Trügerische Sicherheit bei Kreditkarten

Beim Einkauf gibt es verschiedene Möglichkeiten der Bezahlung. Einige zahlen gern bar, andere mit der Bank- oder Kreditkarte. Die Kreditkarte kann durchaus Vorteile haben. Zum Beispiel erfolgt die Belastung des Kontos nicht sofort, sondern in der Regel einmal im Monat durch Aufsummierung aller angefallenen Ausgaben, die mit der Kreditkarte beglichen wurden. Durch diese einmalige Abbuchung fällt eine möglicherweise zu zahlende Buchungsgebühr nur einmal und nicht mehrfach an.

Kreditkarten erleichtern das Bezahlen,
sind aber auch nicht selten ein Sicherheitsrisiko.

Kreditkarten können aber auch ein Risiko sein. Wer beispielsweise eine Kreditkarte wie Visa- oder MasterCard besitzt, ist oft ein interessantes Ziel für Betrüger. Diese setzen unterschiedliche Tricks ein, um an die persönlichen Daten der Kreditkarteninhaber zu kommen. Beliebt sind sogenannte Phishing-E-Mails. Dabei wird der Eindruck erweckt, dass die E-Mail vom echten Anbieter der Karte kommt. Tatsächlich wurde die E-Mail aber von den Betrügern verfasst. Der Kunde wird aufgefordert, sich auf der Internetseite der Bank einzuloggen. Der erforderliche Link wird gleich mitgeliefert. Dieser Link führt aber gar nicht zum Onlineauftritt des Anbieters, sondern auf die Internetseite der Betrüger. Diese sieht der Original-Seite zum Verwechseln ähnlich. Gibt der Kunde dort seine sensiblen Daten ein, besitzen die Betrüger die erforderlichen Informationen, um ihm sein Geld zu stehlen. Solche Phishing-E-Mails können auch schädliche Software enthalten, die sich auf den Rechner zu installieren versucht. Derartige Mails werden dem Phishing-Radar der Verbraucherzentrale NRW seit vielen Monaten regelmäßig gemeldet.

Besitzern einer Visa- oder MasterCard droht aber auch von einer anderen Seite Gefahr – paradoxerweise ausgerechnet von den Kreditkartenunternehmen, weil diese die Zahlung mit der Kreditkarte im Onlinehandel sicherer machen wollen. Visa- und MasterCard haben ein sog. 3D-Sicherheitsverfahren entwickelt. Dieses Verfahren, bei Visa „Veryfied by Visa“ und bei MasterCard „MasterCard securecode“ genannt, sieht vor, dass Kunden beim Kauf im Internet eine ihnen zugewiesene persönliche Geheimzahl angeben, um sich gegenüber dem Kreditkartenunternehmen zu autorisieren.

Was auf den ersten Blick vorteilhaft zu sein scheint, birgt für den Kunden jedoch erhebliche Risiken. Betrügern eröffnen sich mit dem neuen System weitere Möglichkeiten, was neue Missbrauchsfälle leider bestätigen:

- So gelang es unbefugten Dritten, allein aufgrund ihrer Kenntnis der Kartennummer und der Person des Karteninhabers einen solchen Code im Internet zu beantragen und auf Kosten des unwissenden Kar-

Auch immer mehr ältere Menschen nutzen das bequeme Onlinebanking.

teninhabers einzukaufen. Beide benötigten Informationen stehen auf der Kreditkarte, sodass Kriminelle nur diese – beispielsweise durch Diebstahl – in ihren Besitz bringen müssen.

- Es ist auch vorgekommen, dass der Sicherheitscode abgefangen wurde, um im Namen und auf Rechnung des Karteninhabers im Internet einzukaufen.

Bisher bestand für Kreditkarteninhaber bei einem Missbrauchsfall im Onlinebanking nicht die Gefahr, auf dem Schaden sitzen zu bleiben. Schließlich gilt beim Einkauf mit Kreditkarten folgende Vorgehensweise: Sie unterschreiben einen Beleg und autorisieren so die Zahlung. Beim Onlinekauf kann Ihnen deshalb in diesem Fall nichts passieren. Sie haben schließlich keinen Beleg unterschrieben, daher können Sie solche Falschbuchungen ohne Probleme korrigieren lassen. In solchen Fällen entsteht Ihnen also kein finanzieller Schaden. Zumindest galt das bisher – vor der Umstellung auf „Veryfied by Visa“ und „MasterCard securecode“.

Inzwischen ist es leider möglich, dass die kartenausgebenden Institute Missbrauchsfälle auf den Kunden abwälzen. Grundsätzlich haften Kunden für eingetretene Schäden nur dann in vollem Umfang, wenn sie grob fahrlässig gehandelt haben, d.h. ihre Sorgfaltspflicht in besonders verwerflicher Weise verletzt haben. Im Normalfall muss ein solch schweres Fehlverhalten nachgewiesen werden. In einigen Fällen wird aber ein solcher Pflichtverstoß des Kunden aufgrund der tatsächlichen Umstände vermutet (sogenannter Anscheinsbeweis). Der Kunde ist nun in der Pflicht, diese Vermutung zu widerlegen, was im Einzelfall sehr schwierig sein kann. Gelingt das nicht, bleibt er womöglich ganz oder teilweise auf dem Schaden sitzen.

Genau diese Gefahr besteht nun auch bei den neuen Sicherheitsverfahren. Allerdings erklärten die beiden Unternehmen Visa und MasterCard sowie die kartenausgebenden Banken nach einer Warnung der Stiftung Warentest, dass der für den Kunden nachteilige Anscheinsbeweis in dieser Fallkonstellation nicht gelte und die Karteninhaber im Missbrauchsfall entschädigt werden.

Dennoch ist Vorsicht geboten: So weigerte sich die Advanzia Bank im Fall einer jungen Lehrerin, deren Daten missbraucht wurden, den Schaden zu ersetzen. Die Bank ging wegen der Eingabe der richtigen Geheimzahl durch die Betrüger einfach davon aus, dass die Kundin ihre Sorgfaltspflicht in grober Weise verletzt habe.

Kunden haben also nicht mehr wie früher das Recht auf ihrer Seite, sondern sind im Zweifel auf die Kulanz des Anbieters angewiesen. Die Verbraucherzentrale NRW rät den Verbrauchern daher zunächst, auf den Einsatz des Sicherheitscodes zu verzichten, bis sämtliche Zweifel an der Sicherheit des Systems und der Haftungsfrage ausgeräumt sind.

Ferner bittet die Verbraucherzentrale NRW die Verbraucher, auch weiterhin betrügerische E-Mails dem Phishing-Radar zu melden. Sie können diese Mails an phishing@vz-nrw.de weiterleiten. Verbraucher können sich auf www.verbraucherfinanzwissen.de auch über die neuesten Phishing-Attacken informieren. ■

Dr. Ralf Scherfling

Zur Person

Der Bankkaufmann und Diplom-Ökonom **Ralf Scherfling** ist als Finanzexperte im Projekt „verbraucherfinanzwissen.de“ der Verbraucherzentrale NRW tätig.

Kontakt:
Verbraucherzentrale NRW
Mintropstr. 27
40215 Düsseldorf
ralf.scherfling@vz-nrw.de