Karten-Blickpunkte

Mobile Payment

Mobile Kooperationen

Noch während das kartenbasierte kontaktlose Zahlen in Deutschland mühsam um den Durchbruch ringt, ist die Anbieterseite im Bereich des Zahlungsverkehrs längst einen Schritt weiter und bastelt an Modellen zum kontaktlosen Bezahlen mit dem Mobiltelefon. Und hier – so jedenfalls der Stand der Dinge – scheint es ohne Kooperationen bislang nicht zu gehen. Die Sparkassenorganisation setzt hier auf die Zusammenarbeit mit Herstellern der mobilen Endgeräte. Visa Europe kooperiert mit Vodafone und Telefónica, Mastercard mit der deutschen Telekom und die Targobank mit E-Plus, wobei die Kartenmarke auch diesmal Mastercard ist.

Weil es ohne die kontaktlose Karte als „Brückentechnologie" noch nicht geht, setzen sowohl die Targobank als auch die Telekom-Gruppe auf die Kombination aus Karte und Sticker fürs Mobiltelefon.

- Die Targobank und E-Plus haben im Juli mit der Ausgabe des Bezahlchips, der auf die Rückseite des Telefon geklebt werden kann, an Mitarbeiter und Kunden in einer Testregion begonnen.

- Die Telekom hat angekündigt, noch in diesem Jahr zunächst in Deutschland, in den kommenden zwei Jahren sukzessive auch in weiteren Ländern Europas eine kontaktlose Mastercard herauszugeben, kombiniert mit einem NFC-Sticker fürs Mobiltelefon. Mit dem Start der Vermarktung von SIM-Karten-basierten NFC-Lösungen soll die Telekom-Mastercard dann auch auf dem Handy verfügbar sein.

Ziel der Telekom ist es, ein „vollständiges Ökosystem rund um das Bezahlen mit dem Smartphone aufzubauen", so Thomas Kiessling, Chief Product and Innovation Officer der Deutschen Telekom. Die eigene Mastercard wird dabei nur ein Baustein sein. So soll der Kunde künftig in der mobilen Brieftasche auch weitere Karten – einschließlich Kundenkarten – hinterlegen können. Denkbare Partner, über die im Markt auch schon spekuliert wird, wären beispielsweise die Deutsche Bahn oder die Lufthansa.

Realität werden soll die schöne neue Welt, für die freilich der NFC-Sticker nicht ausreicht, sondern die ein wirklich NFC-fähiges Endgerät erfordert, schon in Bälde: In Polen soll ein entsprechendes Angebot noch in diesem Jahr auf den Markt kommen. In Deutschland ist für das vierte Quartal dieses Jahres eine Testphase geplant. Im ersten Halbjahr 2013 sollen erste Produkte angeboten werden.

Geworben wird in beiden Kooperationen mit der namentlich für deutsche Verbraucher so wichtigen Transparenz und Sicherheit: Dass jede Transaktion per SMS bestätigt wird, gibt ein sicheres Gefühl und soll zudem die Ausgabenkontrolle erleichtern.

Das alles klingt nicht so sensationell neu. Das Besondere an der Kooperation von Mastercard mit der Telekom ist jedoch, dass sie ohne eine klassische Bank als Herausgeber der Karte auskommt. Emittent ist die Telekom-Tochter Clickandbuy, deren E-Geld-Lizenz einen Bankpartner erübrigt. Durch die kürzlich bekannt gegebenen Projekte tritt Mastercard den Banken gegenüber also gewissermaßen Janusköpfig auf: mit der Targobank als Partner der Banken, durch die Partnerschaft mit der Telekom und deren Tochter Clickandbuy – nicht zum ersten Mal – aber auch an der Seite des neuen Wettbewerbs.

Auch auf dem deutschen Markt beginnt damit Realität zu werden, was schon lange befürchtet wurde: Dass nämlich Nichtbanken, namentlich aus dem Telekommunikationsbereich sich anschicken, Marktanteile im Zahlungsverkehr zu erobern. Das ist sicher noch längst kein Abgesang auf die Rolle der Kreditwirtschaft in einem ihrer Kerngeschäftsfelder. Der Handlungsbedarf für Banken und Sparkassen wird aber deutlich.

