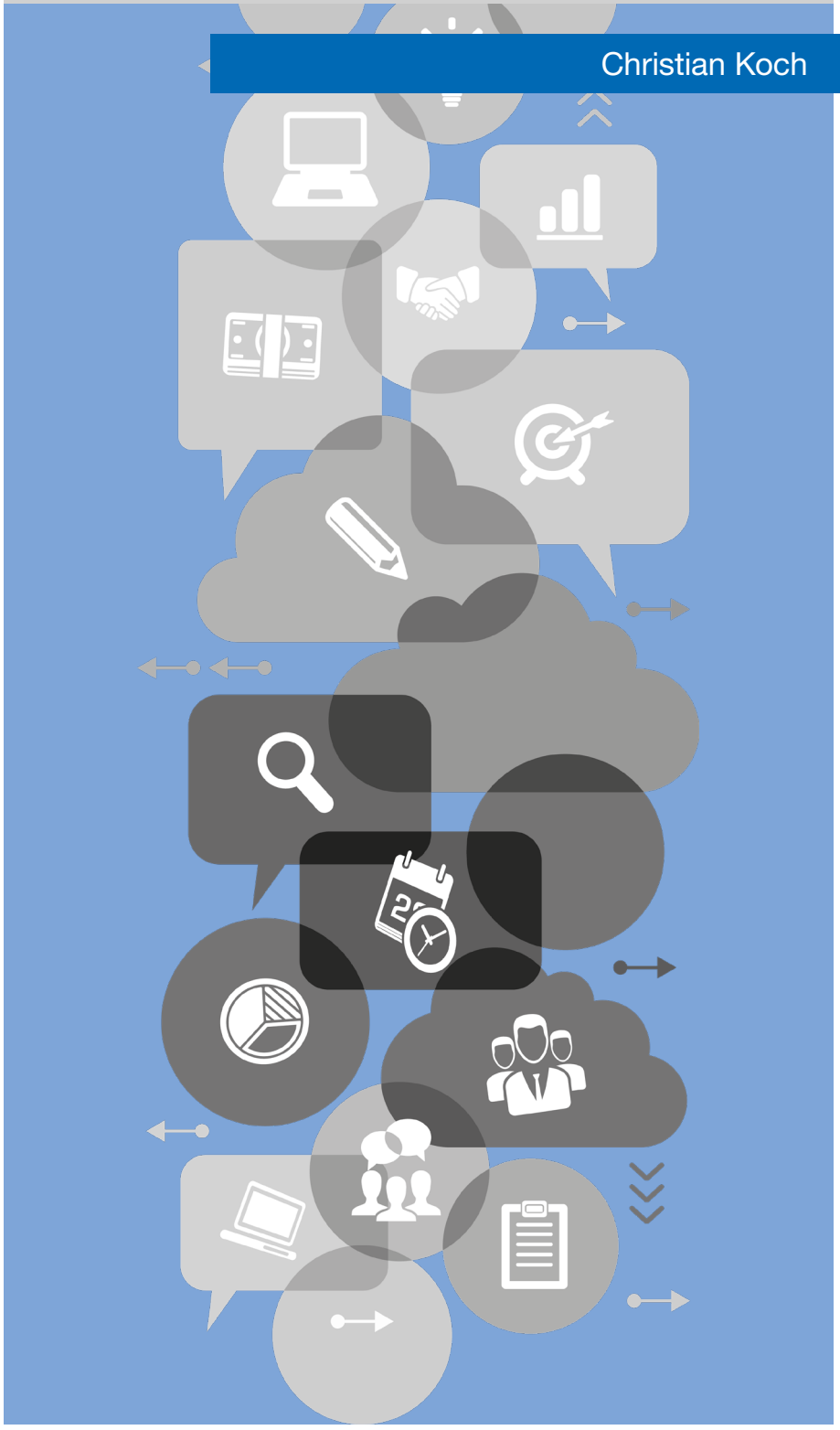
Online Bezahlen



Christian Koch

Schulungshefte der Volksbanken und Raiffeisenbanken

Die Schulungshefte sind seit Generationen ein Begriff in der Ausbildung. Die Hefte vermitteln das Basiswissen speziell für Bankkaufleute in Kreditgenossenschaften. Dies umfasst einerseits wichtige bankfachliche Themen. Andererseits werden aktuelle (z. B. Digitalisierung) und sogenannte weiche Themen (z. B. Knigge) speziell für junge Menschen aufbereitet.

Verständlich geschrieben und umfassend in der Stoffauswahl, sind die Schulungshefte ein ideales Lernmittel für Auszubildende. Die Hefte haben sich auch als Nachschlagewerk am Arbeitsplatz und in der Fortbildung bewährt. Ihre Aktualität ist durch ständige Überarbeitung gewährleistet.

Vertieftes Lesen

Die Schulungshefte sind im Format DIN A4 gestaltet. In der digitalen Form können sie am Bildschirm gelesen werden. Für ein vertieftes Lesen empfehlen wir, die Hefte auszudrucken. In der ausgedruckten Form kann der Leser den Text um handschriftliche Notizen ergänzen und wichtige Passagen mit einem Textmarker hervorheben. In vielen Schulungsheften sind Übungsaufgaben enthalten. Sie helfen Ihnen, das Gelesene zu verstehen und zu verinnerlichen.

Ein Ausdruck in Farbe ist nicht erforderlich. Sie können die Texte in Graustufen ausdrucken. Wenn Ihr Drucker die Option „Drucken von Text mit der Farbe Schwarz“ bietet, können Sie auch diese nutzen. Das erhöht zusätzlich die Lesbarkeit. Einzelne Seiten mit Diagrammen, Grafiken, Schaubildern etc. können gezielt im Format DIN A3 ausgedruckt werden.

Impressum

Redaktionsstand: März 2021
4. Auflage 2021

Satz und Gestaltung: Deutscher Genossenschafts-Verlag eG
Titelbild: istock.com/VLADGRIN

1 Inhalt

Die Geschäftsprozesse in der Kreditwirtschaft sind durch ein hohes Maß an digitaler Technik und kurzen Innovationszyklen gekennzeichnet. Der Kompetenzerwerb im Kontext der digitalen Arbeits- und Geschäftswelt ist integrativer Bestandteil der Lernfelder.

