Maßnahmen gegen die **Kartenkriminalität**

Von Ewald Judt und Robert Komatz

Bildquelle: 420654_R_B_by_Dieter Schütz_pixelio.de

Nur der vollständige Umstieg auf die Chiptechnologie kann eine finale Lösung im Kampf gegen den Fraud sein, halten die Autoren fest. Solange jedoch „Magnetstreifenländer" wie die USA sich dem Chip verweigern, muss die Kreditwirtschaft weitere Sicherheitsmaßnahmen ergreifen. Geldautomatenmanipulationen zum Abgreifen von Kartendaten hat es in Österreich seit mehreren Jahren nicht mehr gegeben. Und auch die erfolgreiche Manipulation von PoS-Terminals kam nur 2006 einmal vor. An Geldautomaten arbeitet die österreichische Kreditwirtschaft mit dem Randomnummern-System, mit dem Schäden – auch durch den Einsatz gefälschter Karten im Ausland – weitgehend verhindert werden. Red.

Datendiebstahl (Kartendaten und PIN) und der Einsatz gefälschter Karten war und ist ein Problem für das Kartengeschäft. Das trifft grundsätzlich für alle Debit- und Kreditkarten zu. Österreich ist dabei – ähnlich wie auch Deutschland – schwergewichtig ein Debitkarten-Land. Ende 2010 gab es über acht Millionen Maestro-Bankomatkarten, wie die Debitkarten in Österreich bezeichnet werden. Damit ist nahezu jeder Zeichnungsberechtigte eines Girokontos mit einer derartigen Karte ausgestattet.

Die Aufmerksamkeit von Pay-Life, der Drehscheibe für die überwältigende Anzahl der Kartentransaktionen in Österreich, gilt daher insbesondere der Sicherheit der Maestro Bankomatkarten.

Pay-Life ist als Issuer und Acquirer sowie als Betreiber des österreichischen Bankomat-Geldausgabeautomatensystems mit 160 Millionen Transaktionen über 20 Milliarden Euro 2010 und der rund 75 000 Bankomat-Kassen-PoS-Terminal-Systems (2010: 360 Millionen Transaktionen über ein Volumen von 18 Milliarden Euro) in allen seinen Funktionen mit Fraud konfrontiert, wobei der Vermeidung des Skimming, dem Datendiebstahl am Geldautomaten oder am PoS-Terminal, und der darauf beruhenden betrügerischen Nutzung von Kartenfälschungen herausragende Bedeutung zukommt.

Die Vermeidung des Datendiebstahls und die Verhinderung von Transaktionen mittels gefälschter Karten kann durch Absicherung der Geldautomaten, durch Absicherung der PoS-Terminals und durch Absicherung des Karteneinsatzes vonstatten gehen.

Zu den Autoren

Dr. Ewald Judt ist Honorarprofessor der Wirtschaftsuniversität Wien und Geschäftsführer der PayLife Bank GmbH, **Robert Komatz** ist Prokurist der PayLife Bank GmbH, Wien.

GAA-Manipulationen seit 1993

Von 1980, dem Jahr seiner Einführung, bis 1990 gab es nahezu keine verbrecherischen Maßnahmen im Zusammenhang mit dem Bankomat-System. Erst seit 1990 wird das System regelmäßig attackiert – mit einfachen Tricks über brutale Gewalt bis zu ausgeklügelten Hitech-Angriffen. All diesem wurde konsequent durch Verbesserungen der Bankomaten selbst und des dahinterstehenden Environments begegnet.

1993 wurde erstmals Hitech gegen Bankomaten eingesetzt, um zu Kartendaten und den PINs zu kommen. Dabei wurden die auf dem Magnetstreifen befindlichen Daten durch einen vor dem Kartenleser angebrachten „zweiten" Kartenleser ausgelesen und die PIN durch ein Keyboard Overlay („zweite" Tastatur) oder eine Minikamera ausgespäht.

Maßnahmen zum Schutz von Kartenleser und PIN-Pad

Die in der Folge getroffenen Maßnahmen betrafen den Schutz des Kartenlesers und den Schutz des PIN-Pads sowie eine Kamerainstallation.

