Missbrauchsprävention: Plädoyer für mehr Kooperation

Von Carlos Gómez-Sáez

Herkömmliche Methoden zur Bekämpfung von Kartenmissbrauch werden künftig nicht mehr ausreichen, so das Ergebnis einer First-Data-Studie. Nicht zuletzt deshalb, weil Sepa auch Skaleneffekte für betrügerische Attacken schafft, ist instituts- und länderübergreifender Informationsaustausch und der Aufbau einer europäischen Betrugsdatenbank gefragt. Behindert wird eine solche Kooperation durch unterschiedlichste Datenschutzbestimmungen in Europa aber auch durch Bedenken der Kartenemittenten hinsichtlich ihres Ansehens und ihrer Wettbewerbsfähigkeit. Dabei wird nach Einschätzung des Autors übersehen, dass bei einer Zunahme missbräuchlicher Transaktionen das Vertrauen der Verbraucher in elektronische Zahlungsmittel generell auf den Spiel steht. Red.

Der Missbrauch mit Kredit- und Debitkarten hat in Europa noch selten an Ländergrenzen halt gemacht. Allerdings bedingen die nationalen Besonderheiten im europäischen Zahlungsverkehr, zum Beispiel die verschiedenen Debitkarten-Programme in ganz Europa, dass nicht nur der Wettbewerb, sondern auch die Ausprägung spezifischer Betrugsmuster beim Kartenmissbrauch bis heute regional beschränkt bleibt. Mit der Single Euro Payments Area (Sepa) kommen neue Herausforderungen auf die Branche zu. Die Finanzdienstleistungsindustrie hat große Anstrengungen in wirtschaftlicher, aufsichtsrechtlicher und technischer Hinsicht unternommen, um mit dem Stichtag 1. Januar 2008 einen einheitlichen europäischen Zahlungsmarkt zu realisieren. Experten warnen jedoch, dass der Betrugsproblematik bei dem Entwurf der neuen, grenzenlosen Sepa-Welt zu wenig Rechnung getragen wurde. Insbesondere wird bemängelt, dass der für eine effektive Missbrauchsbekämpfung erforderliche Datenaustausch in der Sepa durch strikte Regulierung auf europäischer Ebene weitgehend verhindert wird.

Sepa verstärkt Missbrauchsgefahren

First Data hat vor diesem Hintergrund im Frühjahr 2007 das unabhängige Marktforschungsunternehmen Olive Insight mit der Durchführung einer Studie zum „Kampf gegen Kartenmissbrauch" beauftragt, die zu einem besseren Verständnis beitragen soll, wie die Zahlungsverkehrsbranche insgesamt das Problem des Kartenbetrugs einschätzt. Unter anderem wurde gefragt, mit welchen Mitteln die Branche dem Problem begegnet, welche Bedeutung man der europaweiten Zusammenarbeit im Kampf gegen Kartenmissbrauch beimisst und welche Hindernisse bestehen, um sich den Herausforderungen des Kartenmissbrauchs in Europa gemeinsam und erfolgreich stellen zu können.

Die Einschätzungen der Teilnehmer aus führenden Banken und Finanzinstitutionen in ganz Europa unterstreichen die zunehmenden Missbrauchsgefahren, denen die Branche sich auch unabhängig von Sepa – aber durch Sepa auch noch verstärkt – ausgesetzt sieht, zeigen aber auch die Chancen auf, die mit der europaweiten Zusammenarbeit bei Prävention und Bekämpfung von Missbrauch verbunden sind.

Eine Milliarde Euro Betrugsschaden pro Jahr

Dem Thema Kartenmissbrauch kommt in der heutigen Bankenlandschaft eine immer größere Bedeutung zu. Der jährliche Schaden in Europa wird von der EU Fraud Prevention Expert Group auf bis zu eine Milliarde Euro geschätzt.[1)] Die Studie macht deutlich, dass Banken dabei neben dem unmittelbar geldwerten Schaden insbesondere die Wirkung von Betrugsfällen auf ihre Reputation fürchten, die Auswirkungen auf das Vertrauen in die Finanzdienstleister im Allgemeinen und damit auch nachhaltig negative Folgen für Kundenbindung

