Andreas Martin

Sicherheit im **Electronic Banking** – ein Wettbewerbsfaktor?

Vertrauen ist bekanntlich ein wesentlicher Grundpfeiler des Bankgeschäfts. Dies gilt zum einen, die Finanzkrise hat es deutlich herausgearbeitet, im Hinblick auf die Solvabilität von Instituten. Zum anderen ist Vertrauen aber auch ein wichtiger Faktor bei der operativen Abwicklung von Bankgeschäften, insbesondere in der Bereitstellung einer bedarfsgerechten Beratung und qualitativ hochwertiger Produkte, zugleich aber auch von stabilen Prozessen und Systemen.

Zum letztgenannten Bereich gehört neben der möglichst uneingeschränkten Verfügbarkeit ein hohes Sicherheitsniveau. Im konventionellen Zahlungsverkehr gilt dies schon lange als Herausforderung, im Electronic Banking haben neue Missbrauchsformen wie Skimming und Phishing die Notwendigkeit sicherer Verfahren einem breiten Publikum jüngst wieder vor Augen geführt.

Kartenzahlungsverkehr: eine besondere Verpflichtung

Für die genossenschaftliche Finanzgruppe mit ihrer starken Stellung im Retail Banking ist das Thema Sicherheit eine besondere Verpflichtung. 30 Millionen Kunden, davon 16,7 Millionen Mitglieder, vertrauen ihrer Genossenschaftsbank – und als Bankengruppe mit Filial- und Mitarbeiterpräsenz vor Ort müssen die Institute diese Vertrauensvermutung täglich, auch im Kundengespräch, unter Beweis stellen können. Dies wird durch die Online-Kundenzufriedenheitsmessung des BVR bestätigt. Sie zeigt, dass die besten Bewertungen bei den Hauptzufriedenheitsfaktoren – neben der Zufriedenheit mit der Beratung – auf die Merkmale Vertrauenswürdigkeit und Zuverlässigkeit entfallen. Zu Recht erwarten die Kunden, dass ihnen ihre Bank performante und sichere Systeme bereitstellt – und sie zugleich darüber informiert, wo eine Mitwirkung des Kunden zur Gewährleistung sicherer Transaktionen unabdingbar ist.

Die Sicherheit des kartengestützten Zahlungsverkehrs stellt sowohl für die Banken und ihre Karteninhaber als auch für die Akzeptanten gleichermaßen einen strategischen Erfolgsfaktor dar. Immer mehr Kunden wollen ihre Einkäufe im Einzelhandel bargeldlos bezahlen. So stieg der Anteil der Kartenzahlungen laut Erhebungen des EHI Retail Institute in diesem Jahrzehnt von 27 Prozent im Jahr 2001 auf 38,4 Prozent des abgewickelten Umsatzes im Jahr 2010, das sind rund 144 Milliarden Euro. Wichtigstes Kartenzahlungsverfahren war dabei die Girocard mit 20 Prozent vom Gesamtumsatz. Um diese Kartentransaktionen wirksam abzusichern, hat die genossenschaftliche Finanzgruppe als eine der ersten Bankengruppen konsequent in die Sicherheit ihrer Karteninfrastruktur investiert. So war sie einer der Vorreiter bei der Einführung des EMV-Chipkartenstandards.

Dr. Andreas Martin, Mitglied des Vorstands, Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. (BVR), Berlin

Ebenso wie die Einlagensicherung gehörten die Sicherheitsstandards im Bankgeschäft zu den Differenzierungsmerkmalen am Markt, mit denen allenfalls durch dezente Aufklärungsarbeit geworben wird. Nichtsdestotrotz ist es gerade für die großen Bankengruppen, die dank der Vielzahl ihrer Kunden ein lohnendes Ziel für Betrugs- und Missbrauchsmanöver bieten, von ganz elementarer Bedeutung, im Bereich der Sicherheitsvorkehrungen und der Prävention von Straftaten im elektronischen Bankgeschäft mit an der Spitze des technisch Machbaren zu stehen. Denn bei den heutigen Dimensionen der Transaktionen, so lässt es der Autor anklingen, hätte der Entzug von Kundenvertrauen bei den Zahlungstransaktionen verheerende Wirkungen auf die betroffenen Banken wie auch deren Kunden in der Wirtschaft. Höchste Sicherheitsstandards, so sein Hinweis in Richtung der Verbraucherschützer, haben allerdings ihren Preis, den die Kunden freilich akzeptieren, sofern man sie über die Notwendigkeit und den Nutzen der Weiterentwicklungen hinreichend aufklärt. (Red.)