Hinsichtlich des Schutzes des Kartenlesers wurde ein spezielles Plexiglas-Attachment auf dem Kartenleser montiert, der keine Installation eines „zweiten" Kartenlesers mehr ermöglicht. Wird dieses Attachment mit roher Gewalt entfern, geht der Bankomat außer Betrieb.

- Dazu wurde in den Kartenleser eine Zitterfunktion inkludiert, die das Lesen des Magnetstreifens massiv erschwerte.

- Die Ausspähung der PIN mittels eines Keyboard Overlays wurde durch die Anbringung unregelmäßiger Halbkugeln auf dem PIN-Pad verunmöglicht.

Eine Zeitlang gelang es auch, die Installation von Kameras durch ähnliche Maßnahmen zu verhindern. Durch die Miniaturisierung der Kameras gelingt dies allerdings immer seltener.

Darüber hinaus wurde in die Bankomaten ein Kamerasystem bestehend aus Kamera und Festplatte – eingebaut. Die Frontseite des Bankomaten wird in Vier-Sekunden-Intervallen überwacht, sodass auch ohne Transaktionen eventuelle Manipulationen festgehalten werden. Während einer Transaktion werden zwei Fotos – eines, wenn die Karte eingeführt wird, und eines, wenn das Bargeld entnommen wird – gemacht. Die Bilddaten sind auf der Festplatte im Durchschnitt drei Monate verfügbar und werden danach gemäß dem First-in-First out-Prinzip wieder gelöscht. Wenn es notwendig ist, werden die auf der Festplatte innerhalb eines definierten Zeitraums gespeicherten Daten auf einen Server in die Bankomat-Sicherheitsabteilung überspielt.

Alle diese Maßnahmen haben dazu geführt, dass es seit Jahren keine Attacken dieser Art mehr auf das Bankomat-System gibt. Wenn man allerdings das Naturell der Kriminalität in Betracht zieht, muss man davon ausgehen, dass das Bankomat-System auch künftig angegriffen werden wird – mit Methoden, die wir noch nicht kennen. Es gilt dann, erneut unverzüglich Abwehrmaßnahmen zu setzen.

Manipulationssichere PoS-Terminals

Bis heute hat es nur eine Attacke – 2006 – auf das Bankomat-Kasse-PoS-Terminalsystem gegeben, bei dem an zwölf Terminals Daten technisch ausgespäht wurden. Fraudster drangen unentdeckt in der Nacht in ein Unternehmen ein, öffneten unbemerkt die Bankomat-Kasse(n), überwanden alle Sicherungselemente, zapften an Datenleitungen im PoS-Terminal die Magnetstreifendaten ab, spähten durch zusätzliche Einbauten die PIN aus, speicherten Magnetstreifendaten und PIN im Gerät, riefen sie per Funk ab oder holten sie durch erneutes Eindringen später ab, produzierten gefälschte Karten und versuchten mit diesen Bargeld (im Ausland) abzuheben.

Dank einer intensiven Zusammenarbeit mit der Polizei konnte diese Attacke aufgeklärt und die Täter verhaftet werden. Seit damals wird der Absicherung des Bankomat-Kassen-PoS-Terminalsystems große Bedeutung beigemessen und der Erfolg konnte durch eine Reihe von Maßnahmen erreicht werden.

- Eine Software wurde entwickelt, die in der Bankomat-Kasse eine Reihe von Events aufzeichnet und laufend an einen Server übermittelt. Sie konnte bereits nach drei Monaten an die Bankomat-Kassen hinausgeladen werden.

- Des Weiteren wurde eine Software entwickelt, die am Server die von den Bankomat-Kassen übermittelten Events auswertet und auf verdächtige PoS-Terminals aufmerksam macht. Sie kam nach sechs Monaten zum Einsatz. Das hat zu einer hohen Sicherheit der Bankomat-Kassen geführt. In den Jahren seither – von 2007 bis 2010 – wurden lediglich acht weitere Terminals (erfolglos) attackiert. Parallel zu diesen Bemühungen wurde eine neue Generation von Bankomat-Kassen mit verbesserten Sicherheitsfeatures marktreif gemacht und ein Komplettabtausch auf diese neue Bankomat-Kassen-Generation in Angriff genommen, der Ende 2010 abgeschlossen war.

