

Die Diebe werden immer dreister

Kreditkartenbetrüger gehen mit dem technologischen Fortschritt

Betrugsfälle an Kreditkartenautomaten nehmen zwar tendenziell ab, doch die Täter werden immer raffinierter, um an Kundengelder zu kommen.

MARIE-CLAIRE JUR

Skimming ist kein neues Phänomen. Schon 2004 betrug der Schaden, verursacht durch diese Art von Kreditkartenbetrug und -fälschung, insgesamt 21 Mio. Franken. Schweizweit und bezogen auf die Mastercard. Mittels Schutzmassnahmen und Aufklärungskampagnen konnte diese Kriminalitätsform etwas in die Schranken gewiesen werden, doch Theodor Wasescha, Chef Fachstelle Prävention der Kantonspolizei Graubünden, schätzt das aktuelle Schadensvolumen mit 15 Mio. Franken nach wie vor als recht hoch ein. Weshalb er nach wie vor auf die Information der Bevölkerung setzt.

Vorsicht bei allen Kartenterminals

Der Begriff «Skimming», der sich vom Englischen «to skim» ableitet, was so viel wie abheben oder abschöpfen heisst, bezeichnet das Manipulieren von Kartenautomaten. Während lange Zeit vor allem die so genannten Bankautomaten für den Bargeldbezug betroffen waren, haben die Betrüger mittlerweile auch Billettautomaten und Zahlterminals im Detailhandel für ihre kriminellen Machenschaften entdeckt. Unlängst berichteten Medien von diversen Betrugsfällen an Tankstellenautomaten, Ticketautomaten der SBB oder in Grossverteilern. Um Bankkonten plündern zu können, versuchen die Täter, die Magnetstreifen-

daten der Konto-, Debit- oder Kreditkarten zu kopieren und den PIN-Code auszuspähen.

Wie raffiniert diese Betrüger mittlerweile dabei vorgehen, demonstrierte die Kantonspolizei kürzlich an der EBexpo in Scuol. Die Täter setzen für ihre Attacken präparierte Attrappen ein, Aufsätze, die mittlerweile für wenig Geld erworben werden können und die sie auf Karten-Schlitz aufsetzen oder auf das Zahlenfeld.

Winzige Video-Kameras

Eingesetzt werden auch Video-Kameras, dank denen die Bewegungen der Kunden bei der PIN-Code-Eingabe registriert werden können. Diese Kameras sind winzig (Objektiv kleiner als ein Stecknadelkopf), werden oftmals hinter einer Attrappe im oberen Bankomatenbereich angebracht und sind imstande, alle Bewegungen im Bedienungsbereich von Bankomaten zu registrieren und auf einen Computer-Terminal zu übertragen. Dank mittlerweile fälschungssicheren Chips ist es in der Schweiz nicht möglich, mit der Maestro-Karte und Post Finance Card Direct Bargeld an Bankomaten zu beziehen. Aus diesem Grund heben die Skimming-Täter das Geld immer im Ausland ab, vor allem in aussereuropäischen Ländern, in denen dies mit den ergatterten Magnetstreifen- und den PIN-Codes noch möglich ist.

Geschützte PIN-Code-Eingabe

Wie kann man sich vor dieser Form von Kriminalität schützen? Die meisten wissen, dass sie das Nummernfeld bei der Code-Eingabe mit der Hand schützen sollen. «Doch viele tun das nicht

gut genug», betont Wasescha. Wichtig ist es, die Tasten möglichst vollständig, mit beiden Händen abzudecken. Da die Nummernfelder blindengerecht konzipiert sind, also das Nummernfeld in der Mitte (die Zahl 5) in der Regel mit einer von der Fingerkuppe erfühlbaren Struktur versehen ist, ist der Kartenautomat-Kunde in der Lage, seinen PIN-Code einzugeben, ohne die Hände zu heben – und somit etwaige Video-Kameras auszutricksen. Der Schutz vor Betrugerei fängt aber schon vor dem Zücken der Bankkarte an: «Tasten Sie mit der Hand über die verschiedenen Einheiten des Automaten», rät Wasescha. Damit meint er das Nummernfeld, den Kartenschlitz oder auch die Leiste oberhalb des Bedienungsfeldes. Dabei solle man nicht unzimperlich vorgehen, könne ruhig auch mal ziehen und rütteln, um missbräuchlich angebrachte Aufsätze zu entdecken.

Engadin nicht speziell betroffen

Gemäss einer Erhebung der Firma SIX sind die Skimming-Fälle rückläufig. In der Schweiz wurden 2012 369 Vorkommnisse registriert (gegenüber 586 im Vorjahr). Bezogen auf die Graubündner Kantonalbank spricht ihr Sprecher Thomas Müller derzeit lediglich von «Einzelfällen». Zurzeit seien auch keine «Hot Spots», auch nicht im Engadin, feststellbar. «Im Februar 2012 haben wir als eine der ersten Banken eine geografische Einschränkung, das Geoblocking, eingeführt für unsere Maestro-Kunden.»

www.stop-skimming.ch

Fünf goldene Regeln

- 1) Attrappen-Check
- 2) Keine Nähe von fremden Personen bei der Bedienung des Nummernfelds
- 3) PIN-Code verdeckt eingeben
- 4) Jeglichen Verdacht melden
- 5) Kontobewegungen kontrollieren



Theodor Wasescha demonstriert den Einsatz von Bancomat-Attrappen.

Foto: Marie-Claire Jur