Landgericht Köln, 9 S 195/07

Datum:	05.12.2007
Gericht:	Landgericht Köln
Spruchkörper:	9. Zivilkammer
Entscheidungsart:	Urteil
Aktenzeichen:	9 S 195/07
ECLI:	ECLI:DE:LGK:2007:1205.9S195.07.00

Vorinstanz:	Amtsgericht Bergisch Gladbach, 68 C 353/06

Tenor:

Auf die Berufung des Klägers wird das Urteil des Amtsgerichts Bergisch Gladbach vom 03.07.2007 – 68 C 353/06 – abgeändert und wie folgt neu gefasst:

Der Beklagte wird verurteilt an den Kläger 3.137,33 € nebst 5% Zinsen über dem Basiszinssatz seit dem 03.06.2006 zu zahlen.

Die Kosten des Rechtsstreits erster und zweiter Instanz trägt der Beklagte.

Das Urteil ist vorläufig vollstreckbar.

Von der Darstellung des Tatbestandes wird gemäß §§ 540 Abs. 2, 313a Abs. 1 Satz 1 ZPO abgesehen.

Begründung: 1

Die zulässige Berufung des Klägers hat auch in der Sache Erfolg, denn das Amtsgericht hat die Klage zu Unrecht abgewiesen. 2

Das Amtsgericht hat zwar zu Recht und mit zutreffender Begründung einen Bereicherungsanspruch des Klägers abgelehnt. Der Kläger hat gegen den Beklagten jedoch 3

einen Anspruch auf Zahlung von 3.137,33 € nebst Zinsen aus §§ 823 Abs. 2 BGB i.V.m. § 261 Abs. 2, 5 StGB. Der Beklagte hat das vom Konto des Klägers aufgrund eines Computerbetrugs gemäß § 263a Abs. 1 StGB auf sein Konto überwiesene Geld (1.) leichtfertig an eine unbekannte Person in Russland transferiert und sich damit der Geldwäsche schuldig gemacht (2.). Dadurch hat er ein Schutzgesetz im Sinne von § 823 Abs. 2 S. 1 BGB verletzt (3.) und bei dem Kläger einen Vermögensschaden verursacht (4.). Ein Mitverschulden fällt dem Kläger nicht zu Last (5.).

1. 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 unstreitig zu behandeln. 4

Der Beklagte bestreitet lediglich mit Nichtwissen, dass die Überweisung ohne Wissen und Wollen des Klägers erfolgt sei. Dies reicht nicht aus: Schon der Umstand, dass das Konto des Beklagte unstreitig von einem oder mehreren unbekannten Tätern vermutlich osteuropäischer Herkunft zum Transfer von Geldern verwendet worden ist und es sich unstreitig in den beiden weiteren Fällen um Geld von Kontoinhabern handelt, die Opfer von Betrügern geworden sind, spricht dafür, dass auch in vorliegendem Fall die Überweisung des Klägers nicht durch diesen selbst, sondern durch kriminelle Dritte veranlasst worden ist. Es ist auch kein Grund ersichtlich, warum der Kläger Geld an den Beklagten hätte überweisen bzw. eine Überweisung durch Dritte bewusst hätte zulassen sollen. Angesichts dessen wäre von dem Beklagten jedenfalls ein substanziiertes Bestreiten des Klägervortrags zu fordern, worauf die Kammer den Beklagten auch mit der Terminierung hingewiesen hat. Hieran fehlt es. 5

Durch die Überweisung auf das Konto des Beklagten ist das Vermögen des Klägers geschädigt worden. Auf die noch zu erörternde Frage eines ersatzfähigen Schadens im Sinne von § 249 Abs. 1 BGB kommt es insoweit nicht an, weil es für das Vorliegen eines Vermögensschadens im strafrechtlichen Sinne auf eine wirtschaftliche Betrachtungsweise ankommt und auch eine konkrete Vermögensgefährdung ausreicht. Eine konkrete Gefährdung des Vermögens des Klägers ist durch die Überweisung aber in jedem Fall eingetreten, ohne dass es darauf ankommt, ob ihm gegebenenfalls auch ein Anspruch gegen seine Bank auf Gutschrift des Betrages zusteht. 6

