

Missbrauchsbekämpfung: Die Rahmenbedingungen stimmen noch nicht

Interview mit Margit Schneider



Trotz EMV sind die Schadensfälle mit gestohlenen und verlorenen Karten weiterhin hoch. Dennoch zahlen sich die Bemühungen der Kreditwirtschaft um die Missbrauchsprävention aus: Ein beträchtlicher Anteil der Missbrauchsversuche kann abgewehrt werden. Die internationale Zusammenarbeit bei der Missbrauchsbekämpfung wird nach Einschätzung von Margit Schneider allerdings vor allem durch unzureichende gesetzliche Rahmenbedingungen behindert. Red.

Karten Welche Trends gibt es beim Thema Kartenkriminalität?

Seit 1. Juli 2006 werden alle Schadensfälle der Banken und Sparkassen mit verlorenen und gestohlenen Karten sowie mit Kartenfälschungsdelikten an das EKS Net von Euro Kartensysteme gemeldet. Im Gesamtjahr 2006 waren das insgesamt 20 854 Fälle, im ersten Halbjahr 2007 bereits 11 989 Fälle.

Zugenommen haben vor allem die Kartenfälschungen. Die Angriffe auf Geldautomaten haben sich in starkem Maße erhöht. Wir hatten im letzten Jahr insgesamt 308 manipulierte Geldautomaten. Im ersten Halbjahr 2007 waren es 204 manipulierte Geräte. Der Anteil der Attacken ist sogar noch höher, da die Tätergruppen

heute tendenziell einen Automaten mehrmals über einen kürzeren Zeitraum manipulieren, sodass es im Nachhinein sehr schwierig ist, den Zeitraum der Kompromittierung genau festzulegen.

Sobald wir einen Point of Compromise (Ort des Datenabgriffs) identifiziert haben, lassen wir uns die Geldautomatenjournalen kommen und können über EKS Net alle Banken und Sparkassen schnell informieren, sodass Karten, die zum fraglichen Zeitraum an dem betroffenen Automaten eingesetzt wurden, präventiv gesperrt werden können.



Margit Schneider, Leiterin Sicherheitsmanagement Zahlungskarten, EURO Kartensysteme GmbH, Frankfurt am Main

2006 wurden von den Banken 35 000 potenziell von Kartenfälschungen betroffene Karten präventiv gesperrt. Im ersten Halbjahr 2007 waren es bereits ebenso viele.

Karten Sollte EMV nicht das Risiko der Kartenfälschungen stark herabsetzen?

Wenn wir in Europa mit EMV „die Schotten dicht“ machen, bleibt immer noch der Magnetstreifen auf den Karten, damit diese auch international einsetzbar sind. Und solange der Magnetstreifen auf der Karte ist, können die Daten ausgelesen und Dubletten im außereuropäischen Ausland eingesetzt werden.

Generell sehen wir eine zunehmende Internationalisierung der organisierten Kriminalität, indem beispielsweise Tätergruppen aus Osteuropa mit solchen aus Asien kooperieren. Weil die europäischen Banken enorm in die EMV-Infrastruktur investiert haben, macht Europa aber zunehmend Druck in internationalen Gremien, um etwa auch die USA für EMV zu gewinnen.

Karten Wie wirkt sich der Liability Shift aus?

Zurzeit haben wir eine Rückbelastungsquote von 65 Prozent der Betrugstransaktionen durch Kartenfälschung mit EMV-

Karten. Diese Schäden bleiben dann im europäischen Ausland.

Investitionen in die Sicherheit zahlen sich noch in anderer Hinsicht aus: Deutschland ist ein beliebtes Land für den Datenabgriff, aber nicht für den Einsatz von Kartenfälschungen, weil wir schon Anfang der achtziger Jahre das MM-Modul eingeführt haben, mit dem die Kartenechtheit am Geldautomaten geprüft wird. Leider haben unsere europäischen Nachbarn dies aus Kostengründen nicht übernommen. Es führt aber immerhin dazu, dass Dubletten von deutschen Karten in Deutschland nicht eingesetzt werden können.

