#02 DIGITALKOMPAKT LfM

MOBILE PAYMENT

einfach auf den Punkt gebracht.

lfm:
Landesanstalt für Medien
Nordrhein-Westfalen (LfM)

#02 DIGITALKOMPAKT LfM

MOBILE PAYMENT

MOBILE PAYMENT

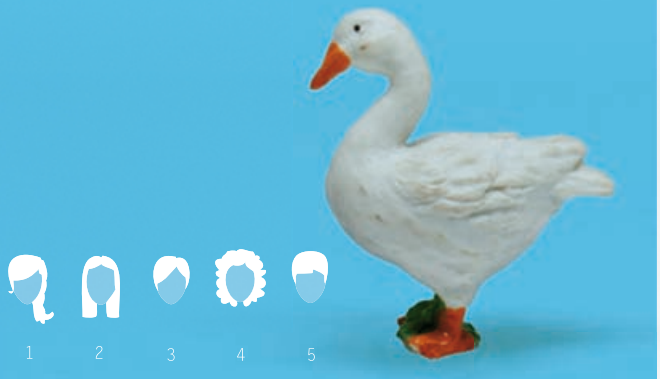
Geld ist unverzichtbar. Täglich benutzt es jeder Mensch, bezahlt damit kleinere und größere Beträge. Dazu verwenden wir aber nicht nur Bargeld, sondern nutzen ganz selbstverständlich Giro- oder Kreditkarte. Hinzu haben sich Kundenkarten, Rabattmarken, Gutscheine oder Coupons gesellt. Als ob dies alles nicht schon genug wäre, gibt es auch noch Aktionswochen, die uns durch Sammelhefte ab einem Mindestumsatz zu neuen Besitzern von Prämienprodukten machen. Das Resultat: Die Geldbörse füllt sich zwangsläufig mit immer mehr Plastikkarten und die Übersicht schwindet langsam aber sicher.

Abhilfe verspricht das neue Konzept des Mobile Payment. Beim mobilen Bezahlen kann unter anderem die sogenannte NFC-Technologie genutzt werden. Der Begriff „Near Field Communication“ steht für die berührungslose Funkübertragung von Daten, typischerweise mit dem Mobiltelefon. Solchermaßen ausgestattete Handys können Zahlungsinformationen, Kredit- oder Kundenkartendaten auf kurze Distanz senden. Aktuell in aller Munde, gilt NFC vielen Experten und Brancheninsidern als der nächste große Trend. Doch bislang sind die Verbraucher skeptisch. Laut einer aktuellen GfK-Studie[1] finden nur 56 Prozent der deutschen Verbraucher Mobile Payment reizvoll.

Anlass genug, in der vorliegenden Ausgabe von Digitalkompakt LfM die verschiedenen Aspekte von Mobile Payment zu beleuchten. Hier finden Sie technische und historische Hintergründe, ergänzt durch eine Übersicht moderner Zahlungslösungen sowie die Perspektiven von Verbraucher- und Datenschutz in Experteninterviews. Die LfM als Herausgeber versteht sich hierbei als Informationslieferant – eine abschließende Meinungsbildung obliegt den Leserinnen und Lesern natürlich selbst.

Die Geschichte des Geldes

Eine Währung ist eine historisch gewachsene Notwendigkeit. In frühen Gesellschaftsformen ernährten sich die Menschen selbst, jagten, züchteten Vieh und bauten Nutzpflanzen an. Doch mit zunehmender Spezialisierung und der Entwicklung von Dienstleistungen wuchsen auch die Bedürfnisse, die bald in reinem Tauschhandel nicht mehr gestillt werden konnten.
Denn wie viele Haarschnitte bekommt man für eine Gans? Und was, wenn der Friseur Vegetarier ist?



Natürlich kann man darüber im Einzelnen feilschen oder über Zwischenhandel dennoch zu einer neuen Frisur kommen – kalkulierbar ist diese Lösung jedoch nicht. Nötig ist also ein allgemeingültiges, beständiges Mittel, über das sich alle Handelspartner einig sind.

Einigkeit bedeutet: Der eine Partner setzt es dazu ein, seine Leistung oder sein Produkt abzugeben und hierfür in einer ausgehandelten Höhe einen adäquaten Gegenwert zu empfangen. Nur durch Abgabe und Annahme ist ein Handel entstanden, dessen Wert in Geld ausgedrückt wird. Heute existiert Geld jedoch in verschiedensten Varianten. So gibt es materielles Geld als Banknoten oder Münzen, aber auch immaterielles Geld, etwa sogenanntes E-Geld oder Buchgeld zum Beispiel auf dem Bankkonto. Dazu kommen unterschiedliche Währungen, Akzeptanzstellen oder Übertragungsarten. Im allgemeinen Sprachgebrauch werden vor allem Bargeld und bargeldlose Zahlungen unterschieden.

Beim Bezahlen an der Kasse hat sich in Deutschland neben Bargeld auch das Bezahlen mittels Girokarte (ehemals EC-Karte genannt) durchgesetzt. Auch Kreditkartenzahlungen sind im Kommen. In den USA werden selbst Kleinstbeträge mittels Kreditkarte beglichen. Bei Beträgen unter 25 Dollar wird dort keine Unterschrift benötigt oder eine Überprüfung der Person durchgeführt. Auch die Wartezeiten, die eine elektronische Zahlung auslöst, sind weitaus kürzer als in Deutschland.

Bargeldlos im Alltag

Doch hierzulande werden ebenfalls viele Zahlungen ausschließlich oder zunehmend rein elektronisch abgewickelt. Einige Beispiele:

- Lohn-/Gehaltszahlung
- Parkuhr mittels Premium-SMS
- Parkhäuser mittels Kreditkarte (meist an Flughäfen oder Hotels)
- Fahrkarte für ÖPNV mittels Geldkarte (Chipkarte)
- Tankstellen (Girokarte, Kreditkarte oder Flottenkarte)
- Größere Geldbeträge (Kauf von Auto oder Haus)
- Zahlungsverkehr im Internet (Überweisung, Kreditkarte)

Wie der Händler es sieht

Jeder Anbieter von Waren oder Dienstleistungen vertraut darauf, dass er für sein Angebot den entsprechenden Geldwert bekommt, ob von der Bank oder direkt durch den Kunden ist zweitrangig. Dafür bietet er die verschiedensten Bezahlmöglichkeiten an – er schafft Akzeptanzstellen – die andere Händler vielleicht nicht bieten. Somit ist der Händler im Wettbewerbsvorteil und öffnet sich einem breiteren Kundenspektrum. Für diesen Service muss er jedoch die kartenausgebenden Unternehmen mit einen gewissen Prozentsatz, der meist zwischen 1,5 und 3 Prozent liegt, am Umsatz beteiligen. Diese Gebühren sind vielen Händlern ein Dorn im Auge, machen sie doch einen erheblichen Teil ihres Gewinns aus. Jedoch ist den wenigsten Verbrauchern bewusst, dass auch das Zahlen mittels Girokarte dem Händler Gebühren verursacht. Selbst der Umgang mit Bargeld ist für den Handel nicht umsonst: Sicherheitsunternehmen sammeln das Geld ein und zahlen es bei der Hausbank ein, wo es auf seine Echtheit geprüft werden muss. Auch diese Services verursachen Kosten. Somit sollte der Einzelhändler daran interessiert sein, möglichst wenig Bargeldbestände vorhalten zu müssen, binden sie doch Kapital, bieten Potenzial für Straftaten und verursachen nachgelagerte Gebühren. Ergo müsste der Händler froh über jede papierlose Bezahlung sein – wären da nicht die Gebühren.

„Bargeld lacht“ sagte der Volksmund dereinst. Aber hat er damit auch heute noch Recht? Fakt ist, dass sowohl Papiergeld als auch seine digitalen Alternativen jeweils Vor- und Nachteile aufweisen. Eine Gegenüberstellung.