Der Weisheit letzter Schluss sind die mannigfachen Kooperationen in Sachen Mobile Payment sicher noch nicht. Sicher ist das Mobile-Payment-Angebot für den Targobank-Kunden schön – so er denn über E-Plus telefoniert. Der Vodafone-Kunde wird sich vielleicht freuen, die Funktionen seiner Visa-Karte ins Handy integrieren zu können. Und wenn die Sparkassenorganisation mit Mobiltelefonherstellern ins Geschäft kommt, mag auch das daraus resultierende Angebot für einen Teil der Kundschaft ganz attraktiv sein. Dass der Verbraucher die Wahl seines mobilen Endgeräts oder der Telefongesellschaft von einem Mobile-Payment-Angebot wird bestimmen lassen, ist aber kaum anzunehmen. Hier werden also Standards erarbeitet werden müssen, damit jede Karte mit jedem mobilen Endgerät und jedem Mobilfunkanbieter funktioniert.

Die mobile Geldbörse, in der man Karten jeder Art hinterlegen kann, wie es zuletzt die Telekom angekündigt hat, ist ein Weg in die richtige Richtung. Wenn dann der Telekom-Kunde nicht mit der Telekom-Mastercard mobil zahlt, sondern mit der

seiner Hausbank, mag das aus Sicht von Clickandbuy zwar bedauerlich sein. Alles andere aber würde vermutlich zu einer geringen Akzeptanz oder gar Kundenverlusten führen. **Red.**

Mobile Payment

Die Brieftasche bleibt

Noch ist die Aussage der diversen Studien zum Thema Mobile Payment relativ eindeutig: Wirklich überzeugt sind die Verbraucher nicht, primär aus Gründen der Sicherheit. Wenn sie sich aber mit dem Bezahlen per Mobiltelefon anfreunden könnten, dann am ehesten mit einem Angebot seitens ihrer Bank. Mag die Kreditwirtschaft auch im großen, gesamtgesellschaftlichen Rahmen an Vertrauen verspielt haben – ihre Kompetenz in Sachen Zahlungsverkehr wird nicht angezweifelt. Dass durch die mannigfachen Kooperationen jetzt der Wettbewerb auch mit den neuen Playern in Gang kommt – mal mit, mal ohne Kreditkarte im Hintergrund –, ist da vielleicht gar nicht so schlecht. Bekanntlich agiert mancher schneller, wenn der Druck wächst.

Dass die Kreditwirtschaft zunächst einmal auf das kontaktlose Bezahlen per Karte setzt, ist trotzdem der richtige Ansatz. Denn diese Brückentechnologie kann Vertrauen in die NFC-Technik schaffen. Und auch bei der prognostizierten raschen Verbreitung NFC-fähiger Telefone wird es noch eine geraume Weile eine Vielzahl von Verbrauchern geben, die nicht über ein solches verfügen.

Der mediale Aufschrei über die Auslesbarkeit dieser Karten im Mai dieses Jahres war gewiss ein deutliches Indiz dafür, dass die breite Öffentlichkeit im Land noch nicht für die mobile Brieftasche bereit ist. Wenn sich der Verbraucher schon über die potenzielle Auslesbarkeit einer einzelnen kontaktlosen Karte und die daraus resultierenden Missbrauchsmöglichkeiten sorgt, wird er dann ohne weiteres sein gesamtes Kartenportfolio in die „Mobile Wallet" auf seinem Handy transferieren wollen?

Gut möglich, dass ein beträchtlicher Teil der technikaffinen Kundschaft solche Ansätze gerne testen wird. Die Karte seiner Bank wird er aber dennoch weiter in der Tasche behalten: aus Gründen der Akzeptanz, aber auch um der Risikostreuung willen. Wenn dann das Mobiltelefon defekt ist, verloren geht, gestohlen oder gehackt wird, dann ist wenigstens nicht die ganze

Sicherheit

Technische Investitionen zahlen sich aus

Auch im Jahr 2011 hat sich die Schere beim Betrug mit Debitkarten weiter zugunsten von ELV geöffnet. Beim Lastschriftverfahren nahm die Zahl der Betrugsfälle weiter ab (wenn auch deutlich weniger stark als im Vorjahr), bei Girocard legte sie weiter zu. Erstmals seit 2003 zurückgegangen ist der Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten – ein Straftatbestand, der 2010 noch um 11,9 Prozent zugenommen hatte. Das zeigt: Die erheblichen Investitionen in die Verbesserung der Sicherheit scheinen endlich Früchte zu tragen. Hier dürften sich vor allem die Maßnahmen gegen Skimming auszahlen, nicht zuletzt aber auch die Chipmigration. Denn Kartendubletten können am GAA oder PoS nur noch in wenigen Ländern eingesetzt werden, ausgespähte Kartendaten nur noch bei denjenigen Onlineshops, die auf 3-D-Secure und die Abfrage der Kartenprüfnummer verzichten. Der Kartendiebstahl ist dagegen weiter im Aufwind. **Red.**

