

Betrügerische Zahlungen via E-Banking-System

Thema: **Missbrauch und Betrug** Fallnummer: **2017/09**

Der Kunde wurde Opfer von Betrügern, welchen es gelang, seine Log-in-Daten für das E-Banking-System abzufangen und Zahlungen zugunsten eines bei einer englischen Bank geführten Kontos einer Firma auszulösen. Die Bank war lediglich bereit, ihn für die Hälfte des überwiesenen Betrags zu entschädigen. Dies erachtete der Kunde als ungenügend. Die Bank lehnte eine Entschädigungspflicht im Ombudsverfahren weiterhin strikte ab, hielt aber die Offerte für eine Kulanzzahlung von 50 % des Schadens aufrecht. Der Kunde nahm diese auf Empfehlung des Ombudsmann schliesslich an.

Der Kunde erhielt ein Telefon, welches angeblich von einem Software-Ingenieur seines Internetproviders stammte. Dieser teilte ihm mit, er müsse nach einer Cyberattacke im System Malware entfernen, welche unter anderem auf den Zugang zu E-Banking-Systemen von Banken Einfluss nehmen könne, und fragte ihn nach seinen Bankverbindungen. Der Kunde gab diese bekannt und wurde vom angeblichen Ingenieur instruiert, er solle auf die Websites dieser Banken nur nach Eingabe eines bestimmten Codes zugreifen. Dies habe er gemacht, worauf die Websites jeweils kurzzeitig verschwanden und dann wieder auf seinem Bildschirm erschienen. Der Anrufer teilte ihm mit, nun könnten er und seine Mitarbeiter die Malware entfernen. Später stieg er in die E-Banking-Systeme seiner Banken mittels der normalen Zugangsprozesse ein und bemerkte nichts Besonderes. Als er einige Tage später wieder auf das E-Banking-System der Bank zugriff, stellte er fest, dass auf seinem Konto eine Zahlung auf das Konto einer ihm unbekanntes Firma bei einer englischen Bank aufgeführt war, welche nicht von ihm ausgelöst worden war. Er teilte dies der Bank umgehend mit, welche ihm versicherte, das Nötige vorzukehren. Es stellte sich schliesslich heraus, dass das Geld auf dem Kundenkonto der Empfängerbank bereits weg war, als seine Bank diese über den Betrug informierte.

Nach Ansicht des Kunden, welcher gegen die unbekanntes Täter Strafanzeige erstattete, war die Bank zur Rückvergütung der ohne seinen Auftrag erfolgten Zahlung verpflichtet. Er machte geltend, die anderen Banken, bei welchen er Konti hatte, seien vom gleichen Betrugsschema betroffen gewesen und hätten die Zahlungen entweder nicht ausgeführt oder hätten bei den Empfängerbanken durch rechtzeitige Reaktion erreicht, dass die ohne seinen Auftrag erfolgten Zahlungen rückvergütet worden seien, sodass ihm dort kein Schaden erwachsen sei. Er habe mit den vorgesehenen Zugangsschritten auf das E-Banking zugegriffen und sei nicht verantwortlich, wenn dadurch Drittpersonen ermöglicht werde, über seine Konti zu verfügen. Im Übrigen hätte die Zahlung von der Bank als ungewöhnlich erkannt werden müssen, da er über dieses Konto noch nie Zahlungen an Dritte getätigt habe. Im Weiteren habe die Bank nach der Meldung des Vorfalls zu lange gewartet, um die Empfängerbank zu kontaktieren, sodass die unbekanntes Täter dort über das Geld verfügen konnten. Schliesslich habe ihm die Bank ursprünglich telefonisch bestätigt, der Betrag habe bei der Empfängerbank sichergestellt werden können. Die Bank lehnte eine Entschädigungspflicht ab und hatte sich lediglich bereit erklärt, ihm aus Kulanz 50 % des überwiesenen Betrags zu erstatten. Darauf wandte sich der Kunde an den Ombudsmann und bat ihn um Einleitung eines Vermittlungsverfahrens.