Bargeld vs. E-Geld

BARGELD

Vorteile

Physisch vorhanden
Bestand gut überprüfbar
Sofort verfügbar
Anonym
Unaufwändig
Sehr hohes Vertrauen

Nachteile

Irrtum oder Betrug beim Wechselgeld möglich
Diebstahl möglich
Falschgeld möglich
Zerstörung möglich
Unhygienisch
Größere Beträge erfordern Platz und sind schwer
Unpassende Stückelung möglich

E-GELD

Vorteile

Kaum Fehlbeträge
Kein Gelegenheitsdiebstahl
Beansprucht keinen Platz
Hygienisch
Kein Falschgeld
Für Sehbehinderte besser geeignet

Nachteile

Aktueller Kontostand nur durch externe Partner/Lösungen überprüfbar
Verzögerte Nutzungsmöglichkeit, etwa bei Überweisung
Zahlungen sind auf einzelne Personen zurückführbar
Zeitaufwändiger
Umgang zum Lernen für Jugendliche ungeeignet
Umgang für ältere Menschen schwierig
Rückabwicklung von Käufen nur über selbe Zahlungsmethode möglich
Handy benötigt zum Bezahlen und Verifizieren Strom

Neutral

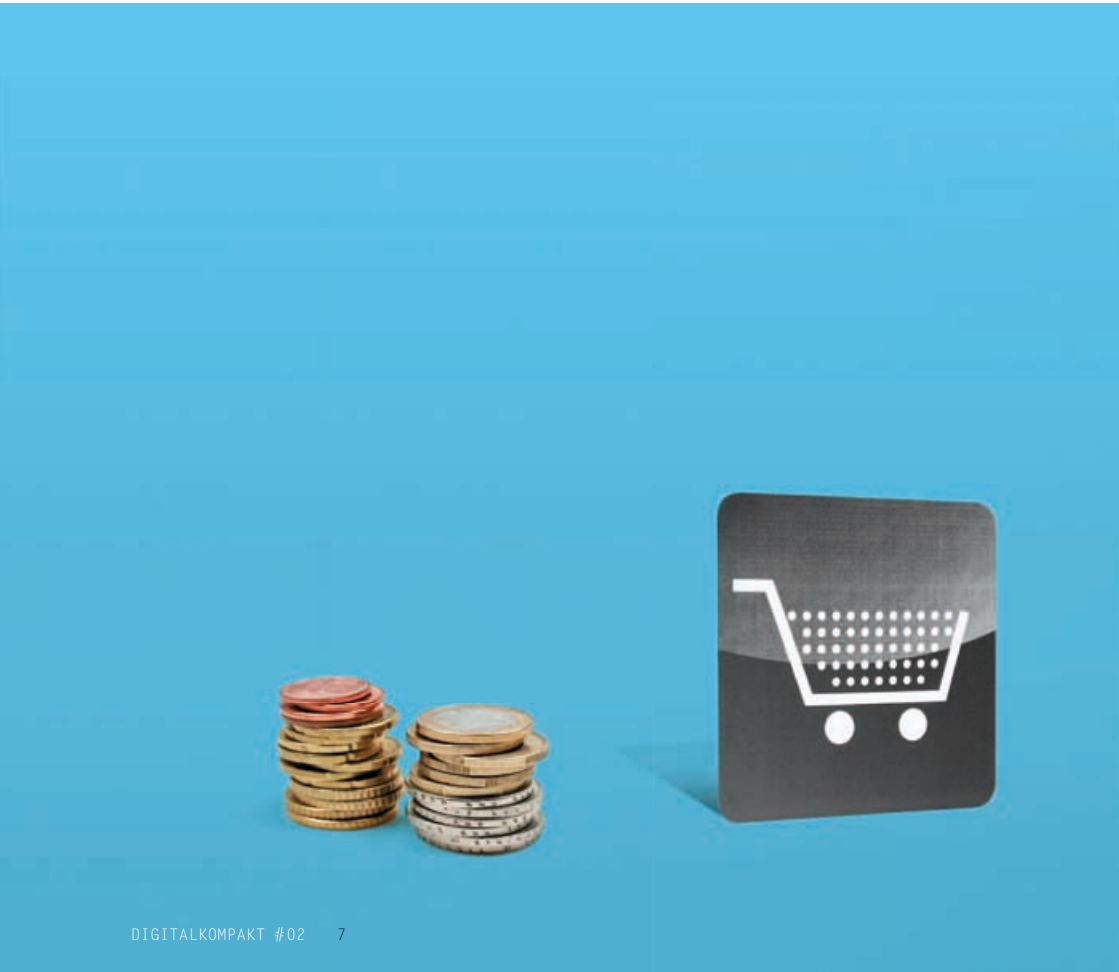
(Können sowohl positiv als auch negativ gewertet werden)

Sämtliche Geldbewegungen werden aufgezeichnet (Überprüfbarkeit, Übersichtlichkeit)
PIN (+ Legitimation) nötig

Transparenz contra Datenschutz

Am kritischsten sollte man die als neutral bezeichneten Punkte des E-Geldes betrachten. Es kann angenehm sein, wenn alle Geldbewegungen aufgezeichnet werden – lässt sich doch so die Haushaltskasse besser führen oder schneller eine Aufstellung für die Lohnsteuererklärung ans Finanzamt anfertigen. Auch ist es gewiss positiv zu bewerten, dass man zur Sicherheit vor jeder Transaktion eine PIN oder ein Passwort eingeben muss.

Diese Vorteile haben aber auch potenzielle Schattenseiten. Mit dem Argument der Terrorismusbekämpfung werden bereits jetzt digitale Kontobewegungen im Euroraum sowie Fluggastdaten grenzübergreifend ausgetauscht. Durch NFC würden nun auch Kleinstgeldbewegungen erfassbar. Bei dieser Erfassung handelt es sich wohlgemerkt nicht um die Absicht der beteiligten Unternehmen. So interessiert es Google nicht, was eine einzelne Person kauft, jedoch werden bestimmte Verhaltensmuster über mehrere 1 000 Menschen hinweg analysiert, um gleiche Werbung oder Angebote auszugeben. Unternehmen können aber vom Staat dazu instrumentalisiert werden, Daten einer einzelnen Person offenzulegen. Nicht umsonst gehören die Kreditkarteninformationen zum festen Bestandteil von angefragten Fluggastdaten. Wer nun bestimmte Waren mit E-Geld bezahlt, könnte dadurch unter Umständen in das Visier von Ermittlern geraten.

