

Verhalten der Bank nach einer Meldung von betrügerisch ausgelösten Zahlungen

Thema: **Missbrauch und Betrug** Fallnummer: **2024/07**

Die Kundin hatte die E-Banking-Einstiegsseite der Bank via Google gesucht und den Link auf dem obersten Suchergebnis angeklickt. Sie gelangte dann auf eine täuschend echt gefälschte Website der Bank und gab dort ihre Zugangsdaten für das E-Banking ein. Die Betrüger konnten mit diesen Daten eine Zahlung über rund CHF 5'000 zulasten ihres Kontos auslösen. Tags darauf stellte sie dies fest und meldete der Bank den Betrugsvorfall. Diese kontaktierte die Empfängerbank fünf Kalendertage später und bat sie erfolglos, den Betrag zu retournieren. Die Kundin reklamierte bei der Bank und erklärte, sie habe die Zahlung nicht auf der App bestätigen müssen, was bei Zahlungen an unbekannte Empfänger üblich sei. Zudem vertrat sie die Ansicht, die Empfängerbank sei zu spät über den Betrug informiert worden. Die Bank antwortete der Kundin, sie habe die Zahlung auf der App bestätigt und erklärte, der Rückruf sei rechtzeitig erfolgt. Im Ombudsverfahren bestätigte die Bank ihre Haltung, so dass der Fall ohne Vermittlungsergebnis abgeschlossen werden musste.

Die Kundin wurde im vorliegenden Fall Opfer eines verbreiteten Betrugsmodells. Bei Google ist es möglich, gegen Entgelt dafür zu sorgen, dass Suchergebnisse für bestimmte Begriffe mit entsprechenden Links zuoberst aufgeführt werden. Dies machen sich offenbar auch Betrüger zunutze, indem sie dafür sorgen, dass ihre gefälschten Phishing Websites, welche den echten Websites von Banken täuschend ähnlichsehen, zuoberst erscheinen, wenn Kunden mit einer Suchmaschine die E-Banking Einstiegsseite ihrer Bank suchen. Google markiert solche bezahlten Suchergebnisse jeweils als «gesponsert». Klickt der Kunde auf den Link im obersten Suchergebnis, kann er auf eine gefälschte Phishing Website geführt werden, auf welcher er die vorgesehenen Log-in Schritte tätigt. Im Hintergrund fischen die Betrüger dem Kunden die notwendigen Zugangsdaten ab und öffnen damit die echte E-Banking Website der Bank. Die Polizei, die Finanzinstitute, die Konsumentenorganisationen und auch der Ombudsman warnen regelmässig vor dieser Betrugsmasche. Erstaunlich ist, dass sie offenbar trotz der gewonnenen Erkenntnisse immer noch funktioniert.

Sobald die Betrüger in das E-Banking des Kunden eingeloggt sind, tätigen sie die mit den erschwindelten Daten möglichen Zahlungstransaktionen. Oft muss der Kunde einen Begünstigten, dem er im E-Banking noch nie eine Zahlung hat zukommen lassen, mittels einer 2-Faktoren-Authentifizierung via eine App oder einen auf sein Mobiltelefon zugeschickten SMS-Code bestätigen. Gemäss der Erfahrung des Ombudsman werden die entsprechenden Sicherheitsmitteilungen von den Kunden leider oft nicht genau gelesen. Damit wird eine wichtige und effiziente Sicherheitsmassnahme der gängigen E-Banking-Systeme übersteuert.

In ihrer Antwort an den Ombudsman erklärte die Bank, sie warne ihre Kunden regelmässig, u.a. mit Hinweisen auf ihrer E-Banking-Einstiegsseite, vor den bekannten Betrugsmodellen, auch vor derjenigen, welcher die Kundin zum Opfer gefallen sei. Die Kundin habe die umstrittene Zahlung tatsächlich mit der App bestätigt. Es gebe keine Hinweise darauf, dass der Bestätigungsprozess nicht funktioniert habe. Für die Bank sei nicht erkennbar gewesen, dass die Kundin Opfer eines Betrugs geworden sei. Gemäss den Bestimmungen zu den elektronischen Dienstleistungen der Bank liege es

in der Verantwortung der Kunden sicherzustellen, dass sie sich bei der Eingabe der Zugangsdaten auf der korrekten E-Banking-Seite befinden.

Mit der Bestätigung in der App sei der Zahlungsauftrag unwiderruflich und könne nicht mehr gestoppt werden. In einem solchen Fall offeriere die Bank den Kunden aber die Möglichkeit, einen Rückruf der ausgeführten Zahlung zu verlangen. Gemäss den internen Richtlinien der Bank habe dieser innerhalb einer bestimmten Anzahl Tage zu erfolgen. Für die Frist seien nur die Bankarbeitstage massgebend. Da zwischen der Betrugsmeldung und dem Rückruf ein Wochenende gelegen habe, sei dieser nach fünf Tagen rechtzeitig erfolgt.

Die Empfängerbank müsse in einem solchen Fall das Einverständnis des Kontoinhabers zur Rückbuchung einholen. Die Bank könne nicht garantieren, dass ein solcher Rückruf erfolgreich sei und sei dafür auch nicht verantwortlich. Im vorliegenden Fall sei die Empfängerbank einen Tag nach dem Rückruf auch darüber informiert worden, dass geltend gemacht werde, die Zahlung habe einen betrügerischen Hintergrund. Die Empfängerbank habe nach zweimaligem Nachfassen rund einen Monat nach dem Rückruf gemeldet, der Empfänger habe kein Einverständnis zur Rückbuchung erteilt.

Die Bank vertrat die Meinung, die Kundin sei alleine für den Schaden verantwortlich. Im vorliegenden Fall habe die Bank alle zumutbaren Massnahmen rechtzeitig getroffen und lehne ein Entgegenkommen deshalb ab.

Der Ombudsman erklärte der Kundin, gemäss den anwendbaren Vertragsbestimmungen liege die Verantwortung für Zahlungen, die vom Kunden mittels 2-Faktoren Authentifizierung über eine App bestätigt worden seien, grundsätzlich beim Kunden. Aufgrund der Erläuterungen der Bank, welche sie mit Kopien der Logfiles dokumentiert hatte, musste er davon ausgehen, dass der Zahlungsauftrag effektiv über die App der Kundin bestätigt worden war. Erfahrungsgemäss würden die Empfänger von betrügerisch erwirkten Überweisungen das Geld bei der Empfängerbank in aller Regel sofort beziehen oder weiterleiten, so dass Rückrufanfragen an die Empfängerbank, die nicht unmittelbar nach dem Auslösen der Transaktion erfolgen, sehr häufig erfolglos seien.

Die Kritik der Kundin, dass die Bank den Rückruf in ihrem Fall verspätet in die Wege geleitet hatte, konnte der Ombudsman allerdings nachvollziehen. Er erachtet es in solchen Fällen als wichtig, dass die Empfängerbank so rasch wie möglich über den geltend gemachten betrügerischen Hintergrund der Zahlung informiert wird. Ein gewöhnlicher Rückruf, wie er bei aufgrund von mangelhaften Angaben fehlgeleiteten Zahlungen üblicherweise getätigt wird, reicht nicht aus, da die Empfänger einer betrügerisch ausgelösten Zahlung einer Rückbuchung wohl nie zustimmen werden. Ob ein rascheres Handeln zu einer erfolgreichen Blockierung und Rücküberweisung der Zahlung geführt hätte, musste im vorliegenden Fall allerdings offen bleiben. Da die Bank ein Entgegenkommen kategorisch ablehnte, musste der Fall ohne Vermittlungsergebnis geschlossen werden.