# Flächendeckendes „Magstripe-Controlling" gegen Skimming

Von Swantje Benkelberg

Bildquelle: 4206564_R_B_by_DieterSchutz_pixelio.de

**Mit der technischen Aufrüstung von Geldautomaten lässt sich das Skimming durchaus eindämmen, wie die Entwicklung im zweiten Halbjahr 2010 zeigt. Zunehmende Angriffe auf weniger geschützte Geräte wie Tank- oder Fahrscheinautomaten lassen andere Maßnahmen wie die Sperrung oder Begrenzung von Einsatzmöglichkeiten im Ausland dennoch wichtiger werden. Hier mahnt das Bundeskriminalamt mehr Einheitlichkeit an.**

Etwa 190 000 Karteninhaber sind im vergangenen Jahr Opfer von Skimming-Delikten geworden. Das schädigt zum einen das ohnehin angeschlagene Image der Kreditwirtschaft und das Vertrauen zum Medium Karte. Einer repräsentativen Umfrage der Putz & Partner AG, Hamburg, zufolge sind 63 Prozent der Bundesbürger der Meinung, das Ansehen der Banken habe darunter gelitten, dass zu wenig unternommen werde, um das Abgreifen von Daten zu verhindern. Daneben gibt es aber auch ganz greifbare Verluste durch Skimming. Den Schaden, der in Deutschland 2010 durch den Einsatz gefälschter Debitkarten entstanden ist, beziffert das Bundeskriminalamt im Bundeslagebild Zahlungskartenkriminalität 2010 auf rund 60 Millionen Euro. Die drastische Steigerungsrate um 50 Prozent gegenüber dem Vorjahr erklärt die Behörde vor allem mit der steigenden Beliebtheit von Kartenfälschungen: Hier ist das Kosten-Nutzen-Verhältnis für die Kriminellen besser als beim Karten-Diebstahl, weil gestohlene Karten zu schnell gesperrt werden. Kartenfälschungen hingegen fallen üblicherweise erst nach einer gewissen zeitlichen Verzögerung auf.

Mit diesen veränderten Vorlieben der kriminellen Szene einher geht der Anstieg bei den Geldautomatenmanipulationen: 3 183 Angriffe wurden 2010 registeriert, rund 55 Prozent mehr als im Vorjahr. Bedingt durch Mehrfachattacken auf einzelne Geräte waren bundesweit 1 765 Automaten (plus 83 Prozent) betroffen.

## Verlagerung auf Tank- und Fahrscheinautomaten?

Der Datenabgriff an Türöffnern spielt dagegen für den Abgriff von Magnetstreifendaten mit einem Anteil von nur noch zwei Prozent (Vorjahr neun Prozent) lediglich eine geringe Rolle, da viele Kreditinstitute die Türöffner mittlerweile entweder abgebaut oder sicherheitstechnisch aufgerüstet haben.

Gewirkt haben offenbar auch die Maßnahmen zur Sicherung der PoS-Terminals gegen Datenabgriffe. Zwar registrierte die Polizei mehrere Fälle, in denen versucht wurde, Kartendaten und PIN durch die Manipulation von Terminals zu erlangen. Zum erfolgreichen Datenabgriff kam es dabei aber nicht – anders als unlängst bei Migros und Coop in der Schweiz.

Neu waren dagegen 2010 Manipulationen an unbedienten Tankautomaten. In insgesamt drei Fällen wurden dabei Kartendaten abgegriffen und für missbräuchliche Geldabhebungen in Kolumbien und den USA eingesetzt. Ob dies als Anzeichen für eine beginnende Verlagerung der Skimming-Aktivitäten von den zunehmend mit Anti-Skimming-Modulen ausgestatteten Geldautomaten zu anderen, weniger geschützten Automaten zu werten ist, lässt das Bundeskriminalamt im Bundeslagebericht zwar noch offen. Jüngste Warnungen vor Manipulationen erstmals auch an Fahrkartenautomaten scheinen aber in diese Richtung zu deuten.