An dem vorsätzlichen Handeln der Täter, ihrer Absicht, sich rechtswidrig zu bereichern, und an der Rechtswidrigkeit des Computerbetrugs bestehen keine Zweifel. 7

2. Indem der Beklagte das Geld per Western Union an eine Person in Russland, die ihm gegenüber den Namen M verwendete (im Folgenden "M" genannt), weitergeleitet hat, hat er sich einer Geldwäsche gemäß § 261 Abs. 2 Nr. 1, 5 StGB schuldig gemacht. 8

a) Der Beklagte hat Geld, das aus einer Katalogtat des § 261 Abs. 1 Nr. 4 StGB stammt – nämlich dem Computerbetrug zum Nachteil des Klägers – einem Dritten verschafft. Dass der oder die Täter gewerblich handelten, ergibt sich ohne weiteres daraus, dass das Konto des Beklagten für insgesamt drei entsprechende Weiterleitungen missbraucht wurde und die Täter – wie der Beklagte in der mündlichen Verhandlung erklärt hat – noch weitere Überweisungen angekündigt hatten. 9

b) An der Rechtswidrigkeit des Verhaltens des Beklagten bestehen keine Zweifel. 10

c) Der Beklagte hat auch leichtfertig nicht erkannt, dass das Geld aus einem Computerbetrug stammt. 11

aa) Leichtfertigkeit im strafrechtlichen Sinne bedeutet einen erhöhten Grad von Fahrlässigkeit, vergleichbar der zivilrechtlichen groben Fahrlässigkeit, wobei im Strafrecht auch die persönlichen Fähigkeiten des Täters zu berücksichtigten sind. Sie kommt in Betracht, wenn der Täter grob unachtsam nicht erkennt, dass er den objektiven Tatbestand verwirklicht oder sich rücksichtslos über die klar erkannte Möglichkeit der Tatbestandsverwirklichung hinwegsetzt (Tröndle-Fischer, StGB, § 15, Rn. 20). 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. Ein wesentlicher Faktor für die Frage, ob Leichtfertigkeit anzunehmen ist, ist auch der Wert des Tatobjekts. Während bei hohen Werten eher zu erwarten ist, dass der Handelnde sich Gedanken über die Herkunft des Geldes macht, kann er bei niedrigen Werten, insbesondere bei Alltagsgeschäften des täglichen Lebens eher darauf vertrauen, dass das Geld redlich erworben wurde (vgl. Tröndle-Fischer, StGB, § 261, Rn. 17; Schönke-Schröder-Stree, StGB, § 261, Rn. 19 jeweils m.w.Nw.). 12

bb) Im vorliegenden Fall lag für den Beklagten bei objektiver Betrachtung auf der Hand, dass das Geld nicht, wie von seiner E-Mail-Bekanntschaft, die sich N nannte (im Folgenden "N" genannt) angegeben, aus einer Erbschaft zu deren Gunsten, sondern aus kriminellen Machenschaften stammen musste. Es gab zahlreiches Anhaltspunkte, aus denen der Beklagte hätte schließen können und müssen, dass er lediglich als Handlanger krimineller Machenschaften missbraucht wurde: 13

"N" erklärte bereits nach einer sehr kurzen Kennenlernphase, in der ausschließlich E-Mails ausgetauscht wurden, den Beklagten zu lieben. Dass sich eine derart tiefe emotionale Beziehung zu einer Person nicht in wenigen Tagen per E-Mail begründen lässt, liegt auf der Hand. Es lag daher von Anfang an nahe, dass "N" nur versuchte, das Vertrauen des Beklagten zu gewinnen. 14