Vorteil der Chiptechnik

Der Sicherheitsvorteil der Chiptechnik gegenüber dem Magnetstreifen besteht darin, dass der Chip gegen Duplizierung oder Veränderungen geschützt ist. Durch den Chip können die Echtheit der Karte und die PIN auch ohne Online-Verbindung geprüft werden. Bereits 1996 wurden die meisten VR-Bank-Cards mit Chips ausgestattet, die jedoch in der ersten Generation noch nicht in den internationalen Zahlungssystemen einsetzbar waren. Deswegen wurde von Europay/Mastercard und Visa der EMV-Standard mit dem Ziel geschaffen, alle europäischen Zahlungskarten an POS-Terminals und Geldautomaten chipfähig zu machen und Betrug zu verhindern. Heute sind alle genossenschaftlichen Girocards und Kreditkarten mit sicheren Mikrochips nach dem EMV-Standard ausgestattet.

V-Pay: Um die flächendeckende internationale Akzeptanz der genossenschaftlichen Debitkarten zu gewährleisten, sind alle Girocards im Co-Branding auch mit einem internationalen Debit-Verfahren von Mastercard oder Visa ausgestattet. Die deutschen Genossenschaftsbanken waren dabei die erste große Bankengruppe in Deutschland, die sich auch für das neue, von Visa Europe entwickelte V-Pay-System entschieden haben. Das besondere Merk-

mal ist das auch im Ausland garantierte hohe Maß an Sicherheit, da beim internationalen Einsatz einer V-Pay-Karte – sowohl bei Bargeldabhebungen wie auch bei Kauftransaktionen – stets der Chip und die PIN geprüft werden. So wird das Betrugsrisiko durch Diebstahl oder Kartenfälschung minimiert. Aktuell haben sich daher bereits mehr als 60 Prozent der genossenschaftlichen Institute für das Co-Branding ihrer VR-Bank-Card mit dem besonders sicheren V-Pay-System entschieden.

116 116: Das unkomplizierte Bezahlen mit Karten auch im Ausland ist bei den Verbrauchern beliebt. Besonders in der Urlaubszeit herrscht Dauereinsatz für Zahlungskarten. Dann nutzen jedoch auch Diebe und Trickbetrüger jede Gelegenheit, um an die Geldbörsen und Karten der Verbraucher zu kommen. Die Bankkunden werden deswegen immer wieder sensibilisiert, mit den Karten genauso sicher umzugehen wie mit Bargeld. Dazu gehört auch, dass gestohlene oder verlorene Zahlungskarten schnellstmöglich gesperrt werden, um eventuellen Missbrauch zu verhindern.

Bundeseinheitliche Sperr-Notrufnummer

Damit sich die Kunden dafür nicht die von Bank zu Bank unterschiedlichen Sperrnummern merken müssen, hat die deutsche Kreditwirtschaft im Jahr 2005 – unter maßgeblicher Rolle der genossenschaftlichen Finanzgruppe, die über eine Tochtergesellschaft die zentrale Sperrannahme betreibt – eine sichere Alternative geschaffen: Die Einführung der bundeseinheitlichen Sperr-Notrufnummer 116 116 hat dem Hotline-Wirrwarr ein Ende gesetzt. Diese Notrufnummer ist weltweit die erste zentrale und einheitliche Rufnummer zum sicheren Sperren von allen elektronischen Berechtigungen wie Kreditkarten, Online-Banking, Handykarten und auch der ID-Funktion des neuen Personalausweises. Im Fall eines Kartenverlustes wird dem Karteninhaber vom Sperr-Notruf 116 116 rund um die Uhr schnell und im Inland gebührenfrei geholfen.

