AG Wiesloch Urteil vom 20.6.2008, 4 C 57/08 nrkr – *Keylogger Phishing*

Fundstelle: CR 2008, 600 (*Erfurth*) = ITRB 2008, 221 (*Intveen*) = jusIT 2008/104, 218 (*Mader*) = WM 2008, 1648

1. Nutzt ein Bankkunde das sog. „einfache“ TAN-Verfahren und steht nicht fest, dass er selbst einen Überweisungsauftrag erteilt hat, trägt die Bank das Haftungsrisiko dafür, dass ein Dritter (sog. „man in the middle“) die Überweisung veranlasst hat.
2. Im Fall der missbräuchlichen Verwendung von Passwörtern und anderen Identitätsmerkmalen des Bankkunden (hier: PINs und TANs) durch sog. „Phishing“-Angriffe oder sog. „Keylogging“ durch Spionageprogramme liegen die Voraussetzungen der Rechtsscheinhaftung des Bankkunden regelmäßig nicht vor.

Leitsätze verfasst von Dr. *Clemens Thiele*, LL.M.

Im Namen des Volkes

Im Rechtsstreit [...] wegen Forderung/Schadensersatz hat das Amtsgericht Wiesloch auf die mündliche Verhandlung vom 11. Juni 2008 durch Richter Schüßler für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 4.698,87 EURO nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz aus 4.127,67 EURO seit dem 19.09.2007 und weitere Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz aus 571,20 EURO seit dem 13.03.2008 zu zahlen.
2. Die Beklagte wird weiter verurteilt, an den Kläger 489,45 EURO nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz hieraus seit dem 13.03.2008 zu zahlen.
3. Im Übrigen wird die Klage abgewiesen.
4. Die Kosten des Verfahrens werden der Beklagten auferlegt.

5. Das Urteil ist vorläufig vollstreckbar gegen Sicherheitsleistung in Höhe von 110 Prozent des aus dem Urteil vollstreckbaren Betrages.

6. Der Streitwert wird auf 4.698,87 EURO festgesetzt.

Tatbestand:

Der vorliegende Fall hat die zivilrechtliche Beurteilung eines möglicherweise durch eine dritte Person erfolgten Zugriffes auf ein Onlinebankingkonto zum Gegenstand.

Der Kläger unterhält bei der Beklagten, einer Bank, das Konto mit der Nummer 6….. Seit etwa dem Jahr 2006 ist dieses Konto für das Onlinebanking aktiviert und sowohl der Kläger als auch seine kontobevollmächtigte Ehefrau nutzten dies. Der Computer ist mit dem Betriebssystem Windows XP und dem Antivirenprogramm „Norton Antivirus“ ausgestattet. Über die weitere konkrete Ausstattung mit einer Firewall und die Funktionsweise des Antivirenprogramms besteht Streit (vgl. As. 97).

Am 18.09.2007 um 11.38 Uhr wurde ein Betrag in Höhe von 4.127,67 EURO unter Angabe des Verwendungszweckes „892400371 EBAY“ und unter Verwendung der „TAN 867216“ an eine Person Namens D. überwiesen (vgl. den Kontoauszug Anlage K 1, As. 27). Die Überweisung wurde mittels eines einfachen TAN Verfahrens durchgeführt, bei dem die Angabe einer jeden TAN aus der TAN Liste geeignet ist, den Vorgang auszulösen. Eine zusätzliche weitere Absicherungen durch das sogenannte i-TAN- oder m-TAN- Verfahren oder ein Chipkartenverfahren fand nicht statt.

Am 19.09.2007 erhielt der Kläger einen Anruf von einem Mitarbeiter der Beklagten, dem die Überweisung als verdächtig aufgefallen war. Der Kläger gab dem Mitarbeiter gegenüber an, dass er

die Überweisung nicht veranlasst habe und der Mitarbeiter sicherte zu, dass man versuchen werde, das Geld von der Empfängerbank zurückzubuchen. Mit Schreiben vom 27.09.2007 wandte sich der Vertreter des Klägers an die Beklagte und begehrte eine Rückbuchung (Anlage 4, As. 33). Diese wurde mit Schreiben vom 09.10.2007 von den Vertretern der Beklagten abgelehnt (Anlage K 5, As. 37).

Ein danach durchgeführter Scan des Computers des Klägers mit einem Antivirenprogramm ergab, dass auf dem Computer 14 sogenannte Schadprogramme vorhanden waren. Im Einzelnen wird hierzu auf die Liste Anlage K 3 (As. 31 ff.) verwiesen. Darüber hinaus beauftragte der Kläger den Sachverständigen H. mit der Auswertung eines vom Kläger selbst gefertigten Virenscans seines Computersystems. Dieser erstattete daraufhin zwei Gutachten. Die Klage wurde am 13.03.2008 den Vertretern der Beklagten zugestellt.

Der Kläger behauptet:

Seine Ehefrau habe am Sonntag, 16.09.2007 vom Familiencomputer drei Überweisungen tätigen wollen (As. 5). Sie habe daraufhin nach Eingabe der Empfängerdaten für die erste Überweisung die TAN 867216 eingegeben und die Überweisung freigegeben. Es sei daraufhin keine Mitteilung erfolgt, dass die Beklagte die Überweisung entgegengenommen habe. Die TAN sei jedoch verschwunden gewesen. In diesem Moment sei die Ehefrau des Klägers davon ausgegangen, dass vergessen worden sei, die TAN bei der letzten Transaktion einige Tage zuvor auszustreichen. Sodann habe die Ehefrau die geplanten Überweisungen durchgeführt.

Die Empfängerin des Geldes D. sei weder dem Kläger noch dessen Ehefrau bekannt und es bestünden keinerlei vertragliche oder tatsächliche Beziehungen zu dieser Person. Die Überweisung sei durch die unbekannten Täter mit Hilfe der sog. Keylogging- Methode durchgeführt worden.

Der Kläger behauptet weiter, er habe den Sachverständigen H. aufgrund der Ablehnung der Rückbuchung durch die Beklagte beauftragt. Dies habe Kosten in Höhe von 571,20 EURO verursacht.

Darüber hinaus sei dem Kläger oder seiner Ehefrau eine Aufklärung über die Risiken des Onlinebanking nicht zuteil geworden.

Der Kläger beantragt zuletzt (As. 3, 343) :

1. Die Beklagte wird verurteilt, an den Kläger 4.698,87 EURO nebst 5 Prozentpunkten Zinsen über dem Basiszinssatz aus 4.127,67 EURO seit dem 18.09.2007, nebst 5 Prozentpunkten Zinsen über dem Basiszinssatz aus 571,20 EURO seit Rechtshängigkeit zu zahlen.