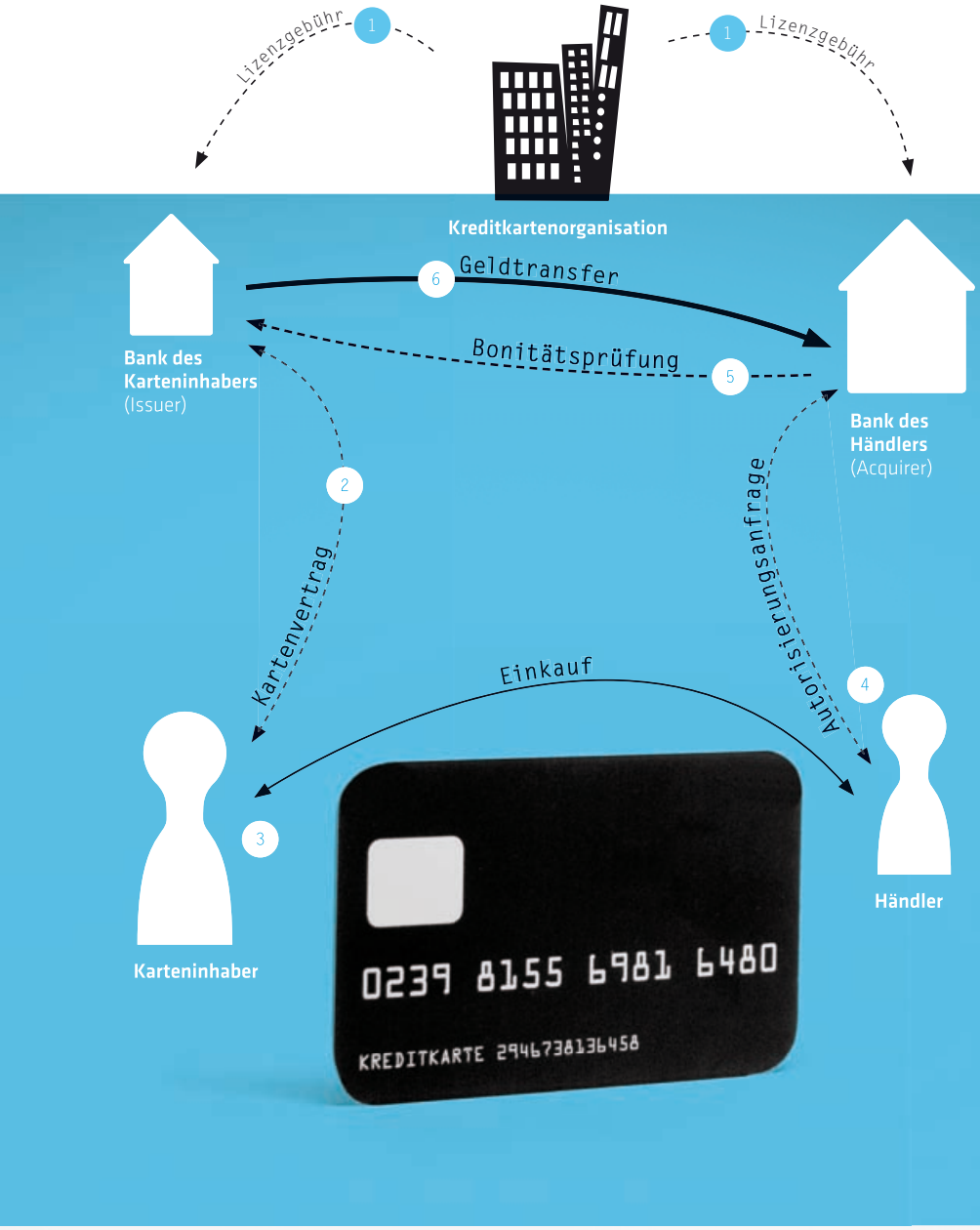


VIELE AKTEURE, WENIG ÜBERSICHT

Auch Zahlungen selbst sind ein Geschäft. So sind etwa bei der Kreditkartenzahlung mehrere Parteien involviert, zu denen die Banken von Käufer und Händler sowie das lizenzgebende Unternehmen zählen, aber teilweise auch zusätzliche Dienstleister. Sie prüfen etwa die Zahlung an sich und gleichen ab, ob der Verbraucher kreditwürdig ist oder stellen Kartenlesegeräte und Terminals zur Verfügung. Dafür verdient jeder Akteur am Bezahlvorgang mit – und das System wird potenziell unsicherer. Neben Manipulationen an Kartenlesegeräten und Geldautomaten per Skimming (siehe Glossar) sind auch die Übertragungswege der elektronischen Zahlung und die Datensicherheit ein wichtiges Thema.

1. Der Lizenzgeber berechtigt zum einen die Bank des Karteninhabers und zum anderen die Bank des Händlers, mit seinen Kreditkarten Zahlungen durchzuführen.
2. Die Bank des Karteninhabers schließt einen Vertrag mit dem Karteninhaber zur Ausstellung und Nutzung der Kreditkarte ab.
3. Mit der Kreditkarte kauft der Karteninhaber bei einem Händler ein.
4. Um die Bonität des Karteninhabers sicherzustellen, stellt der Händler eine elektronische Anfrage an seine Bank und bittet um Autorisierung der Transaktion.
5. Die Händlerbank prüft die Bonität des Karteninhabers, durch entsprechende Anfrage bei der kartenherausgebenden Bank und erteilt nach erfolgreicher Prüfung die Freigabe.
6. Im Anschluss daran veranlasst die Bank des Karteninhabers die Zahlung an die Händlerbank.

Zahlung per Kreditkarte



Der Kampf um die Identität

ÜBERBLICK

ENTWICKLUNG TECHNISCHER ZAHLUNGSLÖSUNGEN

Geschäfte sind Vertrauenssache. Bei allen technischen Versuchen zur Verbesserung von Bezahlvorgängen geht es um die Garantie, dass der Kunde wirklich er selbst ist. Eine Übersicht über die Evolution der Bezahl-Technologie.

Unterschrift

Der Anfang des Systems „Kreditkarte“: In den 1950er-Jahren konnte man in Restaurants und Kaufhäusern mit seinem „guten Namen“ anschreiben lassen. Der Kunde leistete eine Unterschrift an den Händler. Da jedoch nicht jede Bedienung jeden Kunden kennen konnte, händigte man einheitliche Karten (Visitenkarten in Plastikform) aus. Durch die vertrauenswürdige Karte und die Unterschrift hatte der Händler die Garantie, vom Kartenunternehmen den entsprechenden Betrag erstattet zu bekommen. Bevorzugt wurde die Karte von Geschäftsreisenden verwendet, hatten sie hiermit doch eine nationale Akzeptanzstelle an zahlreichen Flughäfen, ohne Bargeld mit sich führen zu müssen. Heute stellen Unterschriften kein alleiniges Sicherheitsmerkmal dar, werden jedoch hin und wieder als biometrisches Merkmal eingesetzt. Man kann mit einer gewissen Sicherheit feststellen, ob es sich um den Karteneigner handelt, kombiniert dies jedoch mit weiteren Lösungen.

Abdruck

Der Abdruck von Erhebungen auf einer Plastikkarte ist die älteste Form des massentauglichen Einsatzes von Kreditkarten. Möchte der Händler die Daten des Käufers aufnehmen, nimmt er Kohlepapier und einen Kartenschlitten, legt Papier und Karte unter den Schlitten und fährt mit dem Schlitten darüber. Hierdurch werden die Erhebungen auf den Durchschlag übertragen. Diese Art der „Datenübertragung” mag aus heutiger Sicht antiquiert erscheinen, war zur Einführung um das Jahr 1950 jedoch der beste Kompromiss. Die Erhebungen konnten nur schwer reproduziert werden und der entsprechende Schlitten funktionierte rein mechanisch, was bei Stromausfällen ein wichtiger Faktor war. Auch heute noch findet man hin und wieder (meist in Taxis) das genutzte Verfahren. Die Technik ist verlässlich, halbwegs transportabel und nicht abhängig von äußeren Faktoren.

ENTWICKLUNG TECHNISCHER ZAHLUNGSLÖSUNGEN

Magnetstreifen

Erst durch Einführung der Magnetstreifen haben die meisten Kartensysteme ihren Durchbruch erfahren. Der Vorteil liegt auf der Hand: Es ist das erste System, das elektronisch ausgelesen werden konnte, wodurch sich falsche Eingaben auf ein Minimum reduzierten. Der Magnetstreifen ist günstig in der Herstellung – kann jedoch heute verhältnismäßig leicht kopiert werden. Magnetstreifenlese- und -schreibgeräte sind im Internet ebenso erhältlich wie passende Blankokarten samt Drucker. Das einfache Kopieren machen sich organisierte Banden zu Nutze, indem sie Karten durch sogenanntes Skimming (engl. für „Abschöpfen“) am Geldautomaten samt PIN auslesen. Meist im Ausland außerhalb der EU wird dann eine Kopie der Karte erstellt, mit der im Namen des Nutzers Geld abgehoben wird. Der geschädigte Verbraucher hat die Beweislast, darzulegen, dass er seine PIN + Karte sicher und getrennt voneinander aufbewahrt hat. Ein weiteres Problem, an das die Planer der Magnetstreifen nicht gedacht haben, sind Geldbörse mit Magnetschließen sowie Warensicherungssysteme der Händler, die ebenfalls mit Magneten arbeiten. Beide können unbeabsichtigt die Daten auf dem Magnetstreifen löschen.

Chip

Der Chip auf der Plastikkarte ist der heutige Stand der Technik, vergleichbar mit dem Chip der SIM-Karte in Handys. Parallel wurde er mit der Geldkarte eingeführt, die den Bürger zum allerersten Mal mit elektronischem Kleingeld in Berührung brachte. Er enthält kleinste Schaltkreise, und kann ähnlich einem Minicomputer Rechenoperationen ausführen und Daten speichern. Der Chip wird bei allen hochsensiblen elektronischen Daten als Zugangskontrolle eingesetzt und ist beispielsweise auf der Gesundheitskarte der Krankenkassen zu finden, auf Bibliothekskarten, Mitarbeiterausweisen und vielen mehr. Auf aktuellen Giro- und Kreditkarten wird er an die Kunden ausgegeben und erhöht damit die Sicherheit am Geldautomaten und ermöglicht die Geldkartenfunktion. Daneben können Verbraucher damit auch bei den meisten Hausbanken am Chip-TAN-Verfahren für das Onlinebanking teilnehmen. Nur mittels des Lesegeräts und dem Chip auf der Karte kann eine TAN-Nummer errechnet werden, mit der man sich gegenüber der Bank etwa für Überweisungen legitimiert.

Premium-Nummer/-SMS

Auch die Mobilfunkanbieter bringen sich beim Thema Bezahlen ins Spiel. Per Premium-SMS oder -Telefonie können Dritte dazu legitimiert werden, Abbuchungen vom Konto des Telefonkunden vorzunehmen. Anfängliche Negativmeldungen über Klingelton-Abofallen oder drastisch überhöhte Telefonrechnungen von Senioren führten jedoch zu einem Vertrauensverlust für diese Technologie. Deutsche Kunden sind, was ihre Telefonrechnung betrifft, in den letzten Jahren enorm sensibel geworden und prüfen misstrauisch auch leichte Erhöhungen in der monatlichen Rechnung.