Karten Welche Länder sind Schwerpunkte für den Einsatz von Dubletten deutscher Karten?

Im Ausland werden deutsche ec-Karteninhaber zurzeit vor allem in Südafrika von Datenabgriffen betroffen. 2003 und 2004 war es die Türkei, auf die rund 30 Prozent des Gesamtbetruges entfielen. Hier wurden zum einen in großem Stil an Händlerterminals Daten abgegriffen. Zum anderen wurden von sogenannten „Wechselstuben“ überhöhte Gebühren berechnet. In Zusammenarbeit mit dem BKA konnte hier eine Tätergruppe von 20 Personen festgenommen werden, sodass die Türkei heute kein Problemland mehr ist. Jetzt richtet sich unser Augenmerk auf Südafrika. Zurzeit haben wir zum Risk Manager der dortigen Mastercard-Dependance Kontakt aufgenommen und versuchen – neben der Zusammenarbeit mit den südafrikanischen Behörden – über Mastercard die dortigen Banken über Methoden zur Betrugsprävention aufzuklären.

Karten Welche Kanäle zur internationalen Zusammenarbeit bei der Missbrauchsbekämpfung gibt es?

Wir sind sowohl reaktiv tätig, um Schwerpunkte der Kriminalität zu bekämpfen, als auch bei der Betrugsprävention.

Mit EAST (European ATM Security Team) gibt es eine von Europol ins Leben gerufene Gruppierung, in der Vertreter fast aller europäischen Länder ein Netz von Ansprechpartnern für den Fall des Falles aufbauen. Die Kommunikation läuft aber vielfach nach dem Prinzip „kreativer Ungehorsam“. Denn die gesetzlichen Rahmenbedingungen stimmen heute noch nicht. So dürfen beispielsweise in Deutschland Polizisten erst nach schriftlicher Genehmigung Auslandstelefonate führen. Das führt dazu, dass wir vielfach für die Polizei solche Aufgaben übernehmen. Von der Serviceleistung her ist dies kein Business Case. Nur so können wir aber sicherstellen, dass wir auch im Ausland die notwendige Unterstützung bekommen.

Doch innerhalb Europas klafft die Rechtsprechung zu Kartendelikten noch immer weit auseinander. Ein Jurist in München setzt sich dafür ein, dass zumindest das Strafmaß für Kartendelikte in Europa vereinheitlicht wird. Bis vor kurzem stand die

Zahlungskartenkriminalität in einigen Ländern noch nicht einmal unter Strafe.

Karten Wie werden manipulierte Geldautomaten erkannt?

Zum einen werden Manipulationen teilweise von Bankmitarbeitern, Geldautomatenbestückern oder Kunden erkannt. Zum anderen überwachen wir alle grenzüberschreitenden Transaktionen. Wenn wir sehen, dass eine große Anzahl von Karten mit der gleichen Bankleitzahl am gleichen Ort benutzt werden, kann dies ein Indiz dafür sein, dass es sich dabei um Kartenfälschungen handelt. Aus den Datenbeständen wird dann der gemeinsame Einsatzort dieser Karten ermittelt – und das ist dann der „Point of Compromise“.