Bei etwa zehn Fahrkartenautomaten der Deutschen Bahn ist es seit März 2011 zum Diebstahl von ec-Kartendaten gekommen, teilten Bahn und LKA Nordrhein-Westfalen mit. Und zuletzt warnte auch das Landeskriminalamt von Rheinland-Pfalz.

Die Vorgehensweise mittels Vorsatzgeräten an Karteneinzugsschlitzen zum Auslesen der Magnetstreifendaten und Minikameras oberhalb des Tastaturfelds zum Ausspähen der Geheimnummern ist dabei die gleiche wie bei den Geldautomaten.

Im Ausland wurden deutsche Kartendaten bei Manipulationen von 533 Geldauto-

maten und PoS-Terminals abgegriffen (minus 14 Prozent), am häufigsten in Frankreich, der Türkei und Italien. In vielen Fällen konnte allerdings der Point of Compromise nicht eindeutig identifiziert werden, sodass eine Vielzahl von Fällen in die Statistik nicht einfließt, die Dunkelziffer also erheblich höher ausfallen dürfte.

Anti-Skimming-Module scheinen durchaus zu greifen. So hat allein der von der Deutschen Bank vorgenommene Austausch mehrerer Hunderter Geldautomaten einer älteren Baureihe, die für Skimming besonders anfällig war, die Anzahl der erfolgreichen Attacken im zweiten Halbjahr 2010 wieder sinken lassen, so das Bundeskriminalamt.

**Vermeidung durch optische Oberflächenvermessung?**

Eine andere technische Lösung bietet die optische Oberflächenprüfung, wie sie in der Industrie zum Beispiel für Bauteilkontrolle, Lötstellenkontrolle oder Lackprüfungen eingesetzt wird, und auf die zum Beispiel Kai-Uwe Kirchen von der Rotho Kunststoff AG, Würenlingen, als Möglichkeit verweist. Der Ansatz dabei: Bei jedem noch so kleinen Eingriff am Geldautomaten wird dessen eigentliche Kontur verändert. Mit bloßem Auge sind die von den Tätern angebrachten Vorsätze am Karteneinzugschlitz und PIN-Eingabefeld praktisch nicht zu erkennen, mit der optischen Vermessung und mittels Zeilen- oder Flächenkamera aber sehr wohl. Dabei wird das von der Kamera aufgenommene Bild mit einem Sollbild verglichen. Bei der geringsten Veränderung können die Geräte sofort außer Betrieb genommen werden.

Ein vergleichbares Verfahren hat Wincor Nixdorf unter dem Namen „Optical Security Guard" seit 2010 im Angebot – optional, wie auch die übrigen Anti-Skimming-Module die seit 2003 im Angebot sind. Dabei wird das Bedienfeld von Geldautomaten mit unterschiedlichen Kameras überwacht, um so Manipulationen zu erkennen.

