

Betrügerisch erschlichene Kreditkartenzahlung

Thema: **Missbrauch und Betrug** Fallnummer: **2020/10**

Die Kundin erhielt ein E-Mail, welches angeblich von der Post stammte. Darin wurde sie aufgefordert, für die Lieferung eines Pakets 2.99 CHF zu bezahlen und dafür einen Link anzuwählen. Da sie ein Zalando-Paket erwartete, folgte sie den Anweisungen. Darauf erschien eine Website, welche sie für diejenige der Post hielt, auf welcher sie ihre Kreditkartendaten eingab. Sie erhielt darauf ein SMS der Kreditkartenherausgeberin mit einem Code, welchen sie auf der Website ebenfalls eingab. Kurz darauf bestätigte ihr die Kreditkartenherausgeberin eine Zahlung von 1500 CHF. Sie nahm sofort mit der Kreditkartenherausgeberin Kontakt auf, welche den Vorfall abklärte. Nachdem sich diese weigerte, die Kundin zu entschädigen, unterbreitete letztere den Fall dem Ombudsman. Im Rahmen des Ombudsverfahrens erklärte sich die Kreditkartenherausgeberin bereit, die Kundin mit 800 CHF zu entschädigen. Diese nahm das Vergleichsangebot an.

Das Betrugsschema, welches vornehmlich auf Kunden der Post und von Kurierdiensten zielt, ist leider bekannt. Unter dem Vorwand, dass sie für ein Paket einen kleinen Betrag nachzahlen müssen, werden die Kunden per SMS oder per E-Mail auf eine gefälschte Website gelockt, wo sie für die vermeintliche Zahlung ihre Kreditkartendaten eingeben. Eine solche Betrugsmethode nennt man «Phishing». Tatsächlich lösen die Betrüger mit den gestohlenen Daten dann eine viel grössere Zahlung aus. Im konkreten Fall wurde mit der Belastung der Kreditkarte der Kundin die Rechnung eines ausländischen Reisebüros über 1500 CHF beglichen. Obschon der Betrug von der Kundin sofort entdeckt und gemeldet wurde, da sie eine Funktion der Kreditkartenherausgeberin nutzte, mit welcher ihr die Kartenbelastungen jeweils unverzüglich per SMS gemeldet werden, sah sich die Kreditkartenherausgeberin ausserstande, die Vollendung der von den Betrügern mit den Daten der Kundin veranlassten Transaktion zu verhindern. Dies aufgrund einer Regelung des massgebenden Kreditkartennetzwerks, wonach eine Rückbelastung einer solchen Transaktion im sogenannten Chargeback-Verfahren dann nicht möglich ist, wenn der Karteninhaber diese im Rahmen einer 2-Faktoren-Authentifizierung autorisiert hat.

Bei einer 2-Faktoren-Authentifizierung muss ein Karteninhaber eine online erfolgte Kreditkartentransaktion auf einer App oder mit einem per SMS auf eine von ihm vorgängig bei der Kartenherausgeberin registrierte Telefonnummer versandten Code zusätzlich bestätigen. Bei gewissen Authentifizierungssystemen wird nicht nur die Telefonnummer, sondern auch das damit verbundene Gerät vorgängig registriert. Nutzt ein Händler, welcher Kreditkarten akzeptiert, ein solches System, muss er sich keine Rückbelastung gefallen lassen und kann sicher sein, dass er das der Kreditkarte belastete Geld behalten darf.

Die auf den Fall anwendbaren Kreditkartenbedingungen sahen vor, dass die Kreditkartenherausgeberin Schäden für die missbräuchliche Verwendung der Kreditkarte dann übernimmt, wenn der Kunde sämtliche ihm obliegenden Pflichten aus den Kreditkartenbedingungen, namentlich die Sorgfaltspflichten, eingehalten hat und ihn auch sonst kein Verschulden trifft. Die Kreditkartenherausgeberin argumentierte, die Kundin habe vorliegend eine zentrale Sorgfaltspflicht verletzt, indem sie die Kartendaten und den Bestätigungscode auf der Phishing Website, welche sie für die echte Website der Post gehalten hatte, den Betrügern und damit unbekanntem Dritten bekannt gegeben hatte.

Auf den Einwand des Ombudsmann, dass die Kundin damit lediglich die für eine Bezahlung notwendigen Angaben gemacht und die Phishing Website nicht als solche erkannt hatte, entgegnete die Kreditkartenherausgeberin, ihrer Meinung nach stelle es grundsätzlich eine Sorgfaltspflichtverletzung dar, wenn ein Kunde auf eine solche Phishing Website hereinfalle. Es sei heute allgemein bekannt, dass man Links von unbekanntem Absendern nicht anklicken solle. Aufgrund der Absenderadresse des E-Mails sei klar gewesen, dass dieses nicht von der Post stamme. Zudem hätte man durch Anklicken der Adresse der Website erkennen können, dass diese nur vordergründig von der Post stamme. Im Hintergrund wäre die tatsächliche Adresse der Phishing Website erkennbar gewesen. Schliesslich sei es ungewöhnlich, dass im Zusammenhang mit der Lieferung eines Pakets ein derart ungerader Betrag eingefordert werde und die Kundin habe den ihr per SMS zugestellten Bestätigungscode verwendet. Dieser lautete wie folgt: «Ihr Code für die Zahlung lautet: XXX». Zudem wurde auf eine App verwiesen, mit welcher eine solche Bestätigung noch einfacher hätte erfolgen können. Der Betrag der Zahlung und der Dienstleister waren aus der SMS nicht ersichtlich. Die Kreditkartenherausgeberin erklärte, dass dies dem damaligen Stand entsprochen habe und in der Zwischenzeit dahingehend geändert worden sei, dass der Betrag und der Dienstleister zusammen mit dem verlangten Code immer ersichtlich seien.

Der Ombudsmann bat die Kreditkartenherausgeberin, ihre Haltung zu überdenken. Sie setzte seines Erachtens bei den Kunden ein technisches Verständnis voraus, welches im breiten Publikum nach Ansicht des Ombudsmann wohl kaum so vorhanden ist. Zudem hatte die Tatsache, dass der Bestätigungscode ohne Angaben zur Höhe der Zahlung und des Dienstleisters versandt worden war, nicht unwesentlich dazu beigetragen, dass der Betrug erfolgreich war. Die Kreditkartenherausgeberin zeigte sich schliesslich bereit, der Kundin 800 CHF und damit etwas mehr als 50 % des Schadens zu erstatten, was diese akzeptierte.