2. Der Beklagte wird ferner verurteilt, an den Kläger 489,45 EURO nebst 5 Prozentpunkten Zinsen über dem Basiszinssatz hieraus seit Rechtshängigkeit zu zahlen.

Die Beklagte beantragt, die Klage abzuweisen.

Die Beklagte behauptet:

In rechtlicher Hinsicht nimmt die Beklagte den Standpunkt ein, dass aufgrund der Verwendung von PIN und TAN bei der Überweisung der Anscheinsbeweis dafür spreche, dass der Kontoinhaber selbst oder ein von ihm beauftragter Dritter die Überweisung getätigt haben muss (As. 93). Die Einwendungen der Klägerin seien „vom Ansatz her bereits nicht einmal geeignet, diesen Anscheinsbeweis zu entkräften“ (As. 95). Erst wenn bewiesen sei, dass die Überweisung durch einen Schädling ausgeführt sei, käme es zu einer „Abwägung des beiderseitigen Verschuldens“ (As. 97).

Durch das vorgelegte Gutachten des Herrn H. werde lediglich die Möglichkeit aufgezeigt, dass die aufgefundenen Schädlinge die Überweisung ausgeführt hätten. Selbst wenn die Überweisung jedoch von einem Schädling auf den Computer des Klägers ausgeführt worden sei, habe die Beklagte einen Schadensersatzanspruch gegen den Kläger (As. 329). Noch vor der den Gegenstand des vorliegenden Rechtsstreits bildenden Überweisung habe die Beklagte zahlreiche Hinweise zur

Sicherheit des Onlinebanking im Internet zur Verfügung gestellt (As. 101) und eine Informationsbroschüre zugesandt, die auf die gegenüber dem einfachen TAN Verfahren sichereren Vatianten wie mTAN und das HBCI-Chipkartenverfahren hinweisen.

Darüber hinaus sei der Computer des Klägers nicht mit einer „Firewall“ ausgestattet gewesen. Diese alleine ermögliche es, den vorgefundenen Schädlingen den Zugang zum Computer zu verwehren (As. 97).

Hinsichtlich der Einzelheiten des Parteivorbringens wird auf die gewechselten Schriftsätze nebst Anlagen und die Protokolle der mündlichen Verhandlungen verwiesen. Das Gericht hat die Akte 61 Js 28344/07 der Staatsanwaltschaft Heilbronn beigezogen und zum Gegenstand der mündlichen Verhandlung gemacht. Auch wurde sie den Parteivertretern zur Verfügung gestellt (As. 315 und 317). Das Gericht hat Beweis erhoben durch Einvernehme der Zeugin W.. Hinsichtlich des Ergebnisses der Beweisaufnahme wird auf das Protokoll As. 337 ff verwiesen. Darüber hinaus wurde der Kläger informatorisch angehört (As. 329 ff.).

Entscheidungsgründe:

Der Klage war stattzugeben, da die Bank keinen Anspruch gegen den Kläger hatte, den sie durch Abbuchung vom Konto des Klägers befriedigen durfte. Ein Anspruch ergibt sich nicht aus einem Überweisungsvertrag mit dem Kläger – ggf. vertreten durch seine Ehefrau – (hierzu I. und III.). Auch die Verletzung einer Nebenpflicht, die zu einem Gegenanspruch der Beklagten gegen den Kläger führen könnte, ist nicht zur Überzeugung des Gerichts nachgewiesen (hierzu II. und III.). Daher waren auch die darüber hinaus geltend gemachten Kosten für das Gutachten und die Einschaltung eines Rechtsanwaltes zu erstatten (hierzu IV.).

I. Kein Überweisungsvertrag

A. Im konkreten Fall liegt der Abbuchung zur Überzeugung des Gerichts kein wirksamer Überweisungsvertrag zu Grunde.

1.) Rechtliche Ausgangslage

Die Beklagte hat nur dann einen Aufwendungsersatzanspruch gegen den Bankkunden, den sie durch Abbuchung vom Konto des Bankkunden befriedigen darf, wenn dieser oder eine von ihm beauftragte Person einen Überweisungsantrag abgegeben hat. Ohne wirksames Angebot des Kunden auf Abschluss eines Überweisungsvertrages kann das Konto nicht belastet werden, da es an einer Weisung fehlt. Das Fälschungsrisiko des Überweisungsauftrages trägt die Bank (Assies, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 52 unter Hinweis auf BGH, NJW 2001, 2968, 3183 und 3190 zu gefälschten Überweisungsträgern und Rn. 350 ff. zum Onlinebanking). Es kann dahinstehen ob der Auffassung Richters (in Assies, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 6. Kapitel, Rn. 313) zuzustimmen ist, dass die „Verwendung der Legitimationsmedien [PIN und TAN] keinen Beweis im Rechtssinne für die Identität des Nutzers und die Berechtigung zur Kontonutzung darstellen.“ Im konkreten Fall wäre dieser jedenfalls widerlegt.

2.) Im konkreten Fall ergibt sich aus der Aussage der Zeugin W., die sich mit dem Ermittlungsergebnis der Staatsanwaltschaft Heilbronn im Verfahren 61 Js 28344/07 deckt, dass weder der Kläger noch dessen Ehefrau einen Überweisungsauftrag gegeben haben.

a.) Aussage der Ehefrau des Klägers

Die Zeugin W., die die TAN, mit der die den vorliegenden Rechtsstreit auslösende Überweisung ausgeführt wurde, in den PC eingegeben hat, hat angegeben, die Überweisung an die Empfängerin D. nicht ausgeführt zu haben (As. 343). Auch habe sie keinerlei Kontakt zu dieser Person gehabt.

b.) Beurteilung der Glaubwürdigkeit der Aussage

Die Zeugin schilderte den „klassischen Fall“ eines Zugriffes auf ein Bankkonto mittels des Einsatzes „bösartiger Software“ (vgl. zu den technischen Differenzierungen Assies/Richter,

Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 321 ff, 330, Erfurth, WM 2006, 2198). Das Gericht hat keinen Anlass an den Angaben der Zeugin zu zweifeln. Zwar hat sie ein gewisses Motiv, die Unwahrheit zu sagen, da ihr Ehemann ein wirtschaftliches Interesse am Ausgang des Prozesses hat. Auf der anderen Seite ist jedoch zu berücksichtigen, dass die Aussage selbst bereits zahlreiche Wahrheitssignale enthielt. So bejahte sie etwa die Frage, dass sie ein ebay Konto unterhalte (As. 337). Da die Überweisung den Verwendungszweck „ebay“ aufwies hätte es nahegelegen, dies zu verschweigen, wenn die Zeugin hätte lügen wollen. Auch schilderten sowohl der Kläger als auch seine Frau beide übereinstimmend facettenreich die Installierung des Antivirenprogrammes durch den Freund und Kollegen des Mannes. Bei der Frage, ob jeweils das neueste Programm von dem Freund installiert werde, sage die Zeugin, dass sie dies nicht wisse. Auch bei der Frage der automatischen Aktualisierung zeigte sie sich nicht sicher. Gerade die letzten beiden Antworten werden vom Gericht ebenfalls als Wahrheitssignale eingestuft, da ein Lügner in dieser Situation klare und für den Kläger günstigere Antworten hätte geben können.

c.) Übereinstimmung der Aussage mit dem Ermittlungsergebnis der Staatsanwaltschaft Heilbronn

Vor allem aber decken sich die Angaben der Zeugin und des Klägers mit dem in der beigezogenen Akte 61 Js 28344/07 gegen die Empfängerin des Geldes und Beschuldigte D. sichtbaren Ermittlungsergebnis. Diese Akte war dem Kläger bei Einreichung der Klage noch nicht zur Verfügung gestellt worden. Hieraus ergibt sich, dass der Kläger selbst bereits am 19.09.2007 um 12.20 Uhr und damit kurz nach der Benachrichtigung durch die Bank über die Abbuchung bei der Kriminalpolizeiaußenstelle in Wiesloch bei KK P. Anzeige erstattet hatte. Die Empfängerin des Geldes hat in ihrer Vernehmung vom 08.04.2008 angegeben, das Geld abgehoben und mittels einer mit Western Union durchgeführten Barüberweisung nach St. Petersburg transferiert zu haben. Diese Vorgehensweise entspricht – was aus der Tätigkeit des Abteilungsrichters bei der Staatsanwaltschaft Heidelberg gerichtsbekannt ist – der Deliktstypik in derartigen Fällen der Onlinekriminalität.

Zwar ist der Beklagten zuzugeben, dass es durchaus theoretisch möglich ist, dass der Kläger auch Opfer eines Eingehungsbetruges im Rahmen eines Ebaykaufes wurde und die Empfängerin des Geldes D. als Finanzagentin für den Betrüger auftrat oder die Empfängerin Verkäuferin eines Gegenstandes bei ebay war (As. 95) . Es finden sich jedoch für diese These keinerlei Anhaltspunkte. Auch spricht das Vorhandensein von Schadprogrammen, die jedenfalls nach den Angaben des Gutachters H. geeignet sind, einen Keylogging Angriff durchzuführen, für die von der Zeugin geschilderte Version. Auch die ebenfalls in dem Verfahren 61 Js 28344/07 geführten Geschädigten L. und S., deren Gelder auch an die Empfängerin D. flossen, schilderten eine Tat im Zusammenhang mit Onlinebanking und auch auf einem der PC des L. wurden Bankdaten ausspähende Trojaner aufgefunden. Auch bei der Tat zu Lasten der S. wurden ausweislich ihrer Angaben in der Vernehmung vom 24.09.2007 der Verwendungszweck „ebay“ angegeben

d.) Übereinstimmung der Aussage mit dem vorgelegten Privatgutachten

Schließlich lassen sich die Angaben auch mit der von dem vom Kläger als Privatgutachten vorgelegten Auswertung eines Scans seines Computers in Übereinstimmung bringen. Dieses kommt zu dem Ergebnis, dass die dort aufgefundenen Viren - ohne dass entscheidungserheblich auf die exakte Funktionsweise der Viren ankommt (s.o.) - HTML/ADODB.Exploit.gen und PR7PSW.Sinowal.EV einen Zugriff auf den Computer im vorbeschriebenen Sinne ermöglichen (s. Seite 4 des Gutachtens Anlage K 6; As. 49).

3.) Eine Rechtsscheinshaftung des Klägers scheidet ebenfalls aus.

Die Vorrausetzungen der Rechtsscheinshaftung des Bankkunden im Fall der Verwendung von Passwörtern und anderen Identitätsmerkmalen werden in der Literatur als „noch sehr unscharf“ bezeichnet (Borges, Rechtsfragen des Phishing, NJW 2005, 3313). Nach Borges a.a.O. werden die Voraussetzungen regelmäßig nicht erfüllt sein, da der Kunde, solange er nicht weiß, dass er getäuscht wurde, keine Möglichkeit hat, den Missbrauch von PIN und TAN zu verhindern. Nach

OLG Köln, MMR 2002, 813 (zu einer Emailadresse) ist eine Anscheinsvollmacht bei Benutzung einer Emailadresse nicht gegeben, da der Inhaber der Adresse nicht die Möglichkeit habe, das Verhalten eines Dritten vorauszusehen. Am ehesten dürfte eine Rechtsscheinshaftung nach Auffassung des Gerichts deshalb abzulehnen sein, da ein vom Kläger bewusst gesetzter Rechtsschein nicht vorhanden ist, dies jedoch - von den ausdrücklich normierten Fällen des „reinen Rechtsscheinsprinzips“ abgesehen - Voraussetzung für die Annahme einer Rechtsscheinshaftung ist (vgl. zum Vorstehenden Gernhuber, Bürgerliches Recht, 3. Auflage, S. 69, 73 und 79 sowie Canaris, Die Vertrauenshaftung im deutschen Privatrecht, § 43 (= S. 517).

B. Die Frage, ob zugunsten der Beklagten in den Fällen, in denen unter Verwendung der übermittelten PIN und TAN eine Überweisung durchgeführt wird, ein Anscheinsbeweis dafür eingreift, dass diese Überweisung vom Kontoinhaber oder einer beauftragten Person durchgeführt wurde (zum Streitstand Borges, NJW, 2005, 3313, 3316), kann vorliegend dahingestellt bleiben. Der Anscheinsbeweis setzt nämlich voraus, dass sich unter Berücksichtigung aller unstreitigen und festgestellten Einzelumstände und besonderen Merkmale des Sachverhaltes ein für die zu beweisende Tatsache nach der Lebenserfahrung typischer Geschehensablauf ergibt. Dann kann von einer feststehenden Ursache auf einen bestimmten Erfolg oder umgekehrt geschlossen werden. Ein Anscheinsbeweis kann jedoch erschüttert werden, indem konkrete Tatsachen behauptet oder bewiesen werden, aus denen sich die ernsthafte Möglichkeit eines vom Gewöhnlichen abweichenden Verlaufes ergibt. Im konkreten Fall wäre durch die unter A. gemachten Ausführungen ein Anscheinsbeweis erschüttert.