Zum Autor

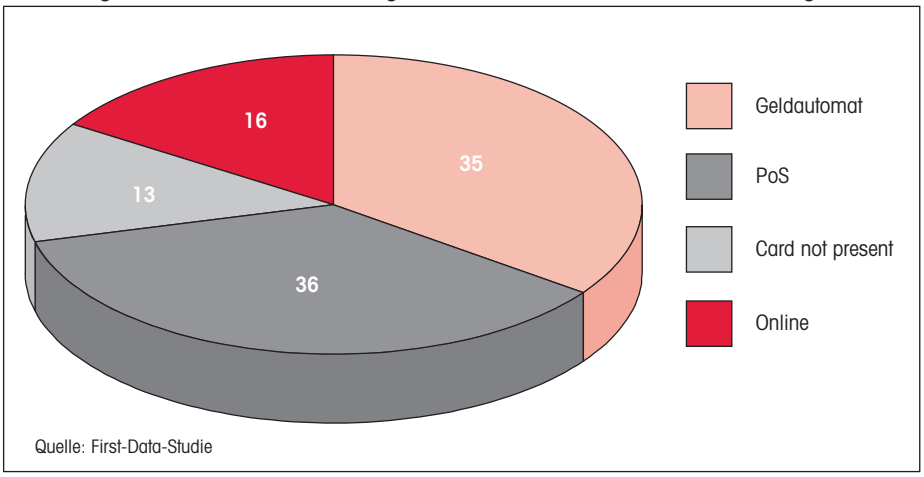
Carlos Gómez-Sáez ist Bereichsleiter Produktmanagement & Marketing bei First Data International, Bad Vilbel.

und Kundenakquisition sehen (vergleiche Abbildung 1).

Besonders besorgt sind Banken heute mit Blick auf die neu aufkommenden Betrugsszenarien. Zwar sind die traditionellen Betrugsfelder am Point of Sale (PoS) und am Geldausgabeautomaten (GAA) laut Aussage der im Rahmen der Studie Befragten auch heute noch für mehr als 70 Prozent der gesamten betrügerischen Umsätze verantwortlich (siehe Abbildung 2).

Dennoch herrscht in der Branche die Meinung vor, dass missbräuchliche Transaktionen am PoS und am GAA in Zukunft langfristig besser abgewehrt werden können, als dies zum Beispiel für den Betrug im Onlinebereich gilt.

Abbildung 2: Prozentuale Verteilung der von den Banken erlittenen Betrugsarten



Quelle: First-Data-Studie

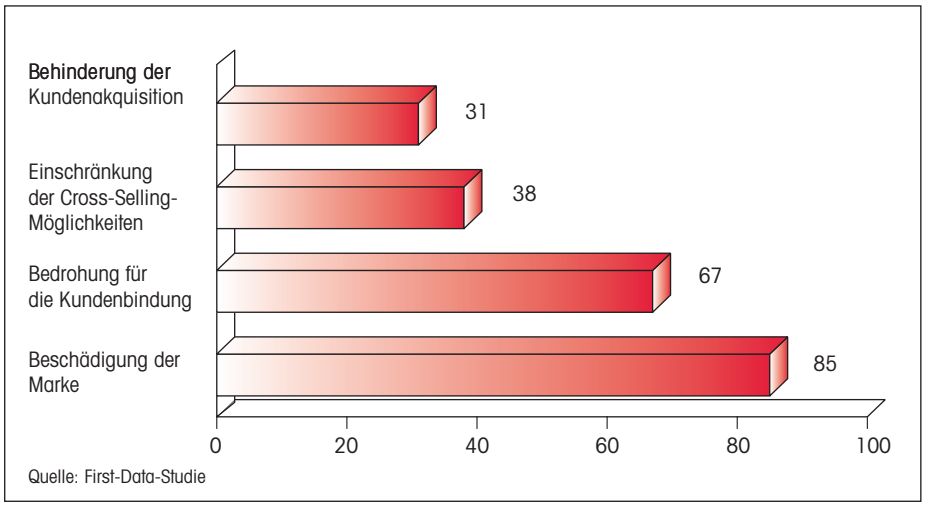
Hauptproblem Online-Betrug

Obwohl das Thema Kartenmissbrauch in den Segmenten Onlinebanking und Fernabsatzgeschäft (Onlineshopping, Telefon- und Mail-Order) derzeit von geringerer Bedeutung ist, berichtet ein Drittel der Befragten im Rahmen der Studie über einen Anstieg beim Missbrauch im Onlinebereich. 38 Prozent melden eine Zunahme von Phishing-Attacken, die sich dabei durch eine immer größere Raffinesse auszeichnen.

