

## **Per Mausklick zum Konto: Das Risiko trägt der Kunde**

### ***Wer am Onlinebanking teilnimmt, sollte Vorsicht walten lassen***

Sowohl im privaten als auch im geschäftlichen Bereich setzt sich das Onlinebanking immer mehr durch: eine Vielzahl von Kunden wickelt ihre Bankgeschäfte bequem von zu Hause oder vom Arbeitsplatz ab. Diese Entwicklung wird von den Geldinstituten gefördert, weil sie aufgrund der Reduzierung des Filialnetzes ganz erhebliche Kosten einsparen.

Wie sieht es allerdings aus, wenn beim Onlinebanking etwas schief geht und wer haftet bei Missbrauch? Gerade hier ist die Unkenntnis groß und viele Nutzer fühlen sich über die rechtlichen Fragen nicht ausreichend informiert. Für große Verunsicherung sorgt auch die zunehmende Verbreitung von Viren und Phishing-E-Mails, die sensible Daten ausspionieren können.

Was ist also aus juristischer Sicht zu beachten?

Wenngleich die Rechtslage bei vielen Einzelfragen noch ungeklärt ist, muss der Kunde damit rechnen, dass bei der Verwendung der korrekten PIN und TAN der Beweis des ersten Anscheins für ein Tätigwerden des Berechtigten spricht. Mit anderen Worten muss der Kunde in einem solchen Schadensfall seine Unschuld beweisen. Gelingt ihm das nicht, haftet er selbst für den Schaden. Nur ganz wenige Banken sind hier verbraucherfreundlicher und haben in ihren Allgemeinen Geschäftsbedingungen die Beweislast umgekehrt, so dass die Bank dem Kunden fehlerhaftes Verhalten nachweisen muss und nicht umgekehrt.

Für den Bankkunden bedeutet dies, dass er bei Online-Bankgeschäften strikt bestimmte Vorsichtsmaßnahmen beachten muss,

Er sollte sich davor hüten, PINs und TANs auf dem Rechner zu speichern oder sie sonst frei zugänglich aufzubewahren.

Ebenso sollte er es vermeiden, das Onlinebanking an öffentlich zugänglichen Orten (z.B. Internetcafés) zu nutzen und unbekannte E-Mails zu öffnen, welche Viren und Trojaner enthalten können.

Wichtig ist zudem das Onlinekonto nach Möglichkeit einmal täglich zu überprüfen, damit Unregelmäßigkeiten sofort erkannt werden können. Im Fall des Missbrauchverdachts muss der Kunde die PIN unverzüglich ändern und nicht verbrauchte TANs sperren lassen. Dies kann am schnellsten dadurch erreicht werden, dass PIN oder TAN dreimal falsch eingegeben werden und dann die Bank von sich aus den Zugang zum Konto sperrt.

In der Rechtsprechung noch nicht abschließend geklärt ist die Frage, ob und in welchen Fällen der erwähnte Anscheinsbeweis vom Kunden erschüttert werden kann. Hier geht es also um den Aspekt, dass der Kunde die ernsthafte Möglichkeit einer Veranlassung des Bankgeschäfts durch einen Dritten darlegen und erforderlichenfalls auch beweisen muss. Voraussetzung hierfür dürfte sein, dass der Kunde etwa die Phishing-E-Mail oder den Trojaner noch auf seinem PC nachweisen kann.

In der Praxis werden diese rechtlichen Probleme oftmals dadurch entschärft, dass Haftungsbeschränkungen etwa auf 10% des Schadens vereinbart werden oder dass Banken – in der Regel allerdings erst auf Nachfrage – zu Kulanzleistungen bereit sind. Dies liegt nicht zuletzt auch daran, dass manche Sicherheitssysteme von Banken nicht auf dem letzten Stand der Technik sind und hierdurch ein Missbrauch zumindest begünstigt wird.

**DR. THOMAS STORCH**

*Der Autor ist Rechtsanwalt mit dem Spezialgebiet Immobilien- und Kapitalanlagerecht.*