Aus der polizeilichen Kriminalstatistik

Straftat	Anzahl Fälle 2010	Anzahl Fälle 2011	Veränderung zum Vorjahr	Aufklärungsquote 2010*	Aufklärungsquote 2011*
			in Prozent		
Diebstahl von unbaren Zahlungsmitteln	129 550	140 628	+ 8,6	9,5	8,4
Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel	68 528	66 521	- 2,9	37,2	36,6
davon:					
Debitkarten ohne PIN	13 785	13 589	- 1,4	42,5	43,8
Debitkarten mit PIN	23 612	24 923	+ 5,6	40,7	37,4
Kreditkarten	8 974	8 886	- 1,0	34,9	36,2
Daten von Zahlungskarten	19 100	16 061	- 15,9	27,3	27,1
Sonstige unbare Zahlungsmittel	2 420	3 062	+ 26,5	54,1	50,4
Missbrauch von Scheck- und Kreditkarten	3 977	2 651	- 33,3	91,5	86,1
Geld- und Wertzeichenfälschung inklusive Vorbereitungshandlungen	889	831	- 6,5	100,9*)	70,5
Inverkehrbringen von Falschgeld	2 237	1 612	- 27,9	100,1*)	100,2*)
Fälschung von Zahlungskarten, Schecks und Wechseln	6 603	4 590	- 30,5	30,0	28,9
darunter:					
Gebrauch falscher Zahlungskarten, Schecks und Wechsel	3 029	2 435	- 19,6	37,1	38,8
Nachmachen, Verfälschen, Verschaffen oder Überlassen falscher Zahlungskarten, Schecks oder Wechsel	3 574	2 155	- 37,7	24,0	17,7

*) im Berichtszeitraum wurden auch Straftaten aus dem Vorjahr aufgeklärt
Quelle: Polizeiliche Kriminalstatistik

„digitale Identität" in Gefahr. So wie die physische Karte noch eine Zeitlang mit der Parallelität von Chip und Magnetstreifen leben wird, dürfte also auch der technikaffine Kunde bei den bargeldlosen Zahlverfahren auf mittlere Sicht eher zweigleisig fahren – Mobile Payment einerseits, Karte andererseits.

Für den Einzelhandel heißt das alles, dass sich künftig auch der stationäre Handel einer Bandbreite an Angeboten gegenüber sehen wird, wie es sie bisher nur im E-Commerce gab. Ein ähnlich breites Portfolio an Zahlungsoptionen, wie es sich in der Onlinekasse verhältnismäßig einfach umsetzen wird, stößt aber im Laden vor Ort an gewisse Grenzen. Wenn jeder der neuen Anbieter mit einem eigenen Terminal oder terminal-ähnlichem Gerät daherkommt, ist diese schnell erreicht. Doch selbst wenn hier Standards gesetzt werden, bleibt der Faktor Mensch als Begrenzung. Schon beim Nebeneinander von Paypass und Girogo hat der Einzelhandel erfahren müssen, dass zu viel Verschiedenes zu Verwirrung führt (siehe Beitrag Schrage auf Seite 18). Manche Mobile-Payment-Konzepte werden sich deshalb vielleicht im Remote-Bereich durchsetzen, im Präsenzgeschäft aber nicht.

Die Brieftasche – mag sie durch die verschiedensten Karten auch noch so dick geworden sein, wird uns also wohl noch eine ganze Weile begleiten. Nicht zuletzt kann die Vision vom Verbraucher, den die Technik komplett von seiner klobigen Brieftasche befreit, schon allein deshalb nicht so bald Realität werden, weil dann auch nationale und internationale Behörden auf die kontaktlose Kontrolle von Ausweisen oder Führerscheinen eingestellt sein müssten. Und die Arztpraxen, die sich noch mit der elektronischen Gesundheitskarte herumplagen, werden wohl auch nicht so ohne weiteres auf NFC-Technik umstellen, um eine virtuelle Gesundheitskarte auslesen zu können.