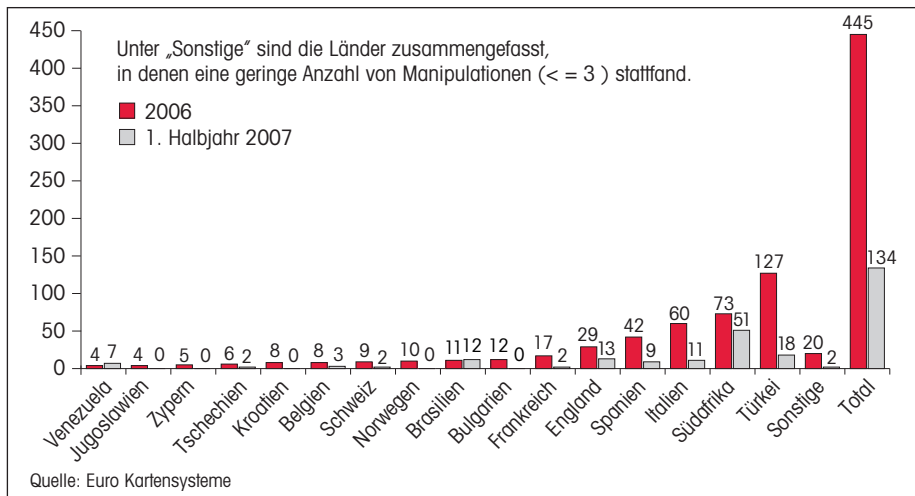
Karten Gibt es einen Trend zur Nachrüstung älterer Geldautomaten mit moderner Sicherheitstechnik?

Kartenkriminalität: Erlangungstaten 2006/2007

Örtlichkeit	Anzahl Fälle		Prozent-Anteil	
	2006	1. Hj. 2007	2006	1. Hj. 2007
Diebstahl/Pkw	1 496	768	7,17	5,62
Einbruchsdiebstahl Wohnung/Ferienwohnung	1 204	644	5,77	4,89
Diebstahl/Hotel/Pension	258	98	1,24	0,75
Diebstahl/Arbeitsplatz	936	506	4,49	4,12
Diebstahl/Kaufhaus/Geschäft	2 299	1 158	11,03	9,49
Diebstahl/öffentliche Verkehrsmittel	1 006	393	4,72	3,17
Diebstahl/Gaststätte	517	226	2,48	1,87
Diebstahl/Campingplatz	34	11	0,16	0,06
Diebstahl/Bad/Sauna/Sportstätte	72	86	0,36	0,76
Straßenraub	1 252	581	6,00	4,91
Diebstahl/Bahnhof	349	145	1,67	1,23
Diebstahl/Krankenhaus	176	92	0,85	0,69
Diebstahl/Flughafen	82	28	0,38	0,22
Postwegverlust	513	205	2,46	1,57
Trickdiebstahl (Lebanese Loop)	278	213	1,33	1,66
Verlust	–	106	–	0,65
Counterfeit (POC)	5 936	4 947	28,56	41,26
Unbekannt/Sonstige	4 446	1 782	21,33	16,21
Total	20 854	11 989	100,00	100,00

Quelle: Euro Kartensysteme

Anzahl manipulierter ausländischer Geldausgabeautomaten und PoS-Terminals



Wir hatten in Deutschland im ersten Halbjahr 2007 rund 400 Attacken an Geldautomaten. Fast die Hälfte davon konnte abgewehrt werden. Daraus wird ersichtlich, dass erhebliche Maßnahmen getroffen werden. Bei rund 53 000 Geldautomaten in Deutschland erfordert das aber eine gewaltige Investition von den Banken. Altgeräte, die sich nicht mehr auf EMV umrüsten lassen, müssen bis 2010 ausgetauscht werden. Andere Geräte können durch mechanische Eingriffe aufgerüstet werden, was etwa 2 000 bis 3 000 Euro kostet. Und die jüngeren Modelle können für einige hundert Euro per Software-Update umgestellt werden.

Insbesondere Institute, deren Automaten bereits attackiert wurden, haben ihre Geräte zudem mit Anti-Skimming-Modulen für den Karteneinzugsschlitz ausgestattet. Auch diese sind allerdings nur bedingt sicher, weil man bereits im Internet Anleitungen herunterladen kann, wie sich diese Vorrichtungen entfernen lassen. Sicherer sind Magnetstörsender, die beim Auslesen des Magnetstreifens die Daten so zerstücken, dass damit nichts anzufangen ist.