3-D Secure bei Kreditkarten: 3-D Secure ist das Verfahren für zusätzliche Sicherheit bei Online-Kartenzahlungen im Internet. Es wurde von den Kreditkartenorganisation entwickelt und wird von Mastercard als „Mastercard Securecode", von Visa unter dem Namen „Verified by Visa", angeboten. 3-D Secure reduziert erfolgreich das Betrugsrisiko im Internet und den Ausfall von Zahlungen durch Kartenmissbrauch. Deswegen wird den Shop-Betreibern, die sicheres 3-D Secure einsetzen, der Zahlungseingang von den Kartenorganisationen garantiert. Bei einer Zahlung mit 3-D Secure wird online eine Verbindung zum Kartenherausgeber hergestellt, damit der Käufer seine Identität mittels eines persönlichen Codes bestätigt. Dieser Code kann entweder ein eigenes Passwort, eine SMS-TAN oder mit dem TAN-Generator des Kartenchips generiert sein. Nur wenn die Authentisierung erfolgreich war, wird die Kreditkartenzahlung ausgeführt. So hat der Händler, der in seinem Webshop das 3-D-Secure-Verfahren anbietet, die Sicherheit, dass er eine Garantie für einen autorisierten Einkauf erhält.

Frei wählbare PIN ab 2012: Die Girocard ist für die meisten Deutschen die wichtigste Karte im Portemonnaie. Damit ist sie die sichere Alternative zum Bargeld. Um am Automaten Geld abheben und im Handel bezahlen zu können, muss der Kunde seine persönliche PIN wissen. Denn die PIN muss stets geheim bleiben und darf niemals notiert werden. War noch vor 20 Jahren die ec-PIN meist die einzige PIN für den Bankkunden, hat heutzutage jeder Nutzer im Schnitt mindestens vier verschiedene Passwörter beziehungsweise Geheimzahlen. Die meisten davon sind jedoch auf einfacher zu merkende Zahlen einstellbar. Die genossenschaftliche Finanzgruppe hat dieses Kundenbedürfnis erkannt und macht deswegen als erste Bankengruppe nun auch die PIN der Girocard für den Benutzer individuell änderbar. Ab Februar 2012 können alle Kunden ihre Wunsch-PIN für ihre VR-Bankcard kostenlos an allen 19 000 Geldautomaten der Volksbanken und Raiffeisenbanken wählen. Mit der selbst gewählten PIN wird der sichere Gebrauch der Girocard damit für die Kunden noch einfacher und komfortabler. Auch die genossenschaftlichen Kreditkarten werden schrittweise für die neue Funktion vorbereitet.

Sicherheit im Online-Banking

HBCI/Fin-TS, auch auf der Debitkarte: Bereits über 60 Prozent aller Internetnutzer nutzen heute auch die Möglichkeit zum Online-Banking. Neben der Bequemlichkeit spielt dabei für die Kunden die Sicherheit eine wachsende Rolle bei der Wahl ihrer Online-Bankverbindung. So wird das Angebot von zeitgemäßen Sicherheitsverfahren immer mehr zum Wettbewerbsfaktor. Deswegen achten die Volksbanken und Raiffeisenbanken darauf, ihren Kunden die modernsten und sichersten Verfahren für ihr Online-Banking anzubieten. So wurde 1996 zusammen mit der deutschen Kreditwirtschaft die erste Version von HBCI, dem Vorläufer des Financial Transaction Standard Fin-TS, für das Electronic Banking entwickelt und in der Finanzgruppe eingeführt. Fin-TS bildet so eine öffentliche, standardisierte und sichere Schnittstelle für das Online-Banking. Fin-TS-Homebanking mit HBCI-Signaturchipkarte und Chipkartenleser stellt das höchste Maß an Sicherheit dar. Viele Volksbanken Raiffeisenbanken bieten dabei die Signaturfunktion ihren Kunden nicht nur auf der speziellen HBCI-Signaturchipkarte, sondern auch bereits integ-

riert in den Chip ihrer VR-Bank-Card an, sodass der Kunde nur eine einzige Karte benötigt.

