E-Banking – die Haftung des Kunden im Lichte der technischen Entwicklung

Marc Oliver Felix

Institut für IT-Sicherheit und Sicherheitsrecht (ISL)
ITZ, Innstraße 43, D-94032 Passau
marc-oliver.felix@uni-passau.de

Schlagworte: IT-Sicherheit, Haftung, Anscheinsbeweis, Sorgfaltspflichten
Abstract: Der elektronische Bankverkehr ist mit zahlreichen Risiken verbunden, von denen das sog. Phishing nur das bekannteste Beispiel ist. Auf Grund der stetigen technischen Entwicklung, insbesondere auch im Bereich der Internetkriminalität, lassen sich die Risiken im E-Banking nur schwer abschätzen. Auch bei einem optimalen Verhalten des Kunden lassen sich rechtswidrige Transaktionen nie mit letzter Sicherheit ausschließen. Umso mehr gewinnt die Problematik der Haftung im Missbrauchsfall an Bedeutung. In diesem Zusammenhang stellt sich die Frage, ob der Bank ein Anscheinsbeweis dergestalt zu Gute kommen soll, dass die Transaktion entweder rechtmäßig durchgeführt wurde oder den Kunden eine Sorgfaltspflichtverletzung zur Last fällt. Diese Frage wurde noch nicht höchstrichterlich geklärt und ist in der Literatur umstritten. Der Verfasser setzt sich mit den Argumenten beider Seiten auseinander und lehnt insbesondere im Hinblick auf die fehlende Überschaubarkeit der technischen Entwicklungen und Angriffsszenarien einen Anscheinsbeweis ab.

1. Einleitung

Die Anzahl der Online-Banking-Nutzer in Deutschland steigt stetig an. Mittlerweile führen mehr als ein Drittel der Deutschen ihre Bankgeschäfte online durch. Im Vergleich zu 2005 hat sich die Zahl der elektronischen Bankzugänge um 200 % erhöht[1]. Damit gewinnt auch die Frage nach der Sicherheit des E-Banking zunehmend an Bedeutung. Zum einen ist das Internet ein sehr unsicheres Kommunikationsmedium, was sich vor allem in den fehlenden Sicherheitsvorkehrungen in den Internetprotokollen zeigt. Zum anderen ist eine zunehmende Professionalisierung im Bereich

1 Die Bank 10/2007, http://www.die-bank.de/index.asp?issue=102007&art=573.

der Internet-Kriminalität festzustellen. So hat sich beispielsweise im Zeitraum zwischen 2000 und 2006 die Anzahl der Keylogging-Programme um das Zwanzigfache erhöht[2]. Auch wenn sich die Angriffe auf E-Banking-Zugänge bisher zahlenmäßig in Grenzen halten[3], muss angesichts der dynamischen technischen Entwicklung jederzeit mit einer Zunahme dieser Delikte gerechnet werden. Die rechtlichen Probleme im Zusammenhang mit dem Missbrauch von Online-Banking werden in Zukunft also noch an Bedeutung gewinnen. In diesem Zusammenhang stellt sich insbesondere die Frage, wer den Schaden trägt, wenn der Online-Zugang eines Kunden für unrechtmäßige Transaktionen missbraucht wurde.

1.1 Die verwendeten Verfahren im E-Banking

1.1.1 PIN/TAN-Verfahren

Das PIN/TAN-Verfahren ist immer noch das am häufigsten zum Einsatz kommende Verfahren im Bereich des E-Banking. Der Kunde muss sich zum einen über die dauerhaft gültige persönliche Identifikationsnummer (PIN), zum anderen über die nur einmalig gültige Transaktionsnummer (TAN) aus einer Liste legitimieren. Damit erfolgt eine doppelte Legitimation über Wissen, etwa im Gegensatz zum EC-Karten-Verfahren, wo eine Legitimation über Wissen (PIN) und Besitz (EC-Karte) erfolgt. In seiner einfachen Form gilt das PIN/TAN-Verfahren als relativ unsicher, da sich die Legitimationsdaten im Wege von Phishing-, Pharming- oder Keylogging-Angriffen ausspionieren und auch zeitlich versetzt für Transaktionen verwenden lassen. Als sicherer gilt das indizierte TAN-Verfahren (iTAN), bei dem eine vorgegebene TAN mit einem bestimmten Index aus der Liste zu verwenden ist. Auch dieses Verfahren lässt sich jedoch etwa im Wege eines Man-in-the-Middle-Angriffs überwinden[4]. Eine interessante Alternative bietet das sogenannte mTAN-Verfahren, bei welchem dem Kunden nach Übermittlung seiner Daten eine Transaktionsnummer mittels SMS übermittelt wird. Durch die Verwendung eines zweiten Kommunikationskanals sollen technikbasierte Angriffe erheblich erschwert werden[5].