Vergleichbare Betrügereien, bei denen den Personen deren Konto verwendet wird (sogenannte Finanzagenten), aber im Regelfall eine finanzielle Beteiligung an den zu transferierenden Geldern versprochen wird, sind seit langem bekannt und Gegenstand häufiger Meldungen in den Medien. Am bekanntesten ist wohl die schon in der "analogen" Zeit per Fax aufgekommene "O Connection", bei der dem Kontoinhaber erklärt wird, man benötige sein Konto, um Geldaus einem – im Regelfall krisengeschüttelten – Land zu transferieren und ihm eine hohe prozentuale Beteiligung verspricht. Ziel dieser Betrügereien in ihrer ursprünglichen Form war es allerdings, den Empfänger des Faxes (später der E-Mail) dazu zu veranlassen, eine Art Anschubfinanzierung an die Täter zu leisten. Die Kammer verkennt nicht, dass der vorliegende Fall sich dem gegenüber durch ein deutlich subtileres, nicht einmal an die Geldgier des Kontoinhabers, sondern seine persönlichen Gefühle appellierendes Vorgehen der Täter auszeichnet. 15

Die eingehenden Gelder stammten nicht von einem Konto, sondern von drei verschiedenen, die auch nicht etwa den gleichen, sondern wiederum drei verschiedene Kontoinhaber aufwiesen. Da es sich um Geld des angeblich verstorbenen Vaters von "N" handeln sollte, wäre zu erwarten gewesen, dass Geld von einem Konto einer Person namens N überwiesen wird, aber nicht von drei unterschiedlichen Personen. Die vom Beklagten angeführte Erklärung, er sei davon ausgegangen, dass es sich um die Erwerber der Wertpapiere handele, erscheint wenig überzeugend: Wertpapiere werden üblicherweise an der Börse 16

gehandelt. Der Verkauf von Wertpapieren zwischen Privatpersonen wäre daher bereits für sich genommen auffällig.

Einen nachvollziehbarer Grund, warum zum Transfer des Geldes das Konto des Beklagten benötigt werde, hat "N" nicht angegeben. Selbst wenn man als richtig oder jedenfalls nicht evident falsch unterstellt, dass, wie von "N" in der E-Mail vom 27.02.2006 behauptet, in Russland die Währung Euro verboten wäre, wäre das Konto des Beklagten nicht benötigt worden. Denn angeblich sollte "M" als von "N" beauftragter Börsenmakler Wertpapiere von deren verstorbenem Vater in Deutschland verkaufen. Die Erlöse sollten dann auf das Konto des Beklagten überwiesen und dann von diesem per Western Union nach Russland transferiert werden. Warum "M" diesen Transfer nicht selbst von dem oder den Konten vornehmen konnte, auf denen sich die Erlöse der Wertpapiere befanden, wird nicht erklärt und ist auch nicht nachvollziehbar. Selbst bei einem Verkauf von Wertpapieren nicht im Börsenhandel, sondern unmittelbar an private Käufer, hätte es näher gelegen, dass die Käufer den Kaufpreis unmittelbar an "M" entrichten. 17

Schließlich ist auch die Verwendung von Western Union für den Geldtransfer verdächtigt. Es ist kein Grund ersichtlich, warum das Geld nicht per Auslandsüberweisung auf ein Konto des angeblichen Börsenmaklers "M" transferiert werden konnte. Ein Anlass für die Verwendung eines Weges, der eine anonyme Geldübermittlung ermöglicht, war nicht gegeben. 18

Dass der Beklagte all diese Umstände ignoriert hat, kann in der Gesamtschau nur als besonders unachtsam bezeichnet werden. 19

Es sind auch keine Gründe vorgetragen oder sonst ersichtlich, warum der Beklagte persönlich nicht in der Lage gewesen sein sollte, diese Umstände zu erkennen und deren Bedeutung nachzuvollziehen. Im Gegenteil, der Beklagte hat in der mündlichen Verhandlung selbst eingeräumt, er sei ab dem Moment, in dem "N" Geld in Spiel gebracht habe, misstrauisch geworden und habe sich fortan ständig Gedanken darüber gemacht, was er tun solle. Dementsprechend hat der Beklagte "N" um Belege für die Rechtmäßigkeit der Transaktionen gebeten. Hierauf hat er eingescannte Dokumente in kyrillischer Schrift erhalten, die er von einer der russischen Sprache mächtigen Rechtsanwältin prüfen ließ. Dabei soll es sich nach seinem unwidersprochen gebliebenen Vortrag um eine Lizenz für Wertpapiergeschäfte sowie einen Vertrag zwischen "N" und "M" handeln, wonach dieser Wertpapiere für "N" veräußern sollte. Inwieweit sich hieraus ergeben soll, dass die Überweisungen auf sein Konto rechtmäßig erfolgten und das Geld "N" zustand, erläutert der Beklagte indessen nicht. 20

