Vorsicht beim Zahlen mit Karte

Ärgerlicher Datendiebstahl durch Skimming an Automaten – Polizei warnt vor Phishing

Betrüger versuchen mit grossem Einfallsreichtum, an die Daten von Bankkarteninhabern zu kommen. Jüngst haben sie ihre Bemühungen intensiviert und auf «neue» Bereiche ausgedehnt.

Werner Grundlehner

Zahlreiche Schweizer haben in den vergangenen Tagen eine unangenehme Begegnung mit einem Bancomaten erlebt. Der Automat zog ihre Karte ein – ohne dass die Kunden mehrmals eine falsche PIN eingegeben oder zu wenig Guthaben auf dem Bankkonto gehabt hätten. Vielmehr war das Einbehalten der Karten eine Sicherheitsmassnahme der Banken, denn in den letzten Tagen sind einzelne der 30 Billettautomaten im Bahnhof Zürich von Betrügern manipuliert worden – teilweise mehrmals hintereinander. Dies sei geschehen, obwohl die Automaten regelmässig kontrolliert würden, hält eine SBB-Sprecherin fest.

In Sekunden manipuliert

Das Vergehen wird Skimming (Abschöpfen) genannt. Mithilfe einer technischen Veränderung gelangen Betrüger in den Besitz von Kontodaten und PIN-Code. Meist wird ein täuschend echter Karteneinzug über das Original gesteckt und eine Kamera installiert, die die Eingabe des Codes aufzeichnet. Mit den Daten versuchen die Betrüger, die Konten der Betroffenen zu plündern. Eine derartige technische Veränderung hätten Profis in wenigen Augenblicken unbemerkt am Automaten angebracht, sagt ein Polizeisprecher. Dafür postierten sie einige Helfer als Sichtschutz um sich herum. Das falle an einem sehr stark frequentierten Ort wie dem Bahnhof kaum auf.

Manipulierte Automaten erfassen die Daten aller benutzten Karten – seien das Maestro-, Post- oder American-Express-Karten. Die Banken analysieren deshalb, nachdem sie von den SBB Kenntnis von der Manipulation erhalten haben, die Daten aus den betroffenen Automaten und ziehen alle Karten ein, die im fraglichen Zeitraum am Billettautomaten zur Zahlung eingesetzt wurden. Gleichzeitig wird den Kunden eine neue Karte zugeschickt.

Hat sich der Anwender korrekt verhalten, übernehmen die Banken einen allfälligen Schaden durch nicht autorisierte Bezüge. Die Institute sind daran interessiert, dass der Zahlungsverkehr mittels Karte weiter an Gewicht gewinnt. Zudem müsse man die Relation sehen, sagt ein Banksprecher. Vom gesamten Volumen im Kartengeschäft machten Betrugsfälle einen sehr kleinen Anteil aus. Korrekt verhält man sich, wenn man die allgemeinen Geschäftsbedingungen einhält, den PIN-Code verdeckt eingibt sowie Code und Karte getrennt aufbewahrt.

Die Banken offerieren zudem weitere Hilfsmittel, um Datendiebstähle zu verhindern oder einzuschränken. So bietet die UBS einen Service an, mit dem der Kunde nach jeder Zahlung per Karte ein SMS erhält. Eine weitere Vorsichtsmassnahme ist das Geo-Blocking: Der Kunde entscheidet damit, wo die Karte überhaupt eingesetzt werden darf. So können etwa die Kunden der UBS wählen, ob ihre Karte in der Schweiz und im Fürstentum Liechtenstein, in Europa oder global eingesetzt werden darf. In Vorbereitung ist eine Dienstleistung, mit welcher der Kunde via E-Banking selbst festlegt, in welchen Ländern seine Karte nutzbar sein soll.

Eine Technik von gestern

Skimming liesse sich einfach eindämmen. In den meisten westlichen Ländern werden von den Automaten die Daten, die im Chip auf der Vorderseite der Karte gespeichert sind, verwendet. Die Daten des Chips lassen sich nicht kopieren. Die Informationen auf dem Magnetstreifen werden nur noch für Anwendungen in Schwellenländern und den USA verwendet. Das ist auch der Grund, weshalb die Bezüge mit den gestohlenen Daten jeweils nicht in Europa getätigt werden.

Die Skimming-Versuche mögen – besonders in der Wahrnehmung der Konsumenten – zunehmen, die Erfolgsquote dieser Betrügereien nimmt laut Polizei jedoch ab. Mehr Sorgen bereitet mittlerweile das Phishing. Hier werden Kunden per gefälschter E-Mail aufgefordert, Kontodaten ihrer Hausbank zu bestätigen – beispielsweise, weil die Bezahlung für ein Online-Auktionshaus schiefgelaufen sei. Neuerdings versuchen die Betrüger auch mittels «Voice Phishing» in den Besitz der kostbaren Daten zu kommen. Ein Betrüger, der vorgibt, ein Bankangestellter zu sein, versucht dabei, direkt über das Telefon die Daten zu erschleichen.