---

2 *Erfurth,* WM 2006, 2198 (2204).

3 So zumindest *Karper*, DuD 2006, 215 (219).

4 *Borges,* NJW 2005, 3313 (3314).

5 Security Manager 11/2006 – http://www.securitymanager.de/magazin/artikel_1205_banken_mehr_sicherheit_mit_mtan.html.

1.1.2 HBCI / FIN-TS

HBCI ist ein vom Bundesverband deutscher Banken (BdB) entwickelter Standard, bei dem die Authentifizierung im Wege der elektronischen Signatur erfolgt[6]. Im Gegensatz zum PIN/TAN-Verfahren wird an Stelle der Transaktionsnummer eine Chipkarte verwendet. Die Legitimation erfolgt hier also wie beim EC-Karten-Verfahren über Wissen (PIN) und Besitz (Chipkarte). Im Jahr 2002 wurde der FinTS-Standard eingeführt, der sowohl das PIN/TAN als auch das HBCI-Verfahren unterstützt[7]. Im Rahmen von FinTS gibt es mehrere Umsetzungen des HBCI-Verfahrens. Angestrebt wird das Verfahren mit der ZKA-Banken-Signaturkarte, da nur dieses Verfahren es ermöglicht, den Anforderungen aus dem Signaturgesetz zu genügen und rechtsverbindliche Signaturen zu schaffen[8].

1.2 Die wichtigsten Angriffsszenarien

1.2.1 Phishing

Die bekannteste Angriffsmethode ist das sog. Phishing. Die Täter versenden wahllos an einen größeren Kreis von Internetnutzern eine Spam-Mail, in der Absicht, auch die Kunden einer bestimmten Bank zu erreichen. In der Mail wird der Nutzer aufgefordert, einem Link zu folgen und seine persönlichen Daten einzugeben. Der Kunde wird so auf eine Website geleitet, die der Homepage der Bank im Wege des Website-Spoofings nachgebildet ist[9]. Das Website-Spoofing ist mittlerweile sehr ausgereift und erfasst neben dem einfachen Kopieren von Bilddateien auch das Nachbilden der URL (etwa durch Verwendung eines anderen Unicode-Schriftsatzes) sowie das Verfälschen von Verschlüsselung und Sicherheitszertifikaten[10].

Das Phishing stellt allerdings keine sehr zielgerichtete Angriffstechnik dar, weil die Mail in der Regel an einen willkürlich ausgewählten Nutzerkreis versandt wird. Zudem werden Phishing-Angriffe zumeist sehr schnell

6 *Stockhausen,* WM 2001, 605.
7 FinTS 4.0 Kompendium 6 / 2004 – http://www.hbci-zka.de/dokumente/diverse/fints40_kompendium.pdf, 3.
8 FinTS 4.0 Kompendium 6 / 2004 – http://www.hbci-zka.de/dokumente/diverse/fints40_kompendium.pdf, 30.
9 *Borges,* NJW 2005, 3313.
10 *Erfurth,* WM 2006, 2198 (2202 f.).

bemerkt, da die meisten Nutzer beim Empfang der Spam-Mail Verdacht schöpfen.