NFC

Von NFC (engl. „Near Field Communication“) wird man in nächster Zeit vermehrt hören. Hierbei handelt es sich im engsten Sinne um eine Funktechnik, die nur auf kurzen Distanzen funktioniert. Was der bekannte Strichcode (Barcode) auf optischer Basis darstellt, ist NFC in elektronischer Form, beide können eine Identität abbilden. Der NFC-Chip kann ähnlich dem Ladegerät für elektrische Zahnbürsten den benötigten Strom aus der Umgebung aufnehmen und Daten zurück an den Empfänger senden, aber auch an eine eigene Stromquelle gekoppelt sein. Die Flexibilität in der Stromversorgung und eine relativ günstige Herstellung, kombiniert mit den Aspekten, dass sich globale Firmen schon auf einen technischen Standard geeinigt haben und die Daten von Grund auf verschlüsselt sind, sprechen für NFC. Die neue Technik wird bereits in verschiedenen Produkten und Pilotversuchen eingesetzt (siehe Seite 18).

WAS IST MOBILE PAYMENT EIGENTLICH?

Während die NFC-Technologie gerade erst in größerem Rahmen ausprobiert wird, kann man auf andere Arten mit dem Handy schon seit mehreren Jahren am Geschäftsleben teilnehmen. So können Nutzer per SMS die Parkuhr befüllen, spenden oder an TV-Gewinnspielen teilnehmen. Mit bis zu vier Jahre alten Handys kann man mittels App Fahrscheine für den öffentlichen Nahverkehr oder Flugtickets kaufen. Und natürlich ermöglicht jedes internetfähige Handy Einkäufe und Zahlungen auf jeder beliebigen Internetseite – einfach per Eingabe der persönlichen Kreditkartendaten.

Der Begriff „Mobile Payment“ ist somit sehr stark an das Konzept des „Online Payment“ gebunden. Im engeren Sinne spricht man von Mobile Payment unter folgenden Voraussetzungen:

1. Mittels einer speziell auf das Handy zugeschnittenen Lösung (App oder spezielle Internetseite) wird unter Zuhilfenahme eines entfernten Servers eine Zahlung getätigt.

2. Das Handy wird als einzigartig angesehen, stellt also eine Art „Ausweis” dar und wird einer natürlichen Person zugewiesen. Dies kann durch die Handynummer, Kartennummer (IMEI) oder das Benutzerkonto sichergestellt werden.

3. Sensoren des Handys (GPS, Kamera, Lagesensor, Mikrophon) vereinfachen die Zahlung oder sichern diese zusätzlich ab.

DAS NÄCHSTE GROSSE DING?

2012 wird das Jahr, in dem das Handy Kontakt mit der Geldbörse aufnimmt, so die Meinung vieler Experten. Einer davon ist Frank-J. Arnold, selbst Entwickler von Vertriebs- und Zahlungsdiensten für den Mobilfunk. Für Digitalkompakt analysiert er die Chancen für Mobile Payment.

Die aktuellen technischen Entwicklungen im Bereich Smartphone und NFC machen es klar: Noch nie waren die Voraussetzungen für einen Erfolg so günstig. Im Internet gibt es mittlerweile seit rund 15 Jahren Versuche, Mobile Payment für die Masse zu etablieren, bislang ohne durchschlagenden Erfolg. Das zeigten ambitionierte internationale Bezahl-Dienste wie Paybox oder Luupay, letzterer wurde im März 2009 bereits wieder eingestellt.

Und in Deutschland? Das Dilemma vieler Versuche ist: Es gibt wenig benutzerfreundliche Systeme, die oft eine aufwändige Registrierung und/oder Kontoaufladung erfordern und insgesamt viel zu viele kleine Insellösungen. Außerdem hat der Markt zumindest bei Bezahlvarianten via Telefonrechnung ein Imageproblem, das unter anderem von unseriösen Abofallen in der Vergangenheit herrührt. Für die Anbieter kann es für die Zukunft nur eine Konsequenz geben: Maximale Usability und Transparenz. Jeder Kaufprozess muss schnell, einfach und sicher sein. Anonym, also ohne Registrierung oder die Angabe von Konto- oder Kreditkartendaten, muss der Nutzer digitale Güter innerhalb von 30 bis 40 Sekunden bezahlen und downloaden können. Maximale Transparenz heißt dabei, dass der Kunde genau erkennt, was er kauft und den Kauf auf seiner Mobilfunkrechnung auch verständlich nachvollziehen kann. Hier haben die deutschen Mobilfunkanbieter in den vergangenen Monaten unter anderem durch die „Clean Market Initiative“ (www.mehrwertdienstekompetenz.de) Boden gutgemacht: Verbindliche Vorgaben sollen unseriöse Angebote aus dem Markt verdrängen und das Vertrauen der Endkunden in Mobile Payment stärken.

Fazit Schon in wenigen Jahren muss man also hoffentlich nur noch sein Handy dabei haben, um den Wochenendeinkauf zu bezahlen und anschließend zum Essen oder ins Kino zu gehen. Die Marktanalysten von Juniper Research erwarten jedenfalls, dass 2015 rund 670 Mrd. Dollar weltweit mit Mobile Payment umgesetzt werden.

Frank-J. Arnold

EIN NEUER MARKT FÜR GLOBAL PLAYER

Wenn es um Finanzangelegenheiten geht, haben Banken und Sparkassen einen enormen Vertrauensvorschuss. Dennoch gibt es Unternehmen, die auch in die Geldbeutel deutscher Verbraucherinnen und Verbraucher Einzug gehalten haben.

Neben Telekommunikationsanbietern und Kundenbindungsprogrammen wie Payback genießen auch Internetshops von Amazon bis Ebay, Suchmaschinenbetreiber wie Google oder Firmen aus der Unterhaltungselektronik wie Apple oder Nokia mehr Vertrauen. Dieser Markt ist derzeit besonders stark im Umbruch, setzen verschiedene Unternehmen doch die größte Hoffnung in die Einführung von NFC. Als federführend kann man Google mit seinem Dienst „Google Wallet" zusammen mit Mastercard, Citi (US-amerikanische Bank), Sprint (US-amerikanischer Mobilfunkanbieter) und First Data (Dienstleister für bargeldlosen Zahlungsverkehr) bezeichnen. Mit der Technologie wird ein Datenaustausch ohne große Nutzerinteraktion möglich. Da NFC-Daten auch sehr stark verschlüsselt werden können, wird die Technik für Finanzdienstleistungen interessant. So können Kredit- oder Girokartendaten übertragen werden, ebenso kann man auf ein lokal auf einem Geldchip gespeichertes Guthaben zugreifen. Viele Unternehmen haben sich bereits auf ein System geeinigt. So ist eine breite technische Kompatibilität garantiert.

Angesichts des Potenzials, das die beteiligten Global Player in dieser Technik sehen, darf wohl von einem großen Erfolgsdruck ausgegangen werden. Für die Verbraucher heißt das: Mit Kampagnen für diese Bezahlvariante darf gerechnet werden.

« N-Mark-Logo™ für NFC-zertifizierte Geräte

WELCHE OPTIONEN HABEN NFC-NUTZER?

Wenn heutzutage von NFC die Rede ist, ist meist der Einsatz im Mobiltelefon gemeint. Dabei beschränkt sich die Technik gar nicht auf den Handyeinsatz – und selbst dort gibt es verschiedene Verwendungsmöglichkeiten.

Grundsätzlich gibt es für das mobile Bezahlen mittels NFC verschiedene Varianten. Im Gegensatz zu älteren Techniken wie Magnetstreifen oder Chip-Karte wurde NFC offen angelegt. So kann der Nutzer etwa seine Kreditkarte, aber auch Daten von Kunden- oder Punktekarten auf sein Handy übertragen und nutzen, als seien es die originalen Plastikkarten. Möchte man mittels Kreditkarte zahlen, öffnet man im Handy ein Programm und wählt die entsprechende Karte aus. Hält man nun das Mobiltelefon an das Lesegerät der Kasse, werden alle Daten automatisch übertragen – die Zahlung ist beendet. Gleichzeitig könnte man sich auch die Punkte für den Einkauf etwa bei Payback automatisch gutschreiben lassen. Alternativ dazu ließe sich auf dem Handy ein Geldbetrag digital speichern und per NFC abbuchen. In diesem Fall wäre keine Übertragung von Kartendaten nötig. Übrigens ist NFC-Technik nicht zwingend mit einem Mobiltelefon verbunden – auch können etwa Giro- oder Kundenkarten mit einem NFC-Chip ausgerüstet werden.