Da der Missbrauch im Onlinebereich Betrügern die Möglichkeit bietet, im Vergleich zu anderen Betrugsarten schneller und bequemer eine höhere Betrugsrate zu erzielen, ist auch weiterhin mit einem signifikanten Anstieg im Bereich des Online-Betrugs zu rechnen. Das gilt insbesondere für jene Regionen in Osteuropa, in denen die Internet-Nutzung heute noch gering ist, für die Zukunft aber stark anwachsen wird.

Auf absehbare Zeit werden in diesen Ländern daher Computerprogramme, die unerwünschte Funktionen ausführen – sogenannte „Malware" – und die über kompromittierte Webserver verbreitet werden, das Manipulieren von Datenbanken und der Diebstahl persönlicher Kundendaten ebenso wie in Westeuropa zu einem wesentlichen Problem für Banken werden.

Abbildung 1: Die schwerwiegendsten Auswirkungen von Kartenbetrug aus Bankensicht (in Prozent)



Quelle: First-Data-Studie

Missbrauchsprävention: Traditionelle Instrumente reichen nicht mehr

Im Kampf gegen den Missbrauch spielt die Technologie weiterhin eine entscheidende Rolle. Das bestätigten die Banken auch im Rahmen der Befragung. Eine Reihe von Banken prüft derzeit den Einsatz fortschrittlicher Instrumente und Technologien oder ist bereits dabei, diese zu implementieren. Die damit verbundene Zielsetzung ist nicht nur, den Missbrauch noch wirkungsvoller zu bekämpfen, sondern auch, belastbare Informationen darüber zu gewinnen, in welchem Ausmaß das Unternehmen tatsächlich betroffen ist.

Bestimmte Methoden zur Prävention und Entdeckung von Kartenmissbrauch, wie die Überwachung von Transaktionen, ein Kunden-„Profiling", die Überprüfung von Kartenanträgen und Einträgen in öffentlichen Verzeichnissen wurden in den vergangenen Jahren bereits erfolgreich zur Missbrauchsbekämpfung eingesetzt.

Die Branche ist sich indessen bewusst, dass diese traditionellen Instrumente allein nicht ausreichen werden, Schwachstellen so schnell zu entdecken und zu beheben,

wie dies künftig erforderlich sein wird. Um innovative Tools bei der Datenanalyse anzuwenden, bedarf es zusätzlicher Untersuchungen: So können zum Beispiel sogenannte Link-Analysen Banken dabei helfen, einen Gesamtüberblick über den Kartenmissbrauch und die damit verbundenen Kosten über das gesamte Unternehmen hinweg zu erhalten. Einige Institute konnten auch bei der Aufdeckung potenzieller Betrugsnetze sowie dem Aufspüren von Konten, die durch bestimmte Betrugsmuster gekennzeichnet waren, bereits beträchtliche Erfolge erzielen. Auch die „Zwei-Faktor-Authentifizierung" verspricht eine gewisse Unabhängigkeit von statischen Daten. Implementierungskosten und Bedenken hinsichtlich der Erfahrungen der Karteninhaber bleiben in diesem Bereich die entscheidenden Herausforderungen für den erfolgreichen Einsatz der Technik.

Betrug ist teilweise vorhersehbar

Um effektive Lösungen zu finden, müssen Kreditinstitute aber auch über die eigene Organisation hinaus denken. Das gilt umso mehr, als viele Banken heute der Meinung sind, dass Betrug in gewissen Grenzen vorhersehbar ist. So ist zum Beispiel in Bezug auf die relativ neu eingeführte Chip-Technologie bekannt, dass Betrüger bereits nach Schwachstellen suchen.