1.2.2 DNS-Spoofing und Pharming

Wesentlich effektiver in dieser Hinsicht sind die Techniken des DNS-Spoofing und Pharming, bei welchen der Nutzer ohne sein Zutun auf eine fremde Website geleitet wird. Das DNS-Spoofing nutzt Schwächen des DNS (Domain-Name-System) aus. Für die Navigation im Internet muss jeder vom Nutzer angegebenen URL die IP-Adresse des Zielrechners zugeordnet werden. Die Zuordnung erfolgt über Tabellen, auf die der Browser beim Aufruf der URL zugreift. Im Wege des DNS-Spoofing wird die Zuordnung in den Tabellen verfälscht.

Da das DNS-System allerdings recht schwer zu manipulieren ist, setzen Angreifer zumeist eine Stufe früher, nämlich im Rechner des Nutzers im Wege des Pharming-Angriffs an. Der PC des Nutzers kann eine Host-Datei, also eine lokale Zuordnungstabelle von IP und URL erstellen. In der Regel überprüft der PC-Client des Nutzers zunächst die Host-Datei nach einer IP-Adresse für die angeforderte URL[11]. Beim Pharming wird die lokale Host-Datei etwa durch Trojaner oder Würmer manipuliert[12].

Wie auch beim Phishing verfälscht der Täter die Seite der Bank im Wege des Website-Spoofings, um den Kunden über deren Identität zu täuschen.

1.2.3 Keylogger

Eine passive Angriffstechnik stellt der Einsatz von sog. (Software-)Keyloggern dar. Ein Keylogger protokolliert die Eingaben des Nutzers und schickt sie an den Täter. Der Keylogger kann etwa in Gestalt eines Trojaners in den Rechner des Kunden eingeschleust werden. Der Keylogger kann zusätzlich mit einer Funktion versehen werden, die verhindert, dass bestimmte Informationen (also insbesondere die TAN) versandt werden[13]. Damit lassen sich die abgefangenen Informationen später für eine Transaktion des Täters nutzen.

---

11 *Karper,* DuD 2006, 215 (216).
12 *Borges,* NJW 2005, 3313 (3314).
13 *Borges,* a. a. O.

1.2.4 Man-in-the-Middle-Angriff

Im Rahmen dieses Angriffs schaltet sich der Angreifer in die Kommunikation zwischen Kunde und Bank, fängt die Daten des Kunden ab, verfälscht diese und leitet sie manipuliert an die Bank weiter. Beim aktiven Angriff leitet der Angreifer die Daten zeitgleich, beim passiven Angriff zeitlich versetzt weiter. Diese Angriffsform gilt als sehr gefährlich. Durch sie kann beispielsweise auch das indizierte TAN-Verfahren überwunden werden[14]. Ein mögliches Einfallstor für Man-in-the-Middle-Angriffe sind drahtlose Netzwerke (WLANs)[15].

1.2.5 Website-Spoofing

Auch Angriffe allein auf Basis des Website-Spoofings kommen in Betracht. So wird berichtet, dass Kriminelle Fehler in den Internet-Seiten der Bank ausgenutzt haben, um deren Inhalte gegen eigene auszutauschen[16].

2. Die aktuelle Rechtslage

2.1 Zustandekommen eines Vertrages

Durch Online-Transaktionen kommt ein Überweisungsvertrag (§ 676a BGB) zu Stande, der einen Unterfall des Geschäftsbesorgungsvertrags nach § 675 BGB darstellt. Die Bank erwirbt hierdurch einen Aufwendungsersatzanspruch nach §§ 675, 670 BGB. Der Überweisungsvertrag setzt wie alle Verträge zwei übereinstimmende Willenserklärungen voraus, die auch in elektronischer Form, also durch Mausklick abgegeben werden können. Nimmt der Angreifer eine unbefugte Transaktion vor, so fehlt es jedoch in der Regel an einer wirksamen Anweisung und mithin am Vertragsschluss[17].

14 *Borges,* a. a. O.

15 Resoom-Magazine, 5 / 2007 – http://www.resoom-magazine.de/news-special-display-pages/detailed-article/article/man-in-the-middle-attack/?tx_ttnews%5Bback Pid%5D=167&cHash=bd94a5be9d.

16 *Hanau,* VersR 2005, 1215 (1220).

