In Kooperation mit:
BITKOM e.V.
davit im DAV
eco e.V.
VPRT e.V.

MMR
MultiMedia und Recht

Zeitschrift für Informations-, Telekommunikations- und Medienrecht

Sonderdruck

ULRICH SCHULTE AM HÜLSE / MICHAEL KRAUS

Das Abgreifen von Zugangsdaten zum Online-Banking

Ausgeklügelte technische Angriffsformen und zivilrechtliche Haftungsfragen

eCommerce

www.mmr.de

7/2016

Seiten 435–440
19. Jahrgang
Verlag C.H.BECK München

MMR MultiMedia und Recht

Redaktion: Anke Zimmer-Helfrich, Chefredakteurin (verantwortlich für den Textteil); Ass. iur. Edith Pollmeier, Redakteurin; RAin Ruth Schrödl, Redakteurin; Marianne Gerstmeyr, Redaktionsassistentin, Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: 089/381 89-427, Telefax: 089/38189-197, E-Mail: mmr@beck.de

Manuskripte: Manuskripte sind an die Redaktion zu senden. Der Verlag haftet nicht für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss schriftlich erfolgen. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag C.H.BECK an seinem Beitrag für die Dauer des gesetzlichen Urheberrechts das exklusive, räumlich und zeitlich unbeschränkte Recht zur Vervielfältigung und Verbreitung in körperlicher Form, das Recht zur öffentlichen Wiedergabe und Zugänglichmachung, das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht zur sonstigen Verwertung in elektronischer Form. Hierzu zählen auch heute noch nicht bekannte Nutzungsformen. Das in § 38 Abs. 4 UrhG niedergelegte zwingende Zweitverwertungsrecht des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt.

Anzeigenabteilung: Verlag C.H.BECK, Anzeigenabteilung, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München.
Media-Beratung: Telefon 089/3 81 89-687, Telefax 089/3 81 89-589.
Disposition, Herstellung Anzeigen, technische Daten: Telefon (0 89) 3 81 89-603, Telefax 089/3 81 89-589, E-Mail anzeigen@beck.de.
Verantwortlich für den Anzeigenteil: Bertram Götz

Verlag: Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Tel.: 089/381 89-0, Telefax: 089/38 18 93 98, Postbank München IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX.

Erscheinungsweise: Monatlich.

Bezugspreise 2016: Jährlich € 405,– (inkl. MwSt.). Vorzugspreis für Studenten und Rechtsreferendare € 199,– (inkl. MwSt.). Vorzugspreis für Mitglieder der davit € 305,– (inkl. MwSt.). Alle Abopreise inklusive Newsdienst MMR-Aktuell und MMRDIREKT. Einzelheft: € 39,– (inkl. MwSt.); Versandkosten jeweils zuzüglich. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden.
Jahrestitelei und -register sind nur noch mit dem jeweiligen Heft lieferbar.

Bestellungen über jede Buchhandlung und beim Verlag. Vertriebskooperation in der Schweiz: Helbing & Lichtenhahn Verlag AG (CH) & Co.KG, Elisabethenstraße 8, CH-4051 Basel, Tel.: +41 (0)61 228 90 70, Fax: +41 (0)61 228 90 71, E-Mail: zeitschriften@helbing.ch.

KundenServiceCenter: Tel.: 089/3 81 89-750, Fax: 089/3 81 89-358, E-Mail: bestellung@beck.de

Abbestellungen müssen 6 Wochen vor Jahresschluss erfolgen.

Adressenänderungen: Teilen Sie uns rechtzeitig Ihre Adressenänderungen mit. Dabei geben Sie bitte neben dem Titel der Zeitschrift die neue und die alte Adresse an.
Hinweis gemäß § 4 Abs. 3 der Postdienst-Datenschutzverordnung: Bei Anschriftsänderungen des Beziehers kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeantrag gestellt ist. Hiergegen kann der Bezieher innerhalb von 14 Tagen nach Erscheinen des Heftes beim Verlag widersprechen.

Satz: FotoSatz Pfeifer GmbH, 82166 Gräfelfing.

Druck: Druckhaus NOMOS, In den Lissen 12, 76547 Sinzheim.