Banken und ihre Dienstleister müssen daher sehr wachsam sein und sorgfältig jede neue Entwicklung, jedes neue Produkt und jeden neuen Vertriebskanal analysieren, um sicherzustellen, dass alle Elemente in der Prozesskette so stabil und betrugsresistent wie möglich sind. Denn gerade wenn Betrug in Teilen vorhersehbar ist, ist es von großer Bedeutung, den globalen Betrugstrends und Entwicklungen frühzeitig Rechnung zu tragen. Schließlich lehrt die Erfahrung aus der Beobachtung von Betrugsmethoden und ihrer Entwicklung, dass Schwachstellen bei neuen Produkten, Vertriebskanälen, Dienstleistungen oder Technologien von Betrügern sehr schnell erkannt und ausgenutzt werden. Neue Betrugsattacken treten typischerweise zunächst in kleinerem Ausmaß auf, dann erfolgt zumeist eine exponentielle Ausbreitung des neuen Musters. Ein deutlicher Hinweis darauf, dass organisierte Banden miteinander kommunizieren und voneinander lernen. Es ist höchste Zeit, dass Banken, Dienstleister und Ermittlungsbehörden damit ebenfalls beginnen.

Länderübergreifender Informationsaustausch

Ein länderübergreifender Informations- und Erfahrungsaustausch auf Seiten der Banken, insbesondere mit jenen Banken, die als Folge betrügerischer Transaktionen bereits Verluste erlitten haben, ist dafür ein zentrales Instrument. Nur so können andere Marktteilnehmer in die Lage versetzt werden, entsprechende Abwehrmaßnahmen, Software oder technische Lösungen zu entwickeln, um die neu bekannten Schwachstellen umgehend zu beheben, bevor eine Dienstleistung oder ein Produkt in ihrem Markt angeboten wird. Dies erfordert – von allen Beteiligten der Finanzdienstleistungsbranche – eine koordinierte und strukturierte Vorgehensweise. Eine Forderung, die mit der Einführung von Sepa noch an Dringlichkeit gewinnt.

Zwei-Faktor-Authentifizierung in Kürze

Die Zwei-Faktor-Authentifizierung ist ein Login-Verfahren, das neben Benutzernamen und Passwörtern einen weiteren Faktor vom Benutzer verlangt.

- Der eine Faktor besteht darin, „dass der Nutzer etwas weiß" – üblicherweise sein Passwort oder seine PIN.
- Der andere Faktor basiert darauf, „dass der Nutzer etwas besitzt" – beispielsweise einen greifbaren Gegenstand wie eine Smartcard, eine Art Kreditkarte mit Sicherheitschip.

Single Euro Fraud Area?

Mit dem Start eines einheitlichen europäischen Zahlungsraumes am 1. Januar 2008 gewinnt der Kampf gegen den Kartenmissbrauch eine gesamteuropäische Dimension. Denn die Sepa-Anforderungen zur Standardisierung der Zahlungssysteme führen zu einer Öffnung beziehungsweise Anpassung der nationalen Debitkartensysteme. Viele dieser Systeme verfügen heute über sehr hoch entwickelte Lösungen zur Missbrauchsprävention und -bekämpfung, die auf nationalen, technischen Spezifikationen basieren.

Da sich diese Programme für eine Sepakonforme Zukunft absehbar an gemeinsamen Sepa-Standards orientieren müssen, werden sie insgesamt aber anfälliger für Manipulationen. Denn einheitliche Standards schaffen nicht nur Effizienzgewinne in der Netznutzung, sie schaffen auch Skaleneffekte für betrügerische Attacken auf die Infrastruktur.

Parallel zu dieser technischen Entwicklung wird die Einführung eines „grenzenlosen" Zahlungsraums zu einer Zunahme grenzüberschreitender Zahlungstransaktionen führen und somit auch zu einem Anstieg betrügerischer, grenzüberschreitender Transaktionen.