17 *Karper,* DuD 2006, 215 (216).

2.2 Anscheinsvollmacht

Damit stellt sich die Frage, ob sich der Kunde das Verhalten des Täters ausnahmsweise zurechnen lassen muss. Da eine Stellvertretung i. S. v. §§ 164 ff. BGB nicht vorliegt und eine Duldungsvollmacht mangels Kenntnis vonseiten des Kunden ausscheidet, kommt nur die Anscheinsvollmacht in Betracht. Eine Anscheinsvollmacht liegt vor, wenn der Geschäftsherr keine Kenntnis vom Auftreten eines Dritten hat, es jedoch bei Anwendung der pflichtgemäßen Sorgfalt hätte erkennen und verhindern können, ihn insofern also ein Verschulden trifft[18]. Da es sich beim Verschulden um eine anspruchsbegründende Tatsache handelt, trägt die Bank hierfür die Beweislast. Damit ergeben sich für die Bank häufig unüberwindbare Beweisprobleme, da sie keinen Einblick in die Sphäre des Kunden hat.

2.3 Schadensersatzansprüche der Bank aus § 280 I BGB

Aus dem Vertragsverhältnis mit der Bank ergibt sich für den Kunden die Pflicht, ihre Anweisungen zu befolgen und die Sicherheit des Online-Bankings nicht zu gefährden. Verletzt der Kunde diese Pflichten und erleidet die Bank in Folge eines Angriffs auf das Konto des Kunden einen Schaden, so steht ihr ein Ersatzanspruch nach § 280 I BGB zu. Die Bank trägt die Beweislast für eine Pflichtverletzung des Kunden. Die Beweislastumkehr des § 280 I S. 2 BGB bezieht sich nur auf das Verschulden[19]. Damit ergeben sich in der Praxis dieselben beweisrechtlichen Probleme wie bei der Anscheinsvollmacht.

2.4 Anscheinsbeweis zu Gunsten der Bank

Angesichts dieser Beweisschwierigkeiten stellt sich die Frage, ob der Bank eine Beweiserleichterung in Form des Anscheinsbeweises zugutekommen soll. Im Rahmen des Anscheinsbeweises wird von bestimmten Umständen auf ein bestimmtes Ergebnis geschlossen. Der Prozessgegner kann den Anscheinsbeweis widerlegen, indem er Tatsachen vorträgt und gegebenenfalls beweist, aus denen sich die ernsthafte Möglichkeit eines abweichenden Geschehensablaufs ergibt.

---

18 BGH NJW 81, 1728, 98, 1854.
19 *Erfurth,* WM 2006, 2198 (2203).

2.4.1 Anscheinsbeweis nach § 371 a I S. 2 ZPO

Im Rahmen des HBCI-Verfahrens mit ZKA-Signaturkarte wird der Einsatz der elektronischen Signatur in den verschiedenen Stufen des § 2 SigG unterstützt[20]. Damit besteht für die Bank auch die Möglichkeit, sich der fortgeschrittenen elektronischen Signatur im Sinne des § 2 Nr. 3 SigG zu bedienen. In diesem Fall gilt zu Gunsten der Bank der Anscheinsbeweis des § 371 a I S. 2 ZPO, wonach von der Echtheit der elektronischen Erklärung ausgegangen wird, solange keine Tatsachen vorgetragen werden, die ernsthafte Zweifel hieran begründen. Bei Verwendung einer qualifizierten elektronischen Signatur wird also zunächst vermutet, dass die Anweisung wirksam ist. Um die Voraussetzungen des Anscheinsbeweises zu erfüllen, muss die Bank jedoch ihrerseits beweisen, dass die elektronische Signatur alle Anforderungen des § 2 Nr. 3 SigG erfüllt. Dies gelingt in der Praxis jedoch nur, wenn der Empfänger sich auf die Sicherheitsvermutung des § 15 I S. 4 SigG für die Anbieterakkreditierung berufen kann. Die Anbieterakkreditierung ist jedoch in der Praxis noch nicht verbreitet[21]. Auch im Bereich des Online-Bankings hat sich deshalb der Einsatz der qualifizierten elektronischen Signatur noch nicht durchgesetzt.