Wenn aber die Brieftasche mit den diversen Ausweisdokumenten unser Begleiter bleibt, dann hat hier auch noch die Karte für den Zahlungsverkehr ihren Platz. Ob man es bequemer findet, eine kontaktlose Karte oder ein Handy aus der Tasche zu holen und ans Kassenterminal zu halten, ist dann sicher Geschmackssache. Das Zahlen „im Vorbeigehen" wird es so oder so erst einmal nicht geben können. Denn das erforderte einen weitaus größeren Sendebereich zwischen Trägermedium und Terminal als die heute üblichen maximal vier Zentimeter. Und damit würde sich wiederum das Risiko erhöhen. **sb**

Kriminalität

Rückgriff auf Bewährtes

Das Skimming, so legen es die diversen Statistiken nahe, wird als Geschäftsmodell unattraktiver: Die Türöffner an den Bankfilialen sind abgebaut, die Geldautomaten mit Anti-Skimming-Modulen ausgerüstet, und das Vordringen von EMV erschwert die Einsetzbarkeit von Kartendubletten. Auch der Kriminelle, der sich mit seinem technisch aufgepeppten Mobiltelefon durch den vollbesetzten Bus schlängelt und dabei massenweise zahlungsverkehrsrelevante Daten von kontaktlosen Karten abgreift, ist vor allem eine Zwangsvorstellung des deutschen Bedenkenträgers. In diesem Umfeld, so scheint es, werden Diebstähle außerhalb der digitalen Welt wieder attraktiver. Euro Kartensysteme warnt deshalb vor Trickbetrügern am Geldautomaten. Sie lenken Karteninhaber nach Eingabe der PIN und des gewünschten Geldbetrags ab, sodass ein Komplize das Bargeld entnehmen kann. **Red.**

Sicherheit

Chip & PIN ist nicht alles

Das Jahr 2008 hat beim Kartenbetrug in Europa ein Wendepunkt erreicht. Seitdem gingen die Faud-Verluste wieder zurück, lagen jedoch 2011 immer noch um rund 121 Millionen Euro oder rund zehn Prozent höher als 2006. Eine interaktive Europakarte von Fico weist hier allerdings deutliche länderspezifische Unterschiede aus.

Rückgänge gab es in Portugal – und vor allem in Großbritannien, wo die Betrugsverluste um 35 Prozent sanken, auf das niedrigste Niveau seit zehn Jahren. Entfielen 2006 noch 45 Prozent aller Verluste in Europa auf Großbritannien, sank diese Quote auf 20 Prozent im vergangenen Jahr. Damit rangiert das Vereinigte Königreich in der Liste der Länder mit dem höchsten Betrugsrisiko „nur" noch an sechster Stelle – hinter Spanien, der Schweiz, Griechenland, Norwegen und Frankreich. Deutschland kommt in der von Fico erstellten Rangliste auf den neunten Platz von insgesamt 21 untersuchten Ländern und gehört zu denjenigen Ländern mit einem relativ niedrigen Betrugsniveau.

Dennoch ist der Blick auf die Entwicklung von 2006 bis 2011 für Deutschland ernüchternd: Hierzulande stiegen die Verluste von 2006 bis 2011 um 125,6 Prozent auf 142,01 Millionen Euro an. Damit gehört Deutschland zu denjenigen Ländern, in die sich der Fraud von Großbritannien her verlagert hat. In den Niederlanden erhöhten sich die Verluste im gleichen Zeitraum um 73,5 Prozent, und in Russland und Polen haben sie sich sogar mehr als verdreifacht.