Datenschutzbestimmungen nicht an die Sepa-Welt angepasst

Die Möglichkeiten, dieser zunehmenden Bedrohung durch gezielten Datenaustausch zu begegnen, sind heute noch immer durch massive Hindernisse für den grenzüberschreitenden Austausch von Daten zur Missbrauchsentdeckung und -prävention eingeschränkt. Während Betrüger also ohne jegliche Einschränkungen über Grenzen hinweg operieren können,

gilt dies nicht für Banken und Ermittlungsbehörden. Die Gefahren in diesem Zusammenhang sind von der Europäischen Union und der Europäischen Kommission schon lange erkannt:

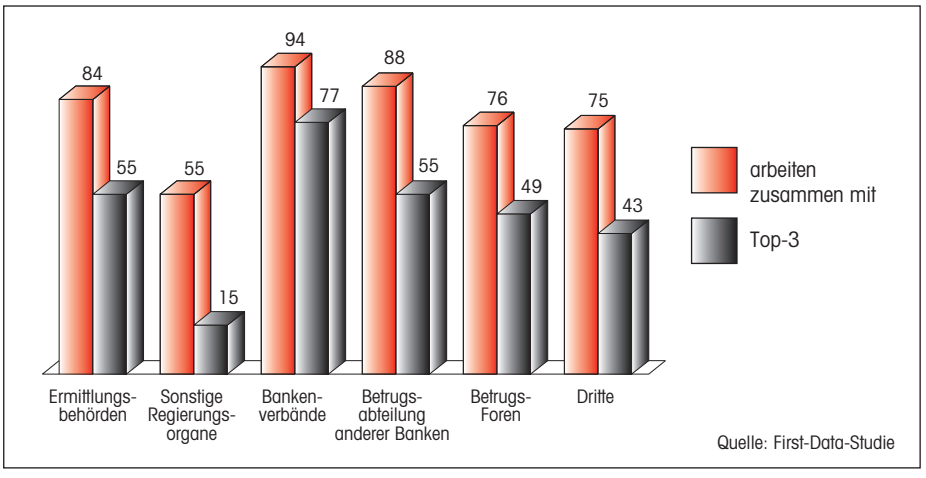
- Im Oktober 2004 verkündete die EU-Kommission, dass sie eine Klarstellung und Harmonisierung der Datenschutzbestimmungen in der EU anstrebt.

- Die EU Fraud Prevention Expert Group (FPEG) warnte im Dezember 2006, dass Betrüger eine weiter bestehende Fragmentierung der Missbrauchsbekämpfung innerhalb der EU-Mitgliedsstaaten in der Sepa zu ihrem Vorteil nutzen könnten, um ihre betrügerischen und grenzüberschreitenden Aktivitäten weiter auszubauen. Sie empfahl damals, dass die Zahlungsindustrie auf diese Bedrohung reagieren müsse, indem sie Instrumente entwickelt, die es ermöglichen, Betrugsszenarien auf einem breiteren EU-Level aufzudecken und zu verhindern.

- Auch die FPEG-Untergruppe Data Management fordert in diesem Zusammenhang: „Im Hinblick auf die Zahlungsverkehrsbranche sollte die Einführung Sepa-konformer Programme naturgemäß auch Sepa-konforme Datenbanken zur Folge haben (entweder innerhalb eines Programms oder in Form von konsolidierten, programmübergreifenden Datenbanken)". Die Gruppe stellt jedoch fest, dass „die existierenden Datenschutzbestimmungen nicht an die künftige Sepa-Welt angepasst sind, in der paneuropäische Datenbanken benötigt werden."

Denn beim Austausch von grenzüberschreitenden Informationen zur Aufdeckung und Bekämpfung von Kartenmissbrauch existieren heute noch erhebliche Barrieren. Dazu zählen Hürden in Bezug auf den Datenfluss sowie die strikten nationalen Datenschutzbestimmungen für die Verarbeitung persönlicher Daten. Diese Problematik verhindert in zahlreichen Ländern die Erstellung von Anti-Betrugsdatenbanken.

Abbildung 3: Mit welchen Unternehmen/Gremien Banken im Kampf gegen Kartenbetrug zusammenarbeiten (in Prozent der Befragten)



Auch wenn die Entwicklung einheitlicher Datenschutzbestimmungen innerhalb der Europäischen Union eine mögliche Antwort auf das gegenwärtige Problem wäre, ist dies noch ein langer Weg. Paragraf 71 des Entwurfs der Payment Services Directive (Dezember 2005) beinhaltet einen Absatz, der die Mitgliedsstaaten verpflichtet, „die Verarbeitung persönlicher Daten durch Zahlungssysteme oder Zahlungsverkehrsdienstleister zu gestatten, wenn dies für die Vorbeugung, Untersuchung, Aufdeckung und Verfolgung von Zahlungsbetrug erforderlich ist".[2)] Eine verbindliche Anordnung des grenzüberschreitenden Datenaustauschs ist jedoch nicht vorgesehen.