Lediglich als obiter dictum sei darauf hingewiesen, dass das Gericht gewisse Zweifel daran hat, ob bei Verwendung des im konkreten Fall angewendeten „einfachen TAN- Verfahrens“ ohne zusätzliche Absicherung durch das i-TAN Verfahren oder andere Sicherheitsmechanismen ein Anscheinsbeweis anzunehmen ist, der zum Inhalt hat, dass im Falle der Auslösung der Überweisung unter Verwendung der PIN und TAN der Kunde entweder den Überweisungsauftrag erteilt hat oder jedenfalls ein Schadensersatzanspruch der Bank besteht. Zum einen ist dem Gericht aufgrund der vormaligen Tätigkeit des Abteilungsrichters bei der Staatsanwaltschaft Heidelberg unter anderem im Bereich der Onlinekriminaltität bekannt, dass in zahlreichen Fällen die Daten etwa durch sog. Pharming an die Täter gelangen. In diesen Fällen ist dem Kunden nicht bekannt, dass er auf eine andere Homepage umgeleitet wird. Auch das LG Konstanz (MMR, 2002, 835, 836) sprach bereits im Jahr 2002 – die Gefahren durch Onlinekriminalität haben sich seither gesteigert (s. As. 191) – nach sachverständiger Beratung davon, dass das Ausspähen von Passworten mittels sog. Trojanischer Pferde eine „durchaus reelle Gefahr“ darstelle. Auch Stube (in Assies, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 6. Kapitel, Rn. 54) spricht von der „mangelnden Systemsicherheit (…) des besonders störanfälligen PIN/TAN Systems“ und Erfurth (WM 2006, 2098, 2204 ff.) ist vor allem wegen des „rasant gestiegenen Einsatz“ von Keyloggern der Ansicht, dass ein Anscheinsbeweis nicht anzunehmen sei. Darüber hinaus sind Grundsätze der Entscheidung des Bundesgerichtshofes zum Anscheinsbeweis bei EC Karten (BGH, Urteil v. 05.102.004; XI ZR 210/03) möglicherweise nicht übertragbar. Zum einen handelt es sich bei der vorliegenden Fallkonstellation teilweise um eine täuschungsbedingte (klassisches Phishing) oder unbemerkte (Keylogging, Pharming) Preisgabe der Daten an den Täter, während der Kunde die Daten eigentlich seiner Bank geben will, während es sich beim typischen EC Karten Fall um einen Diebstahl der Karte handelt. Insofern ist es vermutlich nicht möglich, wie dies der Bundesgerichtshof im o.g. Urteil getan hat, aus der Verschlüsselungstechnologie selbst einen Rückschluss darauf zu ziehen, dass die PIN dann gerade unsorgfältig verwahrt worden sein musste. Es entspricht gerade der Deliktstypik, dass der Bankkunde die Informationen versehentlich an den Täter herausgibt (vgl. ausführlich zum technischen Hintergrund der Entscheidung zum Anscheinsbeweis bei EC Karten: Assies, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 6. Kapitel, Rn. 162). Zum anderen hat der Gesetzgeber in § 292 a ZPO gerade einen Anscheinsbeweis für die sog. Elekronische Signatur nach dem SigG eingeführt. Es käme dann auf die Frage an, ob sich hieraus ein Umkehrschluss ziehen lässt, das in anderen

Fällen ein Anscheinsbeweis nicht anzuwenden ist oder ob im Falle eines der elektronischen Signatur vergleichbaren Schutzniveaus eine analoge Anwendung möglich ist (zur logischen Gleichrangigkeit dieser Argumentationsfiguren Engisch, Einführung in das juristische Denken, 10. Auflage, S. 192).

II. Kein Gegenanspruch der Beklagten aus §§ 280, 241 Abs. 2 BGB

Da eine - dem Kläger gem. § 278 BGB zuzurechnende - Pflichtverletzung der Ehefrau des Klägers nicht von der Beklagten nachgewiesen ist, besteht kein Schadensersatzanspruch der Beklagten, den diese durch Abbuchung vom Konto des Klägers hätte befriedigen können.

1.) Sorgfaltsanforderungen an den Umgang mit PIN und TAN Im konkreten Fall sind die allgemeinen Sorgfaltsanforderungen im Umgang mit der TAN und die Streitfrage, inwieweit diese einschlägig sind, wenn ein Kunde diese auf eine sog. Phishing-Mail antwortet, nicht entscheidungserheblich.

2.) Sorgfaltsanforderungen an die Absicherung eines Computers

a.) Rechtliche Ausganglage.

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 (so auch Assies/Richter, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 354). Auch Erfurth (WM 2006, 2198, 220) verlangt „das zur Nutzung des Mediums notwendige Wissen, aber gerade kein fachspezifisches IT-Hintergrundwissen“ Eine irgendwie geartete Absicherung des Computers ist daher zu erwarten (so auch Assies/Richter, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 358; kundenfreundlicher jedoch Kind/Werner, CR 2006, 353 ff.). Hierbei ist jedoch zu beachten, dass das Kreditinstitut grundsätzlich das Risiko des Missbrauches der Sicherungsmedien trägt und dies nicht umfassend auf den Kunden abwälzen kann. Bei der Konkretisierung des Maßstabes ist weiterhin zu beachten, dass die Beklagte im Interesse einer vereinfachten Abwicklung und der Einsparung von Personalkosten (zu diesem Aspekt vgl. den Schriftsatz der Beklagten vom 13.03.2008; As. 99) weitgehend den Nutzern das Onlinebanking zur Verfügung stellte. Auch ist dem Abteilungsrichter aus seiner Tätigkeit als Staatsanwalt gerichtsbekannt, dass viele Personen einen als sorglos zu bezeichnenden Umgang mit den Gefahren des Internet pflegen und durch die immer benutzerfreundlichere Ausgestaltung der Personalcomputer und der Internetanwendungen kaum ein ernstzunehmendes Fachwissen besitzen müssen, um Onlinebanking zu betreiben. Letztlich ist es die unternehmerische Entscheidung der Bank, diesen Personen das Onlinebanking zur Verfügung zu stellen, was sich auf die anzuwendenden Sorgfaltsanforderungen auswirkt.