Sekretariat der Kultusministerkonferenz,
Referat Berufliche Bildung, Weiterbildung und Sport,
Rahmenlehrplan für den Ausbildungsberuf Bankkaufmann und Bankkauffrau

(Beschluss der Kultusministerkonferenz vom 13.12.2019),
Teil IV Berufsbezogene Vorbemerkungen

Dr. Christian Koch

1 Bankazubis werden fit für das Banking der Zukunft

Seit Jahrzehnten gilt der Beruf Bankkaufmann/Bankkauffrau als einer der Klassiker unter den dualen Erstausbildungen. Nach mehr als 20 Jahren wurde das Berufsbild grundlegend überarbeitet und modernisiert. Der Ausbildungsjahrgang 2020 ist der erste, der nach dem neuen Berufsbild ausgebildet wird. Stichworte zum neuen Berufsbild sind:

- konsequente Ausrichtung an der Kundenbeziehung,
- verstärkte Nutzung digitaler Kanäle,
- ganzheitliche Kundenberatung,
- projektorientierte Arbeitsweisen,
- Optimierung und Weiterentwicklung von standardisierten Prozessen.

Vertraut mit digitalen Zugangskanälen

Die Auszubildenden sollen früh mit den digitalen Zugangskanälen zu Bankgeschäften vertraut gemacht werden. Sie sollen „Kunden bei der Nutzung analoger oder digitaler Zugangskanäle zu Bankgeschäften unterstützen, Nutzen für den Kunden herausstellen und sicherheitsrelevante Informationen geben."

So ist es bei der Berufsbildposition 1 „Serviceleistungen anbieten“ beschrieben.

Vor diesem Hintergrund wurde das vorliegende Schulungsheft an das Berufsbild 2020 angepasst und auf den aktuellen Stand gebracht.

Ergänzend dazu lohnt sich ein Blick in die Schulungshefte „Aktuelles“, „Glossar” und „Zahlen – Daten – Fakten”.

2 Online Bezahlen – wie geht das?

Heutzutage ist es alltäglich, dass wir über das Internet Waren bestellen und Dienstleistungen in Anspruch nehmen. Im Jahr 2020 betrug der E-Commerce-Anteil am gesamten Handelsumsatz in Deutschland rund 11 Prozent. Dies entspricht rund 73 Milliarden Euro.

Und wie bezahlen wir online? Diese Frage beantwortet das vorliegende Schulungsheft. Dabei liegt ein Schwerpunkt auf den Onlinebanking-Angeboten der Banken und Sparkassen sowie dem Bezahlverfahren der Deutschen Kreditwirtschaft „paydirekt“.

Aber auch die klassischen Bezahlverfahren, wie die Kreditkarte, der Kauf auf Rechnung und gegen Vorkasse, werden beleuchtet. Ein Überblick über virtuelle Währungen darf selbstverständlich nicht fehlen.

3 Klassische Bezahlverfahren

Auch heutzutage nutzen insbesondere kleinere Online-Händler noch die klassischen Bezahlverfahren, um ihre Waren und Dienstleistungen im Internet zu verkaufen. Allein die herkömmlichen Verfahren umfassen fünf unterschiedliche Bezahlmöglichkeiten:

3.1 Vorkasse

Bei der Vorkasse tritt der Käufer in Vorleistung. Das heißt, erst wenn der fällige Betrag bezahlt ist (in der Regel durch Überweisung), versendet der Händler die Ware. Damit entsteht automatisch eine längere zeitliche Lücke zwischen Kauf und Lieferung. Darüber hinaus setzt diese Art der Bezahlung erhebliches Vertrauen in den Verkäufer voraus. Denn ist das Geld erst überwiesen, ist man auf das Wohlwollen des Verkäufers angewiesen, dass dieser die online bestellte Ware auch tatsächlich liefert. Aufgrund dieser Nachteile ist die Bezahlart Vorkasse nicht sehr verbreitet.

3.2 Rechnung

Das Risiko der Nichtlieferung besteht beim Bezahlen auf Rechnung nicht. Hier bietet der Online-Händler die Möglichkeit, die Ware erst nach Lieferung zu bezahlen. Der Käufer erhält die Ware direkt nach der Bestellung und muss den geschuldeten Betrag erst danach überweisen. Dies bietet im Vergleich zur Vorkasse erhebliche Vorteile für den Käufer. Dieser kann die Ware prüfen und sodann bezahlen (in der Regel per Überweisung). Im Jahr 2019 wurden rund 32,8 Prozent aller Warenkäufe im E-Commerce per Rechnung (Überweisung nach Erhalt) bezahlt.

3.3 Bankeinzug

Eine im Internet sehr weit verbreitete Bezahlart (19 Prozent im Jahr 2019) ist der Bankeinzug. Dabei bedient sich der Online-Händler des Lastschriftverfahrens, indem er vom Käufer unter Abfrage der Bankverbindung (BIC, IBAN) ein SEPA-Lastschriftmandat einholt, das ihn berechtigt, den Kaufpreis vom Konto des Käufers per Lastschrift einzuziehen. Der Händler reicht die Lastschriften auf der Grundlage einer mit seinem Kreditinstitut geschlossenen Lastschriftinkassovereinbarung zum Einzug ein. Der Käufer kann – ohne Angabe von Gründen – der Belastungsbuchung innerhalb von acht Wochen widersprechen und von seiner Bank Erstattung des belasteten Betrages verlangen. Aufgrund des unbedingten Widerspruchsrechts ist das Risiko für den Käufer beim Kauf per Bankeinzug im E-Commerce sehr gering.

3.4 Nachnahme

Bietet der Online-Shop Zahlung per Nachnahme an, zahlt der Käufer die bestellte Ware zum Zeitpunkt der Lieferung, also entweder direkt an den Zusteller oder bei der Abholung in der Filiale des Transportunternehmens. Das Lieferunternehmen leitet die Einnahmen später an den Händler weiter. Neben der Barzahlung bieten die Unternehmen auch die Bezahlung mit girocard oder Kreditkarte an. Die meisten Internetshops verlangen eine separate Gebühr für die Nachnahme. Im Jahr 2019 wurden 1,9 Prozent aller Warenkäufe im E-Commerce per Nachnahme bezahlt.