ISSN 1434-596X

ULRICH SCHULTE AM HÜLSE / MICHAEL KRAUS

Das Abgreifen von Zugangsdaten zum Online-Banking

Ausgeklügelte technische Angriffsformen und zivilrechtliche Haftungsfragen

eCommerce

Die fortschreitende Digitalisierung hat durch das Online-Banking den papierenen Überweisungsauftrag abgelöst und damit die Bankenlandschaft nachhaltig verändert. Diesen Veränderungen tragen auch Kriminelle Rechnung, deren Ziel es ist, nicht-autorisierte Zahlungsanweisungen vorzunehmen. Der folgende Beitrag (im Anschluss an MMR 2010, 84 ff.) berichtet von den aktuellen Methoden der Täter beim Abgreifen von Kontozugangsdaten und unterzieht die ergangenen Gerichtsentscheidungen seit der Umsetzung der sog. Sepa-Richtlinie einer rechtlichen Prüfung. Lesedauer: 18 Minuten

I. Erkenntnisse aus Statistiken und Fallauswertungen

Die Täter des Abgreifens von Zugangsdaten zum Online-Banking machen es sich zunutze, dass bei der Kommunikation zwischen Zahlungsdienstleister und Zahler kein persönlicher Kontakt mehr stattfindet, sondern diese durch Fernkommunikationsmittel geprägt ist.

1. Schadensumfang

Zwar fällt der Schadensumfang in Deutschland im internationalen Vergleich zum angelsächsischen Rechtsraum, der eine größere Angriffsfläche bietet, geringer aus.[1] Der internationale Blick sollte jedoch nicht darüber hinwegtäuschen, dass Deutschland ein beliebtes Angriffsziel für das Abgreifen von Zugangsdaten zum Online-Banking in Europa ist. Seit Jahren ist speziell auf den deutschen Bankensektor ausgerichtete Schadsoftware bekannt, die längst über das technische Potenzial verfügt, u.a. sowohl das indizierte TAN-Verfahren (iTAN) als auch das mobile oder SMS-TAN-Verfahren (mTAN) erfolgreich anzugreifen, auch mittels Echtzeitmanipulationen. Diese Entwicklung zeigt, dass die Täterseite jederzeit in der Lage ist, mit verbesserten Sicherheitsmechanismen im Online-Banking, wenn auch mit zeitlicher Verzögerung, Schritt zu halten.[2]

2. Erkenntnisse aus den Fallzahlen

Die rückschauende Betrachtung der bekannt gewordenen Fallzahlen, zu denen eine erhebliche Dunkelziffer existiert, zeigt einerseits ein Absinken, nachdem Zahlungsdienstleister flächendeckend Verbesserungen im Online-Banking eingeführt haben.[3] So ergaben sich sinkende Fallzahlen im Jahr 2008 als Folge der damaligen Einführung des iTAN-Verfahrens und im Jahr 2012 u.a. als Folge der Einführung des mTAN-Verfahrens und anderer neuer Online-Banking-Verfahren (Abb. 1).

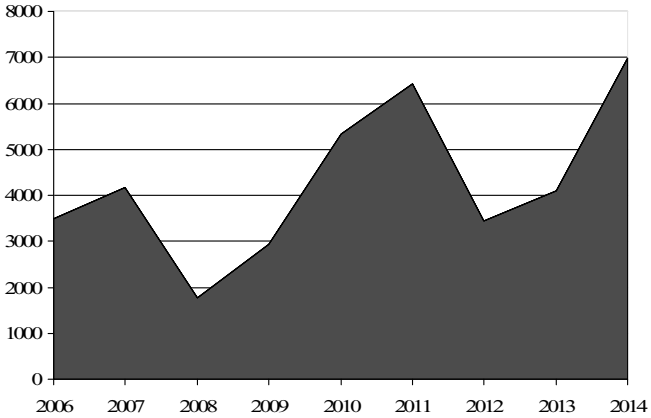

Abb. 1: Beim BKA bekannt gewordene Fallzahlen „Phishing" 2006-2014. Aus den dem BKA gemeldeten Fällen zeichnet sich ein Auf und Ab von sinkenden und steigenden Fallzahlen mit einer Tendenz nach oben ab.

Andererseits hielt der Trend der sinkenden Fallzahlen jeweils nur ein Jahr an und es gelang den Tätern offenkundig mühelos, die Verbesserungen bei den Online-Banking-Systemen kurz darauf wieder zu überwinden. Darauf lassen die steigenden Fallzahlen in den Jahren 2009-2011 und 2013-2014 schließen.

