CENTRE DE DROIT
BANCAIRE ET FINANCIER

Betrügerische Bankaufträge

Kommunikation per E-Mail bleibt riskant

Par Célian Hirsch le 23 Juni 2021

Wer, die Bank oder die Kunden, muss den Schaden tragen, der durch die Ausführung von Aufträgen von Hackern verursacht wurde ? Kurz nach dem BGE 146 III 326 (siehe cdbf.ch/1150/), in dem das Bundesgericht ein grobes Verschulden einer Handelsgesellschaft verneinte, wurde das Tessiner *Tribunale d'appello* mit der gleichen Problematik konfrontiert. Im Gegensatz zur Entscheidung des Bundesgerichts stellt es ein grobes Verschulden der Bank fest und betont die Gefahr von E-Mail-Kommunikation (Urteil 12.2019.148 vom 18. September 2020).

Zwei Brüder, die im Beratungsgeschäft im Zusammenhang mit dem Bergbausektor tätig sind, eröffnen ein Bankkonto bei einer Tessiner Bank. Sie kommunizieren hauptsächlich per E-Mail mit ihrem Kundenbetreuer und investieren unter anderem eine Million Dollar in Gold.

Mehrere Monate nach der Kontoeröffnung erhält die Bank als Anhang einer E-Mail, die scheinbar von den Kunden stammt, zwei Überweisungsaufträge an eine chinesische Bank. Diese Aufträge in Höhe von 222.400 USD werden jedoch von der Compliance-Abteilung blockiert. Nach einigen E-Mail-Wechseln erhält die Bank die angeblichen Rechnungen zu den Aufträgen. Sie beziehen sich auf den Kauf von Einspritzpumpen, Schläuchen und Anschlüssen. Die Bank führt daraufhin die Aufträge aus.

Einige Tage später wird der Betrug entdeckt. Es ist jedoch zu spät, um die nach China geflossenen Gelder zurückzuerhalten. Eine von der Bank eingereichte Strafanzeige bleibt ohne Ergebnis.

Die Kunden reichten erfolgreich einen Zahlungsantrag gegen die Bank beim *Pretore (*Amtsgericht) in Lugano ein. Der Richter stellte insbesondere fest, dass die Parteien nicht vereinbart hatten, dass Aufträge per E-Mail übermittelt werden können. Darüber hinaus hätten die Mitarbeiter, die keine Schulung in IT-Sicherheit erhalten hatten, erkennen müssen, dass die beiden Aufträge verdächtig und ungewöhnlich waren. Sie hätten die Kunden anrufen müssen. Darüber hinaus ist das Bestimmungsland der Aufträge, nämlich China, dafür bekannt, dass es dort zu IT-Betrug kommt. Selbst wenn die Aufträge vertragsgemäß übermittelt worden wären (z. B. per Fax), hätte die Bank daher aufgrund ihres groben Verschuldens den Schaden nicht auf die Kunden abwälzen können.

In ihrer Berufung beim *Tribunale d'appello* Tessin argumentiert die Bank zunächst, dass die Aufträge per Fax und damit vertragsgemäß übermittelt worden seien. Auf jeden Fall sei die

Kommunikation per E-Mail nicht nur von den Kunden vorgeschrieben, sondern auch von diesen durch konkludentes Handeln akzeptiert worden. Schließlich seien die Aufträge üblich und nicht verdächtig gewesen. Die Bank habe daher bei ihrer Ausführung keinen groben Fehler begangen.

Das Kantonsgericht erinnert zunächst daran, dass es in der Sache um die Ausführung betrügerischer Bankaufträge geht. Es geht also darum, festzustellen, ob die Bank die Anweisungen vertragsgemäß ausgeführt hat und ob sie, falls dies der Fall ist, den erlittenen Schaden wirksam auf ihre Kunden übertragen konnte.