Mittlerweile gibt es eine Fülle von zusätzlichen Maßnahmen, um PoS-Terminals sicherer zu machen. Das geht

- von einem unregelmäßiges Design (Abwandlungen der äußeren Form sollen verhindern, dass ein zweiter Kartenleser und eine zweite Tastatur unbemerkt platziert werden kann),

- dem Ausgießen des Hohlraums im PoS-Terminal mit Kunstharz (schützt vor Eindringen in das Terminal, macht aber statt Wartung Terminalersatz notwendig),

- Verschweißung der Schale (erschwert das Öffnen des Terminals und führt dazu, dass dies leicht erkannt wird; aber: teurere Wartung, da neue Schale erforderlich),

- Anbringen eines Sicherheitssiegels (muss so angebracht sein, dass ein Aufbrechen ersichtlich wird)

- bis zur Beleuchtung des Karteneinzugsschlitzes (Einbauten zum Lesen des Magnetstreifens werden leichter erkannt, da Beleuchtung reduziert wird beziehungsweise Einbauten Schatten werfen).

Chiptechnik bewährt sich

Der ultimative Einsatz gegen gefälschte Karten sind Chip-Transaktionen. Österreich ist bereits 1996 für alle Maestro Bankomatkarten und alle Bankomaten auf Transaktionen mit dem proprietären Paychip umgestiegen – es gab daraufhin keine Transaktionen mit gefälschten Karten in Österreich mehr. Von 2004 bis 2007 hat Österreich alle Karten mit dem EMV-Chip ausgestattet – seither geht die Anzahl an Transaktionen mit gefälschten Karten in der Sepa, der Single European Payment Area, und in den anderen Ländern, die bei Geldautomaten und PoS-

Terminals auf EMV umgestiegen sind, drastisch zurück und nähert sich der Null.

Schwachstelle sind und bleiben die Länder, die erst im Umstieg auf EMV begriffen sind und die „Magnetstreifenländer", das sind die Länder, die sich noch nicht für einen Umstieg auf EMV entschlossen haben, insbesondere die USA. Es ist zu erwarten, dass der grenzüberschreitende Fraud sich sukzessive in diese Länder verlagern wird. Bis alle Märkte „Chipländer" sein werden, gilt es jedoch für Transaktionen in diesen Ländern spezielle Vorsorge walten zu lassen.

Transaktionsmonitoring zur Betrugserkennung

Für die Issuer gilt es ein Transaktionsmonitoring mit intelligenten Systemen zu betreiben, um Auffälligkeiten bei der Kartennutzung insbesondere bei Magnetstreifen-Transaktionen zu erkennen. Derartige Systeme ermöglichen die Ablehnung (Nicht-Autorisierung) verdächtiger Transaktionen mit gefälschten Karten. Dieses Screening ist eine effektive Maßnahme, sofern sie im Zuge einer Autorisierung erfolgt. Aber auch wenn das Monitoring im Nachhinein erfolgt, befähigt der Einsatz derartiger Systeme auch zur Sperre der betroffenen Karte(n) oder weiterer Recherchen.

Dieses Monitoring der Kartentransaktionen wird durch die Reduktion der Länder, wo es noch Magnetstreifentransaktionen gibt, einfacher. Weiter ist damit ein besseres und sichereres Reagieren bei Fälschungsverdacht möglich.

MM-Merkmal und Randomnummern

Weitergehende Maßnahmen zur Verhinderung des Einsatzes gefälschter Karten bedürfen einer engen Zusammenarbeit von Kartenemittenten und insbesondere den Geldautomatenbetreibern eines Landes. Dazu gehört das MM-Merkmal, das gegen den Einsatz gefälschter (deutscher) Karten hilft – allerdings nur bei Geldautomaten in Deutschland.