NFC selbst stellt also kein Bankkonto oder dergleichen dar. Es ist lediglich ein Vehikel zur Datenübertragung, ähnlich dem Magnetstreifen der Girokarte. Der Nutzer spart durch das viel schnellere Verfahren Zeit und bei der Anwendung im Mobiltelefon gewinnt er außerdem Übersicht und viel Platz im Geldbeutel – vielfältige Plastikkarten werden somit überflüssig. Doch natürlich gibt es auch Kritikpunkte. Neben datenschutzrechtlichen Themen (siehe Interview Seite 22) ist das größte Manko der meisten neuen Lösungen, dass diese auf einem vollen Handyakku basieren. Ist in dem Mobiltelefon eine mobil gekaufte Fahrkarte oder ein Flugticket gespeichert, der Akku währenddessen jedoch leer geworden, kommt man bei einer Kontrolle in Erklärungsnöte. Im besten Fall kann man die Fahrkarte nachreichen – im schlimmsten Fall kann man deswegen den Flug nicht antreten.

SCHON IM EINSATZ

Derzeit ist NFC schon in verschiedenen Geräten und Medien implementiert. Darunter sind der neue ePersonalausweis, diverse neue Handymodelle von Nokia und Google sowie spezielle Kreditkarten von Visa und Mastercard. Darüber hinaus sind in Deutschland bereits verschiedene ganz konkrete Anwendungen für Mobile Payment in Funktion – mit und ohne NFC.

HandyTicket

Eine verbreitete Lösung, die bislang ohne NFC auskommt, ist der mobile Ticketverkauf für den ÖPNV in vielen Verkehrsverbünden. Über eine entsprechende App kann man – nach vorheriger Registrierung – Fahrscheine kaufen. Vor dem Fahrtantritt mit Bus oder Bahn wählt man über das Handy den passenden Fahrschein aus und bekommt ihn auf das Gerät geschickt, ganz ohne Papierticket, Wartezeit und Kleingeldnöte. Erfolgt eine Fahrkartenkontrolle, zeigt man auf dem Handydisplay den erhaltenen speziellen QR-Code plus tagesaktuellem Stichwort (z.B. „Baum Auto“), den der Kontrolleur mit einem Lesegerät prüft.

Girogo

Die Sparkassen rüsten auf. Nicht nur moderne Handys bekommen NFC-Technik, auch Bankkarten können damit ausgestattet werden. Bis Mitte April 2012 sollen in einem Pilotversuch im Raum Hannover, Braunschweig und Wolfsburg rund 1,3 Millionen Kunden die „Girogo“ genannte Zahlfunktion per Prepaid-Chip testen. Dafür wurde die Girokarte, die klassisch mit Magnetstreifen, Unterschrift und Chip ausgestattet ist, um NFC erweitert. So können die Kunden beim Bezahlen an der Kasse je nach Terminal wählen, wie sie bezahlen wollen. Nach Angaben des Deutschen Sparkassen- und Giroverbands soll im August 2012 die bundesweite NFC-Einführung erfolgen. Bis Ende 2013 sollen schon 30 Millionen Karten ausgetauscht sein.

Touch&Travel

Die Deutsche Bahn testet im Pilotprojekt „Touch&Travel“ das Bahnreisen der Zukunft. Mit diesem Service kann man ohne vorherigen Kauf eines entsprechenden Tickets mit dem Zug zu seinem Ziel fahren. Vor dem Einstieg in den Zug hält der Fahrgast sein NFC-taugliches Handy an einen sogenannten Touchpoint am Bahngleis und registriert so den Beginn seiner Fahrt. Am Ziel angekommen, checkt er ebenfalls an einem Touchpoint aus. Touch&Travel erhält anschließend vom Mobilfunkbetreiber das Bewegungsprofil des Reisenden und errechnet hieraus den entsprechenden Fahrpreis. Abgerechnet wird anschließend per Bankeinzug.

Dabei ist zu beachten, dass die Reisenden für die komplette Dauer der Fahrt „getracked“, also lokalisiert werden. Der Fahrpreis errechnet sich somit aus Daten, die bisher nur dem Mobilfunkanbieter bekannt waren. Dabei legt die Deutsche Bahn nach eigenen Angaben höchsten Wert auf Datenschutz und Transparenz. So erklärt Projektleiterin Birgit Wirth auf Anfrage von Digitalkompakt: „Die Routeninformation an sich interessiert uns nicht. Sie ist ist nur das Vehikel, um die richtige Preisinformation zu bekommen. An der Ortung per se besteht kein Interesse.“ Als Kunde muss man sämtlichen Weitergaben von persönlichen und sensiblen Daten erstmalig aktiv und bewusst zustimmen.

mpass

Drei deutsche Mobilfunkunternehmen bieten unter dem gemeinsamen Namen „mpass“ eine mobile Bezahllösung an, die heute bereits mittels eines SMS-TAN-ähnlichen Verfahrens funktioniert. Dabei wird der Betrag nicht mit der Telefonrechnung, sondern direkt mit dem verknüpften Bankkonto beglichen. Voraussetzung ist ein deutsches Bankkonto und ein Mobilfunkvertrag, daher ist der Dienst erst ab 18 Jahren zugänglich. Ab 2012 will mpass zusätzlich die Möglichkeit bieten, mit jedem Handy und einem aufgeklebten NFC-Sticker Zahlungen ausführen zu können. Auch hier werden die Zahlungen dann per Lastschrift vom Konto beglichen.

Sind Verbraucher mit Mobile Payment überfordert?

Funktioniert das wirklich? Und was, wenn nicht? Ein Digitalkompakt-Interview mit Finanzexpertin Dr. Annabel Oelmann über die Sorgen der deutschen Verbraucher – besonders, wenn es ums Geld geht.

Dr. Annabel Oelmann ist bei der Verbraucherzentrale NRW in Düsseldorf als Gruppenleiterin Finanzdienstleistungen tätig.

DIGITALKOMPAKT *Mobiles Bezahlen ist auf dem Vormarsch. Aber reichen die Vorteile für eine breite Akzeptanz? Welche Probleme sehen Sie aus der Perspektive des Verbraucherschutzes?*

OELMANN In erster Linie bieten alle mobilen Bezahlmöglichkeiten dem Verbraucher natürlich Vorteile. Weniger Kleingeld in der Tasche ist der offensichtlichste. Auch ist die Sicherheit zumindest im Vergleich zum Bargeld sogar besser. Man sollte sich vor Augen halten: Das Bargeld ist weg, wenn man es verliert, während es bei mobilen Bezahlsystemen hingegen Sicherheitsmechanismen gibt. Besonders bequem ist die Kombination mit dem Handy, das heutzutage sowieso jeder dabeihat. Nachteile sehen wir eher dann, wenn zusätzliche Kosten für den eigentlichen Bezahlprozess verlangt werden. Auch hat noch nicht jeder ein modernes Handy mit Internetzugang.

Wir steuern also auf eine technische Ausgrenzung zu?

OELMANN Ja, genau. Oder den Zwang, in eine spezielle technische Ausrichtung wechseln zu müssen. Ein weiterer Nachteil ist auch, dass man sich der Technik ausliefert. Wir hatten erste Fälle, in denen die Verbraucher schilderten, sie hätten mit dem Handy beispielsweise ein Flugticket bezahlt, und mussten das anschließend mit dem Handy nachweisen. Und dann war der Handyakku leer. Auf so etwas zu achten, ist die Pflicht des Verbrauchers – dennoch ist das einer der Schwachpunkte.

Ein anderer wichtiger Aspekt ist die Erziehung zum Umgang mit Geld. So werden Kinder und Jugendliche in manchen Geschäftsmodellen mit virtuellen Währungen (Credits) statt Euros konfrontiert. Behindert E-Geld die Entwicklung?

OELMANN Ja. Auf einer Karte merken die jungen Nutzer gar nicht mehr, wie viel sie wirklich ausgeben. Durch Credits wird das nochmal schwerer, wenn auch noch Wechselkurse ins Spiel kommen. Dadurch fehlt ihnen ein wichtiger Entwicklungsschritt: die langsame Gewöhnung an Geld und seinen Wert. So sollten Kinder im Grundschulalter das Taschengeld noch wöchentlich, später monatlich bekommen. Es braucht einen Lernprozess hin zu größeren Beträgen und dem vernünftigen Umgang damit.