2.5 Anscheinsbeweis zu Gunsten der Bank beim Einsatz des PIN/TAN-Verfahrens

Im Bereich des PIN/TAN-Verfahrens ist die Beweislage noch nicht höchstrichterlich geklärt.

Das LG Köln nimmt lediglich einen Anscheinsbeweis dahingehend an, dass der Angriff gegen den Kunden und nicht gegen den Server der Bank verübt wurde, lehnt aber im Hinblick auf die Vielzahl der Angriffsmöglichkeiten eine weitergehende Beweiserleichterung zu Gunsten der Bank ab. Es stellt in seiner Begründung klar, dass eine Vielzahl der Angriffe auch ohne ein Verschulden des Kunden erfolgen könne[22]. Auch das LG Karlsruhe verneint einen Anscheinsbeweis zu Lasten des Konteninhabers[23].

---

20 FinTS 4.0 Kompendium 6 / 2004 – http://www.hbci-zka.de/dokumente/diverse/fints40_kompendium.pdf, 32.

21 *Heckmann,* juris-Praxiskommentar, Kapitel 6, Rn 159.

22 LG Köln 5. 12. 2007, 9 S 195/07.

23 LG Karlsruhe 5. 10. 2007, 3 O 47/07 – Zu Ansprüchen der Bank gegen den Finanzagenten beim sog. Phishing und zum Mitverschulden der Bank. Das Gericht führt aus, dass auch in Fällen des Phishing nicht notwendigerweise von einer Sorgfaltspflichtverletzung des Kunden auszugehen sei.

3. Rechtliche Bewertung des Anscheinsbeweises

3.1 Argumente für den Anscheinsbeweis

In Anlehnung an die höchstrichterliche Rechtsprechung zum EC-Karten-Verfahren fordern Teile der Literatur auch im Bereich des PIN/TAN-Verfahrens einen Anscheinsbeweis zu Gunsten der Bank. Nach Ansicht des BGH[24] wird bei Abhebungen mittels EC-Karte zunächst angenommen, dass diese entweder vonseiten des rechtmäßigen Inhabers erfolgt ist, oder dieser die Abhebung durch eine Pflichtverletzung ermöglicht hat.

Dementsprechend soll im PIN/TAN-Verfahren im Wege des Anscheinsbeweises angenommen werden, dass die Abhebung entweder durch den Berechtigten selbst vorgenommen oder durch fahrlässiges Verhalten von seiner Seite ermöglicht wurde[25].

In diesem Zusammenhang wird auf den hohen Sicherheitsstandard des PIN/TAN-Verfahrens verwiesen[26]. Auch die Sicherheitsrisiken des Internets und die zunehmende Verbreitung von Malware stünden dem nicht entgegen, da trotz allem erfolgreiche Angriffe auf das Online-Banking bisher nur in Einzelfällen erfolgt seien[27].

Mitunter werden dem Kunden sehr hohe Sorgfaltspflichten abverlangt, die einer allgemeinen Verkehrssicherungspflicht für den eigenen Rechner nahekommen. Dies wird mit der umfangreichen Medienberichterstattung, der besonderen Sensibilität der Verbindungsdaten sowie einem offensiven Umgang der Softwarehersteller mit Sicherheitslücken begründet[28].

Nach dieser Ansicht wird der Bankkunde durch den Anscheinsbeweis auch nicht unbillig belastet. Er könne nämlich die Annahme der Fahrlässigkeit widerlegen, indem er vorträgt, die notwendigen Sicherheitsmaßnahmen ergriffen zu haben[29].

Schwieriger kann sich die Beweislage indes gestalten, soweit es um die Frage geht, ob die Verfügung von Seiten des Berechtigten vorgenommen wurde. Hier wird es zum Teil für ausreichend erachtet, die ernsthafte Mög-

24 BGH 5. 10. 2004, XI ZR 210 / 03 – NJW 2004, 3623.
25 *Karper,* DuD 2006, 215 (218).
26 *Karper,* DuD 2006, 215 (218); *Wiesgickl,* WM 2000, 1039 (1050); *Hanau,* VersR 2005, 1215 (1220).
27 *Karper,* DuD 2006, 215 (219).
28 *Karper,* DuD 2006, 215 (217).
29 *Karper,* DuD 2006, 215 (219).

lichkeit von Angriffen durch Medienberichte und einschlägige Fachliteratur zu belegen[30].