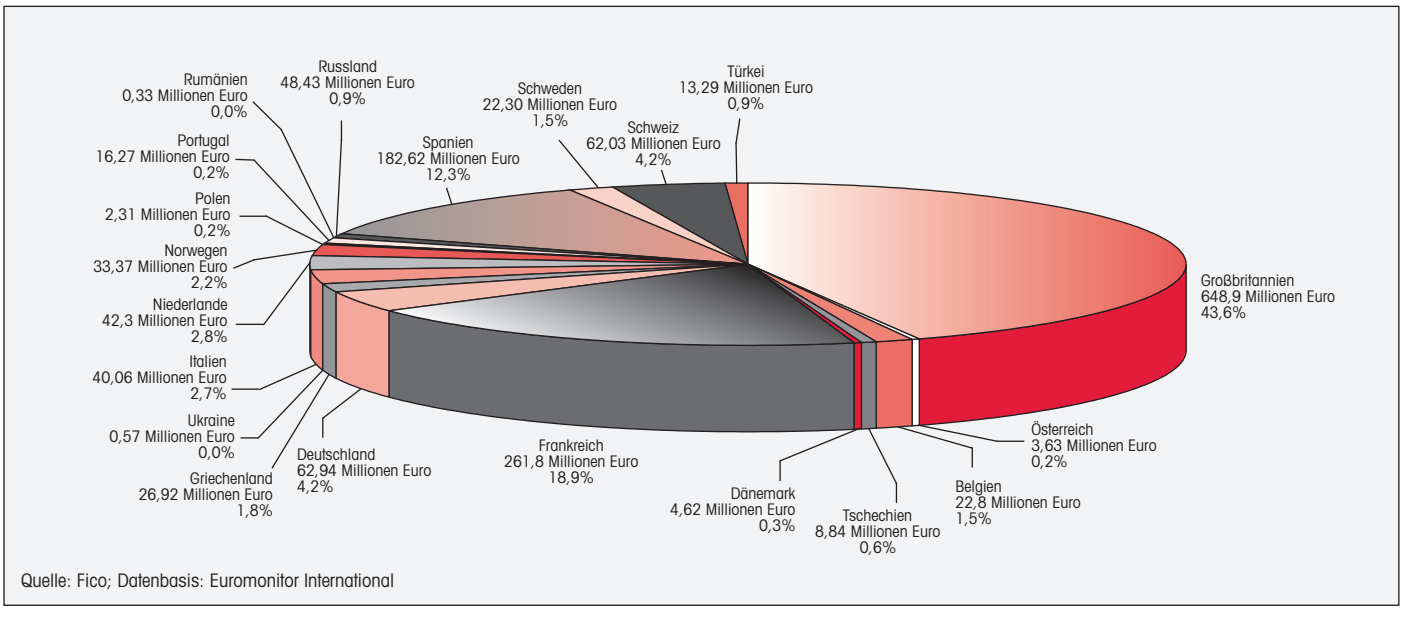
Als Hauptgrund für die rückläufige Entwicklung in Großbritannien und den Anstieg in anderen Ländern macht Fico den Umstieg vom unterschriftsbasierten auf das PIN-gestützte Verfahren aus, der in Großbritannien im Jahr 2006 vollzogen wurde. Dass die Engländer den vollen Umstieg auf EMV frühzeitig vollzogen haben, ist naheliegend, spielt doch die Kreditkartenzahlung dort eine weitaus größere Rolle als etwa in Deutschland. Doch die Entwicklung zeigt, dass auch hierzulande der bereits absehbare Umstieg auf Chip & PIN nicht nur bei der Girocard, sondern auch bei Kreditkarten letztlich geboten sein wird – aus Sicherheitsgründen, aber auch

im Hinblick auf eine verbesserte Akzeptanz. Schließlich gehen die Acquirer davon aus, dass die Discounter sich erst dann für die Kreditkartenakzeptanz öffnen werden, wenn dies ohne Unterschriftsbelege möglich sein wird.

Die starke Zunahme der Betrugsverluste in Deutschland ist aber vermutlich nicht allein auf die Verwendung des unterschriftsbasierten Verfahrens bei Kreditkartenzahlungen zurückzuführen. Denn 60 Prozent der Verluste entfallen auf den Card-not-present-Bereich in den weder PIN noch Unterschrift zum Einsatz kommen. Dieses Betrugsmuster hat seit 2006 um 300 Prozent zugenommen. Wenn also Teile der Kreditwirtschaft darauf dringen, dass die Kartengesellschaften die Verwendung von 3-D-Secure oder wenigstens die Abfrage der Prüfnummer im E-Commerce zur Pflicht machen sollen, hat dies sicher nicht nur damit zu tun, dass durch diese Sicherheitslücke das kontaktlose Zahlen in Misskredit gebracht werden könnte.