Neben den klassischen Banken rücken private Unternehmen in den Fokus für Finanzgeschäfte. Neben Online-Auktionen oder Versandhandel treten diese nun auf und verwalten das private Geldkonto. Ist der Verbraucher diesem Trend aufgeschlossen?

OELMANN Das Hauptproblem für die Verbraucher ist, dass bereits im normalen Bankbereich viele Dinge ungeklärt sind. Und jetzt kommt eine völlig neue Variante dazu, die auch juristisch und organisatorisch geregelt werden muss: Wer ist wofür zuständig? Wer wendet sich an wen? Wo finden Gerichtsverfahren statt? All das führt natürlich zu massiver Unsicherheit.

Mit NFC wird ein komplett neues – und berührungsloses – Bezahlverfahren auf den Verbraucher zukommen. Hier könnte sich die Angst vor fehlender Nachverfolgbarkeit als schwierig herausstellen.

OELMANN Man hat natürlich die Angst, dass man irgendwo langgeht und unbemerkt Geld vom Konto abgezogen wird. Hier setze ich auf die Anbieter, mit Nachdruck zu verdeutlichen, dass dem nicht so ist.

Letztlich ist es egal, mit welcher Übertragungsart das Geld abgebucht wurde – man benötigt immer eine Bestätigung – im besten Fall in Papierform. Wird die doppelte Bestätigung Pflicht werden?

OELMANN Das ist uns sehr wichtig und sollte für alle Finanztransaktionen im weitesten Sinne gelten. Dem Verbraucher sollte aber auch klar sein: „Hier muss ich besonders darauf achten, hier muss ich regelmäßig prüfen“. Viele Bezahlvarianten werden außerdem auch mit Lastschrift beglichen. Das heißt, der Nutzer hat auch die Möglichkeit, gegen eine Zahlung Einspruch zu erheben oder zurückzufordern.

Wird der gläserne Bürger Wirklichkeit?

Ist Mobile Payment ein Versuch, mehr staatliche Überwachungsmöglichkeiten in unseren Alltag zu bringen? Der Düsseldorfer Medienrechtler Udo Vetter hält im Digitalkompakt-Interview jedenfalls dem Bargeld die Stange.

Udo Vetter (* 1964) ist Rechtsanwalt in Düsseldorf und Lehrbeauftragter für Medienrecht an der Fachhochschule Düsseldorf. Bekannt ist er durch sein Blog law blog und durch Interviews und Auftritte als Rechtsexperte. Beachtung fanden zudem seine Vorträge bei Veranstaltungen des Chaos Computer Clubs.

DIGITALKOMPAKT *Mobile Payment mittels NFC-Technik wird 2012 einer der großen Treiber für digitales Bezahlen werden. Wie sehen Sie dieser Entwicklung aus juristischer Sicht entgegen?*

VETTER Die Technik ist ja in aller Munde: Googles Android-System wird mit der neuen Version serienmäßig ausgeliefert werden. Das ist eine der nächsten großen Sachen, wenn Bezahlen – sowohl offline, als auch online – ohne die Bewegung körperlicher Gegenstände oder die willentliche Eingabe von Daten geschehen kann. Frühere Versuche wie die Geldkarte oder SMS-Payment sind ja im Ansatz gescheitert oder gelten zumindest als gescheitert. Ob NFC nun eine Revolution wird, wird von der Einfachheit der Nutzung, der Sicherheit der Daten und der Bequemlichkeit abhängen.

Man kann bereits mittels SMS oder Apps bezahlen. Meistens handelt es sich hierbei jedoch um unterschiedliche Insellösungen, eine globale Lösung mit der jeder vertraut ist wie beim Bezahlen per Geldschein gibt es nicht. NFC könnte hier behilflich sein, digital einen einheitlichen Standard zu bieten...

VETTER Das Interessante daran ist, dass es bereits globalisierte Zahlungsmöglichkeiten gibt, wie etwa Kreditkarten oder Bitcoin. Wenn aber bald das Handy und damit das Google- oder iTunes-Konto zum grenzüberschreitenden Portemonnaie werden, dann ist das aus Nutzersicht eine unglaublich attraktive Angelegenheit – wenn die Umstände der Dateneingabe entfallen. Man darf allerdings nicht unterschätzen, dass speziell die Deutschen sehr vorsichtig hinsichtlich Online-Zahlungen sind. Das System muss wirklich funktionieren, wenn man sicher gehen will, dass es nicht bereits innerhalb des Bezahlvorgangs scheitert.

Die Einführung einer neuen Technik verunsichert uns – und windige Geschäftemacher versuchen, daraus Profit zu machen. Gab es bei ähnlichen technischen Einführungen ein Lernen des Bürgers? Oder wird es die gleichen Schreckensmeldungen wie bei der Geldkarte oder Online Payment geben?

VETTER Das hängt von der technischen Intelligenz der beteiligten Unternehmen ab. Beim Mobile Payment haben wir es natürlich mit einer Kernfrage zu tun, einem umwälzenden Projekt, das von vornherein klappen muss. Sollte es relevante Sicherheitslücken aufweisen, ist das Bezahlen mittels NFC erst einmal Geschichte und wird in 10 bis 15 Jahren wiederkommen. Ich gehe davon aus, dass das den Verantwortlichen in den Konzernen, die vorwiegend in den USA sitzen, bewusst ist. Sie werden versuchen, einen perfekten Start hinzulegen, der auch den Sicherheitsbedenken der Bürger gerecht wird.

Gewiss werden wie üblich Hacker-Verbände wie der Chaos Computer Club (CCC) und andere Organisationen geradezu dazu aufgerufen, nach Sicherheitslücken zu suchen. Und es wird sicherlich welche geben – die Frage ist jedoch, wie weit das die Nutzer beunruhigen wird. Eine Grundskepsis gibt es schon deswegen, weil das „Geld ausgeben“ automatisiert wird. Es ist schließlich keine bewusste Handlung wie das Überreichen von Geldschein oder Kreditkarte mehr nötig.

Mit vielen Mobile-Lösungen können Zahlungen in Kleinstbeträgen auf internationaler Ebene bis zu einzelnen Personen zurückverfolgt werden. Der vielmals beschworene „gläserne Bürger“ wird nun richtig gläsern, wenn der Kauf eines Kaugummis der Person „Max Mustermann“ zugerechnet werden kann. Ist dieses Szenario denkbar? Ist dies aus rechtlicher Sicht problematisch? »

WIRD DER GLÄSERNE BÜRGER WIRKLICHKEIT?

VETTER Das elektronische Bezahlen ist immer problematisch. So gibt es in Schweden die Gesetzesinitiative, das Bargeld abzuschaffen, um den Ermittlungsbehörden die Überwachung aller Geldbewegungen zu ermöglichen. Es gibt also ein staatliches Interesse, den Bargeldverkehr zurückzudrängen, das mit Terrorismus und Kriminalitätsbekämpfung zu tun hat. Dafür kann man aber nicht die anbietenden Unternehmen verantwortlich machen. Natürlich haben auch Google oder Apple Interesse an Kundendaten. Ich weigere mich aber, den Anbietern von vereinfachender und schönermachender Technologie im Voraus zu unterstellen, sie würden uns ausspionieren wollen. Das glaube ich nicht. Wenn herauskäme, dass Google Missbrauch mit den Daten betreibt, wäre das Geschäftsmodell zerstört. Abgesehen davon: Jeder der etwa eine Payback-Karte hat, gibt wesentlich mehr Daten preis als wenn er Bezahlvorgänge über solche Unternehmen abwickeln lässt. Und wer mit der Girokarte oder Kreditkarte bezahlt, hinterlässt heute ja genauso Spuren, im Supermarkt, an der Tankstelle, im Hotel.

So erzeugt jede Form von elektronischer Bezahlung eine unvermeidliche Datenspur, auf die Behörden Zugriff haben. Aus datenschutzrechtlicher Perspektive sollte tatsächlich Bargeld das Mittel erster Wahl sein. Denn es kann keiner garantieren, dass Daten, die heute aus normalen Beweggründen erfasst wurden, morgen nicht dazu verwendet werden, Profile von Menschen zu erstellen. Es ist mein gutes Recht, mein Privat- oder Berufsleben nicht transparent werden zu lassen. Dafür ist die Barzahlung, auch wenn sie veraltet erscheinen mag, immer noch die beste Methode. Außerdem freut sich der Rezeptionist im Hotel viel mehr, schließlich müsste er bei einer Kreditkartenzahlung Prozente an den Lizenzgeber entrichten.

