Kartenmanagement-**Glossar**

ATM Fraud

Von Ewald Judt ▬ 1965 kam es zu einer Erfindung, die unser Leben veränderte: der Geldausgabeautomat. Wurden die Geräte von Banken vorerst nur zögerlich eingesetzt, boomt ihre Aufstellung seit den achtziger Jahren. Heute sind sie durch eine Kooperation der Banken nahezu überall in der Welt zu finden. Die Technik der Geldausgabeautomaten wurde laufend verbessert. Die heutige Generation basiert einerseits weiterhin auf dem Magnetstreifen und andererseits auf dem fälschungssicheren Chip. Ab 2011 wird es in Europa nahezu nur mehr Chiptransaktionen geben. Lediglich in Übersee werden noch Magnetstreifentransaktionen vorkommen.

Da Geldausgabeautomaten von Anfang an als Risikogeräte angesehen wurden, gab es bereits früh Hinweise für Kunden, ihre Karte sicher aufzubewahren, die PIN geheim zu halten und sicher einzugeben und einen Kartenverlust so schnell wie möglich zu melden. Und tatsächlich gibt es seit der Etablierung der Geldausgabeautomaten als Massenauszahlungsmedium laufend Attacken auf ihre Sicherheit. Diese reichen von brutaler Gewalt, einfachen Tricks bis zu Hightech-Angriffen. Brutale Gewalt kommt beim Herausreißen von Geldausgabeautomaten aus ihrer Verankerung, ihrem Abtransport mit nachträglichem Aufbrechen der Geldkassetten sowie der Sprengung von Automaten mit Gas und Mitnahme der Geldkassette vor. Wirksame Mittel dagegen sind das Verschrauben der Geldausgabeautomaten und das Platzieren von Farbpatronen, welche die Banknoten nicht mehr verwertbar machen.

Ein einfacher Trick der Betrüger ist das Blockieren des Geldausgabeschlitzes und nach Weggang des Karteninhabers das Herausholen des Geldes. Dagegen hilft, dass in einem solchen Fall der Geldausgabeautomat außer Betrieb geht. Ein anderer Trick ist das Blockieren des Kartenlesers (mit Herausholen der Karten nach Weggang des Karteninhabers) verbunden mit dem Ausspähen der PIN. Die erfolgreiche Gegenmaßnahme ist in einem solchen Fall die Nichtausgabe der Banknoten und eine vom Karteninhaber zu veranlassende Kartensperre.

Der häufigste Hightech-Angriff ist die Ausspähung der Magnetstreifendaten sowie der PIN, die anschließende Produktion von gefälschten Karten und deren Einsatz dort, wo (noch) Magnetstreifentransaktionen möglich sind. Maßnahmen sind hier sowohl von Seiten der ATM-Betreiber als auch von Seiten der kartenausgebenden Banken möglich und notwendig.

Gegen die Ausspähung der Magnetstreifendaten hilft der Schutz des Kartenlesers vor dem Anbringen eines Magnetstreifenlesegerätes. Entsprechende Devices sind verfügbar, wobei deren Entfernung das Außerbetriebnehmen des Geldausgabeautomaten zur Folge haben sollte. Auch eine Zitterfunktion behindert das Auslesen der Magnetstreifendaten. Der Schutz vor dem Anbringen eines zweiten PIN-Pads, das über dem PIN-Pad angebracht wird, ist zum Beispiel durch das unregelmäßige Anbringen von unregelmäßigen Halbkugeln möglich. Desgleichen kann durch die Ausstattung des Geldausgabeautomaten/des Umfelds mit einer Kamera eine Attacke frühzeitig erkannt und besser aufgeklärt werden.

Gegen den Einsatz gefälschter Karten hilft (bei deutschen Karten) das MM-Merkmal bei allen (deutschen) Geldausgabeautomaten mit einer MM-Box – nicht jedoch im Ausland. In Österreich, Frankreich und Spanien geht man mit einem Randomnummern-System gegen den Einsatz gefälschter Karten vor. Dieses wirkt auch beim Karteneinsatz im Ausland, sofern die jeweilige echte Karte zwischenzeitlich im Inland eingesetzt wurde.

Sicherheitsschwachstelle USA

Gegen den Einsatz gefälschter Karten auf Magnetstreifenbasis helfen nur Chiptransaktionen. Wenngleich dies in Europa in Bälde realisiert sein wird und auch in einigen anderen Ländern/Regionen der Umstieg auf den Chip forciert wird, bleibt insbesondere mit den USA eine große Sicherheitsschwachstelle. Allerdings ist durch die Reduktion der Länder, in denen es (noch) Magnetstreifentransaktionen gibt, ein einfacheres Monitoring der Kartentransaktionen und ein besseres Reagieren bei Fälschungsverdacht möglich. Bis zum weltweiten Chip-only-Einsatz kann die Problemlösung nur darin bestehen, dass ATM-Betreiber ihr System State-of-the-art konfigurieren und ausgebende Banken ihre Karten bestmöglich schützen sowie ihr Karteneinsatzmonitoring optimieren.

Unabhängig von der bisher bekannten ATM-Kriminalität kann man davon ausgehen, dass es künftig aufgrund der kriminellen Energie weitere Attacken auf Geldausgabeautomaten geben wird – mit Methoden, die wir noch nicht kennen. Daher wird es zweckmäßig sein, derartige Angriffe frühzeitig zu erkennen und dagegen Maßnahmen zu setzen, wozu allerdings mehr internationale Kooperation notwendig ist.

Dr. Ewald Judt ist Honorarprofessor der Wirtschaftsuniversität Wien und Geschäftsführer der PayLife Bank GmbH; ewald.judt@paylife.at/www.paylife.at. ▬