Secoder: Um die Signaturchipkarte beziehungsweise VR-Bank-Card mit Signaturfunktion wirkungsvoll einsetzen zu können, benötigt der Kunde noch den richtigen Kartenleser. Der Kartenleser erstellt mit der Karte die Signatur der Transaktion. Dabei ist wichtig, dass der PC die vom Nutzer gewünschte Transaktion nicht unbemerkt manipuliert. Um dies zu vermeiden, hat die deutsche Kreditwirtschaft den Secoder Kartenleser entwickelt. Dieser eignet sich zur Absicherung im Online-Banking, zum Bezahlen im Internet, zur Nutzung der elektronischen Signatur und für den Altersnachweis auf Web-Seiten. Der Secoder hat eine eigene PIN-Tastatur, um die PIN bei der Eingabe zu schützen, und eine eingebaute Firewall, die direkte Angriffe aus dem PC auf die Karte und die Geheimzahl des Nutzers abfängt. Der Secoder-Kartenleser erfüllt auch die Anforderungen an einen sicheren Einsatz des Personalausweises und wird deswegen von der Bundesregierung gefördert.

Features für Mobiltelefone

Smart TAN frühzeitig angeboten: Eine sichere Alternative zum Signatur-basierten Fin-TS/HBCI-Verfahren bieten Verfahren mit TAN-Generatoren. Auch hier war die genossenschaftliche Finanzgruppe Vorreiter, als sie 2004 das Smart-TAN-Verfahren einführte: die TAN wird mittels Kartenleser und VR-Bank-Card generiert. Das Verfahren wurde bei den Kunden der Volksbanken und Raiffeisenbanken so beliebt, dass es rasch die damals üblichen TAN-Listen ablöste. Bis heute wurden Sicherheit und Komfort des Konzepts mehrfach verbessert. Heute werden bei Smart TAN plus auch Teilinformationen der Transaktion in den Leser eingelesen und gehen in die TAN-Erzeugung ein, sodass die TAN transaktionsabhängig ist und für eine andere Transaktion nicht verwendet werden kann. Mit Hilfe elektronischer Lichtsensoren können die modernen Leser die Transaktionsdaten selbstständig über einen Barcode einlesen. Der Nutzer bestätigt nur noch die am eingebauten Display angezeigten Daten. Dieses Verfahren schützt vor Phishing- beziehungsweise Man-in-the-Middle-Angriffen, da die im Display angezeigten Daten vor der Bestätigung vom Kunden auf ihre Richtigkeit geprüft werden.

Mobile TAN und Abschaltung i-TAN: Die Nutzung des Mobiltelefons für die verschiedensten Zwecke wird für immer mehr Kunden zum Alltag. Die Volksbanken und Raiffeisenbanken haben diesen Trend frühzeitig aufgegriffen und bieten seit 2007 die mobile TAN als alternatives Sicherheitsfeature an. Dies ist eine extra für die gewünschte Transaktion erzeugte TAN, die von der Bank mit einer SMS auf das registrierte Handy des Kunden geschickt wird. In der SMS stehen die Eckdaten der Transaktion, sodass sich der Benutzer vergewissern kann, für welche Transaktion die TAN dient. Der Nutzer sollte dabei darauf achten, das Telefon als getrennten Kanal zu behandeln und nicht für andere Zwecke, wie mobiles Banking, zu nutzen. Mit der Einführung der mobile TAN zusammen mit Smart TAN plus haben die Volksbanken und Raiffeisenbanken sichere Alternativen, um das i-TAN-Verfahren endgültig bis Ende 2011 abzulösen.

