

Tankstelle statt Geldautomat

Für Betrüger wird es immer schwieriger, EC-Kartendaten abzugreifen. Kein Wunder, dass viele Ban

Von Andreas Jalsovec

München – Es war eine böse Überraschung für die Autofahrer: Mit ihrer EC-Karte hatten sie den Sprit an einem Tankautomaten bezahlt. Kurz darauf wurde Geld von ihrem Konto abgebucht. Betrüger hatten die Selbstbedienungs-Zapfsäule manipuliert, Kontodaten und Geheimzahl bei der Eingabe abgegriffen und mit kopierten Karten im Ausland Geld abgehoben. Betroffen waren nur zwei Tankautomaten – doch die Schadenssumme sei beträchtlich gewesen, heißt es bei Euro Kartensysteme, dem Unternehmen, das für die Kreditwirtschaft solche Betrugsfälle registriert.

Die Masche am Tankautomaten ist einer der neuesten Versuche von Betrügern, an die Bankdaten argloser Nutzer zu kommen und damit deren Girokonto zu plündern. Schon fast ein verzweifelter Versuch: Denn beim Hauptzielobjekt der Datendiebe, den Geldautomaten der Banken, tun sich die organisierten Banden immer schwerer, mit ihren Manipulationen erfolgreich zu sein. Das zeigen die neuesten Zahlen von Euro Kartensysteme zu den Betrugsfällen an Bankautomaten, die der SZ vorliegen.

„Der Schaden durch solche Manipulationen hat sich in den ersten drei Quartalen 2011 halbiert“, berichtet Margit Schneider, die das Sicherheitsmanagement für Zahlungskarten bei Euro Kartensysteme leitet. Auch die Zahl der Angriffe auf Automaten ging deutlich zurück: So versuchten Betrüger in den ersten neun Monaten 2010 noch fast 1500 Mal, Bankautomaten zu präparieren, um dort EC-Kartendaten zu erspähen. Im selben Zeitraum 2011 waren es keine 700 Fälle mehr (Graphik).

Für den deutlichen Rückgang gibt es nach Schneiders Angaben mehrere Gründe. Zum einen hätten viele Banken ihre Geldautomaten mit Störsendern ausgestattet. Sie verhindern das „Skimming“ – das Ablesen der Kartendaten vom Magnetstreifen. Zum anderen hätten die Geldhäuser die Bedienung der Türöffner an den Filialen mit der EC-Karte abgeschaltet oder so geändert, dass die Karte nur noch halb eingesteckt werden muss. Die Daten lassen sich dann dort nicht mehr lesen.

Der wichtigste Grund für den „durchschlagenden Erfolg“ bei der Betrugsbekämpfung, so Schneider, sei jedoch die europaweite Einführung des sogenannten EMV-Chips. Er befindet sich mittlerweile auf jeder EC-Karte. Zieht man am Automaten Geld, dann werden die Daten nur noch vom Chip mit der speziellen Si-

cherheitstechnik gelesen und nicht mehr vom Magnetstreifen. Das macht es für die Betrüger deutlich schwerer, an das Geld ihrer Opfer zu kommen.

Zwar haben die meisten Karten auch noch Magnetstreifen. Von diesen lassen sich nach wie vor Daten lesen und Kartenkopien mit identischen Streifen herstellen. Damit an anderen Automaten Barres abzuheben, ist aber innerhalb Europas kaum mehr möglich. „Die EMV-Technik erschwert es den Betrügern erheb-

lich, gestohlene Kontodaten überhaupt zu nutzen“, sagt Schneider.

Die Diebe weichen deshalb in immer entferntere Länder aus, um an das Geld zu kommen. Noch vor drei Jahren wurde mit gestohlenen Kartendaten vor allem in Italien, Niederlande und Rumänien Geld gezogen. Heute liegen die USA, Russland und Kolumbien vorn. So wird in den Vereinigten Staaten gut jede fünfte kopierte Karte eingesetzt, um illegal Geld von deutschen Konten abzuheben

(Graphik). In den meisten Geldautomaten sind die Mastercard umstellen, 2015 v
„So lange es M sen die Kunden rechnen“, warnt nicht nur am F Tankstellen mit auch Fahrkarten Ziel der Betrüger.

Daten-Attacken

Ein neuer Sicherheits-Chip auf EC-Karten hat die Zahl der Angriffe auf Geldautomaten in Deutschland deutlich sinken lassen (links). Die deutschen Datendiebe müssen außerdem immer weiter reisen, um mit den kopierten Daten das Geld im Ausland abzuheben.

Manipulationen an Bankautomaten

— 2010 (Jan. bis Sept. insgesamt 1469)
— 2011 (Jan. bis Sept. insgesamt 687)



Wo kopierte Karten eingesetzt werden

Angaben in Prozent des Gesamtschadens



SZ-Graphik; Quelle: Euro-Kartensystem GmbH; Foto: dpa