Es steht viel auf dem Spiel

Im Falle einer Implementierung von Paragraf 71 würde den Datenschutzbehörden basierend auf den aktuellen europäischen Datenschutzbestimmungen (European Data Protection Directive) eines jeden Landes noch immer eine große Kontrollbefugnis bleiben.

Das Risiko, dass im Rahmen von Sepa die Zahl der missbräuchlichen Transaktionen steigen wird, bleibt groß, und es steht viel auf dem Spiel. Dazu die EU Fraud Prevention Expert Group: „Die Umsetzung solider Maßnahmen zur Missbrauchsprävention für den bargeldlosen Zahlungsverkehr ist für die Schaffung eines einheitlichen europäischen Zahlungsverkehrsraums von enormer Bedeutung." Ohne die Umsetzung dieser Maßnahmen besteht die Gefahr, dass das Vertrauen der Verbraucher in elektronische Zahlungsmittel durch eine Zunahme missbräuchlicher Transaktionen sinkt und somit die Prinzipien, die der Errichtung einer Sepa zugrunde liegen, untergraben werden.

Noch zu wenig Bereitschaft zur Kooperation

Die Ergebnisse der Studie zum „Kampf gegen Kartenmissbrauch" zeigen, dass die Banken die oben aufgeführten Einschätzungen zur Sepa teilen. Sie unterstreichen, wie wichtig ein länderübergreifender Informationsaustausch im einheitlichen europäischen Zahlungsverkehrsraum sein wird, um den Missbrauch in den unterschiedlichen Akzeptanzfeldern (GAA, PoS, Onlinebanking und Fernabsatzgeschäft) aufzudecken und effektiv bekämpfen zu können.

Die Untersuchung veranschaulicht aber auch, warum Unsicherheit und Unwissenheit – sowohl in Bezug auf das bestehende Gefahrenausmaß als auch die zahlreichen Gefahrenquellen – die in diesem Bereich unternommenen Anstrengungen

noch immer negativ beeinflussen: Unzureichende Informationen über die aus dem Missbrauch resultierenden Kosten einerseits sowie die jeweils individuellen Überlegungen der einzelnen Spieler hinsichtlich ihres Ansehens und ihrer Wettbewerbsfähigkeit andererseits reduzieren die Bereitschaft der einzelnen Banken zum Informationsaustausch.

Darüber hinaus schränken, wie bereits dargestellt, umfassende Datenschutzbestimmungen den Austausch von Informationen ein – beziehungsweise Banken befinden sich weitestgehend in dem Glauben, dass diese Bestimmungen sie daran hindern.

Länderübergreifende Betrugsdatenbank aufbauen

Unsere Zuversicht für den effektiven Kampf gegen Kartenmissbrauch gründen daher im Potenzial eines umfassenden Informationsaustausches und in der gegenseitigen Aufklärung. Denn Bankenverbände und Handelsorganisationen fördern bereits aktiv den Datenaustausch zwischen Banken ebenso wie eine effizientere Zusammenarbeit mit den Ermittlungsbehörden (siehe Abbildung 3). Die Europäische Union und das European Payments Council haben ebenfalls signalisiert, dass eine länderübergreifende Betrugsdatenbank notwendig ist, um im Rahmen des einheitlichen europäischen Zahlungsverkehrsraums Sepa den Missbrauch nachhaltig zu bekämpfen.

Im Kampf gegen Kartenmissbrauch muss die gesamte Branche zusammenarbeiten und auf Worte Taten folgen lassen. Es gilt sicherzustellen, dass die Kreditwirtschaft einschließlich der Aufsichts- und Ermittlungsbehörden adäquate Maßnahmen durchführt, um gemeinsam dem weltweiten Betrügernetz den Kampf anzusagen.

Fußnoten
[1)] FPEG Report „FPEG Subgroup on Data Management: Report from the Secretariat" vom 8. Dezember 2006.
[2)] The Payment Services Directive.