In Bezug auf das Kommunikationsmittel der betrügerischen Aufträge ist das Kantonsgericht der Ansicht, dass es nicht mit Sicherheit feststellen kann, ob die Aufträge nur als E-Mail-Anhang oder auch per Fax übermittelt wurden, wie die Bank behauptet. Es entscheidet die Frage nicht und geht zur zweiten Stufe über, die sich auf das Verschulden der Bank bezieht.

Das *Tribunale d'appello* erkennt an, dass die Kunden selbst sich für eine Kommunikation mit der Bank per E-Mail entschieden haben. Die Bank habe dies jedoch von Anfang an akzeptiert und genutzt. Da die Hacker durch den Zugriff auf den elektronischen Austausch diese Kommunikation nutzen konnten, um sich besser zu tarnen, sei die Bank fahrlässig gewesen, da sie die Kunden nie auf dieses Risiko aufmerksam gemacht habe. Darüber hinaus war die Kommunikation mit ausländischen Kunden per E-Mail für die Bank eine übliche Praxis und Kommunikationsform. Der ehemalige IT-Manager erklärte im Verfahren, dass es sich um eine bekannte Risikosituation handelte. Das Appellationsgericht kam zu dem Schluss, dass diese „Situation erhöhter Gefahr" die Bank dazu verpflichtet habe, angemessene Maßnahmen zu ergreifen und mit einer gewissen Vorsicht zu handeln.

Im vorliegenden Fall war sich die Bank bewusst, dass die Aufträge eine genauere Überprüfung erforderten, da sie zunächst blockiert wurden. Diese Überprüfungen blieben jedoch unvollständig. Tatsächlich hatten die von den Hackern übermittelten Rechnungen nichts mit der Tätigkeit der Kunden zu tun (Kauf von Einspritzpumpen, Schläuchen und Anschlüssen). Außerdem handelte es sich um ein privates Bankkonto und nicht um ein Geschäftskonto. Diese Rechnungen, die zur Begründung der Aufträge bestimmt waren, waren offensichtlich verdächtig. Darüber hinaus ist bekannt, dass China als Zielland von Zahlungen ein hohes Betrugsrisiko aufweist. Auch die Erwähnung einer „Dringlichkeit" bei der Ausführung der Aufträge sollte Zweifel aufkommen lassen. Schließlich hätte die Bank einfach einen *Call-back* vornehmen können, zumal die Bank bereits in der Vergangenheit telefonischen Kontakt mit ihren Kunden hatte.

Unter Berücksichtigung all dieser Umstände, des Billigkeitsgrundsatzes (Art. 4 CC) und des richterlichen Ermessens bestätigt das *Tribunale d'appello* die Einschätzung des *Pretore* : Die Bank hat einen schweren Fehler begangen. Daher kann sie den Schaden, der durch die Ausführung betrügerischer Aufträge entstanden ist, nicht auf die Kunden abwälzen.

Wie in der Einleitung angekündigt, weist dieses Tessiner Urteil gewisse Ähnlichkeiten mit dem BGE 146 III 326 auf (siehe cdbf.ch/1150/). In beiden Fällen führte die Bank Aufträge von Hackern aus, die per E-Mail übermittelt wurden. In beiden Fällen konnten sich die Hacker von den E-Mails zwischen der Bank und ihrem Kunden inspirieren lassen, um zumindest auf dieser Ebene unbemerkt zu bleiben. Allerdings wurden im BGE die Aufträge zugunsten einer bekannten Bank im Vereinigten Königreich ausgeführt und nicht zugunsten einer Bank in einem

Risikoland. Dieses Kriterium allein reichte zwar nicht aus, konnte aber dennoch eine wichtige Rolle bei der Beurteilung des Fehlverhaltens der Bank spielen (zu den anderen relevanten Kriterien siehe Liégeois Fabien/Hirsch Célian, Ordres bancaires frauduleux : discours de la méthode, *in :* La Semaine judiciaire II, Doctrine, 2021, Nr. 4, S. 135).

Reproduction autorisée avec la référence suivante: Célian Hirsch, Kommunikation per E-Mail bleibt riskant, publié le 23 Juni 2021 par le Centre de droit bancaire et financier, https://cdbf.ch/de/1188/