Nach seinen Angaben in der mündlichen Verhandlung hat der Beklagte auch mit Freunden über die Angelegenheit gesprochen, die ihm teilweise geraten hätten, sein Konto nicht zur Verfügung zu stellen. Er habe sich letztlich aber gedacht, wenn die Überweisungen nicht in Ordnung wären, würden sich die Kontoinhaber schon melden. Dies lässt sich indessen nicht damit in Übereinstimmung bringen, dass der Beklagte jedenfalls im vorliegenden Fall das Geld sofort am Tag nach der Gutschrift auf sein Konto nach Russland transferiert hat. Selbst ein Geschädigter, der täglich sein Konto kontrolliert, hätte kaum eine Chance gehabt, binnen eines Tages eine Rückbuchung des Betrages zu veranlassen oder den Beklagten zu kontaktieren. 21

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. Der Beklagte hat dagegen nicht einmal versucht, die Identität von "N" zu überprüfen. 22

3. Indem er sich einer Geldwäsche schuldig gemacht hat, hat der Beklagte ein Schutzgesetz verletzt. § 261 StGB schützt entgegen der Ansicht des Amtsgerichts auch das durch die Vortat verletzte Rechtsgut, hier also das Vermögen des Klägers (vgl. LK-Ruß, StGB, 11. Auflage, § 261, Rn. 4; Tröndle-Fischer, StGB, 54. Auflage, § 261, Rn. 3 jeweils m.w.Nw.). 23

4. Dem Kläger ist hierdurch auch ein Schaden entstanden. 24

Entgegen der im Beschluss der Kammer vom 02.08.2007 vertretenen Auffassung ist durch die unbefugte Überweisung des streitgegenständlichen Betrages vom Konto des Klägers auf das Konto des Beklagten, auch ein ersatzfähiger Schaden im Sinne von § 249 Abs. 1 BGB entstanden. Dies gilt unabhängig von der Frage, ob der Kläger einen Anspruch auf Gutschrift des Betrages gegen seine Bank hat. Nach der Rechtsprechung des BGH stünde auch der Umstand, dass der Kontostand des Klägers durch die Überweisung materiell nicht vermindert worden ist, weil die Bank grundsätzlich das Fälschungsrisiko im Überweisungsverkehr trägt, der Annahme eines ersatzfähigen Schadens im Sinne von § 249 BGB nicht entgegen. Allein durch die unrichtige Kontobelastung ist die Möglichkeit des Klägers, über sein Vermögen zu verfügen in einer Weise eingeschränkt, die sich als vermögensrechtlicher Nachteil darstellt (BGH, Urteil vom 31.05.1994 – VI ZR 12/94 –). 25

Durch die Geldwäsche des Beklagten, also den Transfer des Geldes nach Russland, ist der durch den Computerbetrug entstandene Schaden weiter vertieft worden, weil eine einfache Rückbuchung durch die Bank des Klägers nach der Verfügung des Beklagten über den Betrag nicht mehr möglich war (vgl. Palandt-Heinrichs, BGB, Vorb v § 249, Rn. 19). 26

5. Ein Mitverschulden bei der Entstehung des Schadens oder im Rahmen seiner Pflicht zur Schadensabwendung oder -minderung gemäß § 254 Abs. 1 BGB trifft den Kläger nicht. 27

