Missbrauchsprävention: **POC-Identifikation** als Erfolgsfaktor

Von Johannes Praschinger

Auch ohne Kunden durch überschnelle Kartensperre zu verärgern, lässt sich das Risiko von Kartenmissbrauch um die Hälfte reduzieren, meint Johann Praschinger. Dies setzt freilich Risikomanagementsysteme mit integrierter POC-Funktionalität voraus. Daneben rät der Autor auch dringend zu einer horizontalen Sicht auf alle Kanäle statt der bislang verbreiteten „Silo-Strukturen". Letztere seien jedoch noch bei 78 Prozent der Banken gängige Praxis. Red.

Obwohl sich beispielsweise in Großbritannien der EMV-Standard bereits weitgehend durchgesetzt hat, steigt die Zahl der Missbrauchsfälle weiter. Alleine im ersten Halbjahr 2007 verzeichnete die britische Vereinigung zum Zahlungsverkehr APACS einen Zuwachs von 26 Prozent gegenüber dem Vorjahreszeitraum. Nur hat sich der Schwerpunkt der betrügerischen Aktivitäten verlagert. Die Betrüger agieren zunehmend international und technisch beschlagener. Sie suchen immer neue Wege, um an die notwendigen Informationen auf den Karten und die PIN zu kommen.

Hoch im Kurs ist derzeit zum Beispiel das sogenannte „social engineering": Von arglosen Verbrauchern werden per Telefon oder im Internet persönliche Daten abgefragt, die dann dazu genutzt werden, um eine neue Karte inklusive Geheimnummer zu beantragen. Mit dieser vermeintlich echten Karte wird dann das Konto abgeräumt. Ein zweiter problematischer Fall sind nach wie vor Kartenlesegeräte am Point of Sale oder Geldautomaten, insbesondere im außereuropäischen Ausland. Leider ist es für Betrüger ein Leichtes, dort mit Manipulationen an den Geräten die Informationen vom Magnetstreifen der Karte auszulesen und dann an anderer Stelle mit einer Kopie der Karte Geld abzuheben.

Rasche Erkennung des Point of Compromise

Der Anteil dieser Skimming-Fälle am Kartenmissbrauch hat sich in den letzten Monaten deutlich erhöht. Zwar rüsten die Hardware-Hersteller immer weiter auf und haben insbesondere bei Geldautomaten Maßnahmen gegen solche Betrugsversuche unternommen. Aber in vielen Regionen der Welt scheuen die Banken oder Geldautomatenbetreiber bisher die hierfür notwendigen Investitionen. Umso wichtiger ist es für die kartenausgebenden Institute, sehr rasch zu erkennen, von wo der Betrugsversuch ausging.

Einige der innovativeren europäischen Banken haben erkannt, dass die Identifizierung des sogenannten Point of Compromise (POC) ein kritischer Erfolgsfaktor im Kampf gegen Betrug und Missbrauch ist. Ist der POC einmal identifiziert, kann die Bank die notwendigen Entscheidungen treffen, um Schaden von sich und seinen Kunden abzuwenden. Konkret setzt das voraus, dass mit entsprechender technischer Unterstützung bereits nach zwei oder drei Skimming-Versuchen erkannt werden kann, wo der POC liegt. Dann lassen sich beispielsweise rasch alle Karten sperren, die etwa zur selben Zeit am selben Terminal genutzt wurden.

Wahl zwischen Geldverlust und Kundenfrust

Allerdings erfordert diese Entscheidung enormes Fingerspitzengefühl, um einerseits Missbrauch einzudämmen und andererseits die Kunden nicht zu verärgern, deren Karten vorübergehend gesperrt werden. In vielen Fällen reicht die Datenbasis nicht aus, um eine sofortige Sperre zu initiieren. Dann wird die Bank die Transaktionen der betroffenen Karten zunächst sicherheitshalber beobachten und erst dann einschreiten, wenn weitere Auffälligkeiten hinzukommen wie größere Ausgaben in kurzen Abständen. Evident

Zum Autor

Johannes Praschinger ist Director Central Region bei ACI Worldwide, Sulzbach.

ist der Skimming-Versuch natürlich dann, wenn in der Zwischenzeit mit der Originalkarte an anderer, räumlich entfernter Stelle Geld abgehoben oder bezahlt wird. Gleichzeitig kann auch das Kartenlesegerät am Point of Compromise für weitere Transaktionen gesperrt werden, indem es auf eine Blacklist gesetzt wird.

Zusammen genommen lässt sich so das Verlustrisiko um gut die Hälfte begrenzen. All dies ist allerdings nur dann möglich, wenn der Informationsaustausch grenzüberschreitend und schnell funktioniert. Das ist aber wegen unübersichtlicher Datenschutzbestimmungen und technischer Hürden beileibe nicht der Fall.