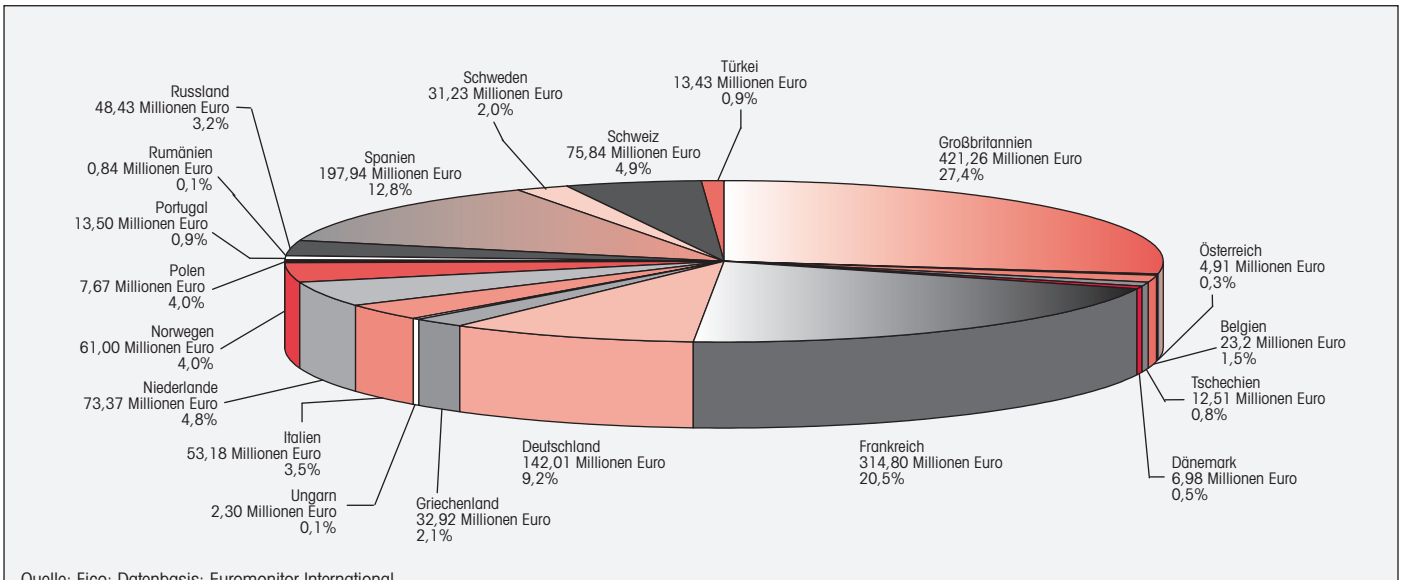
In Italien hat sich der in Deutschland so blühende Card-not-present-Betrug in den letzten Jahren halbiert. Dort hat allerdings der Betrug mit gefälschten Karten seit 2006 um 44 Prozent zugenommen und macht mittlerweile über die Hälfte der Verluste aus. **Red.**

Kartenbetrug in Europa 2006



Quelle: Fico; Datenbasis: Euromonitor International

Kartenbetrug in Europa 2011



Quelle: Fico; Datenbasis: Euromonitor International

Sicherheit

Panikmache bei der Girocard

Im Mai war Girogo an der Reihe, jetzt die Girocard. In der Sendung Monitor hat die ARD am 12. Juli einen Bericht mit dem Titel „Wie Hacker die bargeldlosen Kassensysteme im Einzelhandel knacken" ausgestrahlt. Darin ging es darum, wie PoS-Terminals unter Umgehung der Sicherheitssiegel, also ohne Aufbohren des Geräts, manipuliert werden könnten. Gezeigt wurde, wie ein Terminal an eine Handelskasse angeschlossen und eine Fremdsoftware in den Applikationsprozessor des Terminals aufgespielt wurde. Durch diese Fremdsoftware, also gewissermaßen einen Virus, würde dann eine PIN-Abfrage simuliert.

Da sind sie also wieder, die alten Ängste, die dem Bargeld zu seinem immer noch hohen Anteil im Zahlungsverkehrsmix verhelfen. Kein Wunder also, dass der Terminalhersteller Verifone, an dessen „Artema Hybrid" der Manipulationsversuch demonstriert wurde, und die Deutsche Kreditwirtschaft alarmiert reagierten.

Wie so oft, wurde in dem Bericht wieder einmal nur die halbe Wahrheit dargestellt. Die gezeigte Art des Manipulationsversuchs über die LAN-Schnittstelle kann nämlich nach Angaben von Verifone nicht aus der Ferne ausgeführt werden, weil er auf sogenannten ARP-Paketen beruht, die nicht über DSL-Router oder einen Switch übertragen werden können. Der Täter müsste also direkt beim Terminal vor Ort sein, um die Manipulation vornehmen zu können. Dieses Risiko steht zudem nur in einem ungünstigen Verhältnis zum Nutzen: Denn die Manipulation gelingt maximal für einen Tag. Spätestens bei Durchführung des täglichen Kassenabschlusses würde auffallen, dass das Terminal nicht spezifikationsgerecht arbeitet.