Das Gebot der geringsten Datenerhebung sollte auch bei Bezahlungen gelten. Andererseits muss man eine Zahlung einer einzelnen Person und dem Händler zur Abrechnung zuordnen können. Dies läuft jedoch konträr zur aktuellen Datenschutzdebatte. Aktuellstes Beispiel ist die vieldiskutierte EU-Vorratsdatenspeicherung.

VETTER Die Vorratsdatenspeicherung bezieht sich in erster Linie auf die Telekommunikation. Wobei hier natürlich Graubereiche entstehen. Denn NFC ist auch eine Art von Telekommunikation, wird sie doch über das Mobiltelefon ausgeführt. Spitzfindige Ermittler können damit sicherlich auch an diese Daten gelangen. Somit geht das in eine ähnliche Richtung wie in Schweden: „Bargeld ist im Prinzip gefährlich“ und muss abgeschafft werden. Damit erleben wir hier eine völlige Umkehr der Paradigmen. Bislang ist nach dem Telemediengesetz noch vorgeschrieben, dass Internetnutzung pseudonym oder anonym erfolgen können muss. Doch nun predigen die Politiker, dass sich jeder im Internet identifizieren soll. „Anonymes Bezahlen muss weg“ hört man nun. NFC ist ein faktischer Schritt, Bargeld abzuschaffen – das muss man ganz klar sehen.

Kritisch wird es aber erst dann, wenn für den einzelnen Nutzer nicht mehr absehbar ist, was mit seinen Daten passiert. Und wenn er überhaupt nicht mehr die Wahl hat, anders zu bezahlen. Natürlich ist die Nutzung von Facebook, Google & Co. immer mit einer Preisgabe eigener Daten verbunden. Hier kann man sich aber bewusst dafür oder dagegen entscheiden. Schrecklich wird es nach meiner Meinung erst in dem Augenblick, wenn dem Bürger die Wahlmöglichkeit genommen wird, etwa indem anonyme Bezahlmöglichkeiten abgeschafft werden.

Mobiles Bezahlen soll nicht verteufelt werden, dennoch gibt es viele Dinge, die man wissen sollte, die einem aus dem bisherigen Umgang mit Geld kaum oder gar nicht bewusst waren.

VETTER Das Bürgerliche Gesetzbuch sagt: „Bargeld ist die einzig wahre Zahlungsmethode“ alles andere ist nur eine „Erfüllung statt“ wenn die Zahlung erfolgt ist. Das war sozusagen das „alte“ Denken. Man kann als Bürger standhaft bleiben und es weiterhin so handhaben. Bargeld in den Geruch der Geldwäsche, der organisierten Kriminalität oder gar des Terrorismus zu rücken, das ist schon ein infamer Versuch, unsere Gesellschaft zu „Orwell-isieren“. Man kann immer den guten Willen dahinter sehen, den Politiker haben, aber sie vergessen dabei, dass „die Freiheit in Scheiben stirbt.“ Sie stirbt nicht von heute auf morgen, sondern jedes Stück, das mehr unter die Kontrolle auf Knopfdruck gerät, führt dazu, dass die Freiheit geringer wird. Ohne die persönliche Freiheit des Einzelnen steht die Demokratie nur auf dem Papier! Bargeldzahlung sollte auch ein kleines Signal an die Politik sein: „Lasst mich bitte in Ruhe“.<<

TIPPS ZUM SICHEREN UMGANG MIT PERSÖNLICHEN DATEN

Gesundes Misstrauen im Internet und vor allem beim Onlinebanking gehören inzwischen zur Allgemeinbildung. Also aktuelle Virenscanner installieren, Mails mit fragwürdigen Anhängen nicht öffnen und niemals dem angeblichen Bankberater Kontodaten per E-Mail schicken! Mit der gleichen Vorsicht sollten Sie auch durch den realen (Bezahl-)Alltag gehen.

Mit diesen Schritten bleiben Sie weiterhin „Herr Ihrer Daten“

1. Geben Sie Ihre Karte nicht aus der Hand oder haben Sie zumindest immer im Auge, was mit Ihrer Karte geschieht.
2. Ihre PIN-Nummer ist geheim. Lassen Sie sich beim Eingeben nicht über die Schulter schauen und teilen Sie die PIN niemandem mit. Bewahren Sie auch Ihre TAN-Nummern an einem versteckten Ort auf.
3. Speichern Sie Passwörter, PIN und Ihre TAN-Liste nur dann elektronisch ab, wenn die von Ihnen getroffenen Vorkehrungen zur Datensicherheit dem aktuellen Sicherheitsstandard für sensible Daten entsprechen, z.B. adäquater Passwortschutz und leistungsfähige Firewall, Anti-Virensoftware, regelmäßige Sicherheitschecks etc.. Heften Sie diese wichtigen Daten auch real an einem sicheren Ort ab.
4. Einige Online-Shops bieten zusätzliche Sicherheitsmechanismen der Kreditkartenunternehmen an (z.B. Securecode von MasterCard). Schalten Sie, wenn immer möglich, diese Zusatzfunktionen frei – auch wenn Sie den Komfort schmälern und den Einkaufsprozess verlangsamen.
5. Bestehen Sie bei der Registrierung für einen hochsensiblen Dienst (Bankgeschäft etc.) darauf, dass persönliche Daten durch einen zweiten Übertragungsweg zur Überprüfung an Sie gesendet werden. Ähnlich der Girokarte und PIN, die in zwei separaten Briefen versendet werden.
6. Vorsicht bei Apple iTunes: Einige Minuten nach dem Kauf eines Liedes oder einer neuen App, bleibt Ihr Mobiltelefon in einer Art „Bezahlmodus“. Der Kauf neuer Programme oder Zusatzfunktionen erfordert keine erneute Eingabe des Passwortes. Fehlkäufe und Missbrauch sind hierdurch möglich. Sperren Sie Ihr Handy bewusst.
7. Vorsicht beim Einwählen in öffentlich zugänglichen WLAN-Hotspots, z.B. in großen Hotels oder an Bahnhöfen. Ihre persönlichen Daten können in unverschlüsselten Hotspots oder solchen mit gleichem Schlüssel mittels kostenloser Tools problemlos abgefangen werden! Nutzen Sie wenn möglich eine eigene Leitung z.B. UMTS-Handy an Laptop, privates WLAN oder ein Virtual Private Network (VPN) auch „Tunnel“ genannt.
8. Geben Sie Ihre Kreditkartendaten nur auf vertrauenswürdigen Seiten ein und prüfen Sie möglicherweise besonders günstige Angebote in einem kritischen Preisvergleich.
9. Teilen Sie weder Ihre Kreditkarten- noch Ihre Bankdaten bei überraschenden Werbeanrufen zu Hause oder auf Ihrem Handy mit.
10. Beobachten Sie die Maske Ihrer Bank für das Onlinebanking und geben Sie Ihre Daten nicht ein, wenn die Maske unüblich gestaltet ist.
11. Zum Onlinebanking reicht die einmalige Eingabe Ihrer Zugangsdaten; mehrmaligen Aufforderungen hierzu sollten Sie nicht nachkommen, die Maske könnte dann gefälscht sein. Um sicherzugehen, sollten Internetadressen vollständig eingetippt und nicht über Lesezeichen, Autovervollständigen oder Links dritter Seiten angewählt werden. Sollten Unsicherheiten bestehen, brechen Sie einen Vorgang ab und schließen alle Fenster.
12. Eine sichere Datenverbindung kann man auch daran erkennen, dass in der Browserzeile „https“ statt „http“ steht („s“ für „safe“). Achten Sie auf dieses Kennzeichen – meist durch ein Schloss-Symbol unterstützt – auch beim mobilen Onlinebanking.

WAS TUN IM PROBLEMFALL?

Trotz aller Sicherungsvorkehrungen kann es dennoch passieren: Es kommt zu Streitigkeiten mit dem Händler, der abbuchenden Stelle oder der Bank. An wen wenden Sie sich? Und was ist zu tun, wenn Karte oder Handy gestohlen wurden?