3.2 Kritik

Der Anscheinsbeweis setzt einen Vorgang voraus, der nach der allgemeinen Lebenserfahrung so typisch ist, dass von einer bestimmten Tatsache ohne Beachtung der näheren Umstände des Einzelfalles auf ein bestimmtes Ergebnis geschlossen werden kann. Dies setzt voraus, dass hinreichend gesicherte Erfahrungssätze vorliegen. Bei dem typischen Geschehensablauf muss es sich zudem um einen gleichförmigen Vorgang handeln. Dem Anscheinsbeweis liegen hier zwei verschiedene Erfahrungssätze zu Grunde. Zum einen wird aus der Verwendung des PIN/TAN-Verfahrens auf eine Abbuchung vonseiten des Berechtigten geschlossen. Zum anderen wird im Falle des Missbrauchs eine Sorgfaltspflichtverletzung des Kunden angenommen.

3.2.1 Vornahme der Transaktion durch den Berechtigten

Ein Erfahrungssatz ist nur dann zur Führung des Anscheinsbeweises geeignet, wenn nach anerkanntem Erfahrungswissen bestimmte Kausalzusammenhänge mit sehr hoher Wahrscheinlichkeit zutreffen[31]. Der Anteil der erfolgreichen Angriffe an allen Online-Transaktionen wird als sehr gering eingeschätzt[32]. Allerdings fehlt es im Bereich des Online-Bankings an gesicherten Daten. Weiterhin ist die Gültigkeit der bisherigen Erfahrungswerte für die Zukunft nicht gesichert. Im Bereich der IT-Sicherheit entwickeln sich die Sicherheitstechnologien in einem steten Wettlauf zwischen Angreifern und Sicherheitsexperten fort. Angesichts dieser Dynamik lässt es sich nicht mit ausreichender Gewissheit feststellen, ob ein verwendetes Verfahren noch hinreichend sicher ist.

Selbst modernste Verfahren weisen Sicherheitslücken auf. Als eines der sichersten Verfahren im Bereich des E-Banking gilt zur Zeit das HBCI-Verfahren unter Verwendung von Chipkartenlesern. Hierbei werden die Transaktionsdaten an den Chipkartenleser versandt und dort signiert. Sämtliche geheime Daten werden auf der Chipkarte gespeichert und können nicht

30 *Kind/Werner,* CR 2006, 353 (360).
31 *Erfurth,* WM 2006, 2198 (2204).
32 So zumindest *Karper,* DuD 2006, 215 (219).

ausgelesen werden. Verfügt das Kartenlesegerät über eine eigene Tastatur, so kann auch die eingegebene PIN nicht ausgelesen werden.

Das Problem besteht jedoch darin, dass die Daten nicht im Original, sondern in Form eines Hashwertes an das Lesegerät übermittelt werden. Dieser Hashwert kann ausgetauscht werden, ohne dass sich dies am Bildschirm bemerkbar macht. Dies hat zur Folge, dass die Chipkarte möglicherweise einen anderen Datensatz signiert als den, der am Bildschirm dargestellt wird (sog. Darstellungsproblem)[33].

Allgemein lässt sich sagen, dass die zunehmende Professionalisierung im Bereich der Internetkriminalität und die fortschreitende technische Entwicklung es schwer machen, die Sicherheitslage für die Zukunft abzuschätzen. Soweit Erfahrungswerte vorliegen, sind diese für die Zukunft nicht hinreichend gesichert.

3.2.2 Sorgfaltspflichtverletzung des Berechtigten

Ein derartiger Erfahrungssatz ist nur gerechtfertigt, wenn man entweder das Online-Banking als extrem sicher einstuft oder dem Kunden sehr weitgehende Sorgfaltspflichten auferlegt.