(2.) Soweit in Assies/Richter, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 343 ausgeführt wird, aufgrund der Allgemeinen Geschäftsbedingungen der Banken könne der Kunde aufgrund der bestehenden Vereinbarungen verpflichtet sein, seinen Rechner technisch aufzurüsten, wenn das Gerät durch Zeitablauf zur Verarbeitung der ausdrücklich vereinbarten Sicherheitsmaßnahmen (Hervorhebung vom Gericht) nicht mehr in der Lage ist, ist dies im vorliegenden Rechtsstreit nicht von Bedeutung. Die Beklagte hat eine derartige konkrete Vereinbarung nicht behauptet, sondern lediglich die Empfehlungen und Hinweise auf der Homepage übersendet. Diese haben jedoch keinen Vertragscharakter. Auf die AGB-rechtlichen Vereinbarkeit derartiger Klauseln und zur notwendigen Konkretisierung derartiger Klauseln (vgl. hierzu Assies/Richter, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 360 und Erfurth, WM 2006, 2198, 2200) kommt es daher nicht an. Soweit Assies/Richter, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 356 davon ausgehen, dass auch durch einseitige Hinweise der vom den Kunden anzuwendende Sorgfaltmaßstab erhöht werden kann, widerspricht dies allgemeinen vertragsrechtlichen Grundsätzen zur Begründung von Vertragspflichten (so im Ergebnis auch

Erfurth, WM 2006, 2198, 2201).

b.) Die unter 2.a) herausgearbeiteten Anforderungen wurden im vorliegenden Fall erfüllt.

(1.) Dem Kläger und seiner Frau war „eigentlich klar“, dass ein Antivirenprogramm auf dem Computer installiert sein sollte (Aussage der Zeugin W.; As. 339). Daraufhin habe man über einen Freund und Geschäftskollegen des Klägers das Programm „Norton Antivirus“ installiert. Auch hatte die Zeugin, was sie in der Vernehmung durch eine Handbewegung unterstrich (As. 339), bei der Benutzung des PCs eine Acht auf dieses Programm. Nach den Angaben der Zeugin handelte es sich sogar um eine verbesserte Version des Programms, das nicht unentgeltlich, sondern kostenpflichtig war. Die Installation des Programmes wurde von dem Kläger im Rahmen seiner informatorischen Anhörung bestätigt (As. 337). Allerdings bezeichnete sich die Zeugin W. als „absolut kein Computermensch“ (As. 339). An eine Erläuterung der verschiedenen technischen Aspekte im Rahmen des Gesprächs über das Onlinebanking, das nach Angaben der Zeugin W. „kein langes Gespräch war“, konnten sich weder die Zeugin (As. 339) noch ihr informatorisch angehörter Ehemann erinnern (As. 337). Darüber hinaus hat sich die Ehefrau nach ihren Angaben in der Zeugenvernehmung einmal die Tipps auf der Homepage der Bank angeschaut. Hierin sei darüber informiert worden, dass über TANs nicht auf Anfragen von (angeblichen) „Bankangestellten“ geantwortet werden dürfe und welche Viren gerade im Umlauf seien (As. 337).

(2.) Dies entspricht den gerichtsbekannten durchschnittlichen Sorgfaltsvorkehrungen eines PC Benutzers oder übertrifft diese möglicherweise noch.

(a.) Der Abteilungsrichter ist selbst Benutzer eines internetfähigen Personalcomputers sowie des Onlinebankings und hat im Familien- und Freundeskreis Einblick in die Absicherung zahlreicher Computersysteme. Darüber hinaus war er bei der Staatsanwaltschaft 18 Monate auf einer Abteilung für allgemeine Strafsachen unter anderem im Bereich der Onlinekriminalität tätig und wertete als Staatsanwalt für einen Berichtsentwurf an das Justizministerium zur Onlinekriminalität weitere Akten zu dem vorliegenden Fall vergleichbaren Fällen aus. Aus den vorgenannten Umständen kann das durchschnittliche Absicherungsniveau eines Personalcomputers beurteilt werden.

(b.) Soweit von Seiten der Beklagen betont wurde, dass der Kläger keine Firewall auf seinem Computer installiert gehabt habe und es dadurch zu dem Befall des Computers gekommen sei, rechtfertigt dies keine andere Entscheidung. Zum einen hat das Gericht darauf hingewiesen, dass bei der auf dem Computer des Klägers installierten Windows XP-Version das Service Pack 2 installiert gewesen sei (As. 53) und dass dieses eine Firewall enthalte (As. 345 ff.). Zum anderen ist eine Firewall lediglich in den Empfehlungen, die auf der Homepage zur Verfügung gestellt werden, der Ehefrau des Klägers ausweislich ihrer Angaben im Termin jedoch nicht bekannt waren, erwähnt. Dort heißt es: „Unerlässlich ist deshalb, dass auf ihrem Computer ein Antivirenprogramm sowie eine Firewall installiert sind, die Sie regelmäßig aktualisieren.“ Eine konkrete Vertragspflicht, dass der Kunde sich gleichsam durch den Nachweis des Vorhandenseins einer Firewall gegenüber der Bank exkulpieren muss, kann hierdurch nicht begründet werden. Wenn die Beklagte derartige Anforderungen an ihre Kunden stellt, liegt es an ihr, im Rahmen der Entscheidung, welchen Kunden sie das Onlinebanking zur Verfügung stellt, das hierfür notwendige technische „know how“ vorauszusetzen oder zu vermitteln und eine ausdrückliche vertragliche Vereinbarung hierzu zu treffen.

(c.) Auch geht der Einwand, der Kläger habe pflichtwidrig ein kostenloses Antivirenprogramm benutzt, fehl. Zum einen hat die Zeugin W. angegeben, dass es sich nicht um ein kostenloses Programm gehandelt habe. Zum anderen entspricht es nicht den Anforderungen an einen durchschnittlichen Computerbenutzer, ein kostenpflichtiges Antivirenprogramm zu benutzen.

(3.) Die Einholung eines Schachverständigengutachtens hierzu war entbehrlich (s.a. die Hinweise As. 329 im Protokoll vom 11.06.2008)

(a.) Soweit der Beklagenvertreter ein Sachverständigengutachten zum Beweis der Tatsache beantragte, dass aus der Vielzahl der Schädlinge sich ergebe, dass von dem Kläger nichts zum

Schutz des PC unternommen worden sei (As. 99), war dieses Gutachten nicht einzuholen. Es ist – worauf hingewiesen wurde (As. 329) – gerichtsbekannt, dass ein Schutz vor Computerviren immer nur reaktiv auf bereits bekannte Viren erfolgen kann. Die Entdeckung eines Computervirus setzt zwingend die Infizierung eines Computers mit Viren voraus, um diese anschließend zu bekämpfen. Auch die Beklagte hat in ihren im Internet veröffentlichten Hinweisen angegeben, dass sich Trojaner in der Regel unbemerkt installieren und erst mit Hilfe eines Antivirenprogrammes sichtbar würden (As. 125).

