

Manipulationsmöglichkeiten beim Smart-TAN-plus-Verfahren im Onlinebanking und daraus resultierende Kriterien für unautorisierte Zahlungsvorgänge hierüber

Gericht

LG Darmstadt

Datum

28.08.2014

Aktenzeichen

28 O 36/14

Branche/ Lebenslage

Online-Banking, Man-in-the-Middle-Angriff, Smart-TAN-plus-Verfahren

Akteure

Bankkonto-Inhaber, Bank

Wer haftet?

Bankkonto-Inhaber

Haftungsart

Schadensersatz

Haftungsumfang

Verfahrenskosten

Haftungsbegründendes Verhalten

Der Kunde hätte sich vergewissern müssen, dass die angegebene TAN zur Autorisierung eines gewünschten Zahlungsvorgangs (mit dem korrekten Zahlungsempfänger) generiert wurde

Technische Umstände

Die Eingabe der korrekten TAN führte zur Autorisierung des Zahlungsauftrags

Persönliche Umstände

Der Kunde hätte selbst darauf achten müssen, dass Zahlungsempfänger auf dem TAN-Gerät und Zahlungsempfänger der eigentlich gewollten Überweisung übereinstimmen

Möglichkeiten der Haftungsvermeidung

Kunden sollten grundsätzlich die Überweisungsdaten, die mit der Versendung der TAN durch die Bank bestätigt werden, zur Kenntnis und überprüfen, bevor ein Vorgang endgültig durch die Eingabe der TAN autorisiert wird; Banken ist weiterhin zu raten, die Verpflichtung des Kunden, den Überweisungszweck zu prüfen, vertraglich zu vereinbaren

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Die Klägerin verlangt von der Bank die Erstattung von Überweisungszahlungen zu Lasten ihres Kontos, die nicht durch die Klägerin in Auftrag gegeben wurden. Die Klägerin hatte das sog. Smart-TAN-plus-Verfahren verwendet.

Begriffserklärung Smart-TAN-plus: Bei diesem Verfahren werden zunächst die Überweisungsdaten in eine Online-Maske der Bank eingegeben. Die Autorisierung der Überweisung erfolgt mittels EC-Karte und TAN-Generator. Über eine auf dem Bildschirm auftauchende Grafik können die Überweisungsdaten mittels eines optischen Lesegeräts am TAN-Generator auf diesen übertragen werden. Der TAN-Generator erstellt daraufhin eine TAN, die der Bankkunde anschließend in die Online-Maske eingibt.

Die Klägerin hatte zur Autorisierung einer geplanten Überweisung nicht das Übereinstimmen des auf dem TAN-Generator angezeigten Empfängers mit dem beabsichtigten Empfänger überprüft.

Das Gericht lehnte einen Rückzahlungsanspruch der Bankkundin unter Anwendung der Grundsätze des Anscheinsbeweises ab. Die Kundin hätte die Angaben auf dem TAN-Generator überprüfen müssen:

Gem. § 675u S. 2 BGB ist der Zahlungsdienstleister verpflichtet, das Zahlungskonto des Zahlers im Falle eines nicht autorisierten Zahlungsvorganges wieder auf den Stand zu bringen, den es ohne die nicht autorisierte Belastung hätte.

Die Voraussetzungen des § 675u S. 2 BGB liegen [jedoch] nicht vor.

Für die Autorisierung des Zahlungsvorganges ist die Beklagte [Bank] als Zahlungsdienstleister darlegungs- und beweisbelastet, § 675w S. 1 BGB.

[...] beim Online-Banking erbringt der Zahlungsdienstleister den Nachweis der Authentifizierung gem. § 675w S. 2 BGB, wenn er belegt, dass Kundenkennung, PIN und TAN überprüft wurden.

Es sind jedoch immer auch die Umstände des Einzelfalls zu berücksichtigen.

Die Klägerin hat ihr Einverständnis zu den beiden streitgegenständlichen Zahlungsvorgängen zwar nicht selbst erteilt, sondern wurde Opfer eines sog. „Man-in-the-Middle-Angriffs“. Ihr ist die mittels des Zahlungsauthentifizierungsinstruments PIN und TAN erteilte Zustimmung des „Angreifers“ zu den manipulierten Zahlungsvorgängen jedoch nach Rechtsscheinsgrundsätzen zuzurechnen.

Begriffserklärung „Man-in-the-Middle-Angriff“: Bei diesem Angriff schaltet sich ein Dritter unbemerkt in die Kommunikation zweier Kommunikationspartner ein, um an Informationen zu gelangen oder eine [Verschlüsselung](#) auszuhebeln.

Die Klägerin hätte den „Man-in-the-Middle-Angriff“ erkennen und verhindern können.

Das hohe Sicherheitsniveau des Smart-TAN-plus-Verfahrens rechtfertigt diese Ansicht:

Das Smart-Tan-plus-Verfahren weist eine hohe Systemsicherheit auf. Aus technischer Sicht ist es nach derzeitigem Stand so gut wie ausgeschlossen, dass bei Verwendung dieses Verfahrens tatsächlich erfolgte Online-Überweisungen nicht von dem Bankkunden selbst vorgenommen wurden.

ANMERKUNGEN

Die Feststellungen des Gerichts sind vergleichbar mit den Überlegungen des AG Köln, 28.05.2014, Az. 113 C 662/13. Bei bestimmten, sichereren TAN-Verfahren, kann ein Rechtsschein zu Gunsten der Bank angenommen werden, dass bei korrekter Eingabe der TAN eine Autorisierung durch den Kunden vorliegt. Das LG Darmstadt ging in der vorliegenden Entscheidung explizit von einem entsprechenden Anscheinsbeweis aus.

Zum Anscheinsbeweis: Das Gericht legte nahe, dass der Rechtsschein der korrekten Autorisierung womöglich eine gewisse Häufigkeit und Dauer von fälschlich getätigten Überweisungen voraussetzt. Bei zumindest zwei solcher Überweisungen soll das allerdings bereits vorliegen.

Das LG Köln (26.08.2014, 3 O 390/13) stufte in einer Entscheidung ein ähnliches Verhalten eines gewerblichen Kunden zudem als grob fahrlässig ein.

Es genügte nicht, dass der benutzte Rechner des Bankkunden (Geschäftsführers) mit einem Virenschutzprogramm und einer Firewall gesichert war. Der Vorwurf an den Kunden lag in der ausbleibenden Kenntnisnahme der mit der TAN angezeigten Überweisungsdaten, mit denen er hätte erkennen können, dass ein ungewollter Zahlungsauftrag autorisiert werden sollte.

Praxishinweis: Grundsätzlich scheint die Rechtsprechung dazu zu tendieren, bei entsprechend hohem Sicherheitsstandard des ausgewählten TAN-Verfahrens einen Anscheinsbeweis der korrekten Autorisierung zu Gunsten der Bank anzunehmen, wenn diese nachweisen kann, dass die Autorisierungsdaten überprüft und korrekt verwendet wurden.