Mobile App: Durch die immer stärkere Verbreitung von Smartphones am Markt gewinnt diese Plattform das zunehmende Interesse auch für Finanzdienstleistungen. Mobile Applikationen auf Smartphones bringen durch die Datenverarbeitung vor Ort und die automatische Synchronisation „over the air" Vorteile für die mobilen Kunden. Auch die genossenschaftliche Finanzgruppe hat Apps für das mobile Banking entwickelt, die den höchsten Sicherheitsstandards genügen. Die Kunden der Volksbanken und Raiffeisenbanken können so auch unterwegs ihr Banking erledigen und mit Smart TAN plus freigeben. Eine Kombination mit der mobile TAN ist dagegen aus Sicherheitsgründen nicht zu empfehlen und wird daher von der genossenschaftlichen Finanzgruppe ihren Kunden bewusst nicht angeboten.

Sicherheit und Wettbewerb

Dass Sicherheit im Bankgeschäft als vergleichendes Wettbewerbsargument wenig geeignet ist, galt lange Zeit im Kreditgewerbe als gemeinsame Einschätzung. Hierfür gibt es auch gute Gründe. Zum einen ist Sicherheit ein abstraktes Ziel, das immer im Hinblick auf das notwendige Sicherheitsniveau zu betrachten ist – zum Beispiel betragsabhängig. Zum anderen ist Sicherheit eine Momentaufnahme, die vor dem Hintergrund von Releasezyklen und technologischen Entwicklungen zu betrachten ist. Und schließlich ist Sicherheit kein singuläres Ziel, sondern immer auch im Zusammenhang mit Kundennutzen und Bequemlichkeit zu betrachten.

Die fortschreitende Akzeptanz des Electronic Banking – allein in der genossenschaftlichen Finanzgruppe über 30 Millionen Debit- und Kreditkarten beziehungsweise 7,5 Millionen Online-Banking-Nutzer – wäre jedoch ohne jeweils aktuelle Sicherheitsverfahren nicht Realität geworden. Gerade wegen der inzwischen hohen Nutzerzahlen und der ausgeweiteten Einsatzbereiche des Electronic Banking, zum Beispiel im Brokerage, ist es nun aber auch von besonderer Bedeutung, diese Systeme vor Angriffen zu schützen.

Hierzu gehört, technische Migrationen konsequent umzusetzen und Altverfahren aus dem Markt zu nehmen, auch wenn die Umstellung für die Kunden naturgemäß mit einem Umlernen verbunden ist. Dies aber unter Bequemlichkeitsaspekten zurückzustellen und zum Beispiel das i-TAN-Verfahren weiter – wie von einigen Direktbanken angekündigt – betreiben zu wollen, kann sich als fahrlässig erweisen.

Bedienerfreundlichkeit

Und natürlich muss auch die Erkenntnis reifen, dass Sicherheit ihren Preis hat. Es kann nicht sein, dass von Seiten des Verbraucherschutzes kostenlose Girokonten mit kostenloser Kartenausstattung und kostenlosen Online-Banking-Medien gefordert werden, zugleich aber Sicherheit auf höchstem Niveau erwartet wird. Kunden akzeptieren durchaus, dass sichere Chipkarten, mobile TANs oder Smart-TAN-optic-Leser ihren Preis haben, wenn man sie über den Nutzen dieser technischen Weiterentwicklungen entsprechend aufklärt.

Ein hohes Niveau an Sicherheit im Electronic Banking ist unverzichtbar im Wettbewerb, ist ein Basisfaktor für Vertrauen im Retail Banking. Sicherheit ist jedoch kein alleinstehender Wettbewerbsfaktor, sondern immer im Zusammenhang mit der Kundenwahrnehmung zu betrachten. Insofern wird nicht diejenige Bank im Wettbewerb profitieren, die Sicherheit technologisch maximiert, sondern diejenige, die Sicherheitsverfahren „state of the art" mit Bedienerfreundlichkeit und einer transparenten Kundeninformation verbindet.