

Verpflichtung zur Nutzung aktueller Virenschutzsoftware, einer Firewall und Durchführung regelmäßiger Updates bei Online-Banking; Haftung bei Phishing-Attacken

Gericht

LG Köln

Datum

05.12.2007

Aktenzeichen

9 S 195/07

Branche/ Lebenslage

Online-Banking, Schadprogramme, Virenschutz, Firewall, Phishing

Akteure

Bankkonto-Inhaber (Phishing-Opfer), Bankkonto-Inhaber (Klagegegner)

Wer haftet?

Bankkonto-Inhaber (Klagegegner)

Haftungsart

Schadensersatz

Haftungsumfang

Schadensersatz, Verfahrenskosten

Haftungsbegründendes Verhalten

Überweisung einer Geldsumme, die in Folge einer Phishing-Attacke fälschlicherweise auf das eigene Konto gelangt ist. an eine unbekannte Person

Technische Umstände

Versendung des Geldes an unbekannte Dritte erschwerte die Rückgängigmachung der ursprünglichen, aufgrund einer Phishing-Attacke fälschlichen Überweisung

Persönliche Umstände

Der Beklagte handelte leichtfertig, als er fälschlicherweise auf sein Konto transferiertes Geld an eine unbekannte Person im Ausland weiterleitete; er erkannte leichtfertig nicht, dass das weitergeleitete Geld nicht mit Wissen und Wollen des eigentlichen Berechtigten überwiesen wurde

Möglichkeiten der Haftungsvermeidung

Bankkonten-Inhaber sollten vor der Weiterleitung oder „Rücküberweisung“ ihnen grundlos zugeschickter Gelder die Herkunft des Geldes überprüfen bzw. die Bank oder den ursprünglichen Geldinhaber benachrichtigen;

Nutzern des Online-Banking ist auch zur Vorbeugung möglicher Haftungsrisiken gegenüber Dritten zu raten, eine aktuelle Virenschutzsoftware und Firewall zu nutzen und diese regelmäßig zu aktualisieren

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Vom Konto des Klägers waren Gelder abgebucht und auf das Konto des Beklagten übertragen worden. Dieser hatte aufgrund der Täuschung durch eine fremde Person die Gelder abgehoben und an ein Konto in Russland weitergeleitet. Der Kläger verlangte diese Gelder zurück.

Das Gericht entschied, dass sich der Beklagte einer Geldwäsche, § 261 Abs. 2 Nr. 1, Abs. 5 [StGB](#) strafbar gemacht hatte, da sich ihm der kriminelle Hintergrund der überwiesenen Gelder hätte aufdrängen müssen. Er war daher auch dem Kläger zum Schadensersatz verpflichtet. Es sei kein Grund ersichtlich gewesen, warum der Kläger an den Beklagten Gelder hätte überweisen sollen.

Konkret im Rahmen der Geldwäsche ist Leichtfertigkeit anzunehmen, wenn sich die dubiose Herkunft des Geldes aufdrängt und der Täter dies aufgrund besonderer Unachtsamkeit oder Gleichgültigkeit außer Acht lässt und vor etwaigen Zweifeln die Augen verschließt.

Wenn der Beklagte wirklich ernsthaft um eine Klärung der Rechtmäßigkeit der Geldtransfers bemüht gewesen wäre, wäre es ein Leichtes gewesen, sich an die Inhaber der Konten, von denen die Überweisungen stammten, zu wenden.

Dem Kläger machte das Gericht keinen Vorwurf, der zu einer Reduzierung des Schadensersatzes hätte führen können. Es sei nicht davon auszugehen, dass der Kläger durch unzureichende eigene Sicherungsmechanismen zur Verursachung des Schadens beigetragen hätte. Das Gericht hielt es hinsichtlich des Verschuldensvorwurfs gegenüber dem Kläger für entscheidend, wie die Täter an die Kontodaten des Klägers gekommen sind (und welche Sorgfaltsanforderungen den Kläger als Nutzer von Internet und Online-Banking gegenüber dem Beklagten traf).

Der Kläger hat schlüssig vorgetragen, Opfer eines Computerbetruges gemäß § 263a Abs. 1 StGB geworden zu sein. Nach seinem Vortrag haben unbekannte Täter sich seine Kontodaten nebst PIN und TAN beschafft, indem sie diese Daten entweder auf seinem Heimcomputer oder dem Zentralrechner seiner Bank ausspioniert haben, und diese unbefugt benutzt, um die streitgegenständliche Überweisung zu veranlassen. Dieser Vortrag ist als unstrittig zu behandeln.

Für den konkreten Fall des Online-Bankings kann man von einem verständigen, technisch durchschnittlich begabten Anwender fordern, dass er eine aktuelle Virenschutzsoftware und eine Firewall verwendet und regelmäßig Sicherheitsupdates für sein Betriebssystem und die verwendete Software einspielt.

Solange nicht nachgewiesen werden könne, dass der Geschädigte selbst, aufgrund unzureichender Sicherungsvorkehrungen, zumindest teilweise für die Schädigung verantwortlich war, sei ein solcher Vorwurf auch nicht zu machen.

ANMERKUNGEN

Der Entscheidung des Gerichts entsprechend ist es grundsätzlich nicht ausgeschlossen, dass das Opfer einer fälschlichen Überweisung den Vorwurf treffen kann, an ihn zu stellende Sorgfaltsanforderungen außer Acht gelassen zu haben. Daher sind Kunden nicht nur im Verhältnis zur Bank dazu verpflichtet, einen Mindeststandard an Sicherungsvorkehrungen zu treffen, um unbefugten Überweisungsvorgängen vorzubeugen. Aufgrund regelmäßig fehlender vertraglicher Verbindungen zu dritten Bankkunden trifft den Bankkonto-Inhaber, dem Gericht nach, allerdings nur eine allgemeine Sicherungspflicht. Für das LG Köln beinhaltet das aber auch,

dass der Nutzer des Online-Bankings eine aktuelle Virenschutzsoftware und eine Firewall verwendet und regelmäßig Sicherheitsupdates für sein Betriebssystem und die verwendete Software einspielt.

Beweislast: Dass der klagende Geschädigte selbst einen Sorgfaltspflichtverstoß begangen hat, ist von Seiten des Beklagten nachzuweisen. Streitet der Geschädigte eine eigene Mitwirkungshandlung ab, kann der Beklagte einen Beweisantrag hinsichtlich möglicher Spuren auf dem Rechner des Geschädigten stellen.

Haftungsrisiko: Neben einem zivilrechtlichen Anspruch gegenüber dem eigentlichen Geldinhaber kann bei der Weiterleitung an unbekannte Konten im Ausland eine Strafbarkeit wegen Geldwäsche (§ 261 StGB) entstehen.