3. Beteiligte Personen

Der Ablauf des Abgreifens von Zugangsdaten zum Online-Banking vollzieht sich im Mehrpersonenverhältnis. Dies beginnt bei den Tätern, von denen anzunehmen ist, dass sie arbeitsteilig vorgehen: Eine Tätergruppe erstellt z.B. die Schadprogramme, eine andere könnte für die Verteilung der Schadsoftware über das Internet sorgen, während eine dritte Gruppe die ausgespähten Daten einsammelt und für den anschließenden Identitätsmissbrauch aufbereitet. Diese Daten könnten von einer weiteren Tätergruppe kriminell eingesetzt werden.[4] Ziel eines Angriffs sind die Online-Bankkonten meist mehrerer Bankkunden, die in der Sprache der §§ 675f ff. BGB als Zahler bezeichnet werden. Sie unterhalten eine Vertragsbeziehung zu ihrer kontoführenden Bank, die den Auftrag ausführt (anweisende Bank) und als Zahlungsdienstleister bezeichnet wird. Ein Bankkonto kann im

1 In den USA wurde der Schaden durch „Identitätsdiebstahl" schon 2003 auf US$ 2,4 Mrd. geschätzt, vgl. *Löhnig/Würdinger*, WM 2007, 961. Während das *BSI* die monetäre Bewertung vermeidet und Fallzahlen schätzt – für 2010 z.B. 1,107 Mio. Phishing-Fälle, vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2011, S. 23, nennt das *BKA* Geldsummen, die 2007 bei € 16,7 Mio. liegen, 2008 bei € 7,1 Mio., 2009 bei € 11,7 Mio., 2010 bei € 21,2 Mio., vgl. Cybercrime Bundeslagebild 2010, S. 9; 2011 bei € 25,7 Mio., vgl. Cybercrime Bundeslagebild 2011, S. 12; 2012 bei € 13,8 Mio., vgl. Cybercrime Bundeslagebild 2012, S. 7; 2013 bei € 16,4 Mio., vgl. Cybercrime Bundeslagebild 2013, S. 8; 2014 bei € 27,9 Mio., vgl. Cybercrime Bundeslagebild 2014, S. 8. Einer Studie des *DIW* zufolge liegt der volkswirtschaftliche Schaden in Deutschland allein durch Phishing jährlich bei € 793 Mio. Da dies erheblich von den Zahlen des *BKA* abweicht, könnte dies ein sehr hohes Dunkelfeld andeuten, vgl. *Riekmann/Kraus*, Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe, in: DIW Wochenbericht, 12/2015, S. 295, 301.

2 *BKA*, Cybercrime Bundeslagebild 2014, S. 8.

3 2006 wurden dem *BKA* 3.500 Sachverhalte aus dem Bereich Phishing gemeldet, vgl. PM v. 20.11.2007. Diese lagen 2007 bei 4.164, 2008 bei 1.778, 2009 bei 2.923, 2010 bei 5.331, vgl. Cybercrime Bundeslagebild 2010, S. 9; 2011 bei 6.422, vgl. Cybercrime Bundeslagebild 2011, S. 11; 2012 bei 3.440, vgl. Cybercrime Bundeslagebild 2012, S. 6; 2013 bei 4.096, vgl. Cybercrime Bundeslagebild 2013, S. 8; 2014 bei 6.984, vgl. Cybercrime Bundeslagebild 2014, S. 7.

4 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2011, S. 23.

Online-Banking in der Regel nur durch eine Überweisung auf ein anderes Konto abgeräumt werden, dessen Inhaber sich mithilfe der Strafverfolgungsorgane ermitteln lässt. Ein Dritter muss deshalb für die Täter die Funktion des Geldkuriers übernehmen, wobei es für die Täter von Bedeutung ist, dass sie über den Geldkurier nicht entdeckt werden.[5] In einigen Fallvarianten ist der Zahlungsdienstleister des Zahlers zugleich der Zahlungsdienstleister des Geldkuriers. Ist dies nicht der Fall, wäre noch zwischen diesen beiden Zahlungsdienstleistern zu unterscheiden.

II. Fragen zur Haftung zwischen Zahler und Zahlungsdienstleister

Täter setzen gegenwärtig sowohl auf ausgeklügelte technische Angriffsformen mittels Schadsoftware und versuchen zugleich, auch mittels einer Täuschungshandlung zur Erregung eines Irrtums („Social Engineering") an die notwendigen Zugangsinformationen zu gelangen, um die Autorisierungsmechanismen im Online-Banking auszuhebeln und für eigene Zwecke zu missbrauchen.

