Bankomatenbetrug: Anti-Skimming-Modul in Rekordzeit entwickelt

Skimming steht für das illegale Ausspähen der Geheimdaten von Bank- oder Kreditkarten, indem diese von Magnetstreifen abgelesen und auf gefälschte Karten kopiert werden. Um die Skimming-Welle vom letzten Jahr einzudämmen, haben Swisscom IT Service Finance und Ergon für ihre Kunden rasch wirksame Gegenmassnahmen entwickelt: Teilsperren ermöglichen den Karteninhabern, bei aussereuropäischen Reisen nicht vollständig auf den Bargeldbezug von Automaten verzichten zu müssen.

Die Raiffeisenbank betreibt mit 1 500 Geräten die meisten Bankomaten in der Schweiz. Das drittgrösste helvetische Geldinstitut hat über 880 000 Kartenkunden. 2009 führten Swisscom IT Services Finance und Ergon für Raiffeisen einen modernen Bankomaten-Transaktionsserver ein. Gleiche Systeme waren bereits früher an mehrere Kantonalbanken ausgeliefert worden. Sie basieren alle auf dem von Ergon im Auftrag von Swisscom IT Services Finance entwickelten Card-X-Transaktionsserver. Dieser wurde an die Raiffeisen-spezifischen Anforderungen angepasst.

Bei der Entwicklung des Card-X-Transakationsservers hatten die Ausbaufähigkeit, Ausfallsicherheit und Performance höchste Priorität. Der Server ist in der Lage, sämtliche Kartentransaktionen zu autorisieren. Dies umfasst sowohl das Beziehen und Einzahlen von Geld an den hauseigenen Automaten als auch Bezüge an bankfremden Automaten und Terminals weltweit wie das Bezahlen mit Maestro-Karte in einem Geschäft.

Sprunghafter Anstieg der Schadensfälle

Schneller als es den Entwicklern und Bankern lieb war, wurde die flexible Erweiterbarkeit der Systeme wegen steigender Skimming-Attacken auf die Probe gestellt. War im Ausland das Skimming schon seit mehreren Jahren ein grosses Problem, blieb die Schweiz davon lange weitgehend verschont. 2011 stieg die Zahl der registrierten Fälle jedoch sprunghaft an. Allein in den ersten vier Monaten des Jahres waren 225 manipulierte Schweizer Geldautomaten, SBB-Billettautomaten und Zahlungsgeräte in Geschäften registriert worden.

Bei dieser Art Betrug mit Kredit- und Debitkarten kopieren Kriminelle mit speziellen Vorrichtungen den Magnetstreifen der Zahlungskarte. Die Eingabe der PIN wird mit einer kleinen Funkkamera gefilmt, die oberhalb der Tastatur in einer angeklebten Kunststoffleiste versteckt ist. Sind die Magnetstreifen kopiert, werden die gewonnenen Daten an Komplizen weitergesendet, die daraus Kartenkopien erstellen. Mit den gefälschten Karten und der ausspionierten PIN kann so Geld bezogen werden. Die Schäden sind beträchtlich.

Erste Hardware-Gegenmassnahmen greifen: Schutzeinrichtungen für die Tastaturen der Automaten etwa verhindern das Anbringen der Kopieraufsätze. Der Einsatz von EMV-Chips – das Akronym steht für Euro Pay International, Master und Visa – anstelle der Magnetstreifen in europäischen Karten und Bankomaten verhindert die Anwendung der illegalen Kartenkopien erfolgreich. Deshalb werden die Kopien von den Betrügern heute in den USA, Kanada, Südafrika und südamerikanischen Ländern verwendet, dort also, wo die Bankomaten die Daten weiterhin von Magnetstreifen lesen.

Cleveres Limitenmodell

Da galt es, wirksamen Schutz über die Autorisierung zu schaffen. Bis vor kurzem waren die persönlichen Bezugslimiten jedes Karteninhabers unabhängig vom Bezugsort definiert. So konnte man die Limiten zum Beispiel auf maximal 3 000 Schweizer Franken täglich und 5 000 Schweizer Franken pro Monat festlegen. Um den Bezug mit kopierten Karten an Automaten mit Magnetstreifen zu beschränken, erweiterten die Ergon-Ingenieure in Zusammenarbeit mit Swisscom IT Services Finance den Transaktionsserver um ein Geo-Blocking-Modul. Das Kartenlimitenmodell wurde im Dialog zwischen den Entwicklern und den Banken dahingehend erweitert, dass neu länderspezifische Tages- und Monatslimiten definiert werden können. In den Ländern, wo Karten noch mit der Magnetspur authentifiziert werden, reduziert die Bank die Limiten beispielsweise auf maximal 500 Schweizer Franken pro Tag oder 1 000 Schweizer Franken pro Monat. Wie Ergon-Projektleiter Peter Krucker berichtet, werde dadurch der mögliche Schaden markant und wirksam vermindert. Dank der flexiblen Anpassungsmöglichkeiten der Transaktionsserver konnten die Module innert zwei Monaten entwickelt und eingeführt werden. Demgegenüber benötigten andere Hersteller für ihre Lösungen bis zu neun Monate an Entwicklungszeit. Während diese erst noch mit einer Totalsperre bei Anfragen aus dem aussereuropäischen Ausland reagieren, können Kunden der Banken mit dem Card-X-Transaktionsserver wenigstens beschränkt Geld beziehen. Wer mehr Geld benötigt, kann sich vor Reiseantritt bei der Bank anmelden und seine Limiten erhöhen. So konnte eine optimale Kombination von Sicherheit und Kundennutzen erreicht werden.

Foto: CineLandia: djpas/photocase.com