Ob dem Kläger ein Verschuldensvorwurf gemacht werden kann, weil er die unbefugte Überweisung durch aktives Tun oder das Unterlassen der erforderlichen Sicherheits- und Vorsichtsmaßnahmen ermöglicht hat, hängt davon ab, 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 trafen. 28

a) Grundsätzlich hatten die Täter eine Reihe verschiedener Möglichkeiten, die Sicherheitsmechanismen der Bank des Klägers auszuschalten oder zu umgehen (vgl. zusammenfassend etwa Bundesverband deutscher Banken (Hrsg.), Online-Banking-Sicherheit; die Internetseiten der Arbeitsgruppe Identitätsschutz im Internet (anonym1); Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik (anonym2, anonym3); Erfurth, WM 2006, 2198 ff., wobei die verschiedenen Angriffsmethoden teilweise unterschiedlich bezeichnet werden): 29

aa) Die Sicherstellung, dass ein online erteilter Überweisungsauftrag von einer berechtigten Person stammt, erfolgt bei der Bank des Klägers unstreitig durch PIN und TAN. Beim sogenannten PIN/TAN-Verfahren ist die PIN eine Zahlenkombination, die erforderlich ist, um sich per Internet-Browser auf den Online-Banking-Seiten der Bank für den Zugriff auf ein bestimmtes Konto zu authentifizieren. Diese PIN wird dem Kontoinhaber durch die Bank mitgeteilt. Für jede einzelne Transaktion ist sodann die Eingabe einer Transaktionsnummer (TAN) erforderlich. Der Kontoinhaber erhält von der Bank eine Liste von TANs, die jeweils einmal verwendet werden können, wobei die Einhaltung einer Reihenfolge nicht erforderlich ist (anders bei den sogenannten iTANs – Angabe einer bestimmten TAN aus der nummerierten Liste erforderlich –, eTANs – TAN wird durch Kunden bei Bedarf in elektronischem Zufallsgenerator, der von der Bank zur Verfügung gestellt wird, erzeugt – und 30

mTANs – TAN wird dem Kunden auf Anforderung per SMS übersandt –, die vorliegend jedoch nicht in Rede stehen).

Um zu verhindern, dass Dritte den Datenverkehr zwischen Bank und Kunden "abhören", werden die Verbindungen automatisch verschlüsselt (je nach verwendetem Internet-Browser und Bank unterschiedlich stark, aktuell zwischen 128 und 256 bit), was dadurch erkennbar ist, dass die Internetadresse statt mit http:// mit http**s**:// beginnt und in der Statusleiste am unteren Rand des Internet-Browsers ein Schlosssymbol angezeigt wird. Die Verwendung des https-Protokolls ermöglicht zugleich eine Authentifizierung der Internetseite als echte Seite der Bank über ein Zertifikat. Ist das Zertifikat ungültig, erscheint bei den üblichen Internet-Browsern eine Warnmeldung. 31

bb) Um unbefugt an die Kontodaten nebst PIN und TAN eines Kontoinhaber zu gelangen gibt es verschiedene Möglichkeiten: 32

Die Täter können sich die Daten physisch verschaffen, indem sie die Post des Kontoinhabers unbefugt öffnen oder bei diesem einbrechen. Das unbemerkte Öffnen der Post wird durch die Gestaltung der PIN- und TAN-Sendungen in aufreißbaren Umschlägen praktisch unmöglich gemacht, weil es bei Eintreffen der Schreiben beim Kontoinhaber auffällt. Außerdem werden PIN und TAN-Liste in unterschiedlichen Schreiben versandt, die im Regefall wiederum nicht die vollständige Kontonummer enthalten. 33

Nach dem insoweit übereinstimmenden Vortrag der Parteien scheidet vorliegend ein solches Vorgehen der Täter aus. 34

Die Täter verschaffen sich Zugang zum Zentralrechner der Bank des Kontoinhabers, was aufgrund der hohen Sicherheitsmaßnahmen der Banken schwierig, wenn auch nicht unmöglich ist. Da ein erfolgreicher Angriff meist zahlreiche Bankkunden betrifft, wird er im Regelfall auch öffentlich bekannt werden. 35

Die Täter spionieren die Daten mittels sogenannter Malware (Viren, Trojaner etc.) aus, die heimlich auf dem Computer des Kontoinhabers installiert wird (meistens über das Öffnen von per E-Mail versandter Dateien oder den Besuch einer Internetseite, die schädlichen Code enthält). Diese wertet die Eingaben des Computernutzers aus und übermittelt sie an die Täter. Dies ist auch bei gesicherten Verbindungen möglich. Um eine nicht verbrauchte TAN zu erlangen, gibt es sogar Programme, die nach Eingabe der TAN die Verbindung zur Bank unterbrechen (sogenannte Abbruch-Trojaner). 36