Zudem erfolgt bei dem Manipulationsversuch kein Zugriff auf den abgeschirmten Prozessor im Sicherheitsmodul des Terminals, das die kryptografischen Schlüssel enthält. Selbst mittels einer manipulierten Applikation ist somit ein Ausspähen der PIN während einer erfolgreichen Kartenzahlung nicht möglich, so der Terminalhersteller und die Deutsche Kreditwirtschaft.

In Summe heißt das: Die neue Angriffsform stellt tatsächlich eine eher theoretische Möglichkeit dar – es sei denn, der Händler beziehungsweise Mitarbeiter würden aktiv bei der Tat mitwirken – mit vergleichsweise hohem Risiko, entdeckt zu werden. Der vom BKA so gerne apostrophierte „Igor Popow" in Russland kommt mit dieser Methode also nicht zum Zug. Nichtsdestotrotz hat Verifone angekündigt, schnellstmöglich ein Software-Update bereitzustellen, das es einem Angreifer selbst dann unmöglich machen wird, Karteninhabern eine PIN-Abfrage vorzutäuschen, wenn er die vollständige Kontrolle über den Applikationsprozessor hätte. Ein weiteres Software-Update behob ganz schnell die Verwundbarkeit der LAN-Schnittstelle.

Der Imageschaden ist gleichwohl wieder einmal angerichtet. Natürlich hatten Kreditwirtschaft und Terminalhersteller vorab die Möglichkeit, zu dem Beitrag Stellung zu nehmen und entsprechende Gegendarstellungen zu verbreiten. Ob der Kateninhaber dem aber glauben wird (sofern er überhaupt davon erfährt), darf aber bezweifelt werden. Vermutlich würde man sowohl der Bankenseite als auch dem Terminalhersteller unterstellen, die Gefahr kleinreden zu wollen, um die Nutzung des eigenen Systems nicht zu gefährden.

Erklären kann man der breiten Masse die Details, warum ein Angriff auf diese Art höchst unwahrscheinlich ist, sicher nicht. Und so bleibt das altbekannte Kommunikationsproblem der Branche zum Thema Kartensicherheit weiter bestehen. Letztlich bleibt nur, dem Kunden immer wieder zu versichern, dass er im Fall des Falles nicht auf dem Schaden wird sitzen bleiben. Weil aber auch diejenigen Fälle, in denen ein fahrlässiger Karteninhaber seinen Schaden nicht ersetzt bekommt, in den Medien genüsslich breitgetreten werden, ist auch der Glaube an dieses Sicherheitsnetz begrenzt. **sb**

USA

Doppeltes Limit für Transaktionen ohne Unterschrift

Auch ohne Kontaktlos-Technologie gibt es bereits das Zahlen ohne Unterschrift oder PIN. Seit 2010 ist etwa in den USA ein „No Signature Required"-Programm verfügbar. Beträge bis zu 25 US-Dollar können damit ohne Unterschrift oder PIN-Eingabe und ohne Belegausdruck bezahlt werden, sofern der Kunde dies nicht ausdrücklich wünscht. Die Erfahrungen damit waren bisher offenbar nicht schlecht. Sonst hätte Visa nicht im Mai dieses Jahres angekündigt, das Limit für solche Transaktionen in zwei Branchen anzuheben. In Lebensmittel- und Supermärkten sowie bei Discountern können Karteninhaber künftig bis zu 50 Dollar im Schnellverfahren bezahlen. Die Branchen sind sicher vernünftig ausgewählt. Denn im Lebensmittelbereich ist der Kartenbetrug vermutlich weniger attraktiv als etwa in Elektronikmärkten. Dennoch ist die Limiterhöhung zunächst einmal ein Test. Nach Auswertung des Feedbacks von Emittenten, Händlern und Karteninhabern soll entschieden werden, ob sie auf weitere Branchen übertragen wird. In jedem Fall ist die Vorstufe zum kontaktlosen/mobilen Bezahlen damit schon genommen. Der Kunde gewöhnt sich an das Verfahren. Der Rest ist später kaum mehr als ein Technologiewechsel. **Red.**