Abgesehen von der Aufrüstung der Automaten zur Verhinderung von Angriffen richtet sich unser Augenmerk auch auf die Karteninhaber. Hier gilt es, die Kunden

verstärkt aufzuklären und zu sensibilisieren. Wird zum Beispiel bei der PIN-Eingabe die Hand darübergelegt, kann die von den Tätergruppen angebrachte Kamera die PIN nicht ausspähen, und dann nützen auch ausgelesene Kartendaten nichts.

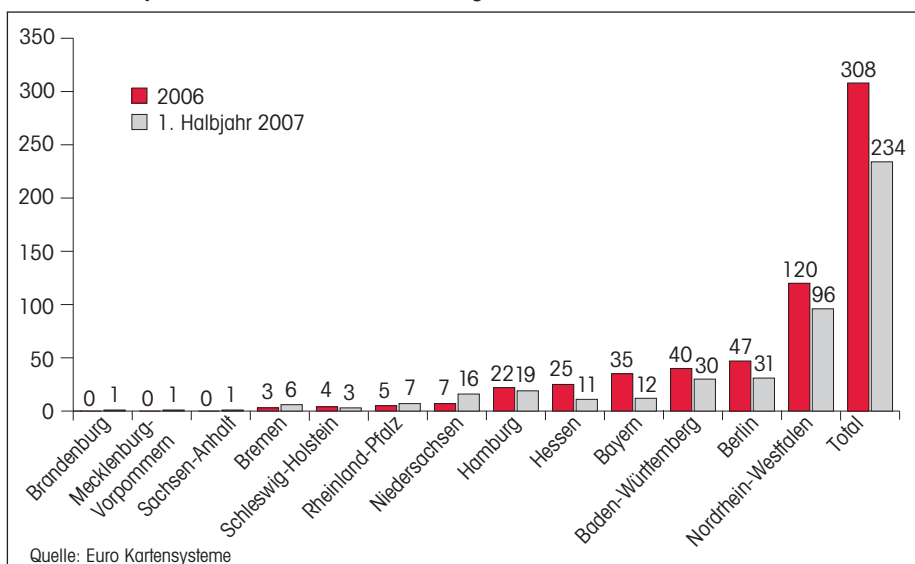
Karten Gibt es Fortschritte bei der Verbrauchererziehung?

Das Sicherheitsbewusstsein beim Karteninhaber muss man sicher noch ein bisschen schüren. Aber ich denke, dass wir schon ganz schön weit gekommen sind. Das wird auch daran deutlich, dass im Inland der Missbrauch mit verlorenen und gestohlenen Karten zurückgeht. Noch immer gibt es natürlich Karteninhaber, die eine am Freitag verlorene Karte erst montags melden. Deshalb ist es wichtig, dass wir die Sperrnotrufnummer verbreiten.

Karten Könnte sich daraus ein Trend ergeben, sicherheitsbewussten Kunden Karten ohne Magnetstreifen anzubieten, die dann eben nur in Europa einsetzbar wären?

Es könnte ein Trend werden. Es gibt sicherlich Kundengruppen, die das gut finden. Momentan kann ich einen solchen Trend aber noch nicht erkennen.

Anzahl manipulierter inländischer Geldausgabeautomaten



Karten Wie wird die Arbeit von Euro Kartensysteme in Sachen Sicherheit finanziert?

Gemäß der Geldautomatenvereinbarung des ZKA werden Angriffe auf das System, die einen Schaden nach sich ziehen, gemeinschaftlich getragen. Jede Bank und Sparkasse zahlt jedes Jahr pro Karte und Jahr die Debit Royalty. Daraus werden unsere Arbeit und der Debitschadenspool, aus dem wir Schäden erstatten, finanziert. Aufgrund der hohen Rückbelastungsquote von Schäden, die mit EMV-Karten verursacht wurden, ist die Debit Royalty für Nicht-EMV-Karten höher.