Auf Grund der Sicherheitslücken der IT-Technik lassen sich jedoch selbst bei maximaler Sorgfalt des Kunden bestimmte Angriffsformen nicht ausschließen. So hat der Kunde beispielsweise keinen Einfluss auf die Sicherheit des DNS-Systems des Service-Providers. Eine weitere nicht beherrschbare Gefahr stellen Zero-Day- und Less-than-Zero-Day-Exploits dar. Diese nutzen noch unveröffentlichte oder nicht geschlossene Sicherheitslücken der Software aus.

Im Übrigen dürfen die Sorgfaltspflichten des Bankkunden auch nicht überspannt werden.

Es ist ein objektiver, verkehrskreisbezogenen Sorgfaltsmaßstab zu Grunde zu legen. Unter Berücksichtigung der Tatsache, dass die meisten Internet- und Software-Anwendungen eine hohe Bedienerfreundlichkeit aufweisen, dürfen vom durchschnittlichen Nutzer keine tiefer gehenden technischen Kenntnisse erwartet werden. Damit kann vom Kunden beispielsweise nicht verlangt werden, dass er seinen Rechner im Sinne der Sicherheit optimal konfiguriert.

Ferner kann vom Bankkunden nicht verlangt werden, dass er von sich aus auf Anwendungen verzichtet, die als unsicher, aber sozialadäquat einzustufen sind. Im Sinne der maximalen IT-Sicherheit müsste der Kunde

33 *Gajek/Liao/Schwenk,* DuD 2007, 816 ff.

etwa aktive Inhalte vermeiden, dürfte das Online-Banking nicht von unsicheren Netzwerken wie bspw. WLANs aus vornehmen und sollte Emails von unbekannten Sendern sofort löschen. Ein derart weitgehender Verzicht ist dem Internetnutzer nicht zumutbar. Demnach kann es dem Kunden beispielsweise auch nicht zur Last gelegt werden, wenn er von einem WLAN-Netzwerk aus Bankgeschäfte tätigt und der Täter die Schwächen des Systems zur Durchführung von Man-in-the-Middle-Attacken ausnutzt.

Ferner ist zu bedenken, dass die meisten Gefahren für das Online-Banking mit den allgemeinen Sicherheitsrisiken von Internet- und PC-Nutzung im Zusammenhang stehen, sich also kaum eingrenzen lassen. Dem durchschnittlichen Internetnutzer kann indes keine allgemeine Verkehrssicherungspflicht für seinen Rechner auferlegt werden. Selbst die Gegenansicht erkennt an, dass dem Durchschnittsnutzer keine zeitnahe Systempflege obliegt[34].

Unter diesen Wertungsgesichtspunkten kann von einem Angriff nicht auf eine Sorgfaltspflichtverletzung des Kunden geschlossen werden.

Ferner fehlt es aber auch an einem gleichförmigen Vorgang, der einem Anscheinsbeweis zugänglich ist. Während etwa im Bereich des EC-Karten-Verfahrens die Angriffe weitestgehend nach demselben Muster erfolgen, machen sich die Täter im Bereich des E-Banking eine Vielzahl verschiedener Angriffstechniken zu Nutze, die ganz unterschiedliche Schwachstellen ausnutzen. So werden im Wege des DNS-Spoofings Sicherheitslücken auf den Servern der Internet-Provider ausgenutzt. Man-in-the-Middle-Angriffe erfolgen häufig unter Ausnutzung der Schwächen von lokalen WLANs. Bei Pharming- und Key-Logging-Angriffen nutzen die Täter Sicherheitslücken im Anwender-PC aus, während Phishing-Angriffen durch die Leichtgläubigkeit oder fehlende Erfahrung des Bankkunden ermöglicht werden. Selbst die Gegenansicht erkennt an, dass „den Angriffsszenarien kaum Grenzen gesetzt sind“[35]. Angesichts der Vielschichtigkeit der Angriffsszenarien kann mithin von einem gleichförmigen Vorgang keine Rede sein.