Schutz vor dieser Art des Angriffs können Virenschutzprogramme bieten, die allerdings regelmäßig (meist täglich) aktualisiert werden müssen, weil auch die schädlichen Programme schnell variiert und weiterentwickelt werden. Eine Firewall verhindert, dass Malware Daten über das Internet versendet oder dass Hacker unbefugten Zugriff auf den Computer des Nutzers nehmen. 37

Malware hinterlässt stets Spuren auf dem infizierten Computer, nämlich zumindest das Schadprogramm selbst. 38

Die Täter lassen sich die Daten vom Kontoinhaber mitteilen. Hierzu gibt es wiederum verschiedene Ansätze: 39

Der aktuell bekannteste Weg ist wohl das sogenannte Phishing, bei dem die Täter versuchen, E-Mails einer Bank nachzuahmen und die Kunden auffordern, ihr Konto – meist aus 40

angeblichen Sicherheitsgründen – durch Eingabe von Kontonummer, PIN und mehreren TANs neu freizuschalten. Im einfachsten Fall wird der Kunde aufgefordert, die Daten in ein Formular in der E-Mail einzutragen oder als Antwort zurückzusenden. Üblicher und erfolgversprechender ist der Weg über einen in der E-Mail integrierten Link auf eine Internetseite, welche die Täter so gestaltet haben, dass sie der Seite der Bank ähnelt (sogenanntes Visual Spoofing), auf der dann die geforderten Daten einzugeben sind. Waren früher die E-Mails und die gefälschten Internetseiten durch sprachliche Fehler und optische Mängel geprägt und daher leicht erkennbar, verwenden die Täter inzwischen teilweise täuschend echte E-Mails und Internetseiten, die auch von aufmerksamen Betrachtern nur schwer als gefälscht zu erkennen sind.

Einen gewissen Schutz bieten Spam-Filter, die anhand von bestimmten Kriterien unter anderem gefälschte Mails erkennen und entweder schon auf dem Mailserver oder auf dem Computer des Nutzers herausfiltern. Auch die gefälschten Internetseiten sind zu erkennen, weil im Regelfall die Adresse in der Adressleiste nicht die der Bank sein wird (oft ist sie aber nur geringfügig abgewandelt), die Verschlüsselung nicht aktiviert ist und die Seite kein gültiges, von der Bank herausgegebenes Authentifizierungszertifikat hat (Verschlüsselung und Zertifikat können aber auf verschiedene Weise vorgetäuscht werden). Auffällig ist auch, dass auf den gefälschten Seiten meistens zugleich die Eingabe von PIN und mehreren TANs gefordert wird, wobei auch hier andere, geschicktere Gestaltungen möglich sind. Den besten Schutz vor Phishing bietet daher schlicht die Beachtung der inzwischen wohl von allen Banken ausgegebenen goldenen Regel: "Geben Sie niemals auf telefonische Anfrage (Ausnahme: Telefon-Banking) oder auf eine E-Mail PIN oder TAN heraus!" 41

Phishing hinterlässt ebenfalls Spuren auf dem Computer des Betroffenen. Neben der Phishing-Mail kann anhand der Verlaufsprotokolle und temporären Dateien des Internet-Browsers meist noch relativ lange nachvollzogen werden, welche Internetseiten aufgesucht worden sind. 42

Eine Variante des Phishing ist das sogenannte Vishing (V für Voice), bei dem die Kontodaten telefonisch abgefragt werden. So hat unstreitig eine der beiden weiteren Geschädigten, von denen Geld auf das Konto des Beklagten überwiesen worden ist, einer unbekannten Person am Telefon 4 TANs mitgeteilt. 43