3.5 Kreditkarte

Neben der Lastschrift gehört das Zahlen mit der Kreditkarte zu den gängigsten, klassischen Bezahlverfahren im Internet (rund 10,7 Prozent im Jahr 2019), da die Abwicklung unkompliziert ist. Durch die Eingabe des Namens, der Kreditkartennummer, der Sicherheitsnummer und des Ablaufdatums der Karte wird die Zahlung an den Online-Händler legitimiert. Aufgrund der Vorgaben der Zweiten Zahlungsdiensterichtlinie sind zudem Mastercard® Identity Check™ und Visa Secure beim Online-Bezahlen im Europäischen Wirtschaftsraum verpflichtend. Da die Zahlung von der kartenausgebenden Bank gegenüber dem Händler garantiert wird, kann der Händler die Ware unmittelbar nach der Bestellung versenden.

4 Onlinebanking

Im Zeitalter moderner Informations- und Kommunikationstechniken bietet der globale Datenaustausch gerade auch den Kreditinstituten die Chance, neue Wege der Interaktion mit ihren Kunden zu gehen. Dabei wird für immer mehr Deutsche das Onlinebanking zu einer Selbstverständlichkeit. So wurden Ende 2019 in Deutschland rund **75 Millionen Konten online** geführt. Dafür gibt es gute Gründe: So sind im Allgemeinen Finanztransaktionen, die online ausgeführt werden, preiswerter als Geschäfte am Bankschalter. Vor allem aber überzeugt die Kunden, dass sie Bankgeschäfte bequem und sicher von zu Hause aus abwickeln können.

4.1 Technische Verfahren des Onlinebanking

Wurde früher das Onlinebanking über geschlossene Netze angeboten, so ist heute die **Online-Abwicklung von Bankgeschäften über das Internet** üblich. Der Vorteil liegt darin, dass das Internet die Kommunikation zwischen unabhängigen Rechnernetzen erlaubt, die auf der Basis unterschiedlicher Betriebssysteme arbeiten. Dem steht der Nachteil gegenüber, dass offene Netze, die ohne Zulassung durch den Netzbetreiber genutzt werden können, naturgemäß ein höheres Risiko beinhalten als geschlossene Netze.

Der Kunde benötigt für das Onlinebanking neben dem Betriebssystem eine spezielle Software zur Darstellung der Internetinhalte, einen sogenannten **Browser.** Der Zugang zum Internet erfolgt über einen Provider. Zur sicheren Übertragung werden spezielle Verschlüsselungsmechanismen eingesetzt. Einzelne Geschäftsvorgänge werden im sicheren Dialog (Secure Dialog, https) durchgeführt (i. d. R. 128-Bit-Verschlüsselung). Bevor der Kunde im Netz Bankgeschäfte tätigen kann, muss er durch das Kreditinstitut freigeschaltet werden.

Das **PIN-/TAN-Verfahren** ermöglicht die Legitimation des Kunden durch eine persönliche Identifikationsnummer (PIN) und die Bestätigung einer einzelnen Anweisung mittels einer einmaligen Transaktionsnummer (TAN). Einzelne Kreditinstitute verwenden zusätzlich eine Bestäti-

gungsnummer (BEN), die dem Kunden nach Eingang seines Auftrags zur Kontrolle übermittelt wird.

Die **PIN** ist mehrstellig und kann sowohl aus Ziffern als auch aus Buchstaben bestehen. Für den erstmaligen Zugang erhält der Kunde von seinem Institut eine „Einstiegs-PIN“, die er nach erfolgter Anmeldung jederzeit (unter Verwendung einer TAN) durch elektronische Erklärung gegenüber seinem Kreditinstitut ändern kann. Sofern die Inanspruchnahme einzelner Dienstleistungen nur unter Zusammenwirken mehrerer Personen möglich ist (Konten mit gemeinschaftlicher Verfügungsbefugnis, Firmenkonten), ist von jedem Mitwirkenden eine gesonderte PIN einzugeben.

Die **TAN** dient nicht der Identifizierung des Kunden, sondern der Legitimation der einzelnen Transaktion, etwa der einzelnen Überweisung. Eine TAN ist nur einmalig verwendbar. Die TAN erhält der Kunde entweder über einen **TAN-Generator** oder über ein **Mobiltelefon**. Anders als die PIN wird die TAN zu Kontrollzwecken am Bildschirm angezeigt. Ob für einen Geschäftsvorgang eine TAN eingegeben werden muss, erfährt der Kunde aus der Benutzerführung auf dem Bildschirm. Über die TAN-Pflicht im Einzelnen entscheidet das Kreditinstitut. Es gibt mehrere gängige **Verfahren zur Erzeugung der TAN.**

4.1.1 Sm@rt-TAN-plus

Das Verfahren stellt zwei Anwendungsmöglichkeiten zur Verfügung: mit manueller Eingabe oder mit optischer Übertragung.

Mit manueller Eingabe

Beim Sm@rt-TAN-plus-Verfahren mit manueller Eingabe schiebt der Kunde seine Chipkarte in einen Kartenleser (TAN-Generator) mit integrierter Tastatur. Anschließend gibt er dort manuell die Daten ein, die für die Erstellung einer TAN benötigt werden. Die Transaktion, etwa eine Überweisung, und die TAN-Übermittlung werden so in zwei Schritte zerlegt und voneinander getrennt durchgeführt. TAN-Nummern können dadurch nicht mehr via Phishing abgefangen, willkürlich geändert oder für einen anderweitigen Überweisungsauftrag verwendet werden. Die erzeugte TAN wird nur für diesen entsprechenden Überweisungsauftrag erstellt und zusätzlich durch den Anwender kontrolliert.

Mit optischer Übertragung

Beim Sm@rt-TAN-plus-Verfahren mit optischer Übertragung der Transaktionsdaten ist die manuelle Eingabe der Auftragsdaten nicht mehr nötig. Die optische Schnittstelle im Lesegerät (TAN-Generator) liest nach dem Einschieben der Chipkarte die notwendigen Kontrolldaten vom Monitor direkt in das Lesegerät ein. Die erforderlichen Daten werden über eine animierte Grafik in die Online-Anwendung eingeblendet. Der Kunde muss daher keine Daten mehr am Lesegerät eingeben, sondern dieses nur vor die animierte Grafik halten und anschließend die am Lesegerät angezeigten Werte mit den Originaldaten, beispielsweise mit einer Rechnung, vergleichen. Danach werden die Angaben mit der < OK-Taste > bestätigt und dem Kunden wird die TAN im Display des TAN-Generators angezeigt.

4.1.2 mobileTAN

Hier erhält der Kunde die TAN zur Autorisierung seiner Transaktion zusammen mit den wesentlichen Transaktionsdaten, wie Betrag und Empfängerkontonummer, per SMS auf sein Handy. Nach Prüfung der in der SMS enthaltenen Daten schließt der Kunde mit der Eingabe der TAN aus der zugesandten SMS in das Online-Formular die Transaktion ab.

4.1.3 HBCI

Die Autorisierung von Transaktionen erfolgt bei diesem Verfahren durch hardwaregestützte Verschlüsselungstechnik. Dazu stellt die Bank dem Kunden eine personalisierte Chipkarte aus. Der Kunde benötigt zusätzlich einen Chipkartenleser, den er an seinen Computer anschließt und eine Software, die den HBCI-Standard (HBCI = Homebanking Computer Interface) unterstützt. Beim Onlinebanking mit Chipkarte entfallen die TAN-Listen, deren jeweilige Freischaltung und die Eingabe der TAN durch den Kunden.

4.1.4 pushTAN

Das pushTAN-Verfahren erfordert neben der eigentlichen Banking-Anwendung am PC oder auf dem mobilen Endgerät eine zusätzliche App auf dem Smartphone oder einem anderen Gerät (z. B. Tablet-PC). Anders als bei der mobileTAN wird die Transaktionsnummer nicht über das Mobilfunknetz übermittelt, sondern über eine verschlüsselte IP-Verbindung aus dem Rechenzentrum der Bank. Zusätzlich wird diese App mit weiteren Sicherheitsmaßnahmen gesondert gegen Angriffe geschützt.

Die pushTAN-App ist unabhängig vom Onlinebanking und nutzt eigene Zugangsdaten. Der Kunde prüft wie bisher die in der App angezeigten Transaktionsdaten, wie Empfänger-IBAN und Betrag, und erfasst danach die TAN in der Banking-Anwendung.

Im Bereich der genossenschaftlichen FinanzGruppe existieren derzeit zwei verschiedene Verfahren: VR-SecureGo und VR-SecureSIGN. Welches Verfahren zur Anwendung kommt, hängt von der jeweiligen Volksbank Raiffeisenbank ab. Aus technischen Gründen bieten manche Banken VR-SecureGo und andere VR-SecureSIGN an.

4.2 Die Zweite Zahlungsdiensterichtlinie (PSD2)

Mit der Umsetzung der Zweiten Zahlungsdiensterichtlinie (PSD2) sind am 14. September 2019 im Europäischen Wirtschaftsraum einheitliche Standards für die Sicherheit elektronischer Zahlungen in Kraft getreten. Die wesentlichen Neuerungen lassen sich wie folgt zusammenfassen:

- Berechtigte Drittanbieter können mit Zustimmung der Kunden Zahlungen auslösen oder Kontoinformationen von Zahlungsverkehrskonten abrufen.
- Die Einwilligung des Kunden vorausgesetzt, können Drittanbieter bei Kartenzahlung die Verfügbarkeit des Kaufbetrages bei seiner Bank anfragen.
- Beim Log-in ins Onlinebanking oder in die VR-BankingApp, beim Online-Shopping mit Kreditkarte sowie bei Zahlungen und beim Abruf von Umsatzinformationen müssen in der Regel zwei voneinander unabhängige Faktoren den Kunden im Sinne einer sogenannten „starken Kundenauthentifizierung“ legitimieren.
- Mastercard® Identity Check™ und Visa Secure werden im Europäischen Wirtschaftsraum beim Online-Bezahlen mit Kreditkarte verpflichtend.
- Elektronische Zahlungen werden für den Kunden transparenter, da er über eine eigene Zugriffsverwaltung den protokollierten Kontozugriff berechtigter Drittanbieter einsehen und die Erlaubnis des „Kontozugriffs für 90 Tage“ auch wieder entziehen kann.
- Mehr Sicherheit für den Kunden durch eine „starke Kundenauthentifizierung“ mit zwei voneinander unabhängigen Faktoren für elek-

tronische Zahlungen über das Konto und die Kreditkarte, durch die Zugriffverwaltung des Kunden auf sein Konto sowie die Dokumentation der Kontozugriffe durch Drittanbieter und durch weitere Sicherheitssysteme seitens der Bank.

4.3 Vertragsrechtliche Grundlagen

Sowohl für das PIN-/TAN-Verfahren als auch für das HBCI-Verfahren gelten im Verhältnis des Kreditinstituts zum Kunden jeweils besondere Klauselwerke. Beim Onlinebanking mit PIN und TAN, mit elektronischer Signatur (HBCI-Software-Version) oder mit elektronischer Signatur (HBCI-Chipkarten-Version) wird zwischen Kreditinstitut und Kunde in der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken die **„Vereinbarung über die Nutzung des Onlinebanking“** geschlossen (DG VERLAG Nr. 283 350).

Auf der Grundlage dieses „Onlinebanking-Vertrages“ ist der Kontoinhaber oder ein Bevollmächtigter (in den vertraglichen Regelwerken einheitlich als „Nutzer“ bezeichnet) berechtigt, mittels den mit der Bank vereinbarten Zugangsmedien (PIN/TAN, elektronische Signatur) auf seine Konten und/oder Depots im Wege des Onlinebanking zuzugreifen.

Ergänzend zu den Regelungen im Onlinebanking-Vertrag werden mit dem Kunden die **„Sonderbedingungen für das Onlinebanking“** (Onlinebanking-Bedingungen – DG VERLAG Nr. 283 300) vereinbart. Hierbei handelt es sich um Allgemeine Geschäftsbedingungen i. S. d. §§ 305 ff. BGB. Geregelt oder modifiziert werden nicht die im Netz abgeschlossenen Rechtsgeschäfte selbst. Regelungsgegenstand sind vielmehr allein die sich aus der elektronischen Abwicklung ergebenden Besonderheiten in genereller Form. Auch der Umfang der im Wege des Onlinebanking angebotenen Dienstleistungen bestimmt sich außerhalb dieser Regelwerke nach freiem Ermessen des jeweiligen Kreditinstituts.

Der Kunde hat keinen Anspruch auf die Nutzung des Onlinebanking-Angebots seiner Bank. Ein **Kontrahierungszwang besteht** folglich nicht. Maßgebliche Kriterien im Rahmen der Ermessensentscheidung des Kreditinstituts über die Zulassung eines Kunden zum Onlinebanking sind dessen Zuverlässigkeit und Bonität. Erstere ist anhand der Erfahrungen aus bestehender Geschäftsbeziehung zu beurteilen.

In Nummer 6 des Onlinebanking-Vertrages ist die übliche **Einbeziehung** der einschlägigen Sonderbedingungen vorgesehen. Diese **„Sonderbe-**

dingungen für das Onlinebanking“ erfüllen insbesondere auch den Zweck, den Kunden auf Missbrauchsmöglichkeiten des Online-Systems durch Dritte sowie auf die sich daraus ergebenden **haftungsrechtlichen Folgen** aufmerksam zu machen. Insbesondere definieren die Onlinebanking-Bedingungen besondere **Sorgfaltspflichten des Teilnehmers:** Danach hat der Teilnehmer seine Authentifizierungselemente vor unbefugtem Zugriff zu schützen (vgl. Nummer 7.1 der Bedingungen). Ansonsten besteht die Gefahr, dass das Onlinebanking missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird. Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

4.3.1 Wissenselemente

Wissenselemente, wie z. B. die PIN, sind geheim zu halten; sie dürfen insbesondere

- nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Onlinebanking in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. girocard mit TAN-Generator, mobiles Endgerät, Signaturkarte) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Onlinebanking und Fingerabdrucksensor) dient.

4.3.2 Besitzelemente

Besitzelemente, wie z. B. die girocard mit TAN-Generator oder ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere

- sind die girocard mit TAN-Generator oder die Signaturkarte vor dem unbefugten Zugriff anderer Personen sicher zu verwahren,
- ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Online-

banking (z. B. Onlinebanking-App, Authentifizierungs-App) nicht nutzen können,

— ist die Anwendung für das Onlinebanking (z. B. Onlinebanking-App, Authentifizierungs-App) auf dem mobilen Endgerät des Nutzers zu deaktivieren, bevor der Nutzer den Besitz an diesem mobilen Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons),

— dürfen die Nachweise des Besitzelements (z. B. TAN) nicht außerhalb des Onlinebanking mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und

— muss der Nutzer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Onlinebanking) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Onlinebanking des Nutzers aktivieren.

4.3.3 Seinselemente

Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem mobilen Endgerät des Nutzers für das Onlinebanking nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für das Onlinebanking genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Onlinebanking das von der Bank ausgegebene Wissenselement (z. B. PIN) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.

Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (z. B. Mobiltelefon), nicht gleichzeitig für das Onlinebanking genutzt werden.

Die für das mobileTAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Nutzer diese Telefonnummer für das Onlinebanking nicht mehr nutzt.

Darüber hinaus wird der Nutzer zur Erhaltung der Sicherheit des Kundensystems verpflichtet, die Sicherheitshinweise der Bank zum Onlinebanking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), zu beachten.

4.3.4 Sperranzeige, Haftung

Zur Haftung des Nutzers gilt: **Nach der Sperranzeige** trifft den Kunden keine Haftung mehr für die danach eintretenden Schäden aufgrund einer missbräuchlichen Nutzung des Onlinebanking. **Vor der Sperranzeige** ist die Haftung des Kunden grundsätzlich auf 50 Euro begrenzt. Diese Grenze gilt allerdings nicht, wenn der Kunde seine Sorgfaltspflichten beim Onlinebanking vorsätzlich oder grob fahrlässig verletzt hat. Selbst bei grober Fahrlässigkeit ist die Haftung des Kunden auf den für die Nutzung des Onlinebanking geltenden Verfügungsrahmen beschränkt, Nummer 10.2.1, Absatz 5 der Sonderbedingungen für das Onlinebanking.

4.4 Missbrauch im Onlinebanking

Um unbefugt an die Kontodaten nebst PIN und TAN eines Kontoinhabers zu gelangen, sind verschiedene Szenarien denkbar.

4.4.1 Einbruch, Diebstahl

Die Täter können sich die Daten physisch verschaffen, indem sie die Post des Kontoinhabers unbefugt öffnen oder bei diesem einbrechen. Das unbemerkte Öffnen der Post wird durch die Gestaltung der PIN- und TAN-Sendungen in aufreißbaren Umschlägen praktisch verhindert, da dies dem Kontoinhaber auffallen würde. PIN- und TAN-Liste (sofern diese überhaupt noch angeboten werden) werden durch die Institute zeitversetzt mit separaten Schreiben versandt, die im Regelfall wiederum nicht die vollständige Kontonummer enthalten. Alternativ könnten sich die Täter Zugang zum Zentralrechner der Bank des Kontoinhabers verschaffen. Dieses Angriffsszenario wird allerdings an den hohen Sicherheitsmaßnahmen der Banken scheitern.

4.4.2 Ausspähen der Daten

Die Täter könnten die Daten mittels sogenannter Malware **(Viren, Trojaner** etc.) ausspionieren, die heimlich auf dem Computer des Kontoinhabers installiert wird (in der Regel beim Öffnen von per E-Mail versandter Dateien oder dem Besuch einer Webseite). Diese wertet die Eingaben des Computernutzers aus und übermittelt sie an die Täter. Dies ist auch bei gesicherten Verbindungen möglich. Um eine nicht verbrauchte TAN zu erlangen, existieren Programme, die nach Eingabe der

TAN die Verbindung zur Bank unterbrechen. Diese Programme werden **Abbruch-Trojaner** genannt.

Trojaner werden auf den unterschiedlichsten Wegen auf die Rechner der Onlinebanking-Nutzer eingeschleust, häufig ohne dass diese die Bedrohung auf ihrem Rechner bemerken. Beim sogenannten **„Man-In-The-Middle-Angriff“** überwachen und manipulieren diese Schadprogramme als „Mann in der Mitte“ den Datenverkehr zwischen dem Browser des Nutzers und dem Rechner der Bank. Wenn der Nutzer eine Überweisung durchführt, fängt das Schadprogramm die Auftragsdaten ab, verändert Betrag und Kontonummer des Empfängers und leitet die manipulierten Daten an die Bank weiter. Kriminelle überweisen sich auf diese Weise, also mithilfe des Schadprogramms, das Geld, das der Zahlungspflichtige eigentlich jemand anderem zukommen lassen wollten. Der Absender des Geldes merkt davon zunächst nichts, weil das Trojanische Pferd die Anzeige im Browserfenster verändert und so eine ordnungsgemäß durchgeführte Transaktion vortäuscht. Erst beim nächsten Blick auf einen Kontoauszug wird der Schaden sichtbar.

Bei sogenannten **„Man-In-The-Browser“**-Attacken greifen die Schadprogramme nicht in den Datenverkehr zwischen dem Rechner des Kontoinhabers und dem Bank-Computer ein, sondern manipulieren nur die Darstellung der Onlinebanking-Website im Browser. Wird bei einem so infizierten Rechner die Adresse der Onlinebanking-Website eingegeben, wird eine normale Verbindung hergestellt. Öffnet sich die Anmelde-Website des Bankportals, sorgt die Schadsoftware aber dafür, dass zwar die korrekte Website aufgerufen, dort aber manipulierte Inhalte angezeigt werden. Unter Vorspiegelung falscher Tatsachen wird der Nutzer zum Beispiel über eine gefälschte Eingabemaske dazu gebracht, bestimmte Daten preiszugeben – zum Beispiel TANs oder die Kreditkartendaten. Gleichzeitig deutet aber die korrekte Adresse in der Adressleiste des Browsers darauf hin, dass alles seine Richtigkeit hat.

Schutz vor dieser Art des Angriffs können **Virenschutzprogramme** bieten, die allerdings regelmäßig (meist täglich) aktualisiert werden müssen, weil auch die schädlichen Programme schnell variiert und weiterentwickelt werden. Eine **Firewall versucht zu verhindern,** dass Malware-Daten über das Internet empfangen oder Hacker unbefugten Zugriff auf den Computer des Nutzers nehmen. Malware hinterlässt stets Spuren auf dem infizierten Computer, nämlich zumindest das Schadprogramm selbst.

4.4.3 Phishing

Die zumindest begrifflich bekannteste Angriffsvariante ist das sogenannte Phishing, bei dem die Täter versuchen, E-Mails einer Bank nachzuahmen und die Kunden auffordern, ihr Konto – üblicherweise unter vorgetäuschten Sicherheitsgründen – durch Eingabe von Kontonummer, PIN und mehreren TANs erneut freizuschalten. Teilweise sollen die Kunden ihre Daten in ein Formular in der E-Mail eintragen oder als Antwort zurücksenden. Üblicher und erfolgversprechender ist der Weg über einen in der E-Mail integrierten Link auf eine Website, welche die Täter so gestaltet haben, dass sie der Seite der Bank ähnelt. Dies wird **Visual Spoofing genannt.** Dort angekommen, wird der Kunde dann aufgefordert PIN und TAN einzugeben.

Frühere Phishing-E-Mails waren häufig leicht zu erkennen, da sie oft viele Rechtschreibfehler enthielten und ihr Erscheinungsbild von dem der Originalnachrichten von Banken stark abwich. Da viele Internetnutzer heute weitaus skeptischer auf E-Mails reagieren, die nicht persönlich an sie adressiert sind und unseriös wirken, gehen Kriminelle nun geschickter vor. So wird immer häufiger das sogenannte **„Spear-Phishing“** betrieben: Dabei beschaffen sich Kriminelle auf illegalen Wegen persönliche Daten und E-Mail-Adressen von einer bestimmten Nutzergruppe und schreiben diese gezielt mit auf sie zugeschnittenen Nachrichten an. Es hat sich gezeigt, dass die persönliche Ansprache bei Internetnutzern zu mangelnder Vorsicht führt.

Diese Tatsache machen sich Angreifer auch zunutze, indem sie zunehmend **Instant-Messaging-Dienste und sogenannte soziale Netzwerke** zur Verbreitung von Phishing-Nachrichten nutzen. Dabei verschicken sie die gefälschten Nachrichten über manipulierte Zugänge im Namen von ahnungslosen Nutzern. Da das „Opfer“ dem Freund vertraut, steigt die Wahrscheinlichkeit, auf solche Nachrichten hereinzufallen und Anhänge zu öffnen oder Links zu folgen.

Einen gewissen **Schutz gegen Phishing-Angriffe** bieten Spam-Filter, die anhand von bestimmten Kriterien unter anderem gefälschte E-Mails erkennen und diese entweder schon auf dem E-Mail-Server oder auf dem Computer des Nutzers herausfiltern. Auch die gefälschten Webseiten sind zu erkennen, da im Regelfall die Adresse in der Adressleiste nicht die der Bank sein wird, die **Verschlüsselung nicht aktiviert** ist und die Seite kein gültiges, von der Bank ausgegebenes Authentifizierungszertifikat besitzt (Verschlüsselung und Zertifikat können allerdings

auf verschiedene Weise vorgetäuscht werden). Auffällig ist auch, dass auf den gefälschten Seiten überwiegend sofort die Eingabe von PIN und mehreren TANs gefordert wird, wobei auch hier andere, geschicktere Gestaltungen möglich sind. Den besten Schutz vor Phishing bietet daher schlicht die Beachtung der inzwischen von allen Banken ausgegebenen goldenen Regel:

„Geben Sie niemals auf telefonische Anfrage (Ausnahme: Telefon-Banking) oder auf eine E-Mail-Anfrage PIN oder TAN heraus!“

Phishing hinterlässt ebenfalls Spuren auf dem Computer des Betroffenen. Neben der Phishing-E-Mail kann anhand der Verlaufsprotokolle und temporären Dateien des Internet-Browsers meist noch relativ lange nachvollzogen werden, welche Webseiten aufgesucht worden sind.

4.4.4 Pharming

Das ebenfalls bekannte „Pharming“ funktioniert wie folgt: Ruft der Kontoinhaber die Website seiner Bank auf, wird die Verbindung auf eine gefälschte Seite der Täter umgeleitet. Dies ist möglich, da es sich bei den üblichen Internetadressen (z. B. www.finanzgruppe.de) nur um eine „Übersetzung“ der eigentlichen Identifikation von Computern im Internet durch die sogenannte IP-Adresse, eine Kombination aus vier Zahlenblöcken von 0 bis 255, handelt. Die „Übersetzung“ erfolgt durch den Domain-Name-Service (DNS) entweder auf dem heimischen Computer des Nutzers in einer lokalen Host-Datei oder durch einen Name-Server. An beiden Stellen können Kriminelle ansetzen: Entweder wird die lokale Host-Datei durch Malware oder Webseiten mit Schadsoftware ausgetauscht oder verändert oder der Eintrag auf dem Name-Server wird verändert. Dies wird Pharming genannt, da es Tätergruppen gibt, die hierzu ganze „Serverfarmen“ betreiben.

Die Veränderung der lokalen Datei kann durch **Antivirenprogramme** und die Vornahme bestimmter **Sicherheitseinstellungen im Internet-Browser** unterbunden werden. Auch wenn die aktuellen Versionen der im Internet verwendeten Kommunikationsprotokolle den Tätern das Pharming erschweren, gibt es hingegen keinen wirksamen technischen Schutz gegen Täter, die Name-Server „kapern“ oder manipulieren. Zur Identifikation der gefälschten Website gelten die gleichen Regeln wie beim Phishing. Auch beim Pharming kann der Aufruf der Webseite der Täter im Regelfall auf dem Computer des Betroffenen nachvollzogen werden.

4.5 Haftung

Kommt es zu **Missbrauchsfällen im Onlinebanking,** stellt sich die Frage, wer hierfür haftet. Stellt der Kunde eine Kontobelastung aufgrund einer missbräuchlichen Verfügung fest, wird er sich regelmäßig an seine Bank wenden und um Erstattung des belasteten Betrages bitten. Nach allgemeinen **Beweisgrundsätzen** muss dann die Bank nachweisen, dass der Kunde den Auftrag (z. B. zur Ausführung einer Überweisung) erteilt hat. Eine solche Beweisführung ist der Bank regelmäßig durch die im Onlinebanking geführten Protokolle (Aufzeichnung der Verwendung von PIN und TAN) möglich. Bestreitet der Kunde indes begründet die Erteilung des Auftrags und trägt er z. B. vor, dass er Opfer eines Phishing- oder Pharming-Angriffs geworden ist, steht der Bank in der Regel kein Aufwendungsersatzanspruch gegen den Kunden zu, da in diesen Fällen der Kunde eben gerade nicht selbst den Auftrag autorisiert hat.

Die Bank ist dann zur **Rückgängigmachung der Belastungsbuchung** aus dem nicht autorisierten Auftrag verpflichtet. Dem Erstattungsanspruch des Kunden stehen aber ggf. Schadensersatzansprüche der Bank gegenüber, wenn der Kunde gegen die mit ihm in den Onlinebanking-Bedingungen vereinbarten **Sorgfaltspflichten** verstoßen hat und dadurch ein Schaden entstanden ist. Denn dann kann die Bank im Rahmen einer gerichtlichen Auseinandersetzung mit ihrem gegen den Kunden bestehenden **Schadensersatzanspruch** gegen den Erstattungsanspruch des Kunden aufrechnen, sodass die bereits erfolgte Erstattung wieder rückgängig gemacht werden kann.

Wie bereits ausgeführt, ist nach den mit dem Kunden vereinbarten Onlinebanking-Bedingungen die **Haftung des Kunden nach der Sperranzeige** ausgeschlossen und **vor der Sperranzeige** grundsätzlich auf **50 Euro** begrenzt. Diese Grenze gilt allerdings nicht, wenn der Kunde seine **Sorgfaltspflichten beim Onlinebanking vorsätzlich oder grob fahrlässig verletzt** hat. In diesen Fällen haftet der Kunde nach den gesetzlichen Regelungen unbegrenzt. Zu seinen Gunsten ist in den Onlinebanking-Bedingungen jedoch vereinbart, dass seine Haftung selbst bei grober Fahrlässigkeit auf den für die Nutzung des Onlinebanking geltenden Verfügungsrahmen beschränkt ist. Beträgt also der Verfügungsrahmen beispielsweise 1.000 Euro pro Tag, haftet der Kunde selbst dann, wenn er sich grob fahrlässig verhält, lediglich in Höhe dieses Verfügungsrahmens.

Ob eine grobe Fahrlässigkeit des Kunden vorliegt, ist stets im Einzelfall zu bewerten. Anhaltspunkte bieten insoweit die mit dem Kunden in den Bedingungen für das Onlinebanking vereinbarten Sorgfaltspflichten.

*„**Grobe Fahrlässigkeit des Teilnehmers** kann insbesondere vorliegen, wenn er*

- *seine PIN nicht geheim gehalten hat, sie also beispielsweise per E-Mail oder SMS weitergegeben oder ungesichert elektronisch gespeichert hat,*
- *die im Rahmen einer Transaktion von der Bank z. B. auf dem Mobiltelefon angezeigten Transaktionen nicht mit den Daten des Auftrags abgeglichen hat, oder*
- *den Verlust seiner Authentifizierungselemente nicht unverzüglich der Bank oder dem Sperranzeigedienst angezeigt hat.“*

Insbesondere in den Fällen, in denen der Kunde **mehrere TANs** aufgrund einer Phishing-E-Mail oder beim Aufsuchen und Einloggen in die gefälschte Onlinebanking-Website eingegeben hat, geht die Rechtsprechung ganz überwiegend von einem grob fahrlässigen Verhalten des Kunden aus. Dabei wird stets betont, dass diese Angriffsvarianten mittlerweile allen, insbesondere internetaffinen Onlinebanking-Nutzern bekannt sein müssen.

4.6 Weitere Angriffsszenarien

Das Risiko, Opfer eines Missbrauchs im Onlinebanking zu werden, besteht immer dann, wenn **fremde Rechner** für das Onlinebanking genutzt werden. Denn Browser speichern Daten der letzten Verbindungen in einem Zwischenspeicher ab – dem sogenannten Cache. Wer Bankgeschäfte etwa im Internetcafé abwickelt, riskiert, dass Kriminelle später diese Informationen im Cache auslesen. Kann man nicht vermeiden, fremde Rechner zu nutzen, sollte der Cache des Browsers in jedem Fall im Anschluss an die Banking-Sitzung gelöscht werden.