Multiperspektivische Betrachtung sichert Entscheidungen ab

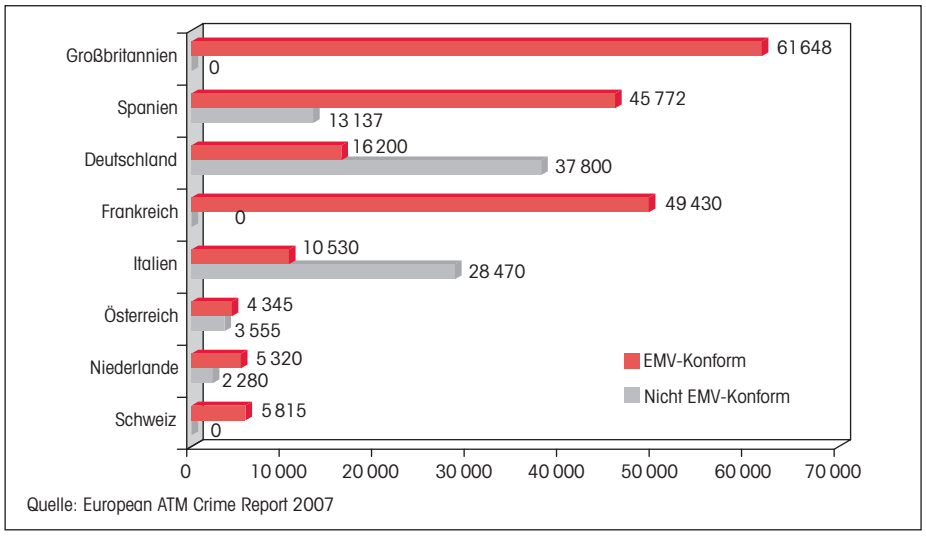
Auch innerhalb der Bank selbst lassen sich die Prozesse noch beschleunigen. Die manuelle Bearbeitung der potenziellen Missbrauchsfälle überfordert die Ressourcen und kostet zu viel Zeit. Gefragt sind daher Risk Management Lösungen, in die POC-Funktionalität eingebaut ist.

Die Analyse der Kartentransaktionen ist aber nur eine Seite der Medaille. Noch genauer und schneller lässt sich agieren, wenn weitere Informationen herangezogen werden können. Dazu zählen zum Beispiel Gewohnheiten des Karteninhabers oder konkrete Ereignisse, die aufeinander bezogen werden können.

Dazu ein Beispiel: Mit einer ec-Karte wird plötzlich ein erklecklicher Betrag in einer noblen Boutique in Paris bezahlt. Das war mit dieser Karte noch niemals zuvor der Fall. Auch lassen sich keine anderen Transaktionen finden, die irgendeine Spur nach Paris aufweisen. Ein klarer Fall von Missbrauch? Wenn man die Information aus dem Debit-Karten-Kanal isoliert betrachtet – vielleicht. Aber bei näherem Hinsehen legt sich die Aufregung wieder: Der Kunde hatte sein Flugticket nach Paris online mit der Kreditkarte bezahlt

In einem anderen Fall transferiert ein Kunde regelmäßig mittels Telefonbanking Geld zwischen zwei Konten – zum Beispiel vom Festgeldkonto auf das Girokonto. Eines Tages nun nutzt der Kunde plötzlich Onlinebanking für diesen Transfer. Rein vom Internetkanal her gedacht ist daran nichts Auffälliges. Aber wenn der Telefonkanal mit in die Betrachtung einbezogen wird, erscheint die letzte Transaktion schon ein wenig verdächtig, sodass die Bank hierauf ihr Augenmerk legen kann, um schnell zu reagieren, wenn plötzlich viel Geld vom Girokonto abgehoben wird.

Anzahl der Geldautomaten mit und ohne EMV-Konformität



Quelle: European ATM Crime Report 2007

Die Bank hat also eine bessere Entscheidungsgrundlage, wenn sie mehrere Informationen aus unterschiedlichen Transaktionskanälen und/oder verschiedenen Kartensystemen kombinieren kann. Dann fällt es deutlich leichter, Betrugsfälle aufzuspüren und im Keim zu ersticken.

Horizontale Kundensicht statt vertikaler Silos

Voraussetzung dafür ist allerdings, dass Risk Management als alle Kanäle umfassendes Konzept verstanden wird und dass die technischen Voraussetzungen dafür geschaffen sind, alle Transaktionskanäle miteinander zu verzahnen. Silo-artige Systeme für jeden einzelnen Kanal sollten definitiv der Vergangenheit angehören. Eine Umfrage des britischen Economist hat aber zutage gefördert, dass immer noch 78 Prozent der Banken Silo-Strukturen pflegen.

Das hat auch damit zu tun, dass die einzelnen Kanäle wie selbstständige Business Units oder Profit-Center geführt werden. Jeder Verantwortungsbereich versucht sein bestes, sein eigenes Risiko möglichst gering zu halten. Dabei allerdings auf Daten aus anderen Centern zurückzugreifen, fällt oft aus technischen, aber auch aus psychologischen Gründen schwer.

Das sogenannte Enterprise Risk Management (ERM) setzt also einen Perspektivwechsel voraus. Nicht mehr der einzelne Bezahl- oder Transaktionsvorgang, nicht mehr jeder Transaktionskanal – mit oder ohne Kartenanteil – steht im Mittelpunkt, sondern der Kunde mit seinen Transaktionsvorlieben und seinen üblichen Verhaltensweisen bei Bankgeschäften. Dadurch ist die Betrachtung von Missbrauch im Kreditwesen nicht nur eingeschränkt auf den Zahlungsverkehr. Auch der Versuch von Geldwäsche kann so bereits im Keim erstickt werden. Letztlich nützt diese Perspektive jeder einzelnen Business Unit und im Ergebnis allen Beteiligten: den Verbrauchern wie der Bank.