

Berechtigte Anforderungen der Bank an die Absicherung des Computers des Kunden vor Schadprogrammen, kein umfassendes Abwälzen des Missbrauchsrisikos der von der Bank den Kunden beim Online-Banking bereitgestellten Sicherungsmedien

Gericht

AG Wiesloch

Datum

20.06.2008

Aktenzeichen

4 C 57/08

Branche/ Lebenslage

Online-Banking, Absicherung des Kundencomputers, Schadprogramme, PIN, TAN

Akteure

Bankkonto-Inhaber, Bank

Wer haftet?

Bank

Haftungsart

Schadenersatz

Haftungsumfang

Schadenersatz, Verfahrenskosten

Haftungsbegründendes Verhalten

Tätigung eines, nicht durch den tatsächlichen Kontoinhaber, veranlassten Zahlungsauftrags

Technische Umstände

Phishing Attacke ermöglichte Klau von Zugangsdaten

Persönliche Umstände

Grundsätzlich trägt die Bank das Missbrauchsrisiko, wenn nicht dem Geschädigten ein nachweisbarer Vorwurf zu machen ist

Möglichkeiten der Haftungsvermeidung

Anforderungen an die Sicherheitsvorkehrungen an Kundengeräte sind zumindest vertraglich festzulegen, sollten diese über die durchschnittlich von Gerichten als zu erwartenden Vorkehrungen hinausgehen; die Sicherungsmechanismen gegen Pharming, Phishing sowie anderer Angriffe auf das Zahlungssystem sollten dem

neusten [Stand der Technik](#) entsprechen, vor möglichen Angriffen sollte möglichst konkret gewarnt werden; Kunden sollten Ihre Bank nach Kenntniserlangung oder Verdacht einer Pharming-, Phishing- oder ähnlichen Attacke umgehend informieren, um ein mögliches Eigenverschulden in der Berechnung des späteren Schadensersatzanspruchs auszuschließen

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Im vorliegenden Fall war die Frage zu klären, welche Partei (Bank oder Bankkonto-Inhaber) dafür einzustehen hat, dass aufgrund der mutmaßlichen Einmischung Dritter die Bank zu einer Überweisung angewiesen wurde, die nicht durch den Bankkunden veranlasst worden war. Der Bankkunde nutze das TAN-Listen-Verfahren.

Vorliegend musste die Bank den überwiesenen Betrag zurückerstatten.

Ohne wirksames Angebot des Kunden auf Abschluss eines Überweisungsvertrags kann das Konto des Kunden nicht belastet werden, da es an einer Weisung fehlt.

Das Fälschungsrisiko des Überweisungsauftrags trägt [grundsätzlich] die Bank.

Eine Rechtsscheinhaftung ist, aufgrund der Unsicherheit des TAN-Verfahrens, nicht gegeben.

Der Bankkunde war auch den eigenen Sorgfaltsanforderungen für die Absicherung seines Computers nachgekommen.

Im Ergebnis kann die Bank von ihren Kunden erwarten, dass diese einem den allgemeinen, an dem Verhalten eines durchschnittlichen PC-Benutzers orientierten Personalcomputer für die Benutzung des Onlinebanking verwenden.

Auch den (nicht als zwingend bestätigten) Sorgfaltsanforderungen an die Reaktion nach der Überweisung hatte der Bankkunde entsprochen.

[Es] spricht vieles dafür, dass ein Bankkunde, nachdem er von einem Angriff eines Dritten auf seine Daten Kenntnis erlangt, die Nebenpflicht hat, die Bank über den Angriff zu informieren.

Aufgrund der Tatsache, dass das System anschließend weiterlief und nicht abstürzte, obwohl das häufig passiert, und die Zeugin (die Ehefrau des Bankkunden) eine nachvollziehbare Erklärung für den Vorgang geben konnte, kann von der Verletzung einer Nebenpflicht nicht ausgegangen werden.

ANMERKUNGEN

Das Gericht äußerte sich, wenn auch nicht entscheidungserheblich, zu der Frage, ob bei Autorisierung des Zahlungsauftrags unter Verwendung von PIN, TAN und sonstigen „richtigen“ Zugangsdaten ein Anscheinsbeweis zu Gunsten der Bank greifen kann, dass die Überweisung durch den Bankkonto-Inhaber getätigt wurde. Nach Ansicht des Gerichtes kann das alleine im Online-Banking und bei Nutzung des sog. iTAN-Verfahrens keinen Anscheinsbeweis begründen. Vielmehr sei zu beachten, dass aufgrund der Vorgehensweise im Bereich der Online-Kriminalität und der Menge an Angriffen, Bankkunden oft nicht erkennen könnten, Opfer einer solchen Attacke geworden zu sein.

Das Gericht ging umfangreich auf mögliche Sicherungsmechanismen ein. Es ging aber auch davon aus, dass die Kunden alles, was von einem durchschnittlichen Kunden zu erwarten wäre (namentlich die Verwendung eines gängigen Virenschutzprogramms), getan hätten. Die Bank dürfe im Übrigen das Missbrauchsrisiko nicht durch zu hohe Schutzvorschriften gänzlich von sich abwälzen.

Es entspricht, laut dem Gericht, nicht den Anforderungen an einen durchschnittlichen Computernutzer, dass dieser ein kostenpflichtiges Virenschutzprogramm verwendet. Die Nutzung eines kostenlos verfügbaren

Programms genüge grundsätzlich.

Dem Kunden kann nicht zur Last gelegt werden, wenn er unter den angebotenen TAN-Verfahren dasjenige wählt, welches am unsichersten ist.

Praxishinweis: Das Gericht ließ ungeklärt, ob die in dieser Entscheidung festgestellten niedrigen Anforderungen an die Nutzung des TAN-Verfahrens im Online-Banking auch für die moderneren Systeme wie iTAN oder mTAN gelten (vgl. jurisPR-BKR 4/2008 Anm. 6).