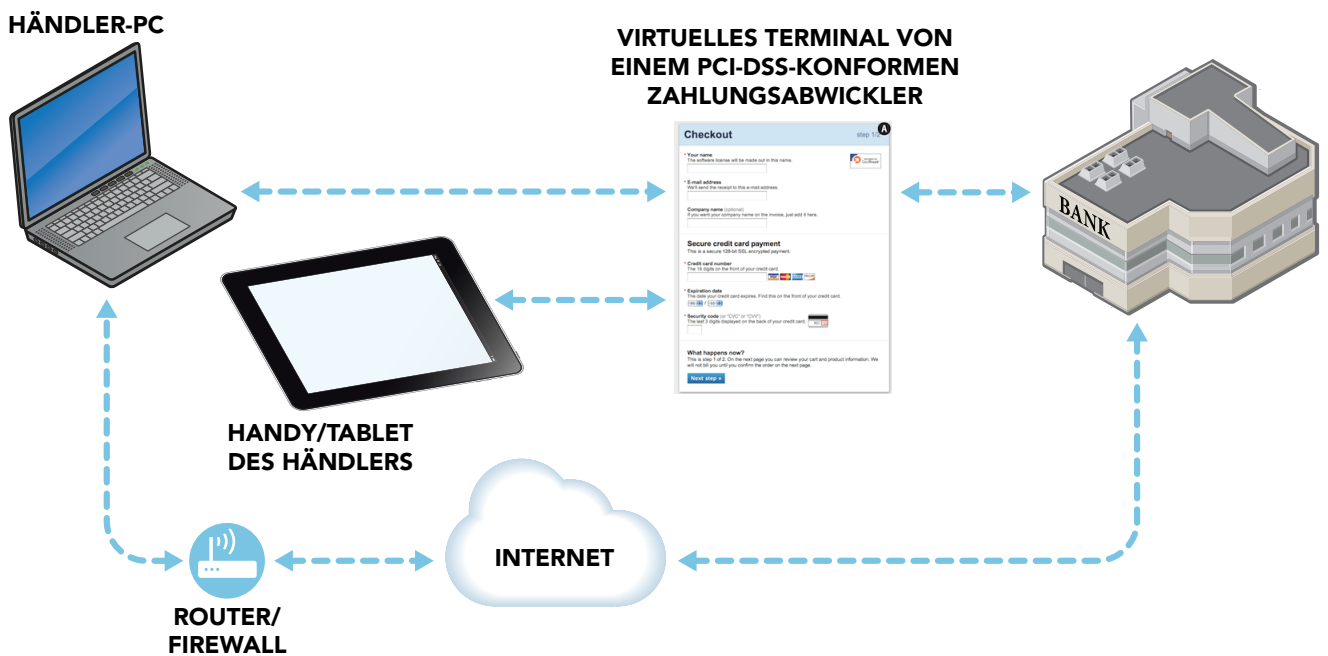
Virtuelles Zahlungsterminal mit Zugriff über den Internetbrowser des Händlers. Zahlungsdaten werden via Internet gesendet.

RISIKOPROFIL

GERING

Was können Sie heute für den Schutz Ihrer Kartendaten tun?*

- Verwenden Sie sichere Passwörter
- Installieren Sie Patches Ihres Zahlungsterminal-Anbieters
- Bitten Sie Ihre Anbieter bei Bedarf um Hilfe
- Beschränken Sie den Remote-Zugriff für Anbieter – geben Sie Hackern keine Chance
- Verwenden Sie Antivirus-Software
- Lassen Sie regelmäßig Scans auf Sicherheitsrisiken durchführen
- Verwenden Sie eine Firewall (bzw. eine persönliche Firewall-Software, falls Sie öffentliche WLAN-Netze nutzen)



*Über die Symbole gelangen Sie zum Leitfaden für sichere Zahlungsverfahren und den Informationen zu diesen grundlegenden Sicherheitsmaßnahmen.

PCI Security Standards Council

Onlinequellen

PCI-Dokumente für Kleinhändler

Quelle	Link	URL
Leitfaden für sichere Zahlungsverfahren	*Leitfaden für sichere Zahlungsverfahren*	*https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf*
Kleinhändler-Fragen an ihre Anbieter	*Kleinhändler-Fragen an ihre Anbieter*	*https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf*
Kleinhändler-Glossar	*Kleinhändler-Glossar*	*https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf*