Online-Banking

Leitfaden

BITKOM

Impressum

Herausgeber: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Steffen von Blumröder, Tel.: 030.27576-126, s.vonblumroeder@bitkom.org

Redaktion: Steffen von Blumröder

Gestaltung / Layout: Design Bureau kokliko / Matthias Winter (BITKOM)

Titelbild: © bloomua – Fotolia.com

Online-Banking

Leitfaden

BITKOM

Inhaltsverzeichnis

Danksagung

Besonderen Dank für die Entstehung dieser Publikation gilt der Arbeitsgruppe Mobile Payments & Banking Innovations des BITKOM Dialogkreises Banking & Financial Services. Insbesondere möchten wir den folgenden Personen für ihren Input danken:

Steffen von Blumröder
BITKOM e.V.

Andreas Ebner
GFT Technologies AG

Frank Schipplick
Sopra Steria GmbH

Marcus Weicht
KPMG

1 Executive Summary

Für fast drei Viertel (74 Prozent) der Bundesbürger sind Computer, Smartphone und Internet unverzichtbar geworden. Das hat eine repräsentative Umfrage zur Bedeutung digitaler Technologien im Auftrag des BITKOM ergeben. Im Vergleich dazu liegt die Nutzung von Online- und Mobile-Banking bei gerade mal 45 Prozent aller Bankkunden! Liegt dies daran, dass Online-/ Mobile-Banking Transaktionen als unsicher empfunden werden oder an einer generellen Unwissenheit über die nutzbaren Funktionalitäten und Sicherheitsverfahren?

Sicherheit steht auch durch die anhaltende Diskussion über Datenschutz und -Sicherheit nach wie vor an erster Stelle. Allerdings spielen gerade für jüngere Endverbraucher auch der Komfort und die User Experience eine zunehmend wichtigere Rolle. Kundennähe und komfortable Anwendungen werden jedoch in größerem Maße von vielen der aktuell diskutierten »FinTech« Start-ups angeboten und weniger von den klassischen Banken. Als FinTechs bezeichnet man Unternehmen, die technologische Lösungen und Plattformen im Finanzsektor anbieten – sich also eher als Technologieunternehmen mit Branchenfokus Finanzwelt verstehen.

Der Trend geht, vergleichbar mit anderen Branchen, zunehmend hin zum mobilen Kanal über Smartphone und Tablet. Dabei hinken die angebotenen Sicherheitslösungen der Banken aktuell dem Kundenverständnis eines komfortablen und nahtlosen Nutzererlebnisses hinterher. Generell sind die Funktionalitäten des Online-Banking mannigfaltig. Von Umsatzabfrage und Zahlungsverkehr, über Depot Verwaltung werden auch immer mehr Mehrwertdienste wie Personal Finance Management (PFM) oder Peer to Peer Zahlungen (P2P) angeboten.

Beim PFM ist es das Ziel verschiedene Konten und Karten entsprechend zusammenzuführen und nach individuellen Parametern auszuwerten, während P2P die Möglichkeit darstellt meiner Peer Group (Freundeskreis) einfach und unkompliziert Geld zu überweisen.

Die aktuellen Bedrohungsszenarien sind recht unterschiedlich. Phising und »Man-in-the-Middle-Angriffe« stehen hier im Vordergrund. Mit unserem Leitfaden möchten wir Ihnen einen Überblick über diese möglichen Szenarien bieten und Maßnahmen aufzeigen, wie man sich am besten schützen kann.

Wir stellen dazu die aktuellen Sicherheitsverfahren dar, die von Banken heute angeboten werden sowie deren Stärken und Schwächen. Für den Endverbraucher ist es wichtig in Bezug auf die möglichen Bedrohungsszenarien eine höhere Sensibilität zu entwickeln. Man kann sich den meisten Betrugsvarianten verhältnismäßig einfach erwehren, wenn man einige grundlegenden Regeln befolgt.

Dies sind grundsätzlich der richtige Umgang mit PIN, Pass- und Kennwort Kombinationen, deren Weitergabe an Dritte und der Schutz meiner Geräte mit entsprechender Anti-Viren / -Trojaner / -Phising Software, sowie die Nutzung moderner Transaktions-Verfahren.

BITKOM möchte mit dem Leitfaden helfen, dem Endkunden die Scheu vor Online- und Mobile-Banking Funktionalitäten und Verfahren zu nehmen und die Sensibilität für Bedrohungsszenarien zu erhöhen.

2 Einleitung

Kaum ein Tag vergeht, ohne dass in den Medien über Angriffe auf Bankkonten, Kreditkarten und Zahlungsdaten berichtet wird. Dabei ist die Berichterstattung immer recht einseitig, da kaum einmal ein Vergleich zwischen Angriffen im analogen und digitalen Leben gezogen wird. Darüber hinaus werden die kriminellen Zugriffe nicht ins Verhältnis sämtlicher Banktransaktionen gebracht.

Bankgeschäfte hat jeder zu erledigen, aber immer weniger Personen möchten dafür eine Bankfiliale aufsuchen. Bequemer geht es von zu Hause per Online-Banking. Eine BITKOM Studie zeigt, dass viele Verbraucher ihre Bankgeschäfte zunehmend über das Internet erledigen. Gut zwei von drei Internetnutzern (68 Prozent) in Deutschland ab 14 Jahren setzen auf Online-Banking. Das entspricht 37 Millionen Bundesbürgern.

Aber welche Technologie ist für den einzelnen am besten geeignet und am sichersten? Einfach im PC-Browser bei der Website der Bank einloggen? Oder doch lieber mit eine PC-Software alle Konten gemeinsam verwalten? Und für wen ist eine Banking-App auf Smartphone oder Tablet die beste Lösung?

Die Entscheidung hängt sehr von den Kundenanforderungen des Einzelnen ab. Viele Wege führen nach Rom und fast genauso viele inzwischen auch in mein Bankkonto. Mit dem vorliegenden Leitfaden möchten wir dem Leser einen einfachen Überblick über die Möglichkeiten bieten, die es derzeit gibt. Sicherheit hängt dabei jedoch auch zum großen Teil vom Nutzungsverhalten des Users ab!

Aus den aktuellen Zahlen des Bundeskriminalamtes (BKA) geht hervor, dass im vergangenen Jahr Phishing Attacken im Vergleich zu 2013 um 20 Prozent zugenommen haben. Mit dem Diebstahl digitaler Identitäten räumen Internetkriminelle wieder häufiger die Konten von Verbrauchern ab. Pro Fall entstand dabei ein durchschnittlicher Schaden von rund 4000 Euro. Beim Phishing versuchen Betrüger mit fingierten E-Mails von Banken oder anderen Finanzdienstleistern an die Zugangsdaten der Nutzer heranzukommen, um anschließend deren Konten abzuräumen.

Immer mehr Deutsche setzen zunehmend ihr Smartphone für alltägliche Dinge des Lebens ein und dies schließt inzwischen auch Bankgeschäfte mit ein. Gerade Banken ohne eigenes Filial- und Automatennetz können ihren Kunden durch mobiles Banking zusätzliche Dienstleistungen bieten. Jeder siebte Besitzer eines Smartphones (15 Prozent) prüft mobil seinen Kontostand, acht Prozent überweisen auf diese Art Geld von ihrem Bankkonto, aber nur ein Prozent handelt bis dato mit Wertpapieren. Dabei gibt es ein deutliches Ost-West-Gefälle: In Westdeutschland ist der Anteil der mobile Banker (18 Prozent der Smartphone-Besitzer) fast doppelt so hoch wie in Ostdeutschland (10 Prozent).

Zusätzlich zum Mobile-Banking würden viele Nutzer gerne sämtliche Zahlungsgeschäfte digital vornehmen und das Portemonnaie durch das so genannte Mobile Wallet auf dem Smartphone ersetzen. Von allen befragten Deutschen kann sich jeder Siebte (14 Prozent) vorstellen, auf sein Portemonnaie komplett zu verzichten und nur noch mit dem Smartphone zu bezahlen. Das sind knapp 10 Millionen Personen. Darunter sind überdurchschnittlich viele Männer (19 Prozent), Jüngere (23 Prozent aller Personen zwischen 14 und 29 Jahren) und Abiturienten (18 Prozent). Bei den Besitzern eines Smartphones ist es jeder fünfte (21 Prozent). Wir haben das Thema Mobile Payments/ Mobile Wallet bewusst aus diesem Leitfaden verband, da wir der Meinung sind das viele Anforderungen sehr unterschiedlich sind. Im aktuellen Mobile Wallet Leitfaden erfahren Sie mehr zu diesem sehr komplexen Ökosystem.

Leitfaden Mobile Wallet

Im nächsten Kapitel möchten wir Ihnen zunächst einen Überblick über die aktuelle Marktsituation in Deutschland und die technologischen Entwicklungen geben sowie die verschiedenen Übertragungskanäle vorstellen. Anschließend werden die wichtigsten Online-Banking Funktionalitäten dargestellt.

Kapitel 4 zeigt die wichtigsten Bedrohungsszenarien sowie die aktuellen und zukünftigen technologischen Authentifizierungs- und Sicherheitslösungen, die von den Banken angeboten werden, auf.

Bevor wir im letzten Abschnitt ein Fazit ziehen, gehen wir in Kapitel 5 kurz auf die fehlende Interoperabilität, sowie die einfachsten Verhaltensregeln ein, um sich vor Zugriffen auf sein Online-Banking Konto zu schützen.

3 Aktuelle Marktsituation und Online / Mobile-Banking Lösungen

Unter Online-Banking versteht man die Erledigung von Bankgeschäften über Datenleitungen mit Hilfe von PCs, Smartphones und anderen elektronischen Endgeräten. In den vergangenen Jahren ist der Anteil der Online-Banking Nutzer[1] stetig gestiegen.

3.1 Wettbewerbssicht im deutschen Retail Banking-Markt

Der deutsche Retail Banking-Markt ist im europäischen Vergleich das am heftigsten umkämpfte Marktsegment. In keinem anderen EU-Land sind so viele Wettbewerber aktiv. Gerade im Bereich des Online- oder Internetbanking streben immer noch neue Anbieter auf den Markt. Dies sind entweder kapitalstarke Ableger von Auslandsbanken oder Geschäftszweige von Unternehmen aus dem Bereich Non-Banking, die zur Erweiterung ihrer Wertschöpfungskette Bankdienstleistungen anbieten. Dies hat massive Auswirkungen auf Kosten und Gebühren von Bankprodukten und somit auf die Erträge von Retail Banken.

Im Wettbewerbsvergleich werden in der digitalen Welt, und dahin steuert auch das deutsche Online-Banking hin, die einzelnen Anbieter aus Kundensicht zunehmend austauschbarer. Die Loyalität der Kunden hängt immer mehr vom Service ab.

Für die Banken stellt dies bereits ein reelles Problem dar, denn die Zufriedenheit der Kunden mit ihrer Bank liegt in Deutschland aktuell bei durchschnittlich -13 Prozent[2]. Mit der weiteren Digitalisierung wird sich dieses Problem noch weiter verschärfen.

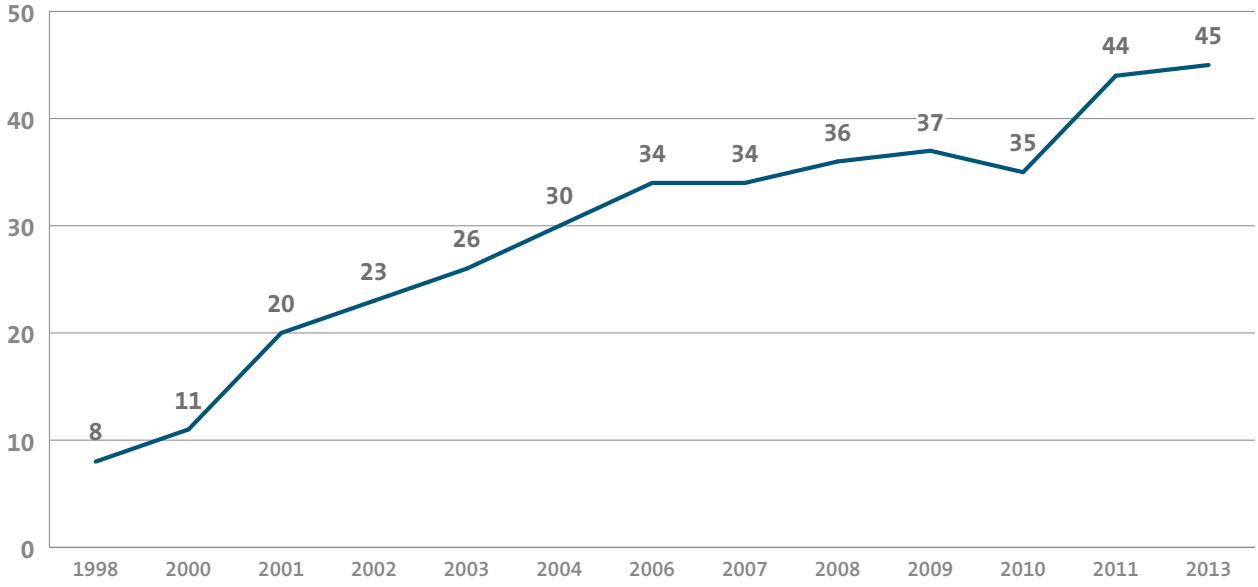


Abbildung 1: Anteil der Nutzer von Online-Banking in Deutschland in den Jahren 1998 bis 2013 in Prozent. (Basis: 1000 Befragte ab 18 Jahren. (Quelle: Bundesverband deutscher Banken © Statista 2014)

1 http://de.statista.com/statistik/daten/studie/3942/umfrage/anteil-der-nutzer-von-online-banking-in-deutschland-seit-1998/

2 Bain & Company, Studie zum Retail-Banking: Private Bankkunden sind unzufrieden wie nie zuvor, Juli 2012

Die Kundenzufriedenheit wird gemäß dieser Studie seit mehr als zehn Jahren mit dem Net Promoter® Score (NPS) gemessen. Diese Kennzahl ergibt sich aus den Antworten auf die Frage: »Auf einer Skala von null bis zehn, wie wahrscheinlich ist es, dass Sie diese Bank einem Freund oder Kollegen weiterempfehlen?« Die Antworten werden drei Kategorien zugeordnet. Dabei hat sich gezeigt, dass nur Werte von neun oder zehn für wirklich loyale Kunden stehen (»Promotoren«), sieben und acht eher »passiv Zufriedene« sind und Bewertungen von sechs oder weniger als »Kritiker« eingestuft werden müssen. Subtrahiert man den Anteil der Kritiker von dem der Promotoren, ergibt sich der NPS. Minuswerte bedeuten, es gibt weit mehr Kritiker als Anhänger.

3.2 Technologieentwicklung

Im Technologiebereich werden neue Endgeräte die Kommunikation mit den Banken im Online- und Mobile-Banking bestimmen.

Im Jahr 2003 war es im Wesentlichen noch ausreichend, dass das Online- Banking mit Microsoft-Produkten auf einem Computer funktioniert. Heute müssen neben dem klassischen Computer eine Vielzahl mobiler Endgeräte und deren Infrastrukturen unterstützt werden: Smartphones, Tablet PC's unter Windows, Mac OS, iOS und Android und den gängigen Browsern. Deshalb ist es für die Banken wichtig, mobile Strategien zu entwickeln und zielgruppengerichtet neue, interessante und im Wettbewerb differenzierende Kommunikationsformen im Beratungsbereich einzuführen.

In Deutschland ist Online-Banking als arriviert anzusehen. Durch die technologischen Entwicklungen befindet sich das deutsche Retail Banking aktuell im Wandel von Online-Banking zum Mobile-Banking. Durch diese Entwicklungen im Mobile-Bereich werden die Banken zusätzlich durch neue Konkurrenten in einem ihrer Stammmärkte, dem Zahlungsverkehr, angegriffen.

3.3 Übertragung der Daten über unterschiedliche Kanäle:

3.3.1 Browserbasiertes Internetbanking über die Website der Bank

Die meisten Banken bieten auf ihrer Internet Seite ein Online-Banking Zugang an, das heißt der Kunde benötigt nur einen Internet Browser. Das Portal der Bank wird über den Browser aufgerufen, die Seiten sind entsprechend den Sicherheitsanforderungen abgesichert. Um auf seine Konten zugreifen zu können, muss sich der Kunde einloggen.

Hiervon zu unterscheiden sind die browserbasierten Webangebote der Kontenaggregationsdienste wie beispielsweise MINT.com oder finanzblick.de. Diese können auf der HBCI- oder ähnlichen Schnittstellen (API) APIs basieren und sind damit in der Regel Multibankenfähig.

Moderne browserbasierte Internetbanking-Systeme zeichnen sich unter anderem durch Portal-Funktionen, Barrierefreiheit, verschiedene Sicherheitsmechanismen (z. B. gegen Phishing), Benachrichtigungsmöglichkeiten (z. B. bei Kontostandsänderung durch SMS oder E-Mail), sichere TAN-Verfahren sowie frei wählbaren Anmeldenamen aus.

3.3.2 Verwendung einer Software zur Durchführung des Online-Bankings (sog. Clientprogramm)

Das Hauptunterscheidungsmerkmal zu browserbasierten Lösungen ist die Multibankenfähigkeit der Clientsoftware. Diese wird in Deutschland durch FinTS umgesetzt.

FinTS steht für »Financial Transaction Services« und ist eine Weiterentwicklung des 1996 von der Deutschen Kreditwirtschaft (DK) veröffentlichten Online-Banking Standards: »Homebanking Computer Interface (HBCI)«. Dieses Protokoll wird für die Abwicklung der Geschäftsvorfälle von den Programmen genutzt.

Damals wie heute ist das Ziel dieses Standards die Vereinheitlichung der Schnittstelle zwischen dem Bankkunden – z. B. repräsentiert durch seine Finanzverwaltungs-Software – und einem oder mehreren Kreditinstituten in identischer Weise. Derzeit unterstützen ca. 2000 Kreditinstitute FinTS.

Herausragende Merkmale von HBCI/FinTS sind die Bankenunabhängigkeit, die Providerunabhängigkeit und die öffentliche Verfügbarkeit des Standards. Dadurch ist es prinzipiell jedem Programmierer oder Softwarehersteller möglich, eine Implementierung der Client-Seite von HBCI zu erstellen und damit auf alle HBCI-fähigen Banken zuzugreifen. Der Standard sieht dazu mehrere Möglichkeiten der Authentifizierung vor. Inzwischen stellen eine Vielzahl von Anbietern die notwendigen Softwarebausteine bereit.

HBCI/FinTS kann ohne zusätzliche Hardware, alleine mit PIN und TAN (verschiedene TAN-Verfahren werden unterstützt) arbeiten. Kryptographische Schlüssel werden dann z. B. in Dateien gespeichert. Bei der Eingabe wird eine Datenverbindung vom Computer zur Bank aufgebaut. Diese Verbindung nutzt je nach HBCI-Version entweder ein eigenes HBCI-Protokoll oder das für Websites übliche Protokoll HTTPS.

Einen höheren Sicherheitsstandard bietet HBCI/FinTS mit einer Chipkarte. Der Schlüssel wird hierbei von der Chipkarte selbst erzeugt und ausschließlich auf dieser gespeichert.

EBICS ist die Erweiterung des Banking Communication Standard (BCS) für die Kommunikation über das Internet unter Verwendung von elektronischen Unterschriften. Es ist der Multibankenstandard für das Firmenkundengeschäft über das Internet.

3.3.3 Apps

Um Online-Banking mit Apps zu nutzen, ist es notwendig die Mobile-Banking Apps auf dem mobilen Endgerät zu installieren. Dies kann beispielsweise ein Smartphone, eine Smartwatch oder ein Tablet sein.

Die Apps verschlüsseln die Daten der Transaktion und schicken diese über das Internet zu den Banken. Einige Mobile-Banking Apps haben im Vergleich zum Online-Banking via PC eine eingeschränkte Funktionalität. Dies kann mehrere Gründe haben. Wenn der Kunde beispielsweise das mTAN-Verfahren zur Autorisierung von Zahlungen nutzt, kann das Smartphone nicht für Zahlungen benutzt werden da keine Kanaltrennung besteht. Andererseits kann es sein das mobile Endgeräte zu klein oder von der Leistung zu schwach sind um die Funktionalitäten abbilden zu können.

Einige Mobile-Banking Apps stellen Funktionalitäten wie QR Code Erkennung, Foto-Überweisung oder Filialfinder bereit.

- Fotoüberweisung App

  Da viele Unternehmen Rechnungen in Papierform mit beigelegtem Überweisungsschein verschicken, müssten die benötigen Transaktionsinformationen in das Online-Banking getippt werden. Um dies zu vereinfachen wurden Fotoüberweisung Apps für Smartphones entwickelt. Mit diesen Apps können entweder die Papierüberweisungsträger oder die komplette Rechnung fotografiert werden. Dabei werden die Daten automatisch in die Online-Banking Transaktion übernommen.

- QR Code App

  Eine Alternative zu der Fotoüberweisung App stellt die QR Code App dar. Um sich die Beilage des Überweisungsträgers zu sparen, senden viele Unternehmen einen QR Code auf ihren Rechnungen mit. Dieser QR Code kann mit einer entsprechenden App ausgelesen werden und die Online-Überweisung wird mit den entsprechenden Daten gefüllt.

3.4 Überblick über die wichtigsten Funktionalitäten

3.4.1 Abwicklung des Zahlungsverkehrs

Bis dato besteht eine der Hauptfunktionalitäten des Online-Banking in der Abwicklung des Zahlungsverkehrs. Dies bedeutet, dass Überweisungen, Lastschriften, Daueraufträge bequem online ausgefüllt und freigegeben werden können.

Beispiele für Geschäftsvorfälle die für Privat- und Geschäftskunden über Online-Banking abgewickelt werden können sind:

- SEPA Überweisungen (Einzel- / Sammel-)
- Auslandsüberweisungen außerhalb des SEPA Raums
- SEPA Lastschriften (Einzel- / Sammel- und Basis- / B2B-)
- Daueraufträge (Einrichtung, Löschung, Änderung)
- Kontoauszüge (Umsätze und Saldenabfrage)
- Terminierte Aufträge
- Umbuchungen auf Unterkonten sowie Überträge
- Lastschriftrückgaben

3.4.2 Umsätze / Finanzübersicht / Finanzstatus

In der Finanzübersicht werden die bestehenden Konten des Kunden mit Kontoständen angezeigt. Damit hat der Kunde eine Übersicht über seine finanzielle Situation. Sollte der Kunde dazu eine FinTS Software verwenden, kann er institutsübergreifend die Salden und Umsätze abrufen. In der Umsatzanzeige stellen die meisten Institute mittlerweile die Umsätze der letzten 180 bis 360 Tage zum Abruf bereit sowie meist auch die Vormerkposten und angekündigte Lastschriften. Zusätzlich kann nach eigenen Kriterien selektiert werden. Es können z. B. nur Umsätze eines bestimmten Monats angezeigt werden.

Der Finanzstatus sollte idealerweise nicht nur die laufenden Kontokorrentkonten enthalten sondern beispielsweise auch Sparkonten, Kreditkarten, Kredite und Depots. Der Bereich des Finanzüberblicks steht durch die Einführung von sogenannter Personal Finance Management (PFM) Software augenblicklich vor großen Veränderungen. PFM ist die Weiterentwicklung des Online-Banking hin zu einem personalisierten Portal. Merkmale sind unter anderem:

- Automatische Kategorisierung der Kontoumsätze
- Aggregation verschiedener Konten, sodass der Kunde auf einem Dashboard einen schnellen Überblick über seine finanzielle Situation bekommt
- die Möglichkeit, Budgets zu erstellen und Sparziele zu definieren
- Reporting der Einnahmen und Ausgaben erhalten

Auf PFM als innovative Weiterentwicklung des Online-Banking gehen wir in einem späteren Kapitel nochmals ein.

3.4.3 Wertpapiere

Manche Banken bieten auch an, die Vermögensverwaltung in das Online-Banking zu integrieren, um neben den Zahlungsfunktionen auch Depots zu verwalten. Es können reine Informationen wie Wertentwicklung, Umsätze, Kursabfragen, Depotaufstellungen und Hintergrundinformation zu den jeweiligen Aktien oder aber auch das sogenannte Trading beinhaltet sein, das heißt der Handel mit Wertpapieren.

3.4.4 Selbstbedienungsfunktionalitäten und Mehrwertservices

Als Beispiel für die sogenannten »Self Services« könnte man Lastschriftrückgaben nennen. Hierzu muss der Kunde dann nicht mehr die Bank kontaktieren, sondern kann direkt in der Umsatzanzeige Lastschriften zurückgeben. Darüber hinaus kann auch die gesamte Mandatsverwaltung für erteilte Mandate oder für gesperrte Lastschrifteinreicher (z. B. wenn Kunden bestimmte Gläubiger IDs für Lastschriften sperren möchten) einfach administriert werden.

Banken können in das Online-Banking auch bankenferne Mehrwertdienste wie beispielsweise das Aufladen von Prepaidkarten für Mobiltelefone oder Geschenkgutscheine für Händler wie Otto, Zalando oder Amazon integrieren. Aus unserer Sicht ist dies ein Feld, indem sich Banken deutlicher voneinander abgrenzen und somit Mehrwerte generieren könnten.

Außerdem kann es als Ausgangspunkt für weitere Produktabschlüsse genutzt werden, beispielweise für die Beantragung von Krediten.

3.4.5 Postbox

In der Postbox werden Kontoauszüge, Kreditkartenabrechnungen und wichtige Meldungen der Bank meist im PDF Format hinterlegt. Von dort können diese durch den Kunden jederzeit heruntergeladen werden.

Die Postbox wurde von einigen Banken schon zum e-Tresor (als Dokumentenverwaltung) erweitert. Das heißt, der Kunde kann dort wichtige Dokumente hochladen und sicher in der (Bank-) Cloud verwahren.

In Zukunft könnten in solchen Nachrichtenboxen auch e-Rechnungen gespeichert und weiterverarbeitet werden. Dies wird in der Schweiz schon praktiziert.

3.4.6 Autorisierungsverfahren

Um Zugang zu einem Online-Banking System zu erlangen oder eine Zahlung aus dem Online-Banking Konto zu genehmigen, werden Autorisierungsverfahren benötigt. Die wichtigsten haben wir in diesem Kapitel aufgeführt.

Normalerweise handelt es sich um PIN / TAN – Verfahren, d.h. eine User Identifizierung und eine Transaktionsnummer als Einmalpasswort, meist sechsstellig.

3.4.7 Schnittstellen

Die Online-Banking Systeme sollten Export- und für Personal Finance Managment Programme idealerweise auch Importfunktionalitäten beinhalten. Es gibt mittlerweile Anbieter, die eine automatische Sicherung der Transaktionsdaten in der Cloud (beispielsweise bei Dropbox oder Google Docs) anbieten.

In Zukunft werden die Banken verstärkt auf offene Plattformen setzen müssen, die wiederum auf offenen Standards und APIs (Application Programming Interface) basieren. Durch diese Standardisierung wird es leichter werden neue Funktionalitäten ein- und gegebenenfalls Drittanbieter anzubinden.

Es gibt mittlerweile auch Zahlverfahren die auf die Online-Banking Plattformen der Banken aufsetzen. In Deutschland beispielsweise giropay oder Sofortüberweisung. Auf europäischer Ebene sind die wichtigsten Player iDeal (Niederlande), eps (Österreich), myBank (Frankreich, Italien, Belgien). MyBank bietet beispielsweise auch e-ID (Identifikationsdienste für Webservices) und e-mandate basierend auf Online-Banking an.

3.5 Zusammenfassung

Neue Technologien und Wettbewerber spielen auch im Bereich des Online-Banking eine zunehmend größere Rolle. Der wichtigste Kanal wird in Zukunft das Smartphone mit seinen zahlreichen Apps sein. Banken müssen hier darauf achten, dass sie dem Endverbraucher neben Sicherheit auch ein gewisses Maß an Komfort und User Experience bieten. Viele Funktionalitäten können zwar auch über das Online-Portal der Hausbank bezogen werden, diese sind jedoch oftmals etwas hölzern in der Usability. Viele Wettbewerber bieten eine deutlich moderner wirkende Oberfläche und teilweise auch Multibankenfähigkeit – sprich der Endverbraucher kann hier unterschiedliche Konten und Optionen abbilden.

4 Bedrohungsszenarien und aktuelle Sicherheitslösungen

Der vermehrte Einsatz von modernen Smartphones für das Online- und/ oder Mobile-Banking erfordert eine neue Sicht auf die Sicherheit. Internetfähige mobile Endgeräte verändern das Verhalten der Verbraucher grundlegend – auch beim Online-Banking. Gerade die jüngere Generation bevorzugt Tablets und Smartphones, während Ältere und Geschäftskunden den PC benutzen.

Wir möchten die wichtigsten Verfahren darstellen und Stärken und Schwächen aufzeigen. Es ist wichtig darzustellen, dass nicht alle dieser Verfahren mit mobilen Geräten möglich sind. Anbieter sollten zukünftig daher bei der Implementierung neuer Sicherheitsverfahren darauf achten, dass die Verfahren sowohl mit mobilen Endgeräten als auch PCs funktionieren.

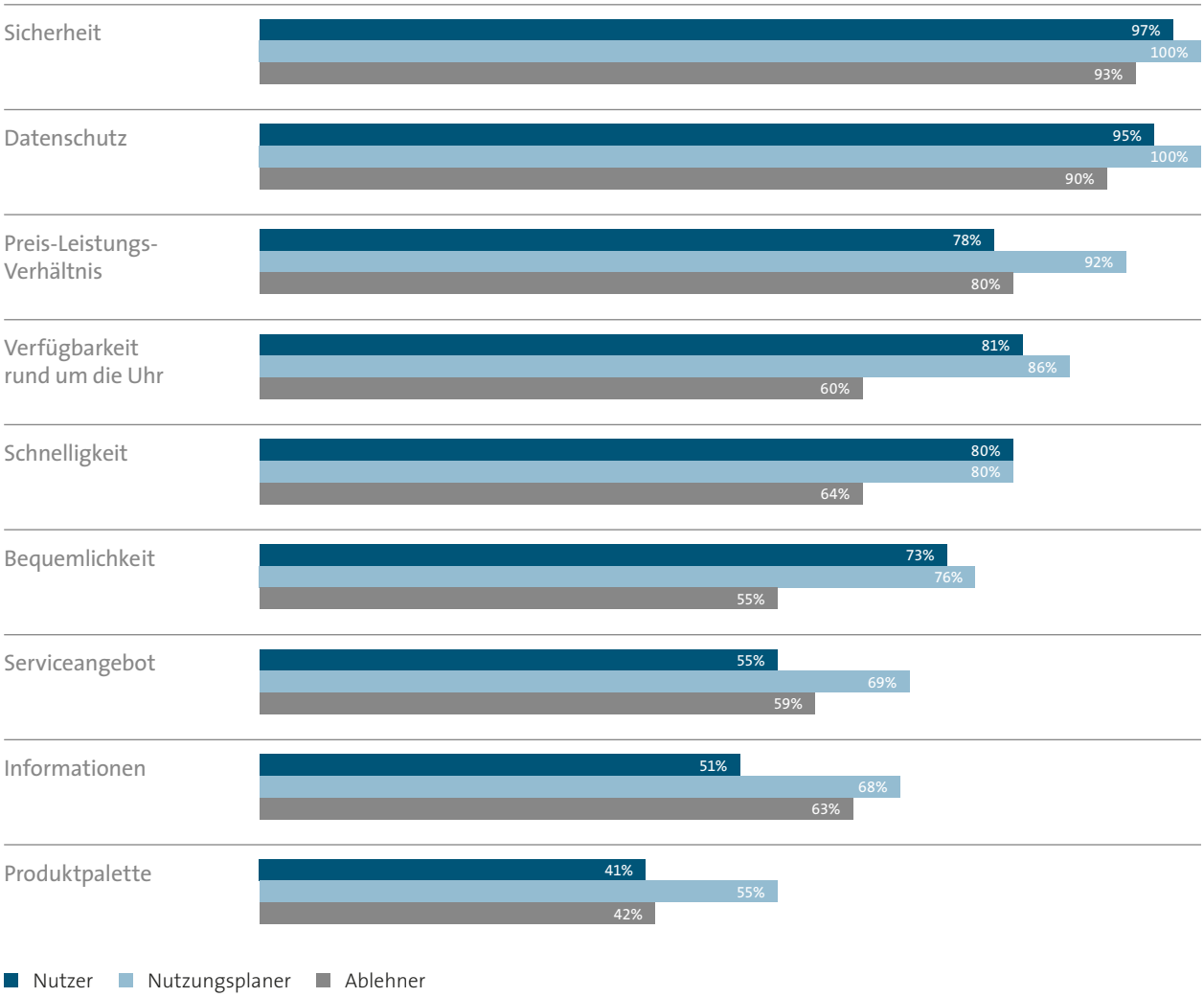


Abbildung 2: Aktuelle Wichtigkeit 2014. (Basis: Online-Banking-Nutzer: n=755; Nutzungsplaner: n=47; Online-Banking-Ablehner: n=184. Top2-Werte Skala 1=unwichtig bis 5= äußerst wichtig. Quelle: d21 Fiducia Studie Online-Banking Sicherheit)

Erschwerend kommt hinzu, dass beim Großteil der Kunden noch kein Problembewusstsein im Zusammenhang mit Online-Banking Applikationen auf mobilen Endgeräten zu erkennen ist. Die meisten Benutzer haben ihr Gerät weder passwortgeschützt, noch einen Virenscanner auf dem Smartphone oder Tablet installiert.

Wie der Studie »Online-Banking Sicherheit«[3] der Initiative d21 und Fiducia entnommen werden kann, steht die Sicherheit und der Datenschutz nach wie vor an höchster Stelle der Benutzer des Online-Banking während die Bequemlichkeit nur auf dem fünften Platz in der Skala liegt.

Die Schlussfolgerung sollte also sein, ein möglichst sicheres Online-Banking anzubieten, dabei aber die Bequemlichkeit nicht zu vernachlässigen. Mehrwerte lassen sich zukünftig nur durch eine kundenfreundliche Benutzeroberfläche generieren.

Beispielsweise könnten verschiedene Sicherheitsstufen eingeführt werden, je nach Risiko der Transaktion. Ein Übertrag auf das eigene Unterkonto könnte bei einer Bank beispielsweise ohne TAN ausgeführt werden, während Auslandsüberweisungen vor allem in exotische Länder nur mit einer sicheren Authentisierung erfolgen können.

4.1 Gefährdungs- und Bedrohungsszenarien /-Muster

In der Diskussion muss man zwischen der Sicherheit der eigentlichen Datenübertragung zur oder von der Bank und der Abwicklung am heimischen PC unterscheiden.

Bei allen Browser- und Client-basierten Electronic Banking-Systemen ist eine Verschlüsselung der Datenübertragung seitens der Banken gewährleistet. Diese ist nach menschlichem Ermessen nicht – oder nur unter erheblichem Zeit- und Ressourcenaufwand – manipulierbar. Das Übertragungsprotokoll HTTPS kann verschiedene Verschlüsselungsalgorithmen nutzen, die unterschiedlich sicher sind. Beim Verbindungsaufbau handeln Webbrowser und Banken-Server den Verschlüsselungsalgorithmus aus, wobei die meisten Banken mit dem Advanced Encryption Standard mit 256 Bit (Stand 2009) oder 512 Bit (2014) langen Schlüsseln arbeiten.

Die erste Angriffsmöglichkeit für einen Betrüger ist der heimische PC. So sollten Computer immer durch einen aktuellen Virenscanner und eine Firewall gesichert werden, um die Verbreitung von Schadprogrammen wie z. B. Viren, Keyloggern oder Trojanern zu unterbinden. Mit solchen Schadprogrammen wäre z. B. die Fernsteuerung des Computers möglich.

Durch Phishing und Pharming wird versucht, direkt an die zur Auftragsunterzeichnung notwendigen Daten (z. B. PIN / TAN) zu gelangen. Jeder Bankkunde kann sich bereits dadurch schützen, wenn die von den Banken zur Verfügung gestellten Zugangsberechtigungen nicht weitergegeben bzw. im Computer hinterlegt werden.

Denkbar wäre auch eine Manipulation des Domain Name Systems zur Umsetzung der URL einer Online-Banking Seite auf die IP-Adresse eines Angreifers (DNS-Spoofing). Dadurch würde der Webbrowser auf einen anderen Webserver geleitet, obwohl die richtige URL eingetippt wurde.

Einen aufwendigeren Angriff auf das Online-Banking stellt der »Man-in-the-Middle-Angriff« dar, bei dem der Angreifer sich zwischen Nutzer und Bank schaltet. Es ist also eine direkte Überwachung des Datenverkehrs in Echtzeit erforderlich. Entsprechende Angriffe werden etwa über Trojaner auf dem Rechner des Benutzers ausgeführt. 2012 empfahl die Europäische Agentur für Netz- und Informationssicherheit daher allen Banken die PCs ihrer Kunden grundsätzlich als infiziert zu betrachten und deshalb Sicherheitsverfahren zu verwenden, bei denen der Kunde noch einmal unabhängig vom PC die tatsächlichen Überweisungsdaten kontrollieren kann, wie etwa mTAN oder Smartcard-basierten Lösungen mit eigenem Kontrolldisplay wie chipTAN.

3 http://www.initiative21.de/wp-content/uploads/2013/01/studie_onlinebanking_fiducia_2013.pdf

Beim Mobile-Banking über Smartphone haben wir die Problematik ungeschützter Geräte. Meistens haben die Smartphones oder Tablets kein Antivirusprogramm installiert. Ein weiteres Problem können Passwörter darstellen. In den allermeisten Fällen sind entweder das komplette Smartphone oder die App in keiner Weise geschützt.

4.2 Aktuelle Authentifikations- und Sicherheitsverfahren

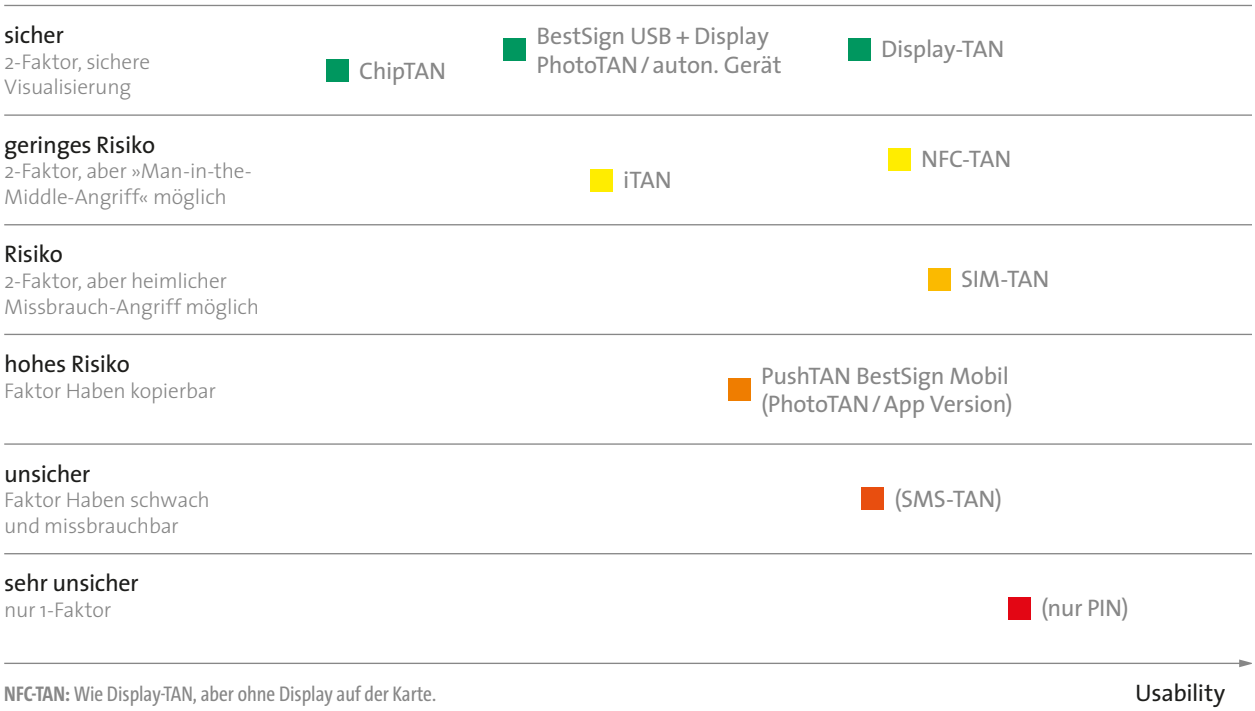
Die klassische TAN-Liste zur Autorisierung von Zahlungen haben wir nicht mehr mit aufgeführt, sie wird aus Sicherheitsgründen nicht mehr verwendet. Auch die iTAN wird mittlerweile als relativ unsicher angesehen und sollte bald von keiner Bank mehr verwendet werden. In Kapitel 5 gehen wir dann auf neue Sicherheitsverfahren ein. Anbei eine Übersicht über die aktuellen und gängigen Sicherheitsverfahren, die von den meisten Banken angeboten werden. Jeder Endnutzer sollte sich bei seiner Bank informieren, welches für ihn zur Verfügung steht.

4.2.1 User Identifizierung (Alias / email / Kontonummer) und PIN

Bei diesem Autorisierungsverfahren wird nur der Login für das Online-Banking Portal benötigt. Einmal eingeloggt werden keine weiteren Sicherheitsabfragen benötigt. Dies ist ausreichend für z. B. Umsatzabfragen oder den Zugang zur Nachrichtenbox.

4.2.2 iTAN

Eine Weiterentwicklung des klassischen TAN-Verfahrens ist das Verfahren der indizierten Transaktionsnummern, kurz iTAN. Der Kunde kann hier die Transaktion nicht mehr mit einer beliebigen TAN aus seiner Liste legitimieren, sondern wird von der Bank aufgefordert, eine bestimmte, durch eine Positionsnummer (Index) gekennzeichnete TAN aus seiner zu diesem Zweck nun durchnummerierten Liste einzugeben. Der TAN-Aufforderung muss der Kunde innerhalb weniger Minuten folgen. Außerdem wird die



NFC-TAN: Wie Display-TAN, aber ohne Display auf der Karte.
Push-TAN etc.: Bank-Credential liegt im Speicher des Smartphones. Extra-Passwort, deshalb schlechtere Usability-Bewertung.
SIM-TAN: Wie Push-TAN, aber Bank-Credential liegt auf SIM-Karte, Secure-Element oder Hardware-Keychain. Kein Extra-Passwort.
iTAN: Ist eventuell als zu sicher bewertet, aber es ist und bleibt ein echtes 2-Faktor Verfahren mit Benutzer-Involvierung.

Abbildung 3: Mobile Banking Sicherheit. (Quelle: GFT / Uni Tübingen)

angeforderte TAN auch im Falle einer Nichtverwendung im entsprechenden Computersystem der Bank als verbraucht gekennzeichnet.

Auch das iTAN-Verfahren kann inzwischen nicht mehr als ausreichend sicher eingestuft werden. Bereits 2009 berichtete das Bundeskriminalamt, dass es im Jahr 2008 1.800 erfolgreiche Phishing-Angriffe, die in der Regel durch Einschleusung von Trojanern erfolgten, registriert hat.

Für das iTAN-Verfahren gibt es zwei verschiedene Angriffsweisen:

1. Durch Einblenden eines Formulars innerhalb des Online-Banking-Systems wird der Bankkunde zur Eingabe mehrerer TANs inklusive Index-Nummer aufgefordert. Teilweise fragt die Schadsoftware die freien Plätze der TAN-Liste ab und gibt die entsprechenden Index-Nummern vor.

2. Bei einem »Man-in-the-Middle-Angriff« schaltet sich die Schadsoftware automatisch ein, sobald der Kunde eine Überweisung tätigen will. Die Schadsoftware tauscht im Hintergrund die Überweisungsdaten aus; mit der angeforderten TAN bestätigt der Bankkunde also in Wirklichkeit die betrügerische Überweisung des Hackers. Auf seinem PC-Bildschirm sieht er immer noch seine Original-Überweisung. Selbst die Umsatzanzeige und der Kontosaldo werden durch die Schadsoftware manipuliert.

Um das Sicherheitsniveau zu verbessern, wurde das iTAN-plus-Verfahren eingeführt. Bei diesem Verfahren wird vor Eingabe der iTAN ein Kontrollbild angezeigt, in welchem sämtliche Transaktionsdaten noch einmal aufgeführt werden. Außerdem wird als digitales Wasserzeichen das Geburtsdatum des Kontoinhabers angezeigt.

Dadurch soll ein automatisches Generieren eines manipulierten Kontrollbildes durch einen Angreifer erschwert werden. Nachteil dieses Verfahrens ist die Verschlechterung der Ergonomie, da das Kontrollbild schwieriger zu lesen ist als die Aufforderung zur iTAN-Eingabe in normaler Textform.

TAN mit Bestätigungsnummer

Das Verfahren kann um eine Bestätigungsnummer (BEN) erweitert werden, mit der die Bank die Transaktionsannahme im Gegenzug quittiert.

Phishing-Angriffe fallen mit diesem Verfahren auf, da keine korrekten BENs zurückgegeben werden. Um einen erfolgreichen »Man-in-the-Middle« durchzuführen, muss dieser fast in Echtzeit stattfinden.

4.2.3 SMS-TAN/ M-TAN

Die Variante des Mobile TAN (mTAN) oder auch sms-TAN genannt, besteht aus der Einbindung des Übertragungskanals SMS. Dabei wird dem Online-Banking-Kunden nach Übersendung der ausgefüllten Überweisung im Internet seitens der Bank per SMS eine nur für diesen Vorgang verwendbare TAN auf sein Mobiltelefon gesendet. Der Auftrag muss anschließend mit dieser TAN bestätigt werden.

Durch den SMS-Versand der TAN gilt mTAN sicherer als das iTAN-Verfahren. Dadurch, dass die Gültigkeitsdauer der TAN begrenzt ist und zusätzlich noch Teile der Ziel-Kontonummer der Überweisung, sowie des Überweisungsbetrages in der SMS übertragen werden und die TAN nur für diese Transaktion gültig ist, soll eine Umleitung auf ein anderes Konto durch einen »Man-in-the-Middle-Angriff« auf die Homebanking-Websites verhindert werden. Auch werden Phishing-Angriffe auf TANs im mTAN-Verfahren erschwert.

Als Vorteil wird angesehen, dass man für Transaktionen unterwegs keine TAN-Liste dabei haben muss. Erfahrungsgemäß wird auch der Verlust des Mobiltelefons eher vom Nutzer bemerkt als der Verlust der Bankkarte oder des TAN-Bogens. Zusätzlich erfährt der Nutzer womöglich per SMS von unautorisierten Überweisungsversuchen, sodass eine Sperrung des Kontos veranlasst werden kann.

Da moderne Smartphones fast überwiegend mit Internetzugang ausgestattet sind, hat das mTAN-Verfahren grundsätzliche Schwächen. Zum einen ist es anfällig

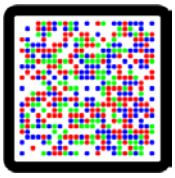
für Phishing-Angriffe, zum anderen wird die Sicherheit deutlich reduziert, wenn die mTAN auf dasselbe Gerät gesendet wird, das auch für das Online-Banking genutzt wird. Bei einem Verlust des Mobiltelefons besteht zudem der einzige Schutz vor missbräuchlichen Transaktionen in den Zugangsdaten zum Banking. TAN-Generatoren bieten in dieser Hinsicht wesentlich mehr Sicherheit, da das Gerät nicht vernetzt ist und für die Nutzung zusätzlich die Chipkarte benötigt wird.

Darüber hinaus kann auf einem Smartphone auch ein Trojaner, der die Kontrolle über das System übernimmt, zuerst Benutzernamen und Passwort des Online-Bankings abhören und anschließend vollautomatisch Überweisungen durchführen, indem er sich erst ins Online-Banking einloggt, dann eine Überweisung ausfüllt, anschließend die SMS der mTAN abfängt und damit die Überweisung legitimiert. Es reicht also für einen Trojaner ein einmaliges Einloggen beim Online-Banking über das Smartphone damit diese Sicherheitslücke ausgenutzt werden kann. Das funktioniert auch, wenn der Angreifer Benutzernamen und Passwort des Online-Bankings auf einem anderen Wege in Erfahrung gebracht hat, z. B. durch einen Trojaner auf dem PC.

Im Dezember 2012 wurde berichtet, dass durch den Trojaner ZeuS bereits über 36 Millionen Euro erbeutet worden sind. Der Trojaner nutzt unter anderem das mTAN Verfahren aus.

Eine weitere Schwachstelle ist die mit der Rufnummer verknüpfte SIM-Karte des Mobiltelefons. Diesbezüglich wurden Angriffe bekannt, bei denen mithilfe erbeuteter Nutzerdaten die Rufnummer des Opfers auf eine neue SIM-Karte portiert oder von den Angreifern eine Zweit-SIM angefordert wurde, mit der sie anschließend das mTAN-Verfahren aushebeln konnten.

4.2.4 photoTAN



Bei dem recht neuen photoTAN Verfahren werden die Transaktionsdaten verschlüsselt als mehrfarbige Mosaikgrafik auf dem Bildschirm angezeigt. Mit einer entsprechenden Smartphone-App wird dieser Code eingelesen und entschlüsselt, die Transaktionsdaten zur Kontrolle auf dem Smartphone angezeigt und die zugehörige TAN generiert. Die so generierte TAN wird dann zur Freigabe der Transaktion eingegeben.

Für die PhotoTAN in der App Version gibt es eine schlechte Sicherheitsbewertung wegen der möglichen Smartphone-Trojaner, die einfach das in der App abgespeicherte Credential der Bank kopieren, und zusammen mit den ebenfalls auf dem Smartphone abgehörten Passwörtern (bei PushTAN zwei) per Internet an ihren Trojaner-Master schicken, der dann alles hat, um eine beliebige Betrugs-Überweisung auszuführen.

Die erzeugten Transaktionsnummern sind auftragsbezogen und zur Entschlüsselung ist eine vorherige Aktivierung (Signierung) des Smartphones erforderlich um sicherzustellen, dass nur dieses die Transaktionsdaten entschlüsseln kann. Alternativ bieten einige Banken auch spezielle TAN-Generatoren (Lesegeräte) für photoTAN an.

Zur Nutzung der photoTAN-App muss der Kunde sich aber zunächst bei der Bank registrieren. Zum Beispiel muss bei einer Bank der Kunde zunächst über das Kundenportal einen Aktivierungsbrief bestellen. Dieser enthält einen QR-Code und eine Einmal-TAN, mit denen man das Smartphone registriert, auf dem die App installiert ist. Diese muss durch ein Passwort geschützt werden. Die App soll sich nicht auf andere Smartphones übertragen lassen und nach zehn falschen Passworteingaben alle Daten löschen. Danach, wie auch nach einem Smartphone-Wechsel, muss der Kunde den gesamten Registrierungsvorgang neu durchlaufen.

In Deutschland bieten bisher die Commerzbank und die Comdirect das PhotoTAN Verfahren an, die Deutsche Bank plant eine Einführung bis Ende des Jahres 2014.

4.2.5 Push-TAN

Ähnlich wie bei mobiler und Photo-TAN brauchen Nutzer für die Push-TAN-Methode ein Smartphone. Allerdings erhalten sie bei diesem Verfahren weder eine SMS noch müssen sie einen Code einscannen. Stattdessen laden Sie zunächst eine App auf ihr Smartphone. Nachdem der Nutzer im Online-Banking einen Auftrag veranlasst hat, wechselt er in die App, die er mit seinen individuellen Zugangsdaten aktiviert. Dort prüft er den Auftrag und lässt sich eine TAN anzeigen. Diese gibt er wie gewohnt im Banking-System ein.

4.2.6 TAN Generatoren (ChipTAN, e-TAN, smartTAN, Flickercode)

Mit einem TAN-Generator können TANs elektronisch erzeugt werden. Hierfür gibt es mehrere unterschiedliche Verfahren.

sm@rt-TAN

Bei diesem Verfahren erhält der Nutzer von seinem Kreditinstitut einen TAN-Generator ohne Zifferntasten. Sobald die Kundenkarte (z. B. eine Maestro-Card oder eine V-Pay-Karte) in den Generator eingesteckt wird, können auf Knopfdruck TANs erzeugt werden. Diese TANs können nur der Reihe nach im Online-Banking eingegeben werden. Werden beispielsweise fünf TANs generiert, jedoch nur die zuletzt erzeugte TAN für eine Transaktion verwendet, sind die vorherigen vier TANs ungültig. Das Kreditinstitut kann als Herausgeber der Kundenkarte die TANs überprüfen.

Die Generierung der TANs erfolgt über den Chip auf der Kundenkarte des Kunden. Der TAN-Generator selbst ist nicht auf den Kunden individualisiert. Bei einem Verlust der Karte können mit einem beliebigen TAN-Generator gültige TANs erzeugt werden. Da für Transaktionen auch die PIN notwendig ist, stellt dies eine überschaubare Gefahr dar.

Dieses Verfahren ist anfällig für Phishing- bzw. »Man-in-the-Middle-Angriffe«, da die generierten TANs für beliebige Transaktionen verwendet werden können. Eine Auftragsbindung findet nicht statt. Die Verbreitung dieses Verfahrens ist gering.

eTAN-Generator

Im Dezember 2006 hat die BW-Bank dieses Verfahren eingeführt. Kunden erhalten einen individualisierten TAN-Generator, der unter Einbeziehung eines geheimen Schlüssels, der aktuellen Uhrzeit und der Kontonummer des Empfängers eine temporär gültige TAN erzeugt. Die Empfängerkontonummer muss über das Ziffernfeld des TAN-Generators eingegeben werden. Weitere Personendaten werden nicht verwendet.

Dieses Verfahren schützt vor Phishing- bzw. »Man-in-the-Middle-Angriffen«, sofern die korrekte Empfängerkontonummer eingegeben wird. Die manuelle Eingabe der Kontonummer ist wenig komfortabel. Bei einem Verlust des TAN-Generators können weiterhin TANs generiert werden. Da für Transaktionen auch die PIN notwendig ist, stellt dies eine überschaubare Gefahr dar.

Bei weiteren Banken (z. B. der Santander Consumer Bank) muss statt der Empfängerkontonummer eine für die jeweilige Überweisung generierte Kontrollnummer (Startcode) eingegeben werden. Im Gegensatz zur Eingabe des Empfängerkontos ist dieses Verfahren für »Man-in-the-Middle-Angriffe« anfällig, da die Empfängerkontonummer nicht kontrolliert wird.

Einige TAN-Generatoren anderer Banken (z. B. von der Bank für Sozialwirtschaft) erstellen zeitlich begrenzt gültige TANs nur anhand eines individuellen geheimen Schlüssels und der Uhrzeit, ohne Eingabe einer Kontrollnummer oder eines Empfängerkontos. Hier ist weder Kartenlesegerät noch Tastatur am Generator erforderlich. Da in diesem Verfahren keinerlei Auftragsbezug besteht, ist es ähnlich anfällig für Phising Attacken, wie das vorher

beschriebene sm@rt-TAN-Verfahren. Allerdings müsste die unerwünschte Transaktion innerhalb des kurzen Gültigkeitszeitraums der TAN veranlasst werden.

chipTAN manuell/Sm@rtTAN plus/SecureTAN plus1

Der Kunde erwirbt ggf. kostenpflichtig einen TAN-Generator mit Ziffernfeld und Karteneinschub als weiteres Elektronikgerät.

Nachdem eine Überweisung im Online-Banking erfasst wurde, wird ein (Start-)Code am Bildschirm angezeigt. Nun muss die persönliche Bankkarte in den TAN-Generator eingesteckt werden und dieser (Start-)Code über das Ziffernfeld des TAN-Generators eingetippt und bestätigt werden. Bei den meisten Instituten müssen danach noch die Empfängerkontonummer (bzw. Teile davon) sowie in manchen Versionen der Betrag der Überweisung eingetippt werden. Ist dies nicht der Fall, ist der Schritt am TAN-Generator ohne Eingabe zu bestätigen.

Aus den am TAN-Generator eingegebenen Daten errechnet der TAN-Generator eine auftragsbezogene TAN, die im Online-Banking erneut manuell mit der Tastatur des Online-Platzes eingegeben wird. Dieses Verfahren schützt vor Phishing- bzw. »Man-in-the-Middle-Angriffen«, nachdem die Empfängerkontonummer und der Betrag genauso, wie am TAN-Generator erneut eingegeben sind.

Bei einem Verlust der Bankkarte können durch den Finder mit einem beliebigen TAN-Generator, der für dieses Verfahren geeignet ist, weiterhin TANs generiert werden. Da für Transaktionen auch die PIN notwendig ist, ist die Gefahr einer Attacke verhältnismäßig gering. Sobald eine Bankkarte gesperrt wird (z. B. bei Diebstahl), werden mit dieser Karte erzeugte TANs vom Kreditinstitut abgelehnt.

chipTAN comfort/SmartTAN optic (Flickering)

Dieses neue Verfahren findet in Deutschland eine zunehmende Verbreitung. Viele Sparkassen und Volks- und Raiffeisenbanken sowie die Postbank setzen es bereits ein. Die Sparkassen und die Postbank nennen dieses optische TAN-Verfahren »chipTAN comfort«, während die Volksbanken die Bezeichnungen »Sm@rtTAN plus« und »SmartTAN optic« dafür verwenden. Die Kunden erwerben dazu einen TAN-Generator mit Ziffernfeld und Karteneinschub. Nachdem eine Überweisung im Online-Banking erfasst wurde, erscheint am Bildschirm eine Grafik, die fünf flackernde Schwarz-Weiß-Flächen enthält. Nun muss die persönliche Bankkarte in den TAN-Generator eingesteckt werden. Sobald der TAN-Generator am Bildschirm an die Grafik gehalten wird, erfolgt eine Datenübertragung durch Lichtsignale. Hierbei werden Teile der Empfängerdaten übertragen, bei einer Einzelüberweisung beispielsweise der (Start-)Code, die Empfängerkontonummer, sowie der Überweisungsbetrag. Auf dem Display des TAN-Generators werden im Anschluss die übermittelten Daten zur Kontrolle und Bestätigung angezeigt. Der TAN-Generator errechnet nun eine auftragsbezogene TAN, die im Online-Banking eingegeben wird.

Dieses Verfahren schützt vor Phishing- bzw. »Man-in-the-Middle-Angriffen«, sofern die im Display angezeigten Daten vor der Bestätigung auf ihre Richtigkeit geprüft werden. Durch die optische Übertragung müssen keine Auftragsdaten am TAN-Generator eingegeben werden. Da für Transaktionen zusätzlich auch die Online-Banking-Zugangsdaten notwendig sind, stellt dabei auch der Verlust der Bankkarte eine überschaubare Gefahr dar. Sobald die Bankkarte gesperrt wird (z. B. bei Diebstahl), werden mit dieser Karte erzeugte TANs vom Kreditinstitut ohnehin abgelehnt.

Angriffsmöglichkeiten zeigen sich in Verbindung mit Sammelüberweisungen. Hier werden im Display des TAN-Generators nur die Anzahl der Posten sowie der Gesamtbetrag angezeigt. Bei einem Angriff könnten nun die einzelnen Überweisungen des Sammlers verändert werden. Solange die Anzahl der Posten und der Gesamtbetrag gleich bleiben, wäre die Manipulation im Display des TAN-Generators nicht erkennbar.

Eine weitere Angriffsmöglichkeit wäre die Umwandlung einer Einzelüberweisung in eine Sammelüberweisung mit einem Posten. Der Nutzer würde in diesem Fall im Display des TAN-Generators nur die Anzahl der Posten (hier »1«) und den Betrag angezeigt bekommen.

Kritisiert wird bei diesem Verfahren allerdings von einigen Benutzern, dass das Gerät bei unterschiedlichen Displaytypen den Flickercode nicht zu erkennen scheint.

In allen Fällen ist die Sicherheit mindestens so hoch wie bei Benutzung von iTAN-Listen. Kontrolliert der Benutzer aber die angezeigten Daten im Display des TAN-Generators und benutzt keine Sammelüberweisung, ist die Sicherheit deutlich erhöht.

Allerdings wird aufgrund der Sicherheitsmaßnahmen von chipTAN inzwischen versucht den Benutzer mittels »Social Engineering« dazu zu bewegen von sich aus, freiwillig eine Überweisung zu Gunsten der Betrüger zu tätigen, indem ihm etwa eine angebliche »Test-Überweisung« vorgespielt wird oder angeblich falsch gebuchtes Geld »zurücküberwiesen« werden soll. In anderen Fällen soll der Nutzer per Überweisung an einem Gewinnspiel teilnehmen oder Daten synchronisieren. Die Banken warnen vor diesen Betrugsversuchen. Eine Bank würde einen Kunden niemals auffordern eine Überweisung zu tätigen, die dieser nicht selbst veranlasst hat.

4.3 Neue Ansätze zur Steigerung der Sicherheit

Die Entwicklung der Online-Banking-Verfahren ist stark geprägt von der IT-Sicherheit bzw. den erfolgreichen Angriffen gegen die Verfahren. Die Voraussetzung für sicheres Online-Banking ist ein sicheres Verfahren zur Authentisierung und Autorisierung. In der Browser-gestützten Variante entspricht das chipTAN-Verfahren dem aktuellen Stand der Technik. Im Bereich des Homebanking, für das auf dem Kundenrechner eine Homebanking-Software installiert werden muss, ist HBCI mit Chipkarte und Secoder-fähigem Kartenleser das sicherste Verfahren, wobei die jeweilige Bank die Secoder-Erweiterung für HBCI unterstützen muss.

