Schadenersatzforderung wegen Zahlungen, welche von Unbekannten per E-Banking ausgelöst wurden

Thema: **Missbrauch und Betrug** Fallnummer: **2020/12**

Die Kundin wurde mutmasslich Opfer eines sogenannten Phishing-Angriffs. Unbekannten Betrügern gelang es, sie auf eine Website zu locken, welche derjenigen der Bank täuschend ähnlich sah. Sie gab dort ihre E-Banking Zugangsdaten ein, welche von den Betrügern abgefangen wurden. Damit lösten diese zulasten des Kontos der Kundin 12 Zahlungen in der Gesamthöhe von rund 150 000 CHF aus. Die Kundin erwartete von der Bank, dass diese ihr den gesamten Schaden ersetze. Die Bank war lediglich bereit, ihr 39 000 CHF zu bezahlen, was die Kundin als nicht ausreichend erachtete. Sie unterbreitete den Fall deshalb dem Ombudsman. Die Bank erhöhte ihr Vergleichsangebot im Rahmen des Ombudsverfahrens auf 75 000 CHF und war somit bereit, den Schaden zur Hälfte zu übernehmen. Die Kundin nahm dieses Angebot an.

Den unbekannten Betrügern gelang es, innerhalb von fünf Tagen über das E-Banking in rund einem Dutzend Transaktionen insgesamt rund 150 000 CHF von zwei Konten der Kundin abzuziehen. Danach sperrte die Bank die Konten der Kundin, weil ihr die Transaktionen als ungewöhnlich aufgefallen waren. Die Kundin vertrat die Auffassung, dass im E-Banking-System der Bank eine Sicherheitslücke bestand und dass die Bank das Eindringen von Betrügern in ihre Konten und das betrügerische Auslösen von Vergütungen viel früher hätte bemerken sollen als erst nach fünf Tagen.

Die Bank äusserte in einem Antwortschreiben auf die Reklamation der Kundin die Vermutung, dass der Rechner, den die Kundin auch für E-Banking-Geschäfte einsetzte, von einem sogenannten Trojaner befallen worden war und dieser Befall dazu führte, dass eine unbekannte Täterschaft in die Lage versetzt wurde, die schädlichen Transaktionen zu veranlassen. Eine eigene Verantwortlichkeit bestritt die Bank, offerierte der Kundin aber dennoch, ihr im Sinne eines reinen Entgegenkommens und ohne Anerkennung einer Rechtspflicht per Saldo aller Ansprüche den Betrag von 39 000 CHF zu bezahlen. Diesen Betrag, der rund einem Viertel ihres Schadens entsprach, erachtete die Kundin als ungenügend.

Die Frage, wann die Bank in einer solchen Situation für nicht autorisierte Transaktionen von Dritten haftet, ist üblicherweise vertraglich geregelt. Die dem Ombudsman bekannten Verträge folgen in der Regel einer sogenannten Risikosphärentheorie. Danach trägt grundsätzlich immer diejenige Partei die Verantwortung für den Bereich, den sie mit gebührender Sorgfalt beeinflussen kann. Eine Bank ist dafür verantwortlich, dass das von ihr betriebene E-Banking den aktuellen Sicherheitsstandards entspricht. Die Verantwortung für die Sicherheit der Endgeräte, mit welchen ein Kunde auf das E-Banking zugreift, obliegt hingegen grundsätzlich ihm.

Nach der Kontaktnahme der Kundin mit dem Ombudsman forderte dieser die Bank in einem ersten Schritt auf, genauer zu beschreiben, wie die einzelnen Transaktionen ausgelöst worden waren, und ihm das Sicherheitskonzept ihres E-Banking Systems im Grundsatz zu erklären. Was auf den Endgeräten der Kundin genau geschehen war, konnte nicht mehr erstellt werden, da diese weder von der Bank, noch von den Behörden untersucht worden waren, bei denen die Kundin Strafanzeige erstattet hatte. Es konnte ebenfalls nicht mehr erstellt werden, über welche IP-Adressen sich die Kundin vor dem Betrug jeweils in das E-Banking System eingeloggt hatte. Die Bank verwendete für