Wenn der Kontoinhaber die Seite seiner Bank aufruft, wird die Verbindung auf eine gefälschte Seite der Täter umgeleitet. Dies ist möglich, weil es sich bei den üblichen Internetadressen (z.B. anonym4) nur um eine "Übersetzung" der eigentlichen Identifikation von Computern im Internet durch die sogenannte IP-Adresse, eine Kombination aus 4 Zahlenblöcken von 0-255, handelt. Die Übersetzung erfolgt durch den Domain-Name-Service (DNS) entweder auf dem heimischen Computer des Nutzers in einer lokalen Host-Datei oder durch einen Nameserver. An beiden Stellen können Kriminelle ansetzen: Entweder wird die lokale Host-Datei durch Malware oder Internetseiten mit Schadcode ausgetauscht oder verändert oder der Eintrag auf dem Nameserver wird verändert (sogenanntes Pharming, weil es Täter gibt, die hierzu ganze "Serverfarmen" betreiben). 44

Die Veränderung der lokalen Datei kann durch Antivirenprogramme und die Vornahme korrekter Sicherheitseinstellungen im Internet-Browser unterbunden werden. Auch wenn die aktuellen Versionen der im Internet verwendeten Kommunikationsprotokolle den Tätern das Pharming erschweren, gibt es dagegen keinen wirksamen technischen Schutz gegen Täter, die Nameserver "kapern" oder manipulieren. Zur Identifikation der gefälschten Seite gelten die gleichen Regeln wie beim Phishing. 45

46

Auch beim Pharming kann der Aufruf der Internetseite der Täter im Regelfall auf dem Computer des Betroffenen nachvollzogen werden.

b) Da die Parteien nicht vertraglich verbunden sind, galt für den Kläger nur die allgemeine Pflicht, diejenige Sorgfalt anzuwenden, die von einem verständigen Menschen erwartet werden kann, um sich vor Schaden zu schützen. Maßstab ist daher die ihm in eigenen Angelegenheiten obliegende Sorgfalt (Palandt-Heinrichs, BGB, § 254, Rn. 8 f.). 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. Ebenso muss ein Kontoinhaber die Warnungen der Banken beachten, PIN und TAN niemals auf telefonische Anforderung oder Anforderung per E-Mail herauszugeben. Außerdem wird man von ihm erwarten können, dass er deutliche Hinweise auf gefälschte E-Mails und Internetseiten seiner Bank erkennt (sprachliche Mängel, deutlich falsche Internet-Adresse, Adresse ohne http**s**://, kein Schlüsselsymbol in der Statusleiste). Weitergehende Sicherheitsmaßnahmen wie etwa die Verwendung bestimmter, besonders leistungsfähiger Virenschutzprogramme oder spezialisierter Programme zum Schutz gegen bestimmte Schadsoftware, die Veränderung der Standard-Sicherheitseinstellungen von Betriebssystem und Programmen, das Arbeiten ohne Administratorrechte, die ständige Überprüfung der Zertifikate oder auch das Erkennen subtiler Abweichungen in der Internetadresse, würden die Sorgfaltsanforderungen dagegen überspannen. 47

c) Im vorliegenden Fall gilt danach Folgendes: 48

aa) Auf welche Weise die Täter des Computerbetrugs sich die Kontodaten des Klägers verschafft haben ist letztlich offen geblieben. 49

Einerseits kann davon, dass, wie der Kläger behauptet, die Täter die Daten auf dem Zentralrechner seiner Bank und somit ganz ohne seine Zutun ausspioniert haben, nicht ausgegangen werden. Der Kläger hat hierfür zwar Beweis angeboten, sein Vortrag ist aber nicht hinreichend substanziiert. Zwar ist grundsätzlich der Beklagte für die Voraussetzungen des Mitverschuldens darlegungs- und beweispflichtig. Vorliegend spricht aber der Beweis des ersten Anscheins dafür, dass die Daten auf eine der oben beschriebenen Methoden beim Kläger selbst ausspioniert worden sind. Es entspricht dem typischen Geschehensablauf, dass die Täter eines Computerbetrugs im Online-Banking die erforderlichen Kontodaten beim Bankkunden, nicht bei der Bank ausspionieren, weil aufgrund der Sicherheitsvorkehrungen der Bank selbst ein "Einbruch" auf deren Server(n), über den bzw. die das Online-Banking abgewickelt wird, ungleich schwieriger ist. 50