In Österreich (und auch in Frankreich und Spanien) setzt man auf das Randomnummern-Verfahren zur Entdeckung gefälschter Karten. Bei der Nutzung einer (österreichischen) Maestro Bankomatkarte an einem (österreichischen) Bankomaten wird im Zuge der Autorisierung eine Randomnummer generiert, die auf den Magnetstreifen der Karte geschrieben wird. Bei neuerlicher Nutzung dieser Karte an einem Bankomaten wird die „alte" Randomnummer durch eine „neue" Randomnummer ersetzt. Somit können Karten, die mit einer „alten" Randomnummer dupliziert worden sind, bei deren Nutzung erkannt werden. Dies erfolgt bei der Autorisierung einer Kartentransaktion auf Magnetstreifenbasis (egal ob diese im In- oder Ausland, an einem ATM oder an einem PoS-Terminal in die Wege geleitet wurde). Beim Einsatz einer Karten mit einer „alten" Randomnummer steht fest, dass der Magnetstreifen ausgespäht und in der Folge die Karte gefälscht wurde.

Die Konsequenz ist, dass die gefälschte Karte am jeweiligen Geldautomaten eingezogen wird und am PoS keine Zahlung mehr möglich ist. Dieses Verfahren wirkt gegen den Einsatz gefälschter Karten – auch beim Karteneinsatz im Ausland, sofern die jeweilige echte Karte zwischenzeitlich bei einem Bankomaten im Inland eingesetzt (und damit die jeweils „alte" Randomnummer durch eine „neue" Randomnummer) ersetzt wurde.

Voraussetzung für die Effektivität eines derartigen Randomnummernverfahrens ist, dass tunlichst alle Geldautomaten eines Landes beim Schreiben von „neuen" Randomnummern mitmachen, es ein zentrales Monitoring der Kartentransaktionen unter Einschluss der Randomnummer und eine zentrale Randomnummern-Vergabestelle in einem Land gibt. Die Vergabe der Randomnummern und das zentrale Monitoring erfüllt in Österreich Pay-Life im Auftrag der österreichischen Banken.

Das Randomnummern-System hilft nicht nur bei der Schadensverhinderung, sondern auch bei der Schadensvermeidung nach dem Entdecken von gefälschten Karten beim Monitoring der Randomnummern. Wenn mehrere Transaktionen mit duplizierten Magnetstreifen (also mit einer falschen Randomnummer) kurz hintereinander vorkommen (was in der Regel der Fall ist), kann leicht der Point of Compromise entdeckt werden. Alle dort im fraglichen Zeitraum eingesetzten (österreichischen) Maestro Bankomatkarten können in der Folge „immunisiert" oder ausgetauscht werden. Auch diese Nachbearbeitung als schadensreduzierende Möglichkeit des Randomnummern-Systems ist sehr effizient, da Fälschungsfälle frühzeitig entdeckt werden – weil die Österreicher über ihre Karte sehr häufig Geld an Bankomaten beziehen – und Schäden daher weitgehend verhindert werden.

Nur der Chip ist eine finale Lösung

Finale Lösung gegen Ausspähung der Magnetstreifendaten und dem Einsatz von gefälschten Karten kann nur der Umstieg auf Chiptransaktionen sein. Kurzfristig ist das Entfernen des Magnetstreifens allerdings keine Lösung, da kundenunfreundlich: Karten ohne Magnetstreifen können an den Geldautomaten und PoS-Terminals, die nur auf Magnetstreifenbasis arbeiten, nicht eingesetzt werden.

Es gilt vielmehr, dass die Card Schemes insbesondere Mastercard Worldwide und Visa International alle Banken/Länder/Regionen, die noch nicht auf den EMV-Chip setzen, überzeugen, auf den EMV-Chip bei Karten, Geldautomaten und PoS-Terminals umzusteigen. Dann könnte in einer abgestimmten Vorgangsweise der Magnetstreifen entweder en bloc bei einem Kartentausch stichtagsbezogen oder sukzessive im Zuge des Re-Issuings der Karten weggelassen werden.