Fraud-Prävention: Neue Kartenstrategien reichen nicht

Von Cornelia Zwirnmann

Beim Thema Fraud ist der Wettlauf der Kreditwirtschaft mit professionellen Hackern ein Dauerthema. Die Sicherheitsverfahren sind bekannt: Anti-Skimming-Module, EMV oder biometrische Verfahren, Kartenstrategien wie Chip-und-PIN-only oder Lösungen, mit denen der Karteninhaber selbst über die Einsetzbarkeit seiner Karte im Ausland entscheiden kann. Um effektiven Schutz zu gewährleisten, müssen diese Maßnahmen freilich durch softwareseitige Lösungen ergänzt werden. Nur die Verbindung der einzelnen Maßnahmenpakete kann greifen. Red.

Kriminalität am Geldautomaten ist ein ernst zu nehmendes Thema. Weltweit werden durch Attacken auf die Sicherheit bei der kartengestützten Bargeldbeschaffung sowie Bezahlvorgängen Schäden in Milliardenhöhe verursacht. Auch hierzulande besteht mit Blick auf die Zahlen des BKA aus 2010 kein Anlass zum Aufatmen.

Ziehen die Experten in den Geldinstituten Bilanz, wird schnell deutlich, dass die Kriminalität an den SB-Geräten 2010 zwar leicht, aber eben nicht wesentlich eingedämmt werden konnte. Bereits per Juni 2010 wurden 1 927 Manipulationsattacken an Geldautomaten in Deutschland registriert. Das entspricht nahezu den Vergleichswerten des gesamten Jahres 2009.

Die Betrugsvarianten florieren: Mit Hilfe von Skimming, Cash Trapping (Manipulation am Ausgabeschacht) und anderen Methoden werden die Bankkunden viel zu oft erfolgreich ihres Geldes beraubt. Ein eklatanter Vertrauensverlust der Betroffenen in die Sicherheit der Bargeldabhebung am Automaten ist die Folge. Zusätzlich stehen die Opfer häufig vor zeitaufwendigen Klärungsprozessen mit ihrer eigenen Hausbank. So flexibel die Institute sich auch in der raschen Erstattung der verlorenen Beträge zeigen: Es bleibt eine unangenehme Angelegenheit für ihre Kunden.

Hardware-Lösungen mit kurzer „Halbwertzeit"

Welchen Wettbewerbsvorteil hätte wohl ein Kreditinstitut, das von sich behaupten kann, seine Kunden vor solchen Attacken weltweit schützen zu können? Doch der Weg dahin ist noch weit, denn auch in Zukunft wird es kaum gelingen, der Kreativität in kriminellen Kreisen Einhalt zu gebieten.

Die Devise für die Zukunft lautet folglich: Banken und Sparkassen müssen schnell in nachhaltige Lösungen investieren.

Verschiedene Lösungsansätze versprachen in der Vergangenheit mehr Sicherheit. Anti-Skimming-Module, beispielsweise, stellen einen hardwareseitigen Lösungsansatz dar. Allerdings können Banken oder Sparkassen nur ihre eigenen Geräte ausstatten. Hardwareseitige Lösungsansätze weisen zudem leider nur eine begrenzte Lebensdauer auf. Sind Anti-Skimming-Module im Augenblick noch wirksam, stehen sie den Manipulationsideen von morgen schon wieder wehrlos gegenüber. Es gibt zahlreiche weitere Beispiele, Betrug am Geldautomaten durch hardwareseitige Investitionen vorzubeugen. Leider eint diese Lösungsansätze ein entscheidender Nachteil: Die Kunden nutzen auch Geräte anderer Institute und können dort nicht von den Schutzmaßnahmen ihrer eigenen Hausbank profitieren.

EMV und Biometrie: Nur weltweite Umsetzung hilft wirklich

Auch EMV, der in Europa verbreitete chipgestützte Sicherheitsstandard, ist ein sinnvoller Ansatz für einen Ausweg aus dem SB-Sicherheitsproblem. Tatsache ist jedoch, dass nicht alle Karten weltweit mit

Zur Autorin

Cornelia Zwirnmann ist Business Consultant bei der SARROS GmbH, Berlin.

EMV-Chips ausgestattet sind. Zudem findet automatisch ein Fallback auf den Magnetstreifen statt, wenn der EMV-Chip nicht vom Automaten gelesen werden kann. Im Sinne der Interoperabilität der Chiptechnologie ist es erforderlich, dass weltweit alle Institute auf diese Technik umstellen.

Ähnlich verhält es sich mit biometrischen Identifikationsmethoden. Solange Irisscan, Fingerabdruck oder Venenscan sich nicht weltweit durchsetzen oder vom Kunden nicht als Identifikationsmöglichkeit akzeptiert werden, ist die SB-Kriminalitätsrate schwer einzudämmen. Solange nicht alle Länder weltweit den gleichen Standard anbieten, wird der Magnetstreifen als paralleles Identifikationsmedium außerhalb europäischer Landesgrenzen beibehalten werden müssen.

Neue Kartenstrategie als Ausweg?