Die Möglichkeit eines abweichenden Geschehensverlaufs hat der Kläger nicht hinreichend dargelegt. Die pauschale Behauptung, die Täter hätten die Daten auf dem Zentralrechner ausspioniert, reicht nicht aus. Der Kläger müsste zumindest konkrete Anhaltspunkte für einen solchen Vorfall vortragen. Selbst wenn ein solcher Vorfall durch die Bank nicht öffentlich gemacht worden wäre, hätte der Kläger gegen die Bank einen Anspruch auf Informationen, so dass dies an seinen Vortrag keine unzumutbaren Anforderungen stellt. 51

Andererseits kann auch der Vortrag des Beklagten, der Kläger müsse die Daten aktiv aufgrund einer Aufforderung per E-Mail oder telefonisch an die Täter herausgegeben haben, der Entscheidung nicht zugrunde gelegt werden. Der Kläger hat dies in zulässiger Weise bestritten und vorgetragen, auf seinem Rechner hätten sich keine Spuren von Phishing gefunden und er habe PIN und TAN auch nie per Telefon mitgeteilt. Die technischen Ausführungen des Beklagten, ein anderer Weg sei unmöglich, sind – wie unter a) ausgeführt 52

– unzutreffend. Für seine Behauptungen bietet der Beklagte auch keinen Beweis an.

Eine Umkehr der Darlegungs- und Beweislast zu Gunsten des Beklagten kann nicht angenommen werden. Zwar geht es letztlich um Vorgänge, die in der Sphäre des Klägers stattgefunden haben. Angesichts der vielfältigen technischen Möglichkeiten, welche die Täter nutzen können, kann von einem durchschnittlichen Nutzer von Online-Banking aber nicht erwartet werden, im Nachhinein nachzuvollziehen, auf welchem Wege die Täter eines Computerbetruges an seine Kontodaten gelangt sind. Allenfalls kann ein substanziiertes Bestreiten gefordert werden, dem der Kläger mit der Behauptung, auf seinem Computer fänden sich keine Spuren von Phishing, jedoch genügt. 53

Es spricht schließlich auch kein Anscheinsbeweis für die Anwendung von Phishing oder Vishing durch die Täter, weil die unterschiedlichen Angriffsmethoden alle gleichermaßen in Betracht kommen. 54

bb) Da vorliegend demnach sämtliche beim Kontoinhaber ansetzenden Möglichkeiten, die Kontodaten zu erlangen, in Betracht gezogen werden müssen, kann letztlich nicht davon ausgegangen werden, dass die Täter die Kontodaten erlangt haben, weil der Kläger diesen Sorgfaltsmaßstab nicht eingehalten hat. Während ein Mitverschulden zu bejahen bzw. jedenfalls zu vermuten sein dürfte, wenn der Kontoinhaber PIN und TAN aufgrund von Phishing oder Vishing herausgibt, können Täter andere Angriffsmethoden wie Malware und Pharming auch dann mit Erfolg einsetzen, wenn der Kontoinhaber sich unter Berücksichtigung der unter b) aufgezeigten Maßstäbe hinreichend schützt und hinreichend aufmerksam ist. Auch aktuelle Virenschutzsoftware kann nicht immer die neuesten Schadprogramme erkennen. Trotz aller Sicherheitsupdates tauchen auch immer wieder neue Sicherheitslücken in Betriebssystemen und Programmen auf. Gerade die Sicherheitseinstellungen des immer noch überwiegend von Internet-Nutzern verwandten Internet Explorers der Firma N sind zudem im Auslieferungszustand alles andere als sicher. Ebenso gibt es gefälschte Internetseiten von Banken, die auch dem aufmerksamen Betrachter täuschen können. 55

Ein Mitverschulden des Klägers scheidet nach alledem aus. 56

6. Die Zinsentscheidung folgt aus §§ 291, 288 ZPO. Die Voraussetzungen des § 849 BGB lagen nicht vor. Der Beklagte hat dem Kläger keine Sache entzogen. 57

7. Die Kostenentscheidung beruht auf § 91 Abs. 1 ZPO. 58

Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus § 708 Nr. 10 ZPO. 59

Streitwert für das Berufungsverfahren: 3.137,33 € 60