Die Bank erläuterte gegenüber dem Ombudsmann die bereits direkt gegenüber dem Kunden eingonnene Haltung noch näher. Sie machte geltend, dass die vorliegende Zahlung nach Eingabe

der erforderlichen Zugangsdaten im E-Banking ausgeführt worden sei, ohne dass Dritte auf die Systeme der Bank Einfluss genommen hätten. Sie sei gestützt auf die vertraglichen Vereinbarungen über das E-Banking berechtigt, solche Transaktionen auszuführen. Der Kunde sei verpflichtet, die Zugangsmittel sorgfältig zu verwahren und unter keinen Umständen Dritten zur Verfügung zu stellen. Es bestehe keine vertragliche Pflicht der Bank, eine per E-Banking in Auftrag gegebene Zahlung jeweils noch zusätzlich auf ihre Plausibilität zu prüfen. Vorliegend hätten aufgrund der Schilderungen des Kunden offenbar Dritte durch Infizierung der Eingabegeräte des Kunden mit Malware seine Zugangsdaten abgefangen. Dies sei ausserhalb der Einflussosphäre der Bank geschehen. Es sei nicht verständlich, weshalb der Kunde nach dem Telefonat mit dem angeblichen Ingenieur seines Internetproviders nicht die Bank kontaktiert und gefragt habe, ob der Zugang zu ihren E-Banking-Systemen tatsächlich gestört sei. Die ausserhalb der Einflussosphäre der Bank zuzuordnenden Risiken aus dem E-Banking müssten gemäss der vertraglichen Vereinbarung vom Kunden getragen werden. Die Bank konnte im Übrigen darlegen, dass sie die Empfängerbank am Morgen nach der Meldung des Kunden unverzüglich über den Vorfall informiert und das Geld zurückgefordert hat. Die Empfängerbank habe leider nicht reagiert, sodass sie gemahnt werden musste. Der Kunde habe den Zeitpunkt der Mahnung als denjenigen der Erstintervention betrachtet und sei deshalb fälschlicherweise von einer verspäteten Reaktion ausgegangen. Die Aussage der Bank, der Betrag habe blockiert werden können, habe eine zweite vom Kunden beanstandete Vergütung betroffen, bei der das Geld tatsächlich rechtzeitig blockiert und dem Kunden wieder gutgeschrieben werden konnte.

Die Bank lehnte auch gegenüber dem Ombudsman eine Entschädigungspflicht ab, wiederholte aber die Offerte, dem Kunden aus Kulanz 50 % des Betrages der Zahlung zu vergüten. Nach Abwägung der Argumente der beiden Parteien empfahl der Ombudsman dem Kunden, die Vergleichsofferte der Bank anzunehmen. Aufgrund der Schilderungen des Vorfalls schien auch ihm plausibel, dass die unbekanntes Betrüger auf die Systeme des Kunden Einfluss genommen hatten und dies tatsächlich ausserhalb des Einflussbereichs der Bank war. Es war vertraglich vereinbart, dass solche Risiken vom Kunden getragen werden müssen, was einer im Markt üblichen Regelung entspricht. Aufgrund der Schilderungen bestanden tatsächlich gewisse Zweifel daran, dass der Kunde im Zusammenhang mit dem geschilderten Telefonat genügend sorgfältig war. Dem Ombudsman ist kein Gerichtsentscheid bekannt, wonach eine Bank verpflichtet wäre, per E-Banking erteilte und automatisch ausgeführte Aufträge noch auf ihre Plausibilität zu überprüfen. Die Rechtsprechung, welche im Zusammenhang mit betrügerisch erteilten Aufträgen entwickelt wurde, welche der Bank auf anderen Kanälen zukommen und von Mitarbeitern geprüft werden, ist nach Ansicht des Ombudsman nicht ohne Weiteres auf die vorliegende Situation anwendbar. Im Übrigen wäre das isolierte Kriterium, dass ab dem fraglichen Konto noch nie Aufträge an Dritte erteilt worden sind, selbst nach der erwähnten Rechtsprechung wohl nicht ausreichend, um den Auftrag als ungewöhnlich einzustufen. Schliesslich konnte die Bank erklären, dass sie die Empfängerbank rechtzeitig nach Meldung des Vorfalls über den Betrug informiert hat. Die Vergleichsofferte der Bank schien ihm deshalb angemessen. Der Kunde nahm diese auf Empfehlung des Ombudsman schliesslich an.