das Einloggen in ihr E-Banking System und für bestimmte Transaktionen, wie z. B. für Zahlungen an neue Empfänger, sowie für den Wechsel von Adressangaben und der Telefonnummer, eine sogenannte 2-Faktoren-Authentifizierung mit einer mTAN. D. h. die Kunden müssen solche Transaktionen mit einem Code bestätigen, welcher ihnen mittels SMS auf ein zweites Endgerät, welches vorgängig registriert worden war, typischerweise ein Mobiltelefon, verschickt wurde. Vorliegend konnte die Bank nachweisen, dass sich die Kundin mit Hilfe eines an sie auf die registrierte Mobiltelefonnummer versandten mTAN in das E-Banking System eingeloggt hatte. Danach registrierte jemand eine neue Mobiltelefonnummer, wofür ebenfalls eine mTAN verwendet wurde, welche der Kundin auf die alte registrierte Mobiltelefonnummer versandt wurde. Der Wechsel dieser Nummer wurde von der Bank per SMS an dieselbe Nummer bestätigt. Kurz darauf wurden die ersten nicht von der Kundin autorisierten Transaktionen mittels einer mTAN ausgelöst, welche die Bank auf die neue Mobiltelefonnummer gesandt hatte, die wahrscheinlich den unbekannten Betrügern zugeordnet werden musste. Die IP-Adresse, über welche die nicht autorisierten Transaktionen in Auftrag gegeben wurden, blieb bei der Bank im Gegensatz zu den früheren, von der Kundin verwendeten IP-Adressen, registriert.

Es lag daher die Vermutung nahe bzw. machte den Anschein, dass die Kundin Opfer der bekannten und im Bereich des Online-Banking wohl dominierenden Betrugsmasche des sogenannten Phishing-Angriffs wurde. Dabei gelingt es den Betrügern, den Bankkunden auf eine Website zu locken oder ihm eine solche vorzuspiegeln, die der echten Website seiner Bank täuschend ähnlich sieht. Versucht der Kunde dann, sich einzuloggen und gibt die erforderlichen Daten ein, fangen die Betrüger diese ab und loggen sich unter Verwendung dieser Daten auf der echten Website der Bank in das Konto des Kunden ein. Möglich ist auch, dass die Betrüger eine Schadsoftware, wie namentlich einen sogenannten Trojaner, auf dem Gerät des Kunden installieren und auf diese Weise Daten ausspähen oder die Kontrolle über sein Gerät übernehmen können.

Es versteht sich, dass die Bank nicht kontrollieren konnte, was auf dem Gerät der Kundin geschah bzw. dass dieses allenfalls mit einem Trojaner infiziert worden war. Demgegenüber lag es aber nahe, dass die Kundin die Login-Daten und die erhaltenen SMS-Codes eingegeben hatte, welche den Wechsel des Mobiltelefons ermöglichten. Dabei schien es dem Ombudsman von besonderer Bedeutung, dass der Wortlaut des SMS-Codes für die Änderung der bei der Bank hinterlegten Mobiltelefonnummer sich von demjenigen für ein Login offenbar unterschied und bei gebotener Sorgfalt als solcher erkennbar war. Gegenüber der Bank anerkannte der Ombudsman, dass die Verwendung eines mTAN Systems grundsätzlich eine starke Autorisierung für E-Banking Transaktionen darstellt. Er äusserte hingegen die Vermutung, dass das an sich bekannte Betrugsschema, welches regelmässig mit einem kurz nach der Änderung der Mobiltelefonnummer erfolgenden Wechsel der für den Zugang zum E-Banking verwendeten IP-Adresse verbunden ist, durch eine weitere Sicherheitshürde für eine solche Änderung hätte erkannt werden können.

Die Bank informierte darauf den Ombudsman, dass das E-Banking System in der Zwischenzeit entsprechend angepasst worden sei und erhöhte das Vergleichsangebot an die Kundin auf 50 % der Schadenssumme. Angesichts der Gesamtumstände des Falles empfahl er der Kundin, dieses Vergleichsangebot anzunehmen. Die Kundin folgte schliesslich seiner Empfehlung.