(b.) Soweit im Termin ein Sachverständigengutachten zum Beweis der Tatsache beantragt wurde, dass sich aus der Auswertung des Sachverständigen H. ergebe, dass der Computer des Klägers seit dem 25.01.2007 nicht mehr aktualisiert worden sei (As. 333), war diesem Antrag nicht nachzukommen. Es handelt sich hierbei um einen Ausforschungsbeweis. Aus der Scanliste Anlage K 3 (As. 31), die auszugsweise in dem Gutachten bei dem jeweiligen Virus wiedergegeben ist, ergibt sich nämlich, dass es sich bei der zur Grundlage des Beweisantrages gemachten Anmerkung im Gutachten „Um die Erkennung zu verbessern wurde die Engine mit folgenden Versionen akualisiert“ um eine Anmerkung des Scanprogrammes handelt, die nichts über den Zustand des Computers des Klägers aussagt. Darüber hinaus ist dieser Vermerk bei mehreren beschriebenen Virentypen mit jeweils anderen Daten aufgeführt, die sich auch noch teilweise nach dem Vorfall liegen (vgl. As. 31). Dies bestätigt auch der Gutacher H. in seinem Gutachten in dem ausdrücklich hervorgehoben wird, dass es sich um eine die Wiedergabe reiner Zitate der Vireninformationen der Firma Avira H + B handle (Anlage K 6 Seite 1 unter 1.; As. 43 und Seite 3 unter 3. am unteren Seitenende).

3.) Sorgfaltsanforderungen an die Reaktion nach der Überweisung

Im konkreten Fall ist auch ein – dem Kläger nach § 278 BGB zuzurechnendes - Fehlverhalten der Ehefrau im Zusammenhang mit der Durchführung der Überweisung des Klägers nicht nachgewiesen. Zwar spricht vieles dafür, wenngleich dies im konkreten Fall nicht zu entscheiden ist, 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 (für die Einstufung als Rechtsscheinstatbestand jedoch Borges, NJW 2005, 3313. Auf S. 3315 heißt es jedoch: „Eine Pflichtverletzung (…) ist zu bejahen, wenn der Kunde nach Entdeckung des Phishing Angriffes untätig bleibt und dadurch weitere Verfügungen des Täters ermöglicht.“). Auch ist dem Abteilungsrichter aus der Tätigkeit bei der Staatsanwaltschaft bekannt, dass es in zahlreichen derartigen Fällen gelingen kann, das Geld von der Empfängerbank zurückzubuchen.

Im konkreten Fall liegt eine Sorgfaltspflichtverletzung jedoch nicht vor. Die Zeugin W. hat in ihrer Vernehmung angegeben, dass nach der TAN der Bildschirm zwei mal für einen Moment schwarz geworden sei (As. 341). Sie beschrieb diesen Zeitraum als eine zehntel Sekunde. Unabhängig davon, ob derartige Zeitschätzungen von einem Zeugen zutreffend vorgenommen werden, ist dennoch festzustellen, dass die Zeugin hiermit einen äußerst kurze Zeitspanne wiedergab. Danach war der Bildschirm nach Angaben der Zeugin wieder so wie er vorher war, lediglich die TAN war verschwunden. Sie habe gedacht, dass die TAN bei der letzten Überweisung verbraucht worden sei und daraufhin ihre Überweisungen mit anderen TANs erfolgreich durchgeführt (As. 341). Aufgrund der Tatsache, dass das System anschließend weiterlief und nicht – was gerichtsbekannt häufig in derartigen Fällen passiert – abstürzte und sich die Zeugin eine nachvollziehbare Erklärung für den Vorgang geben konnte, kann von der Verletzung einer Nebenpflicht nicht ausgegangen werden. Auch die Beklagte ging in ihren Hinweisen - deren Kenntnisnahme von dem Kläger bestritten wurde - davon aus, dass nur das „Abbrechen“ des Onlinebankingsystems Grund zur Benachrichtigung der Bank gebe (Anlage B 1; As. 105)

4.) Sorgfaltsanforderungen an die Auswahl eines sicheren TAN Systems durch den Kläger

Soweit die Beklagte vorbrachte, der Kläger hätte sich trotz Information über das sicherere aber auch kostenpflichtige m-TAN System und das HBCI Chipkartenverfahren für das im vorliegenden Fall verwendete einfache TAN System entschieden (As. 101), kann hieraus keine Haftung des Klägers

abgeleitet werden. Wenn die Beklagte möchte, dass ihre Kunden diese Systeme nutzten, mag sie das weniger sichere aber kostengünstige einfache TAN Verfahren aus ihrem Leistungsangebot nehmen und die sich hieran anschließende Konsequenz einer verminderten Attraktivität ihres Angebotes am Markt ziehen. Wenn sie es anbietet, kann in der Benutzung des Systems als solcher keine Pflichtverletzung des Kunden erblickt werden. Dies gilt um so mehr, als dass die Beklagte auf ihrer Homepage dieses Verfahren als sicher darstellte. Dort heißt es: „Durch die Verwendung von PIN und TAN ist sichergestellt, dass nur Sie mit ihrer Zugangskennung (VR-NetKey) (…) Bankgeschäfte mit der Online-Anwendung durchführen (…) können“ (As. 115). Die anderen Systeme wurden auf der Homepage lediglich „empfohlen“ (As. 147, 149).

III. Diese unter I. und II. beschriebene Rechtsauffassung hält einer die wirtschaftlichen Folgen und durch Missbrauchsmöglichkeiten hervorgerufenen wirtschaftlichen Risiken in Betracht ziehenden Überprüfung stand, da es sich um eine unter Anwendung des zwischenzeitlich überholten „normalen“ TAN Systems vorgenommene Überweisung handelt.

Das Gericht verkennt nicht, dass die oben dargestellte Rechtsauffassung gewisse Missbrauchsrisiken mit sich bringen kann. Die nachfolgenden Ausführungen stellen eine abstrakte Überprüfung der oben herausgearbeiteten Rechtsauffassung dar. Es liegt dem Gericht fern, dem Kläger unlautere Motive zu unterstellen.