Darüber hinaus gibt es eine Vielzahl technischer Maßnahmen, die auf dem Kundenrechner und dem mobilen Endgerät umgesetzt werden sollten. Dazu zählen beispielsweise die Installation von Antivirensoftware und einer Personal Firewall. Allerdings gibt es kein Online-Banking-Verfahren mit absoluter Sicherheit. Zu allen Verfahren wurden schon Angriffe oder Angriffsmöglichkeiten berichtet. Der Wettlauf zwischen Angreifern und Verfahrensentwicklern führt zu einer ständigen Weiterentwicklung. Letztendlich bewegt man sich auch immer im Spannungsdreieck zwischen Benutzerfreundlichkeit (Einfache Bedienbarkeit sowie Bereitstellung eines Online-Banking-Verfahrens ohne zusätzliche Hard- und Softwareinstallationen), Sicherheit und Wirtschaftlichkeit (Kosten für Bank und/oder Kunden).

Gerade für Nutzer älterer TAN-Verfahren, wie TAN-Listen aus Papier oder einfachen TAN-Generatoren (nicht chipTAN), bei denen die Überweisungsdaten nicht in die TAN-Berechnung mit einfließen, kann auch der Einsatz einer Live-CD beziehungsweise eines Live-USB-Sticks mit dem kostenlosen Knoppix sinnvoll sein. Live-Systeme enthalten normalerweise keine Banking-Trojaner und können dadurch den Nutzer vor der Trojaner-Problematik schützen. Diese Maßnahmen konzentrieren sich auf die technischen Aspekte.

Ein ebenso wichtiger Aspekt für sicheres Online-Banking ist, den Wissensstand des Nutzers und sein Bewusstsein für mögliche Betrügereien zu schärfen (»Social Engineering«). Banking-Trojaner wie Tatanga oder Matsnu.J haben deutlich gemacht, dass die bewusste Manipulation des Nutzers eine Umgehung der technischen Sicherheitsmaßnahmen gar nicht notwendig macht. Durch das Vortäuschen falscher Tatsachen, z. B. einer angeblichen »Test-« oder »Rücküberweisung«, unter Ausnutzung der Unwissenheit des Bankkunden wurden schon etliche Bankkunden um erhebliche Beträge betrogen. Für die Bank gilt es ihren Kunden ein Verfahren anzubieten, bei dem die Risiken bzw. das Gefährdungspotenzial überschaubar sind (für die meisten neueren Verfahren ist dies der Fall, insbesondere dann wenn die erzeugten TANs nur eine sehr kurze Gültigkeitsdauer haben) und die Kosten für den Kunden akzeptabel bleiben. Die Erfahrungen der Banken haben z. B. gezeigt, dass Hardwarekosten für einen Chipkartenleser oder einen TAN-Generator bis ca. 10,– € vom Kunden noch akzeptiert werden. Auch

Kommunikationskosten für SMS beim mTAN-Verfahren werden derzeit von den Kunden akzeptiert.

Vielversprechende Ansätze sind aus dem Bereich der Biometrie zu erkennen. Hier sind moderne mobile Endgeräte schon mit Möglichkeiten ausgestattet die eine Autorisierung via Fingerprint (Apple iPhone 5 und Samsung Galaxy S5) ermöglichen.

Außerdem ist die Voice Biometrie im Zusammenspiel mit Spracherkennungssoftware, wie beispielsweise Siri von Apple eine Möglichkeit das Online-Banking auf dem Mobiltelefon bequemer und sicherer zu machen. Hierzu gibt es sehr vielversprechende Forschungsansätze.

4.3.1 NFC-TAN / Display TAN

Bei diesen Verfahren wird wie beim photoTAN Verfahren auf dem PC-Bildschirm ein 2D-Code angezeigt, der mit der Bank-App des Kunden-Smartphones eingescannt werden kann. Anschließend hält der Kunde für die Funk-Übertragung der Überweisungsdaten seine Girokarte an das Smartphone. Bei NFC-TAN wird die TAN direkt auf der Girokarte erzeugt und zum Smartphone/Bankserver zurückgeschickt, bei Display-TAN wird dem Bankkunden vorher noch auf der Girokarte Zielkontonummer und Betrag zum Bestätigen angezeigt.

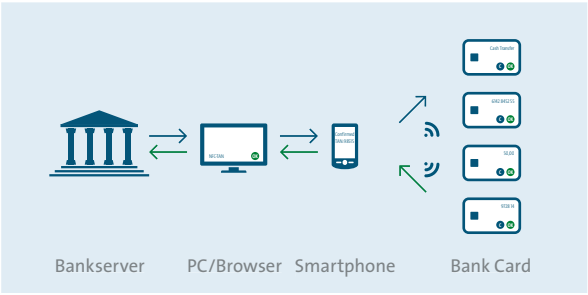


Abbildung 4: Online Banking mit NFC-TAN.
(Quelle: Borchert IT-Sicherheit UG c/o Univ. Tübingen WSI für Informatik)

Anschließend wird die TAN zum Bankserver geschickt. Dafür gibt es drei Möglichkeiten, welche, spielt keine Rolle – es ist nicht sicherheitsrelevant:

- Der Bankkunde liest die TAN von Kartendisplay ab und gibt sie am PC ein.
- Der Bankkunde liest die TAN von Smartphone-Display ab und gibt sie am PC ein.
- Das Smartphone schickt die TAN per Internet zum Bankserver.

Eine gültige TAN kann beim Display-TAN Verfahren nur generiert werden, indem die Überweisungsdaten dem Bankkunden auf der Bankkarte angezeigt werden und der Bankkunde sie dort mit OK bestätigt. Anders ausgedrückt: wenn die TAN für eine Überweisung richtig ist, dann muss der Bankkunde die Überweisungsdaten auf dem Display seiner Bankkarte gesehen und bestätigt haben.

Die verbleibenden Angriffe auf Display-TAN sind also »Man-in-the Middle Angriffe«, die von der Unaufmerksamkeit des Bankkunden ausgehen, oder Social Engineering Angriffe. Mit anderen Worten, es sind also die gleichen Angriffe wie auf ChipTAN, das heißt, Display-TAN hat dasselbe hohe Niveau von Sicherheit wie ChipTAN.

Unter Usability Gesichtspunkten kann man erwähnen, dass kein extra Gerät erforderlich ist. Voraussetzung für den Einsatz von Display-TAN ist ein Bluetooth/BLE-fähiges Smartphone (ab iPhone 4s und Android 4.3.0), NFfähige Girocards und für die Display-Variante ein Display auf der Karte für die Anzeige der TANE[4].

4 http://www.display-tan.com

4.3.2 Neuer Personalausweis (nPA)

Eine in Deutschland für Online-Banking noch wenig genutzte Identifikationsmöglichkeit ist der neue Personalausweis. Dafür ist allerdings eine spezielle Hardware erforderlich.

Bisher wird der nPA von Finanzdienstleistern aber noch sehr wenig eingesetzt. Als Anwendungen sind dabei im Wesentlichen die Authentifizierung für Portalzugänge und nur sehr vereinzelt die Online-Eröffnung eines Bankkontos ausgewählt worden. Für das Online-Banking kommt der nPA bisher nicht zum Einsatz. Dies liegt sicherlich auch daran, dass es einige Aspekte gibt, die aus Sicht der Bank als nachteilig zu werten sind:

1. Die Investitionskosten durch die Entwicklung, Implementierung und Vorhaltung des Legitimationsservices mittels nPA. Außerdem kann ein nPA-basiertes Online-Banking die bisher genutzten Verfahren nicht dauerhaft substituieren, da in absehbarer Zeit nicht von einer 100 Prozent Verfügbarkeit der Online-Ausweisfunktion des nPA bei den Bankkunden bzw. potenziellen Bankkunden auszugehen ist.

2. Durch die Nutzung des nPA würden die Banken die System- und Verfahrenshoheit verlieren; bedingt durch den Einsatz von Hard- und Softwarekomponenten, die nicht durch sie ausgegeben werden können.

3. Verringerung der Kundenbindung: Die mit dem Logo der jeweiligen Bank ausgestatteten Komponenten, die diese ihren Kunden zur Authentifizierung zur Verfügung stellen, stellen für die Banken auch ein Kundenbindungsinstrument dar. Wird dieses Kundenbindungsinstrument zugunsten einer »bankneutralen« Lösung ersetzt, schwindet eine weitere Notwendigkeit, ein bestimmtes Konto zwingend bei einer bestimmten Bank zu führen und zu verwalten. Somit geht ein wichtiges Kundenbindungsinstrument verloren.

Trotz zahlreicher Sicherheitsbedenken, lassen sich sichere Identitäten in Zukunft auch problemlos in Anwendungsbereiche moderner Smartphones übertragen. Das zeigen zum Beispiel aktuelle Entwicklungen der Berliner Bundesdruckerei, die darauf abzielen, Mobiltelefone für temporäre Ausweisfunktionen nutzbar zu machen.

Mithilfe der Online-Ausweisfunktion (eID-Funktion) des Personalausweises können zukünftig auch Online-Banking Anwendungen übertragen und via Sicherheitstoken direkt zur Verwendung freigeschaltet werden. Zur Ausführung einer mobilen Ausweisfunktion über Smartphones Sicherheitselemente, die zum Beispiel in Form einer SIM- oder providerunabhängigen microSD-Karte in ein Smartphone integriert werden. Der Zugang zu einer solchen mobilen Ausweisfunktion kann einfach realisiert werden: Auf Basis einer kostenlos heruntergeladenen App und eines geeigneten Lesegeräts meldet sich der Nutzer über seinen Personalausweis mit aktivierter Online-Ausweisfunktion und seiner geheimen Ausweis-PIN persönlich für die entsprechende Funktion an. Das sichere Ableiten der Identitätsdaten aus dem Sicherheitschip im Ausweisdokument könnte alternativ auch in Behörden über die Self-Service-Terminals der Bundesdruckerei erfolgen. Im zweiten Schritt wird die im Handy integrierte SIM- oder microSD-Karte über die individuelle Karten-PIN für den Empfang der gesicherten Ausweisdaten freigegeben.

Selbst wenn das für mobile Identitätsanwendungen genutzte Smartphone in falsche Hände gerät, bleiben die Daten geschützt: Ohne den Besitz des hoheitlichen Dokuments in Kombination mit der Kenntnis der geheimen Ausweis- und Karten-PIN erfolgt seitens des TSP-Systems keine Freischaltung der angeforderten Daten. Aus technologischer Sicht sind die Weichen zur Realisierung solcher Mobile Wallet-Anwendungen längst gestellt.

4.3.3 Tokenization / Open Authentication

Im Licht zukünftiger APIs zu weiteren Dienstleistungen sollten Banken über die Verwendung von OAuth (Open Authentication) als Authentifizierungs- und Identitätsmanagementlösung nachdenken.

