Und plötzlich war das Geld weg

Online-Banking und seine Risiken / Wer haftet bei Missbrauch?

Herr Arglos nahm seit einigen Monaten am sogenannten Online-Banking teil, nachdem ihm die Kundenberaterin seiner Hausbank dessen Vorzüge erläutert hatte. Überzeugt hatte ihn, dass er nicht mehr auf die Öffnungszeiten der Bank angewiesen war und dass auch die Gebühren für die von Hand ausgefüllten Überweisungsträger wegfallen würden, die seine Bank seit einiger Zeit hierfür erhoben hatte. Eines Tages, als Herr Arglos wieder einmal seine Kontobewegungen überprüfte, stellte er bestürzt fest, dass von seinem Guthaben zwei Tage zuvor 5.000,00 € auf ein ihm unbekanntes Konto transferiert worden waren. Da er diese Überweisung nicht vorgenommen hatte, wandte er sich sofort an seine Bank, die umgehende Ermittlungen einleitete. Es stellte sich heraus, dass es sich um einen Fall des sogenannten „Phishings" handelte, bei dem unbekannte Täter die Daten von Herrn Arglos ausspioniert und dann die Transaktion vorgenommen hatten. Herrn Arglos fiel ein, dass er zwei Wochen zuvor eine E-Mail erhalten hatte, die angeblich von seiner Hausbank stammte und mit der er aufgefordert wurde, für eine Sicherheitsüberprüfung auf einer in der E-Mail genannten Webseite seine Persönliche Identifikationsnummer (PIN) und seine Transaktionsnummer (TAN) mitzuteilen. Pflichtbewusst hatte er dies auch getan. Hierdurch war es den wahren Absendern der E-Mail dann ein Leichtes gewesen, die Überweisung vorzunehmen.

Ein Fall wie der vorliegende ist mittlerweile keine Seltenheit mehr, was auch damit zusammenhängt, dass inzwischen mehr als 30 Millionen Bankkonten im Online-Banking geführt werden, Tendenz steigend. Hierdurch wächst auch die Zahl von betrügerischen Angriffen auf die Nutzer des Online-Bankings. Das sogenannte Phishing (abgeleitet von den englischen Begriffen „password fishing") hat dabei stets das Ziel, in den Besitz der PIN und TAN der Online-Bankkunden zu gelangen, um so Gelder von deren Konten abzweigen zu können. Sobald die Täter in den Besitz der Daten gekommen sind, erfolgt dann eine Überweisung vom Kundenkonto auf ein anderes deutsches Konto eines Kuriers, der den Betrag anschließend abhebt und an einen Empfänger im Ausland transferiert. In derartigen Fällen stellt sich die Frage, wer für den eingetretenen Schaden haftet, wenn die rechtswidrig vorgenommene Überweisung durch die Bank nicht mehr rückgängig gemacht werden kann. Als rechtliche Grundlage für die Belastung des Kundenkontos mit dem Überweisungsbetrag kommt ein Schadensersatzanspruch der Bank in Betracht. Da der Kunde nach den Bedingungen zum Online-Banking grundsätzlich verpflichtet ist, seine PIN und TAN geheim zu halten, wird für die Praxis zur entscheidenden Frage, ob er seine Geheimhaltungspflicht fahrlässig verletzt, wenn er sich durch eine Phishing-Mail täuschen lässt und die PIN und TAN auf der Webseite des Täters eingibt. Hierzu gehen bisher die rechtlichen Ansichten auseinander, wobei teilweise vertreten wird, dass durch ein derartiges Verhalten eines Kunden stets eine Pflichtverletzung vorliege (womit der Kunde den Schaden zu tragen habe), teilweise aber auch, dass es stets auf den Einzelfall

ankomme. Vertreter der ersten Auffassung stellen darauf ab, dass bei Verwendung von PIN und TAN im Online-Banking im Sinne eines Anscheinsbeweises davon auszugehen ist, dass der Kunde die betreffende Transaktion entweder selbst vorgenommen oder zumindest (durch Weitergabe) veranlasst hat bzw. durch unsorgfältige Geheimhaltung zum Missbrauch beigetragen hat. Die Vertreter der zweiten Auffassung stellen darauf ab, dass auch berücksichtigt werden müsse, ob die Bank durch ihr Verhalten Anlass gab, die Phishing-Mail und die Webseite des Täters für echt zu halten, etwa indem sie E-Mails zur Kommunikation mit dem Kunden nutzte, das Design ihrer Login-Seite häufig wechselte oder zahlreiche bzw. unklare Domains (d.h. unterschiedliche Internetadressen) verwendete. In diesen Fällen könnte dann ein (Mit-) Verschulden der Bank gegeben sein, mit der Folge, dass die Bank dem Kunden den abgebuchten Betrag zurückerstatten müsste. Da es bisher kaum Gerichtsurteile zu diesem Problemkreis gibt, kann zurzeit noch nicht mit letzter Sicherheit gesagt werden, ob ein Kunde grundsätzlich auf einem durch Phishing erlittenen Schaden sitzen bleibt oder nicht. Auch deshalb sollten Nutzer des Online-Bankings in jedem Falle regelmäßig ihre Kontobewegungen überprüfen, um gegebenenfalls verdächtige Abbuchungen sofort erkennen zu können. Sollten solche vorliegen, sollte die Bank unverzüglich verständigt werden, gleichzeitig sollten PIN und TAN sofort geändert werden, um gegebenenfalls weiteren Abbuchungen vorzubeugen. Die E-Mail, mit der der Kunde vor der Abbuchung zur Eingabe der Daten aufgefordert wurde, sollte der Bank und auch der Polizei (bei der in jedem Falle Strafanzeige erstattet werden sollte) zur Verfügung gestellt werden, sodass gegebenenfalls ermittelt werden kann, wo sich der von den Tätern genutzte Server befindet. Im Falle von Herrn Arglos gelang es seiner Hausbank aufgrund der Tatsache, dass die Abbuchung erst zwei Tage zuvor erfolgt war, die gesamte Summe zurückzuleiten, sodass Herr Arglos letztlich mit einem „blauen Auge“ und um eine Erfahrung reicher davongekommen war.