1. Wenden Sie sich in erster Linie an das Unternehmen, das eine Forderung gegen Sie stellt. Meist ist es mit einem Anruf, einer E-Mail oder einem Brief getan. Schildern Sie den Fall und dokumentieren Sie jeden Ihrer Schritte mit Ansprechpartner, Uhrzeit und Kommunikationsweg. Lassen Sie sich, wenn möglich, jedes Gespräch schriftlich bestätigen.

2. Sichern Sie möglichst viel „Beweismaterial“. Dies kann von einer gesendeten SMS über den Einzelverbindungsnachweis bis zur Rechnung alles sein, was zur Klärung des Sachverhalts beiträgt.

3. Stoßen Sie bei der Gegenseite auf Widerstand oder wissen nicht, an wen Sie sich konkret wenden sollen? Ziehen Sie eine ansässige Verbraucherzentrale zu Rate. Sie steht Ihnen beratend zur Seite.

4. Sollten alle Bemühungen nicht helfen, wenden Sie sich an einen Anwalt.

5. Wurde Ihre Girokarte oder Kreditkarte gestohlen? Ist Ihr Handy mit NFC-Karte abhanden gekommen? Wählen Sie den einheitlichen Sperr-Notruf 116 116. Hier können Sie neben Bankkarten und Handy-SIM-Karten auch Karten mit Zahlfunktion oder Online-Banking-Accounts sperren lassen.

KOMMENTAR

KLEINGELD WIRD ES AUCH IN ZUKUNFT GEBEN.

So schön die neue Welt des Bezahlens erscheinen mag, so genau sollte man sie prüfen. Mobiles Bezahlen hat zweifelsohne das Potenzial, die Art und Weise des zukünftigen Warenerwerbs nachhaltig zu verändern. Es wird möglich sein, den Einkaufswagen zu füllen und den Laden zu verlassen, ohne an einer sichtbaren Kasse vorbeizugehen. Kein Diebstahl – hat man die Waren doch bereits beim Entnehmen aus dem Regal bezahlt. Dennoch müssen kritische Fragen erlaubt sein: Was ist, wenn man einen Artikel zurückgeben möchte? Wie gehen ältere Mitmenschen mit dieser Technik um, für die sie ein modernes Handy brauchen? Und wie gelangt man etwa an der Tankstelle an sein E-Geld, wenn der Akku auf dem Weg zum Bezahlen seinen Geist aufgibt? Solange all diese Fragen nicht vollkommen geklärt sind und der Verbraucher nicht vollstes Vertrauen in die Technik und die beteiligten Unternehmen hat, wird es auch weiterhin Bargeld geben. Man sollte jederzeit Herr seiner Daten sein. Alleine aus Transparenzgründen muss es zur digitalen Zahlung auch ein überprüfbares Medium (Kassenzettel, E-Mail) geben, um sicher zu sein, dass alles seinen richtigen Weg gegangen ist. Einzelne Handelsketten mögen dies tun – es braucht jedoch nationale oder globale Lösungen, die überall gleich funktionieren.

Die EU wird darauf drängen, nationale Lösungen auf europäischer Ebene zu vereinheitlichen. Neben dem bekannten SEPA, also dem einheitlichen Euro-Zahlungsverkehrsraum für Überweisungen, wird dies auch das elektronische Bezahlen und Mobile Payment betreffen. Bei aller Sorge um den gläsernen Bürger in Zusammenhang mit NFC-Chips sollte man bedenken, dass auch Geldscheine in Zukunft mit einer ähnlichen Technik ausgestattet sein werden. Vergleichbar dem heutigen Reisepass, der elektronisch auslesbar ist, wird man in Zukunft auch Geldscheine elektronisch und damit automatisiert erfassen können. Dies kann den Hausbanken beim Zählen und den Bundesbanken bei einer Inventur helfen, jedoch ist damit auch denkbar, Geldflüsse auf einen einzelnen Bürger zurückzuführen. Was auf der einen Seite mehr Sicherheit suggeriert, kann schnell zu größerer Kontrolle führen.

Ob Bezahlen mit dem Handy, der Kreditkarte oder Bargeld – nicht für alle Probleme, Wünsche und Bedenken wird es stets die passende technische Lösung geben können. Von daher sollte es den Menschen freistehen, wie sie konsumieren, welche Daten sie preisgeben und welcher Zahlungsvariante sie letztendlich am meisten vertrauen.

DER AUTOR DIESER AUSGABE

Andreas Cappell ist Head of Product bei wer-kennt-wen.de. Als Social-Media-Experte und -Unternehmer ist er planend und beratend unter anderem zu den Themen „Mobile Apps“ und „Mobile Payment“ tätig. Bis August 2011 betreute er als Product Manager das Immobilienportal immowelt.de in den Themen Design, Social Media und Mobile Apps. In seinen vorherigen Stationen war er für Siemens Management Consulting und zuletzt für die Werbeagentur Publicis als Art Director in München u.a. für Disney, EADS und MAN tätig.
Andreas Cappell ist begeisterter Blogger und Twitterer.

GLOSSAR

Bitcoin Bitcoin ist eine Form von elektronischem Geld, das dezentral auf der Basis eines Computernetzwerks geschöpft wird. Es verbindet Eigenschaften von Bargeld mit solchen von internationalen elektronischen Überweisungen.

Girokarte ehemals EC-Karte

IMEI Die International Mobile Station Equipment Identity (IMEI) ist eine eindeutige 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät eindeutig identifiziert werden kann.

LBS Location Based Services ermitteln den Standort eines Nutzers anhand seines Mobiltelefons und unterbreiten ihm darauf abgestimmte Angebote, beispielsweise die Speisekarte eines Restaurants in der Nähe.

NFC Die Near Field Communication ist ein Übertragungsstandard zum kontaktlosen Austausch von Daten per Funk über kurze Strecken und wurde 2002 gemeinsam von NXP Semiconductors (vormals Philips) und Sony entwickelt.

Phishing Mit diesem Kunstwort aus „Personal Data“ und „Fishing“ werden Versuche von z.B. Hackern bezeichnet, sich über E-Mail, Internet und ähnliche Wege Identitätsdaten wie Passwörter oder Zugangscodes zu erschwindeln.

QR-Code QR steht für „Quick Response“. In einem QR-Code sind Informationen per zweidimensionalem Strichcode verborgen. Wird er per Handykamera fotografiert leitet eine spezielle App den User sofort auf die mit dem Code verknüpfte Web-Adresse.

SEPA Single Euro Payments Area (Einheitlicher Euro-Zahlungsverkehrsraum) bezeichnet im Bankwesen das Projekt eines europaweit einheitlichen Zahlungsraums. In diesem Zahlungsraum sollen für Kunden keine Unterschiede mehr zwischen nationalen und grenzüberschreitenden Zahlungen bestehen.

Skimming Kopieren des Magnetstreifens, Ausspionieren der PIN am Geldautomaten, Duplizieren der Karte. Dabei wird am Schlitz des Zahlungsterminals ein Lesegerät angebracht, das die Daten der eingeschobenen Karte kopiert. Über eine Videokamera, die das Zahlenfeld anvisiert, wird die Geheimnummer des Kunden aufgenommen. Mit den Daten wird die Karte dupliziert und anschließend zum Schaden des rechtmäßigen Besitzers missbraucht.

IMPRESSUM

Herausgeber
Landesanstalt für Medien
Nordrhein-Westfalen (LfM)
Zollhof 2
40221 Düsseldorf
Tel: 0211.77007-0
Fax: 0211.727170
www.lfm-nrw.de
info@lfm-nrw.de

Verantwortlich für den Inhalt
Dr. Thomas Bauer,
Leiter LfM Projektinitiative NRW digital

Autor
Andreas Cappell, cappellmeister.com

Redaktion
Dr. Dörte Hein, Sabrina Nennstiel (LfM)
Jens Frantzen, text-appeal.de

Gestaltung
Fritjof Wild, serviervorschlag.de

Druck
Börje Halm

Bildnachweise
S.3,4,7,9,14,26,28: Fritjof Wild
S.20: Verbraucherzentrale NRW
S.22: Udo Vetter
S.31: Stefan Aubele

Fußnote
S. 3
[1] GfK-Studie:
http://viewer.zmags.com/publication/c8fb8afd#/c8fb8afd/2

GLOSSAR

Landesanstalt für Medien
Nordrhein-Westfalen (LfM)
Zollhof 2
40221 Düsseldorf
Postfach 10 34 43
40025 Düsseldorf

Telefon
› **02 11 / 7 70 07-0**
Telefax
› **02 11 / 72 71 70**
E-Mail
› **info@lfm-nrw.de**
Internet
› **http://www.lfm-nrw.de**