Schadenersatzforderung wegen einer Zahlung, welche von Unbekannten per E-Banking ausgelöst wurde

Thema: **Missbrauch und Betrug** Fallnummer: **2020/14**

> Im vorliegenden Fall wurde wiederum ein Kunde mittels eines Phishing-Angriffs geschädigt. Er wollte sich an einem Sonntag in das E-Banking seiner Bank einloggen, um den Saldo des Sparkontos seiner Ehefrau abzufragen. Das Einloggen gelang nicht. Er erhielt darauf ein SMS, welches den Betrag von 3000 CHF enthielt. Der Kunde nahm fälschlicherweise an, es handle sich um den Saldo des Kontos. Am Montagmorgen früh konnte er sich wieder problemlos in das E-Banking einloggen und entdeckte eine unautorisierte Überweisung über 3000 CHF. Er nahm sofort mit der Bank Kontakt auf und meldete den Vorfall. Diese kontaktierte die Bank, welche das Konto der Zahlungsempfängerin führte, erst um 16.30 Uhr per SWIFT und verlangte die Rücküberweisung. Es gelang nicht mehr, den Betrag sicherzustellen. Der Kunde machte in der Folge namens seiner Ehefrau einen Schadenersatzanspruch gegen seine Bank geltend. Nachdem er keine Einigung finden konnte, kontaktierte er den Ombudsman. Auch im Ombudsverfahren verweigerte die Bank ein Entgegenkommen.

Die Bank verwendete für ihr E-Banking System eine 2-Faktoren-Authentifizierung mit einem sogenannten mTAN-Code. Dieser wird den Kunden, nachdem sie ihre Login-Daten eingegeben haben, auf ein vorgängig registriertes Mobiltelefon zugestellt. Mit der Eingabe dieses Codes im E-Banking müssen sie dann ihr Login bestätigen. Als der Kunde dies an einem Sonntag versuchte, wurde der Bildschirm nach Eingabe des mTAN schwarz und meldete Unterhaltsarbeiten am E-Banking der Bank. Er brach den Login-Versuch ab und versuchte, sich erneut anzumelden, was wiederum misslang. Aufgrund der Umstände war davon auszugehen, dass sein Rechner wahrscheinlich infiziert war und er die Login-Daten auf einer sogenannten Phishing-Website eingegeben hatte, welche von den Betrügern aufgesetzt worden war, um an diese Daten zu gelangen, und der Website der Bank wohl täuschend ähnlich sah. Mit Hilfe der betrügerisch erlangten Daten loggten sich unbekannte Dritte via E-Banking ein und lösten ab dem Konto seiner Frau eine Überweisung auf das Konto eines sogenannten Money Mules bei einer Drittbank aus. Die Empfängerin, gemäss dem vom Kunden eingeleiteten Strafverfahren eine Studentin, welche über die wahren Vorgänge ebenfalls getäuscht worden war, leitete das Geld danach gegen eine Entschädigung den Betrügern weiter. Diese konnten nicht ermittelt werden und das Geld blieb verschwunden.

Die Grundproblematik dieser Fälle ist, dass der Schaden von den eigentlichen Tätern in aller Regel nicht erhältlich gemacht werden kann. Es stellt sich dann die Frage, ob der Bankkunde oder die Bank diesen ganz oder teilweise tragen muss. Dies ist eine Frage der anwendbaren vertraglichen Regelung. Gemäss den üblichen vertraglichen Bestimmungen kann und muss eine Bank einen Zahlungsauftrag ausführen, welcher gestützt auf die korrekten Legitimationsmittel im E-Banking System eingegeben wurde. Bei der Haftung für Missbräuche folgen die Verträge in der Regel einer Risikosphärentheorie. Diese besagt, dass grundsätzlich diejenige Partei für Fehler haftet, welche in dem Bereich stattfinden, welchen sie beeinflussen kann und die sie mit der gehörigen Sorgfalt hätte verhindern können. Gestützt auf die vertraglichen Regelungen lehnte die Bank vorliegend eine Haftung ab, da ihrer Ansicht nach ihre Systeme einwandfrei funktioniert hatten und der Kunde alleine für die Sicherheit seines Endgeräts verantwortlich war, welches vorliegend mutmasslich infiziert worden war.

Vorliegend stellte sich aber zusätzlich die Frage, ob die Bank gegenüber der Empfängerbank nicht hätte schneller reagieren müssen, damit der von den Betrügern überwiesene Betrag noch hätte sichergestellt werden können. Die Bank vertrat die Ansicht, ihre Reaktion sei zeitgerecht erfolgt. Die Reaktion der Bank, welche erst am späten Nachmittag erfolgte, nachdem die Betrugsmeldung am frühen Morgen eingetroffen war, erschien dem Ombudsman jedoch reichlich spät. Es gehört erfahrungsgemäss zu den typischen Merkmalen eines solchen Betrugs, dass die Täter oder die von ihnen als Hilfspersonen instruierten Money Mules das Geld sofort nach Eintreffen auf dem Empfängerkonto abziehen und somit die Sicherstellung verhindern. Eine Diskussion darüber, ob die Reaktion zeitgerecht erfolgt war, hätte sich erübrigt, wenn auch eine unmittelbar nach Eingang der Betrugsmeldung erfolgte Intervention bei der Empfängerbank verspätet gewesen wäre, weil bereits über das Geld verfügt worden war. Der Ombudsman versuchte deshalb, bei der Empfängerbank in Erfahrung zu bringen, wann genau über das Geld verfügt wurde. Diese verweigerte unter Hinweis auf das Bankgeheimnis eine detaillierte Auskunft und teilte lediglich mit, dass sie solche Meldungen jeweils umgehend bearbeite. Der Ombudsman konnte diesen Punkt deshalb nicht mit der gewünschten Genauigkeit klären, wies den Kunden aber darauf hin, dass die Unterlagen der Strafuntersuchung hier wohl weiterhelfen könnten.

Gemäss der Erfahrung des Ombudsman gehen die Banken mit solchen Schadenfällen unterschiedlich um und zeigen sich mitunter grosszügiger, als die im vorliegenden Fall betroffene Bank. Angesichts der fehlenden Bereitschaft zu einem Entgegenkommen musste er dieses Vermittlungsverfahren mit einem abschliessenden Bescheid an den Kunden leider erfolglos einstellen.