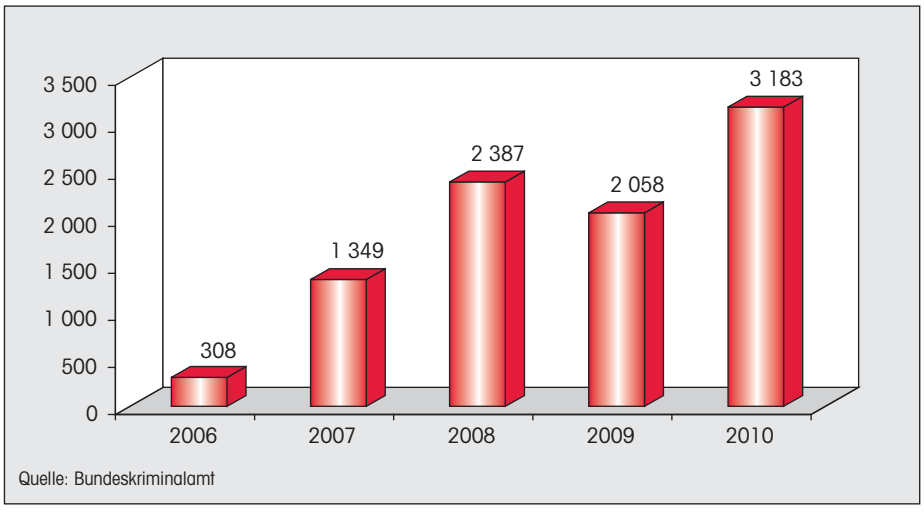
Zur Verhinderung von missbräuchlichen Einsätzen abgegriffener Kartendaten nach Manipulationen von Geldautomaten haben deutsche Banken im vergangenen Jahr über 300 000 Kartendaten vorsorglich gesperrt – eine Maßnahme, die sich freilich im Hinblick auf die Kundenzufriedenheit nur mit Augenmaß in wirklich begründeten Fällen anwenden lässt.

**Magstripe-Controlling als Alternative**

Die zunehmende Skimming-Problematik ist deshalb derzeit eines der stärksten Argumente zur Positionierung von V-Pay: Da es sich um eine reine Chip-Lösung handelt, ist Skimming nicht möglich. Vielleicht auch deshalb ist V-Pay bei den Volks- und Raiffeisenbanken derzeit der Renner bei den Kartenbestellungen, wie der DG-Verlag meldet. Auch die Postbank hat auf V-Pay umgestellt. Doch auch mit Magnetstreifen lässt sich durch das „Magstripe-Controlling", also die bewusste Kontrolle von Magnetstreifenumsätzen das Risiko reduzieren, wie BKA-Präsident Jörg Ziercke anregt. Dazu gehören Maßnahmen wie zum Beispiel

- die Reduzierung der Einsatzmöglichkeiten der Karte nach Risikoländern,
- die Festlegung von Limits für Auslandsabhebungen durch das Kreditinstitut oder den Kunden,
- die Benachrichtigung von Kunden per SMS bei erfolgten Auslandstransaktionen
- oder die grundsätzliche Deaktivierung der Karte für den Einsatz in „Nicht-Chip"-Ländern mit nur gezielter Freischaltung auf Kundenwunsch.

**Anzahl der Angriffe auf Geldautomaten in Deutschland 2006 bis 2010**




Quelle: Bundeskriminalamt

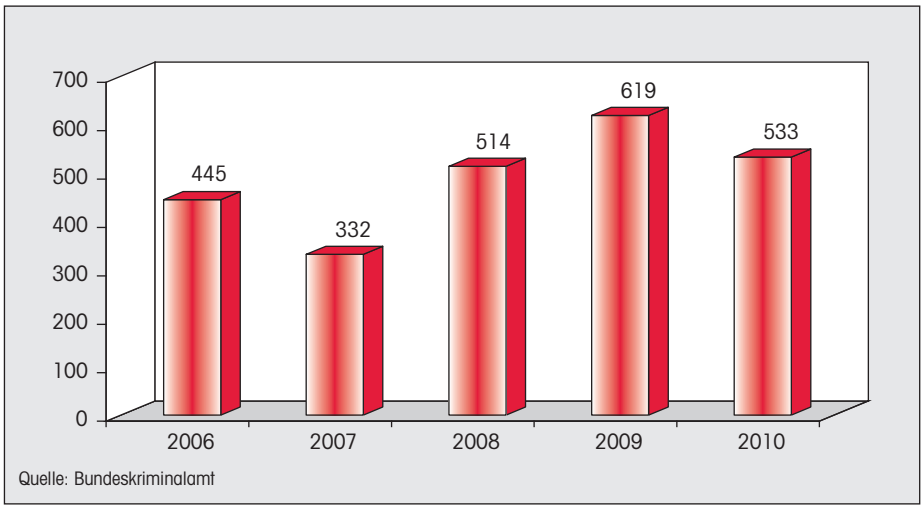
Mastercard hat mit „In Control" längst eine Lösung parat, mit der der Kunde selbst festlegen kann, in welchem Zeitraum seine Karte in welchem Land einsetzbar sein soll. Von deutschen Emittenten wird dieses Konzept aber bislang kaum genutzt. Einige, darunter die Postbank oder Airplus, arbeiten aber mit vergleichbaren Eigenentwicklungen.