Deutschlands Kreditinstitute haben die Notwendigkeit erkannt und sich mit neuen Kartenstrategien auseinandergesetzt. So ist beispielsweise, die Abschaffung des Magnetstreifens im Jahre 2011 ein Kernthema der Branche. Wie und in welcher Form Kunden im Ausland, wo der Magnetstreifen als Identifikationsmedium wohl noch Jahre gebraucht wird, zu Bargeld kommen, wird mal mehr, mal weniger kundenfreundlich gelöst werden.

- Die einen Institute wollen ihren Kunden Zweitkarten anbieten, die nur für den Einsatz im Ausland nutzbar sind.

- Die anderen konzentrieren sich eher auf die kundenindizierte Freischaltung der Karte für den Auslandseinsatz.

- Und dann wäre da noch V-Pay. Das Unternehmen Visa verkündet auf seiner Homepage den Rollout seiner Kartenstrategie in Europa. „Kreditinstitute in ganz Europa haben mit der Ausgabe von V-Pay-Karten begonnen und ergänzen ihre nationalen Debitprogramme mit dem V-Pay-Logo. Dadurch leisten sie einen Beitrag zu einem offeneren und einheitlicheren europäischen Kartenmarkt."[1)]

Eine neue Kartenstrategie soll also die Lösung aller Probleme im Bereich SB-Betrug sein? Vielleicht. Vielleicht auch nicht. Denn in Fachkreisen bestehen neben der Zuversicht und Vertrauen die neuen Kartenstrategien betreffend, auch Zweifel ob ihrer nachhaltigen Wirksamkeit. Schlussendlich werden die kriminellen Energien sich mit an Sicherheit grenzender Wahrscheinlichkeit nicht in Luft auflösen, sondern stets nach neuen Wegen suchen. Es ist also fraglich, wie lange SB-Betrug mit Hilfe neuer Technologien tatsächlich Einhalt geboten werden kann.

Softwareseitige Betrugsprävention auf die Agenda heben

Genau darum sollten Banken und Sparkassen strategisch handeln und zusätzlich zu den bestehenden Aufgaben die softwareseitige Betrugsprävention auf die Agenda heben. Der Markt hält geprüfte Lösungen für mehr Sicherheit in der kartengestützten Bargeldbeschaffung und Bezahlvorgängen bereit. Die Berliner Sarros GmbH hat mit witFD ein Werkzeug entwickelt, das nachhaltig Manipulation verhindert. Mit Hilfe dieser Lösung werden sämtliche Transaktionen der institutseigenen Kunden – ob nun an den eigenen oder fremden SB-Geräten – auf Betrugsverdacht überprüft und bewertet. Mittels eines intelligenten Algorithmus werden die gefälschten Transaktionen erkannt. Den Instituten steht es frei, in welcher Weise auf manipulationsverdächtige Transaktionen reagiert werden soll. Die Möglichkeiten reichen von der Abforderung einer zusätzlichen Identifikation bis hin zum Transaktionsabbruch.

Weltweit und unabhängig von der eingesetzten Sicherheitstechnologie der bargeldbereitstellenden Bank oder Sparkasse lassen sich Betrugsversuche eindämmen und das notwendige Vertrauen in die SB-Geräte erhalten.

- Ein Missbrauch muss umgehend von jedem Automaten, unabhängig von Typ, Ort und Zeit, verhindert werden.

- Missbrauchsverdächtige Transaktionen müssen erkannt und verhindert werden (im Laufe des Autorisierungsprozesses).

- Rechtmäßige Transaktionen dürfen nicht abgewiesen werden.

- Fehlidentifikationen müssen auf ein Minimum reduziert werden.

- Innovative Betrugsvarianten müssen so früh wie möglich erkannt und verarbeitet werden.

- Die Prüfung der Transaktionen muss zeitgleich und ohne zusätzlichen Zeitaufwand mit der Authentizitätsprüfung und der Prüfung des Verfügungsrahmens erfolgen.

witFD erfüllt diese Anforderungen. Und die vergleichsweise einfache Integration der Lösung erfordert keine hohen Anfangsinvestitionen in Hardwarekomponenten und wird selbst höchsten Performanceanforderungen gerecht. Grundsätzlich gilt es, den Fokus auf langfristig wirksame Ansätze zu legen. Schließlich befinden sich die Kreditinstitute weltweit in einem technologischen Wettlauf, wie es das Bundeskriminalamt formuliert: „Im Bereich der Zahlungskartenkriminalität bedienen sich die Täter modernster Technik, um die eingebauten Sicherheitsschranken zu umgehen. Infolge der immer kürzer werdenden technologischen Innovationszyklen hat Präventionstechnologie nur noch eine geringe Halbwertzeit. Eine Kopplung unterschiedlicher präventiver Ansätze ist daher notwendig."[2)] Schaffen es die Geldinstitute mit Hilfe innovativer, bestehender Lösungsangebote, diese miteinander intelligent zu kombinieren, ist ein großer Schritt für mehr Sicherheit im SB-Umfeld getan.

Anmerkungen

[1)] http://www.vpay.com/de/main.html.

[2)] http://www.bka.de/pressemitteilungen/2008/pm080328.html.