Ein weiteres Risiko ist der Internetzugang über **öffentliche WLANs** (Wireless Local Area Network). Die Funkverbindung ist nur dann sicher, wenn der Datenverkehr ausreichend verschlüsselt ist, was bei einem öffentlichen WLAN schwer zu überprüfen ist.

Die Gefahren beim Onlinebanking beschränken sich nicht nur auf PCs. Inzwischen nehmen die Angreifer auch **Handys, Smartphones und**

Tablet-PCs ins Visier. Hier gelten grundsätzlich dieselben Sicherheitsvorkehrungen und Schutzmaßnahmen wie bei einem PC: Insbesondere regelmäßig Updates einspielen, um eventuelle Sicherheitslücken zu schließen. Zu beachten ist zudem, dass mobile Geräte leichter gestohlen werden können als stationäre PCs. Daher dürfen dort auf keinen Fall PIN oder TANs gespeichert werden. Zudem ist zwingend die Tastensperre mit Passwortschutz zu aktivieren. Mobile-Banking-Apps sollten nur über bekannte, seriöse App-Stores auf das Mobiltelefon geladen werden.

4.7 Tipps und Tricks für ein sicheres Onlinebanking

Unter Beachtung der folgenden Grundregeln lässt sich die Sicherheit des Onlinebanking deutlich verbessern – auch wenn es niemals einen vollkommenen Schutz geben wird.

4.7.1 WLAN-Verbindung verschlüsseln

Standard ist heute WPA2 (Wi-Fi Protected Access 2), wobei das Passwort mindestens 20 Zeichen lang sein sollte. WEP (Wired Equivalent Privacy) ist hingegen veraltet und gilt darum als unsicher.

4.7.2 Aktuelle Software verwenden

Es ist stets die aktuelle Software zu verwenden. Dies gilt für den Browser, das Antivirenprogramm und die Firewall. Dabei sollte die automatische Update-Funktion aktiviert werden.

4.7.3 Verschlüsselte Kommunikation: https://

Onlinebanking sollte immer über das geschützte https-Protokoll erfolgen. Ob das der Fall ist, kann man daran erkennen, dass sich der Anfang der Browserzeile verändert. Statt http:// wird dann https:// angezeigt. Bei der Verwendung der aktuellen Browsersoftware wird mittlerweile oftmals ein Zertifikat angezeigt, mit dem die Richtigkeit der Angaben des Servers, mit dem man verbunden ist, von einer unabhängigen Instanz, dem Zertifikathersteller, bestätigt wird. Hier ist zu überprüfen, ob der im Sicherheitszertifikat angegebene Name der Webseite mit dem Namen der aufgerufenen Adresse übereinstimmt. Dass eine Website zertifiziert ist, kann daran erkannt werden, dass nach der URL ein kleines „Schloss-Symbol“ angezeigt wird. Bei einem Klick auf das Schloss-Sym-

bol erhält der Nutzer mehr Informationen über das Zertifikat und ob die Website tatsächlich die ist, für die sie sich ausgibt.

Wenn ein Anbieter sich nicht mit einem gültigen Zertifikat als tatsächlicher Besitzer der Adresse ausweisen kann, erteilt der Browser eine Warnmeldung. In diesem Fall ist die Transaktion sofort abzubrechen und die Bank zu informieren.

4.7.4 Zugangsdaten sorgfältig auswählen und geheim halten

Vertraulichkeit ist beim Onlinebanking oberstes Gebot. PIN und TAN sind nicht für fremde Dritte bestimmt, sondern dienen nur dem Nutzer zur Legitimation und Autorisierung von Aufträgen. Zugangs- und Transaktionsdaten dürfen nicht elektronisch gespeichert werden. Es ist ein sicheres Passwort zu wählen. Bitte nicht das Geburtsdatum oder Ziffernfolgen wie 123456, 000000 oder ähnliche verwenden.

4.7.5 Echtheit der Bank-Website prüfen

Es ist zu überprüfen, ob man sich tatsächlich auf der Website der Bank befindet. Dazu sollte bei jedem Aufruf die Internetadresse der Bank über die Tastatur eingegeben werden. Auch minimale Abweichungen der Internetadresse – etwa Trennungspunkte oder Trennstriche – sind Zeichen für eine Fälschung. Generell verdächtig ist eine Seite, deren Adresse mit einer Nummer und keinem Domain-Namen beginnt (wie etwa http://1357.246.579/…).

Während einer Onlinebanking-Sitzung niemals:

- mehrere TANs für einen Auftrag eingeben;
- eine TAN zur Aufhebung einer angeblichen Kontosperrung eingeben;
- eine TAN zur Rücküberweisung einer (vermeintlich) eingegangenen Zahlung eingeben;
- eine TAN zur Anmeldung zu einem Demokonto eingeben;
- eine TAN zur Durchführung einer Testüberweisung eingeben;
- eine TAN zur Installation von Sicherheitszertifikaten oder Sicherheitssoftware/Apps eingeben.

4.7.6 Onlinebanking nur mit eigenen Geräten

Vorsicht ist insbesondere bei öffentlich zugänglichen Computern, wie etwa in Internetcafés, geboten. In jedem Fall ist nach dem Logout der Cache des PCs zu löschen.

4.7.7 Verfügungslimit minimiert das Missbrauchsvolumen

Durch ein Verfügungslimit kann sichergestellt werden, dass Kriminelle nicht unbemerkt hohe Summen von dem Konto abbuchen.

4.7.8 Kontobewegungen regelmäßig überprüfen

Sind Transaktionen zweifelhaft, ist die Bank umgehend zu informieren.

4.7.9 Auf Phishing-E-Mails nicht reagieren: Löschen!

Banken fordern ihre Kunden niemals per E-Mail dazu auf, vertrauliche Daten wie PIN, TAN oder Kontonummer bekannt zu geben.

4.7.10 Keine Weitergabe der Bankverbindung in sogenannten sozialen Netzwerken

Schon mit der Kontonummer/Bankleitzahl (IBAN/BIC) können Kriminelle unberechtigt Lastschriften ziehen.

4.7.11 Bei Verdacht: Sperren des Onlinebanking-Zugangs

Eine Sperre kann entweder telefonisch oder im Onlinebanking erfolgen.