Die Geburtsstunde von OAuth liegt im Jahr 2007. Das Protokoll findet mittlerweile in vielen konsumentenorientierten Websites wie Yahoo, AOL, Google und Flickr Verwendung. Es ermöglicht dem User (Endnutzer) einer Webanwendung (Service-Provider) private Ressourcen (Protected Resources) wie Fotos, Videos, Kontaktliste und Kontoauszug mit allen anderen Webanwendungen (Konsument) auszutauschen, ohne Nutzername und Passwort der Service-Provider-Webanwendung den Konsumenten-Applikationen preiszugeben. OAuth verwendet ein sogenanntes Token für die Übertragung von Nutzername und Passwort.

Ein Token verwendet man statt des Nutzernamens und des Passworts, um Autorisierung auf privaten Ressourcen zu ermöglichen. Ein Token besteht meistens aus einem zufälligen String (Buchstaben und Zahlen). Es ist eindeutig und schwer zu erraten. Zudem wird es mit einem Konsumenten-Geheimnis kombiniert. OAuth verwendet zwei unterschiedliche Token-Typen: Anfrage- und Zugriffs-Token.

4.4 Zusammenfassung

Wir können zusammenfassend feststellen, dass einer der größten Schwachpunkte in Bezug auf Sicherheit der Mensch ist, sei es durch Unwissenheit oder Mangel an Sensibilisierung.

Im Bereich des Mobile-Banking kann man erkennen, dass die zunehmende Fragmentierung des Betriebssystems Android ein Problem darstellen kann. Sobald die Betriebssystemsoftware nicht auf dem neuesten Stand ist, stellt es ein potenzielles Risiko dar, da die bekannten Bugs nicht beseitigt wurden.

Es gibt hier die Möglichkeit Bankseitig eine App zu deaktivieren, sollten bestimmte Sicherheitsrichtlinien nicht erfüllt werden. Dazu könnte auch das »rooten« des Android Betriebssystem gezählt werden. Dabei wird das Original Android durch eine andere Version ersetzt bei dem der User dann Administratorenrechte bekommt. Dies kann ein Sicherheitsproblem darstellen. Zudem ist es oft so, dass die Banking Apps auf die jeweils neueste Version von Android optimiert wurden und auf alten Systemen nur fehlerhaft laufen.

5 Herausforderungen und Verhaltensregeln

Im folgenden Kapitel gehen wir kurz auf die fehlende Interoperabilität ein und zeigen auf, wie sich Endverbraucher in den gängigen Betrugsszenarien verhalten sollten.

5.1 Fehlende Interoperabilität

Das Problem eines gemeinsamen Standards ist in Deutschland weniger stark vorhanden, zumindest wenn es um den reinen Zahlungsverkehr geht. Hierzulande gibt es den FinTS Standard, bei dem viele Kreditinstitute mitarbeiten.

Mit PFM (Online-Banking 2.0) soll der Kunde aber auch Daten von anderen Anbietern in seine Finanzübersicht aggregieren können, beispielsweise Kreditkartenumsätze, Loyalty Cards oder Depotumsätze. Daher würde es Sinn machen, an einer neuen API zu arbeiten die dann auch Webservices mit abdecken kann. Als Beispiel könnte das Open Bank Project dienen.

Das Problem mit der fehlenden Interoperabilität kann sich im Zuge der erneuerten Payment Service Directive (PSD 2) mit dem »Access to Account« lösen. Bei »Access to Account« sollen Drittanbieter Zugang zu den Kontodaten bekommen. Dafür wäre ein gemeinsamer Standard, der Verantwortlich- und Zuständigkeiten regelt, sehr wichtig. Erste Ansätze für eine europäische Lösung sind in der Open Bank Alliance zu finden.

5.2 Aufklärung zu den gängigen Betrugsszenarien

Im folgenden Abschnitte möchten wir Sie für Szenarien sensibilisieren, die leider häufig vorkommen und mit ein wenig mehr Bewusstsein für das Thema vermieden werden können.

5.2.1 Gesunde Vorsicht bei E-Mails

Banken bitten ihre Kunden nie per E-Mail, vertrauliche Daten im Netz einzugeben. Diese Mails sind gefälscht – am besten sofort löschen. Das gleiche gilt für dubiose E-Mails von Unbekannten, vor allem, wenn eine Datei angehängt ist oder ein Link, dem der Nutzer folgen soll. Hinter dem Anhang könnte ein Schadprogramm stecken, zum Beispiel ein Phishing-Trojaner. Solche verdächtigen Dateien auf keinen Fall öffnen! Hinter dem Link verbirgt sich in der Regel eine präparierte Website, die den Rechner beim Aufruf verseucht. Häufig wird in der E-Mail mit einer Kontosperre gedroht. Mit solchen Einschüchterungen wollen Betrüger Bankkunden unter Druck setzen. Die Nutzer sollten Drohungen ignorieren und Phishing-Mails nie beantworten.

5.2.2 Den Computer und das Smartphone vor Schädlingen schützen

Wichtig ist eine gute Sicherheitsausstattung des Computers und des mobilen Endgerätes. Standard sind ein Anti-Viren-Programm und eine Firewall, um sich vor schädlichen Dateien zu schützen. Die wichtigen Programme eines Computers werden regelmäßig aktualisiert. Updates sind umgehend zu installieren. Datenträger wie Speicherkarten, USB-Sticks oder CDs sollten auf Viren geprüft werden. Öffentliche Computer z.B. in Internet-Cafés sind für Bankgeschäfte nicht geeignet.

5.2.3 Vorsicht beim Aufruf der Bank-Website

Beim Online-Banking sollte die offizielle Adresse der Bank immer direkt eingegeben oder über eigene Lesezeichen (Favoriten) aufgerufen werden. Maßgeblich ist die Adresse, die die Bank in ihren offiziellen Unterlagen angibt. Die Verbindung zum Bankcomputer muss verschlüsselt sein. Das ist erkennbar an den Buchstaben »https« in der Web-Adresse und einem Schloss- oder Schlüssel-Symbol im Browser.

5.2.4 Moderne Transaktions-Verfahren nutzen

Im vorherigen Kapitel haben wir Ihnen die Lösungen aufgezählt, die derzeit von den Banken angeboten werden. Jeder Online-Banking Nutzer sollte sich bei seiner Bank informieren, welche Verfahren zur Verfügung stehen. Manche Verfahren sind gebührenpflichtig. Dies sollte Sie jedoch nicht abschrecken. Ein Angriff aufs eigene Konto könnte teuer und mit sehr viel Aufwand verbunden sein. Für gute Technologie und gute Dienstleistungen muss man auch bereit sein, eine entsprechende Gebühr zu zahlen.

5.2.5 Mit Geheimzahlen richtig umgehen

Passwort (PIN) und Transaktionsnummern nicht auf dem PC speichern. Auch eine automatische Speicherung im Internet-Programm (Browser) ist riskant. Ein frei wählbares Passwort fürs Online-Banking sollte mindestens acht Zeichen lang sein und möglichst aus einer zufälligen Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Fürs Online-Banking unbedingt ein separates Passwort wählen – keines, das auch für andere Dienste im Web genutzt wird. Empfehlenswert ist auch, die PIN rund alle drei Monate zu ändern.

5.2.6 Falls es zu spät ist – Schadensbegrenzung

Nicht immer ist das Geld sofort weg, wenn Kriminelle eine Sicherheitslücke ausgenutzt haben. Opfer sollten zuerst die Bank alarmieren. Wenn eine Phishing-Überweisung nicht lange zurückliegt, kann sie manchmal noch gestoppt oder rückgängig gemacht werden. Entsteht doch ein finanzieller Schaden, unbedingt Anzeige bei der Polizei erstatten. Das ist nötig, um eventuell Geld von der Bank zurückzubekommen. Falls der Kunde nicht grob fahrlässig gehandelt hat, zeigen sich viele Banken kulant.

5.3 Zusammenfassung

Die Beispiele zeigen, dass der Endkunde sich verhältnismäßig einfach vor vielen Betrugsszenarien schützen kann, indem er ein bisschen Feingefühl entwickelt und Skepsis vor sämtlicher komisch wirkender Kommunikation in Zusammenhang mit seinem Konto aufbaut. Darüber hinaus sollte er die entsprechenden Schutzmaßnahmen in die Wege leiten, die aus modernen Transaktions-Verfahren und Antiviren bzw. Trojaner Software bestehen.

6 Fazit

Als Fazit können folgende Punkte festgehalten werden. Neue Technologien und Wettbewerber spielen eine zunehmend größere Rolle und werden in Zukunft sowohl die Bedrohungszenarien verändern, aber auch dafür sorgen das neue Sicherheitsverfahren wie z. B. die Nutzung von biometrischen Merkmalen eingeführt werden. Das Smartphone wird zukünftig zum wichtigsten Kanal in der Kommunikation mit dem Kunden werden. Die neuen Wettbewerber stellen in ihren Geschäftsideen den Kunden deutlich mehr in den Mittelpunkt und bilden ihre Produkte auf Basis der Kundenanforderungen. Sie entwickeln deutlich modernere Oberflächen mit Multibankenfähigkeit. Viele Funktionalitäten können zwar auch über das Online Portal der Hausbank bezogen werden, diese sind jedoch oftmals etwas hölzern in der Usability. Viele Wettbewerber bieten hier intuitivere Anwendungen, die darüber hinaus die User Experience deutlich mehr in den Vordergrund stellen.

Die im letzten Kapitel gezeigten Beispiele für Betrugsszenarien können vom Endkunden verhältnismäßig einfach verhindert werden. Hierzu ist es nötig, dass der Endkunde ein bisschen Feingefühl entwickelt und Skepsis vor sämtlicher komisch wirkender Kommunikation in Zusammenhang mit seinem Konto aufbaut. Darüber hinaus sollte er die entsprechenden Schutzmaßnahmen in die Wege leiten, die aus modernen Transaktions-Verfahren und Antiviren bzw. Trojaner Software bestehen.

Weiterführende Links/ Quellen

- BITKOM, Banking & Financial Services
- GFT Banking
- Steria Mummert Banking
- KPMG Banking
- European Payments Council (EPC)
- HBCI / FinTS
- Open Bank / API


WELCOME TO
INTERNET BANKING

BITKOM vertritt mehr als 2.200 Unternehmen der digitalen Wirtschaft, davon gut 1.400 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 200 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 76 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 10 Prozent kommen aus Europa, 9 Prozent aus den USA und 5 Prozent aus anderen Regionen. BITKOM setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org