1.) Es werden alleine in Deutschland ca. 6,7 Millionen Überweisungsvorgänge pro Jahr getätigt (Assies, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 6. Kapitel, Rn. 1). Alleine diese Zahl bringt zum Ausdruck, dass die hierfür gesetzten rechtlichen Rahmenbedingungen sich als zur Abwicklung eines derartigen „Massengeschäfts“ tauglich erweisen müssen. Auch hat die Rechtsprechung vielfach auf die Bedürfnisse des Bankenverkehrs reagiert. So wurde etwa der Grundsatz der Formenstrenge des Überweisungsauftages entwickelt (vgl. Assies, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 6. Kapitel, Rn. 14 – dort jedoch auch zu den Grenzen bei sich aufdrängendem Missbrauch unter Hinweis auf OLG Karlsruhe, WM 2007, 300). Es wäre in Zeiten der Globalisierung auf der anderen Seite ein leichtes, im Ausland ein Konto einzurichten, auf dieses Geld zu überweisen und anschließend zu behaupten, man habe die Überweisung nicht ausgeführt.

2.) Das Gericht stuft dieses Risiko jedoch im konkreten Fall trotz des Massencharakters des Überweisungsverkehrs als gering ein. Zum einen liegt es seit jeher im Verantwortungsbereich der Bank, dass etwa ein Überweisungsträger gefälscht wird. Auch diese Haftungsverteilung hat den Überweisungsverkehr nicht nennenswert beeinträchtigt. Das Online Banking und das Phänomen des Phishing bringen lediglich die Gefahren eines weiteren Kriminalitäsfeldes mit sich. Vor allem aber wurden aufgrund des zunehmenden Missbrauchs des Onlinebanking neue Identifizierungsverfahren wie i-TAN, n-TAN oder das Chipkartenleseverfahren entwickelt (Assies, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 6. Kapitel, Rn. 142 ff, 259). Gerade durch das i-TAN Verfahren wurden die Schadensursachen reduziert (Assies, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 54). Die vorliegend zu beurteilende Überweisung wurde noch unter Verwendung einer sog. „normalen“ TAN durchgeführt. Seit dem Jahr 2006 sind die fortentwickelten PIN/TAN Systeme bei zahlreichen Banken im Einsatz (Assies/Richter, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 334 mit weiteren Nachweisen) und werden als „Stand der Technik“ bezeichnet (Assies/Strube, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 3. Kapitel, Rn. 54). Die oben herausgearbeitete Rechtsauffassung ist daher – mehr muss im konkreten Fall nicht entschieden werden - auf eine begrenzte Anzahl abgeschlossener Fälle anzuwenden. Dies reduziert das Risiko, durch eine zu „kundenfreundliche“ Rechtsprechung zugleich ein Missbrauchsanreiz für Kriminelle zu liefern. Darüber hinaus ist im Rahmen der Beweiswürdigung eines jeden Falles selbstverständlich die - oben ausführlich dargestellte - Genese der Behauptung, die Überweisung sei nicht von dem Kontoinhaber getätigt worden, zu beachten. Hierbei wird insbesondere die Frage von Bedeutung sein, wann nach Kenntnis vom Überweisungsvorgang die Behauptung aufgestellt wurde und ob diese Behauptung durch die Anzeigenerstattung bei der

Polizei dokumentiert wurde und ob die Behauptung mit dem Ermittlungsergebnis in Einklang zu bringen ist.

IV. Die Kosten für die Einholung des Gutachtens des H. und die Einschaltung eines Rechtsanwaltes sind erstattungsfähig.

A. Gutachterkosten:

Das Gutachten As. 43 wurde in Auftrag gegeben, da die Beklagte sich weigerte, den Betrag wieder gutzuschreiben. Die hierdurch verursachten (bestrittenen - As. 103) Kosten sind durch die Rechnungen As. 77 und 79 und die hierin genannten „Aufträge“ nachgewiesen. Das mit den Daten des Scans und des Gutachtens untermauerte Vorbringen des Beklagtenvertreters, die Weigerung sei nicht die Ursache für die Beauftragung gewesen (As. 97), ist unzutreffend. Der Gutacher wertete nämlich ein vom Kläger zuvor erstelltes Scanprotokoll aus. Angesichts der Komplexität der technischen und rechtlichen Zusammenhänge ist das Gutachten als zur zweckentsprechenden Rechtsverfolgung (s. zu diesem Kriterium s. Palandt, § 249 Rn. 40) notwendiges Gutachten einzustufen.

B. Rechtsanwaltskosten:

Im Falle eines fehlenden Überweisungsauftrages muss die Belastungsbuchung umgehend storniert werden (Assies, Handbuch des Fachanwaltes für Bank- und Kapitalmarktrecht, 1. Auflage, 6. Kapitel, Rn. 52). Am 19.09.2007 hat der Mitarbeiter der Beklagten nach dem unstreitigen Sachvortrag mitgeteilt, dass man versuche, den Betrag von dem Empfängerkonto „zurückzuholen“ (As. 7). Hierin ist eine Selbstmahnung i.S.v. Palandt, § 286 Rn. 25 zu sehen. Da dies trotz der Kommunikation des Klägers mit der Bank am 19.09.2007 nicht erfolgt ist, geriet die Bank in Verzug. Daher ist die vorgerichtliche Tätigkeit des Vertreters des Klägers in Form des Schreibens vom 27.09.2008 (Anlage K4, As. 33) als Verzugsschaden zu ersetzen. Hieraus ergibt sich der in Ziffer 2 zugesprochene Betrag in Höhe von 489,45 EURO (vgl. As 25). Da es sich hierbei um eine gesetzlich geregelte Vergütung handelt und das Schreiben vom 27.09.2008 nachgewiesen ist, konnte dieser Betrag trotz des Bestreitens der Beklagten (As. 103) festgestellt werden.

C. Verfahrensentscheidungen:

Die Klageabweisung im Übrigen beruht darauf, dass der Zinsanspruch erst ab dem 19.09.2007 und nicht - wie beantragt - ab dem 18.09.2007 besteht. Die Kostenentscheidung beruht auf §§ 91 Abs. 1, 92 Abs. 2 Nr. 1 ZPO. Der Ausspruch zur vorläufigen Vollstreckbarkeit beruht auf § 709 BGB. Die - im Urteil mögliche - Streitwertfestsetzung beruht auf §§ 3, 4 ZPO. Die Kosten der außergerichtlichen Beauftragung eines Rechtsanwaltes waren als „Kosten“ i.S.v. § 4 ZPO nicht hinein zurechnen.

Anmerkung[*]

I. Das Problem

Ein Bankkunde nutzte für das Onlinebanking ein einfaches TAN-Verfahren, bei dem die Angabe einer TAN den Überweisungsvorgang auslöst. Von seinem Konto wurde ein Betrag unter Angabe des Verwendungszwecks "... EBAY" unter Einsatz einer bestimmten TAN an eine ihm unbekannte Person überwiesen. Auf Reklamation des Kontoinhabers erfolgte keine Rückbuchung seitens der Bank. Ein vom Kontoinhaber beauftragter Sachverständiger stellte fest, dass auf dessen Computer vierzehn Viren-, Trojaner und sonstige Spionageprogramme vorhanden waren.