3.2.3. Billigkeitserwägungen

Durch den Anscheinsbeweis werden dem Kunden ferner unzumutbare Beweisprobleme auferlegt. Er muss zwar lediglich die ernsthafte Möglichkeit eines abweichenden Geschehensablaufs darlegen. Für die hierfür sprechenden Tatsachen muss er jedoch den Vollbeweis antreten. Dies wirft

34 *Karper,* DuD 2006, 215 (217).
35 *Karper,* DuD 2006, 215 (216).

insofern Probleme auf, als sich technische Zustände im Nachhinein häufig nicht mehr rekonstruieren lassen. Da dem Kunden der Beweis zumeist misslingen dürfte, käme der Anscheinsbeweis vom Ergebnis her einer verschuldensunabhängigen Haftung sehr nahe. Dieses Ergebnis würde jedoch wertungsmäßig dem Verbot der Vereinbarung verschuldensunabhängiger Haftung in AGB widersprechen[36].

Unbilligkeiten ließen sich nur vermeiden, indem man den Kunden den Gegenbeweis über Berichte zu den Angriffsszenarien in Medien und Fachliteratur führen ließe[37]. Dann dürfte aber der Gegenbeweis zumeist gelingen, so dass der Anscheinsbeweis nahezu obsolet wäre. Im Sinne der Rechtsklarheit ist es deswegen vorzuziehen, es bei der üblichen Beweislage zu belassen.

Ferner ist der Bank das Beweisrisiko eher zuzumuten. Sie verfügt nämlich über einen extremen Wissensvorsprung gegenüber dem Kunden, der mangels technischer Kenntnisse nicht dazu in der Lage ist, das Sicherheitsniveau des verwendeten Systems einzuschätzen. Die Bank hat zudem die Möglichkeit, Missbrauchsschäden auf den Kunden umzulagern[38]. Außerdem kann sie durch das Erteilen von Weisungen indirekt das Kundenverhalten beeinflussen.

Ferner profitiert die Bank stärker als der Kunde von der Einführung des Online-Banking. So sind Direktbanken bis zur Hälfte billiger als traditionelle Banken[39].

Zudem bietet eine strenge Haftungsregelung für die Banken auch Anreize, die Sicherheit ihrer Online-Banking-Systeme zu verbessern[40]. Hier könnte man allerdings einwenden, dass für die Banken dann auch die Möglichkeit bestehen müsste, durch den Einsatz besonders sicherer Technologien das Haftungsrisiko zu minimieren. Der Einsatz der qualifizierten elektronischen Signatur stellt im Moment noch keine praktikable Lösung dar. Hier obliegt es aber wohl dem Staat, die Rahmenbedingungen dafür zu schaffen, dass die elektronische Signatur in der Praxis eine stärkere Verbreitung findet.

---

36 *Erfurth,* WM 2006, 2198 (2206).
37 Vgl. *Kind/Werner,* CR 2006, 353 (360).
38 *Erfurth,* WM 2006, 2198 (2206).
39 *Erfurth,* a. a. O.
40 *Erfurth,* a. a. O.

4. Literatur

Max Ulrich Hanau:	Handeln unter fremder Nummer, VersR 2005, 1215 ff.
Irene Karper:	Sorgfaltspflichten beim Online-Banking – Der Bankkunde als Netzwerkprofil? Zur möglichen Neubewertung des Haftungsmaßstabs, DuD 2006, 215 ff.
Lothar Stockhausen:	Die Einführung des HBCI-Standards aus bankrechtlicher Sicht, WM 2001, 605 ff.
Georg Borges:	Rechtsfragen des Phishing – Ein Überblick, NJW 2005, 3313 ff.
Margareta Wiesgickl:	Rechtliche Aspekte des Online-Banking, WM 2000, 1039 ff.
Michael Kind/ Dennis Werner:	Rechte und Pflichten im Umgang mit PIN und TAN, CR 2006, 353 ff.
Sebastian Gajek/ Lijun Liao/ Jörg Schwenk:	Signieren mit Chipkartensystemen in unsicheren Umgebungen, DuD 2007, 816 ff.