### Genossen mit SB-Lösung

Auch die GAD eG in Münster hat aktuell eine Lösung vorgestellt, mit der Kunden der Genossenschaftsbanken künftig ihre Karte selber am Geldautomaten oder SB-Terminal ihrer Hausbank für Auslandseinsätze freigeben oder sperren können – oder auch im Onlinebanking, selbstverständlich gesichert durch eine TAN-Eingabe. Seit August haben rund 430 Volks- und Raiffeisenbanken im Norden und Westen Deutschlands die Möglichkeit, ihren Kunden diesen Service zu bieten.

Die Deutsche Bank hat zuletzt Negativschlagzeilen geerntet, weil sie ihre Girocards für Bargeldabhebung im Ausland generell gesperrt hat und die Funktion nur auf Kundenwunsch freischaltet. Dass Kunden also vor einer Auslandsreise die Bank kontaktieren müssen, damit die Sperre für ausländische Geldautomaten aufgehoben und ein vom Kunden zu definierendes Limit festgelegt wird, wurde vielleicht nicht intensiv genug kommuniziert, sodass einige Kunden im Ausland unangenehm überrascht wurden.

**Anzahl manipulierter Geldautomaten und PoS-Terminals im Ausland, bei denen deutsche Kartendaten abgegriffen wurden**




Quelle: Bundeskriminalamt

Sinnvoll sind solche Maßnahmen aber allemal. Denn der weitaus größte Teil der Kartentransaktionen findet nun einmal im Inland statt. Und der Aufwand, vor einer Reise die Karte entsprechend zu konfigurieren – sei es nun im Internet, am SB-Terminal oder durch Anruf bei der Bank – ist vermutlich geringer als der Ärger darüber, feststellen zu müssen, dass man Opfer von Skimming-Betrügern geworden ist, die mit einer Kartendublette vom Ausland aus das Konto zu räumen versuchen. Hier gilt das gleiche wie bei Onlinebanking: Wer Sicherheit will, muss dafür auch selbst einen Beitrag leisten.

### Sicherheit stärker kommunizieren

Das öffentliche Unverständnis für Einsatzbeschänkungen im Ausland zeigt aber auch, dass das Thema „Sicherheit" noch stärker kommuniziert werden muss – und zwar nicht nur einmal. So ließe sich etwa rechtzeitig zur Urlaubszeit per Plakaten/Aufstellern in den Filialen, Einblendungen an Geldautomaten und auf der Website daran erinnern, Karten entsprechend den Reisezielen konfigurieren zu lassen beziehungsweise sich ergänzend zur V-Pay-Karte rechtzeitig mit einer Kreditkarte zu versorgen, wenn es ins außereuropäische Ausland geht.

Und: Die Kreditwirtschaft müsste auch stärker an einem Strang ziehen. Denn nur wenn die genannten Verfahren flächendeckend eingesetzt werden, sind sie im Kampf gegen die Zahlungskartenkriminalität effektiv. Das hat das Bundeskriminalamt ganz deutlich gemacht. Nur wenn die Einsetzbarkeit von durch Skimming erstellten Kartendubletten eingeschränkt wird, wird die Manipulation von Geld-, Tank- oder Fahrscheinautomaten als „Geschäftsmodell" für die Täter uninteressant.