---

[*] RA Dr. *Clemens Thiele*, LL.M. Tax (GGU), Anwalt.Thiele@eurolawyer.at; Näheres unter http://www.eurolawyer.at.

II. Die Entscheidung des Gerichts

Das deutsche Amtsgericht verurteilte die Bank zum Ersatz des abgebuchten Betrags sowie der Sachverständigenkosten.
Die Bank hätte ihrerseits nur dann einen Aufwendungsersatzanspruch gegen den Kunden, wenn dieser einen Überweisungsauftrag erteilt hätte. Im Zweifel trug die **Bank** das **Fälschungsrisiko des Überweisungsauftrags.** Es konnte dahin gestellt bleiben, ob die Verwendung der Legitimation durch PIN und TAN keinen Beweis im Rechtssinn für die Identität des Nutzers und die Berechtigung zur Kontonutzung darstellte, da im konkreten Fall auch durch das Ermittlungsergebnis der Staatsanwaltschaft zu diesem Vorgang belegt wäre, dass weder der Kontoinhaber noch seine Frau einen Überweisungsauftrag erteilt hätten. Dieses Ergebnis wäre durch das vorliegende Privatgutachten gedeckt, das zu dem Ergebnis kam, dass die aufgefundenen Viren einen Zugriff auf den Computer ermöglicht haben könnten.
Darüber hinaus haftete der Kontoinhaber auch nicht nach den Grundsätzen der Rechtsscheinhaftung, die erforderte, dass der Kunde habe wissen müssen, dass er getäuscht wurde. Anderenfalls hätte er keine Möglichkeit, den Missbrauch von PIN und TAN zu verhindern.
Ein grundsätzlich möglicher Anscheinsbeweis dafür, dass die Überweisung vom Kontoinhaber durchgeführt worden sei, wurde erschüttert, da vorliegend ein konkreter anderer Sachverhalt behauptet und bewiesen worden wäre.
Letztlich scheiterte der Gegenanspruch der Bank aus § 280, 241 Abs 2 BGB daran, dass dem Kläger keine über § 278 BGB zuzurechnende Pflichtverletzung nachgewiesen werden konnte.

III. Kritische Würdigung und Ausblick

Ausgehend von der Feststellung, dass im konkreten Fall kein Überweisungsauftrag des Kunden vorliegt, stellt das Gericht die Sorgfaltspflichtanforderungen des Kunden im Bereich des Onlinebanking sehr ausführlich und vorbildhaft zusammen.
Die Frage der **Rechtsscheinhaftung** des Bankkunden (in Österreich spricht man von „Anscheinshaftung“[1]) für unter seinen Zugangsdaten vorgenommene Transaktionen ist noch nicht geklärt. Das AG Wiesloch bezieht sich in der Begründung auf die Auffassung eines Teils der Lehre,[2] wonach eine solche Haftung daran scheitert, dass der Kunde nicht wissen und verhindern kann, dass eine Täuschung – von wem auch immer – begangen wird.[3]
Bei der strittigen Frage, ob bei Verwendung von PIN und TAN ein Anscheinsbeweis zugunsten der Bank dafür eingreift, dass eine berechtigte Person gehandelt hat, ist heute zu beachten, dass das einfache TAN-Verfahren keine ausreichende Sicherheit gegen das technische Ausspähen bietet. Deshalb besteht nach zunehmend vertretener Ansicht[4] der Anscheinsbeweis wegen des Risikos von Phishing und ähnlichen Angriffen im klassischen PIN/TAN-Verfahren nicht mehr.
Bei den **Sorgfaltspflichten** kann die Bank grundsätzlich (nur) das Verhalten eines durchschnittlichen **Kunden** ohne spezifische IT-Kenntnisse erwarten. Der Kunde muss **aktuellen Virenschutz** vorhalten, eine **Firewall** installieren und regelmäßig **Sicherheitsupdates** des Betriebssystems und der übrigen Programme (insb. wohl Browser) installieren; darüber hinausgehende Maßnahmen wie die Veränderung von Standardeinstellungen von Software sind nicht geboten.[5]
Bemerkenswert erscheint die Auffassung, dass das Gericht auf die **unternehmerische Entscheidung der Bank** abstellt, welchem Kunden sie welches Onlinebanking-Verfahren zur Verfügung stellt.

---

1 Vgl. *Janisch*, Online Banking (2001), 163 mwN zum Meinungsstand hierzulande.
2 *Borges*, Rechtsfragen des Phishing – Ein Überblick, NJW 2005, 3313, 3314.
3 Einschränkend *Graf*, Rechtsfragen des Telebanking (1997), 23.
4 Statt vieler *Borges*, Entscheidungsanmerkung, MMR 2008, 259, 264.
5 Vgl. LG Köln 5.12.2007, 9 S 195/07, ITRB 2008, 50 = MMR 2008, 259 (*Borges*).

Ausblick: Die Entscheidung macht deutlich, welche Sorgfaltspflichten eine Bank beim Kunden voraussetzen darf: die Anforderungen sind niedrig; im Zweifel muss die Bank sicherere Systeme anbieten als das einfache PIN/TAN-Verfahren.
Begründung erhöhter Sorgfaltspflichten: Möchte die Bank weitergehende Sorgfaltspflichten des Kunden begründen, kann sie dies nur im Rahmen der klaren vertraglichen Vereinbarungen, nicht nur durch allgemeine Hinweise z.B. auf ihrer Website. Ob und inwieweit dies im Rahmen von AGB möglich ist, ist vor dem Hintergrund des § 6 KSchG mehr als fraglich. Dabei ist zu beachten, dass die Banken durch das Angebot des Onlinebanking ihr Tagesgeschäft einfach und günstig abwickeln können. Das damit einhergehende Risiko des Missbrauchs haben sie nach der auch für Österreich richtungweisenden Entscheidung[6] selbst unternehmerisch zu tragen.

IV. Zusammenfassung

Nach dem vorliegenden, umfassend begründeten Urteil des deutsche Gerichts haftet die Bank gegenüber ihren Kunden dann für den Schaden unbefugter Abbuchungen, wenn der Kunde seinen Computer den durchschnittlichen Sorgfaltsanforderungen beim Online-Banking nach betreibt und dabei Opfer des sogenannten Phishing (Pharming oder von Malware) wird.

[6] Vgl. *Mader*, Entscheidungsanmerkung, jusIT 2008, 218, 219.