1. Fälle des „Rücküberweisungs-Trojaners"

Eine seit 2011 bekannte Fallgruppe betrifft die Fälle des sog. Rücküberweisungs-Trojaners.[6] Hierbei wird dem Zahler nach dessen Anmeldung zum Online-Banking mithilfe einer Schadsoftware ein Zahlungseingang als angebliche Fehlüberweisung in der digitalen Kontoübersicht vorgespielt, den es real nicht gibt. Der Zahler wird, vermeintlich vom Zahlungsdienstleister, aufgefordert, diese Zahlung an den vermeintlich Berechtigten oder an eine andere Person zu retournieren.

a) „Rücküberweisungs-Trojaner" mit Autorisierung

In einem Fall, den das *LG Karlsruhe* 2014 entschieden hatte, überwies eine Zahlerin einen Geldbetrag i.H.v. € 9.000,– an den Geldempfänger. Zuvor war die Zahlerin aufgefordert worden, an diesen Geldempfänger eine Rücküberweisung in Höhe dieses Betrags zu veranlassen. Haftungsvoraussetzung des Zahlungsdienstleisters gegenüber dem Zahler nach § 675u BGB ist eine nicht-autorisierte Zahlungsanweisung. Liegt dagegen eine Autorisierung des Zahlers vor, ist der Zahlungsdienstleister haftungsfrei, ohne dass es darauf ankäme, ob auch eine Haftung des Zahlers gegenüber dem Zahlungsdienstleister im Wege des Schadensersatzes nach § 675v Abs. 1 oder Abs. 2 BGB in Betracht zu ziehen ist. Das *LG Karlsruhe* ging von einer Autorisierung aus. Eine Anfechtung wegen Irrtums gem. § 119 Abs. 1 BGB scheide in diesem Fall aus, da sich die Zahlerin bei der Abgabe der Zustimmung nicht im Irrtum über deren Inhalt befunden habe. Vielmehr habe sie sich in einem typischen Motivirrtum befunden, indem sie bei der Initiierung der Überweisung von der fälschlichen Vorstellung ausging, der Zahlungsempfänger habe einen Rückzahlungsanspruch. Auch eine Anfechtung wegen arglistiger Täuschung komme nicht in Betracht, da der Täter wiederum ein Dritter i.S.d. § 123 Abs. 2 BGB sei, sodass die Zustimmung gegenüber dem Zahlungsdienstleister nur anfechtbar wäre, wenn dieser die Täuschung kannte oder kennen musste.[7] Ähnlich entschied das *LG Bonn* im Hinblick auf einen „Rücküberweisungs-Fall" beim mTAN-Verfahren. Hierbei spielte die Schadsoftware einer Zahlerin eine Fehlüberweisung des Finanzamts vor, deren „korrekte Empfängerin eine Frau N." gewesen sein soll. An diese Frau N. überwies die derart übertölpelte Zahlerin den Geldbetrag zurück. Deshalb gelangte auch das *LG Bonn* zu der Einschätzung, dass eine autorisierte Zahlungsanweisung vorliege.[8]

b) Tatvariationen

Die Fälle des sog. Rücküberweisungs-Trojaners existieren in Tatvarianten. Um die Erfolgsquote ihrer oftmals vielfachen Manipulationsversuche zu erhöhen, spielen die Täter dem Zahler mithilfe der Schadsoftware einen Zahlungseingang von einem Unternehmen vor, mit dem der Zahler mit einer erhöhten Wahrscheinlichkeit auch tatsächlich eine Vertragsbeziehung unterhält – z.B. mit einem Mobilfunkanbieter mit einer hohen Marktabdeckung oder einem Stromversorger, der in einer bestimmten Stadt eine hohe Marktabdeckung gewährleistet. Die Wahrscheinlichkeit, dass der Zahler auf diese Art dem Irrtum erliegt und zumindest einen Zahlungsauftrag in Gang setzt, ist ungleich höher, wenn die manipulierte Fehlüberweisung scheinbar von einem real existierenden Vertragspartner des Zahlers stammt. Der Zahler wird nun veranlasst, scheinbar an den ihn bereits vertrauten Vertragspartner die Rückzahlung vorzunehmen. Für die Frage der Autorisierung kommt es entscheidend darauf an, ob der Zahler die an den Geldkurier angewiesene Zahlung (und sei es versehentlich) selbst autorisiert hat. Entscheidendes Kriterium hierfür dürfte die IBAN sein. Wurde die vom Zahler beabsichtigte Zahlung jedoch durch die Schadsoftware noch während des Eingabevorgangs manipuliert und wird i.E. eine Zahlung auf das Konto des Geldkuriers allein durch die Schadsoftware autorisiert, liegt keine Autorisierung durch den Zahler vor.

2. Echtzeitmanipulation beim mTAN-Verfahren

Unabhängig von den Fällen des Rücküberweisungs-Trojaners gelingt es den Tätern in anderen Fällen i.R.e. Echtzeitmanipulation eine komplette Zahlungsanweisung zu verändern oder in Gang zu setzen. Dies kann beispielhaft anhand des mTAN-Verfahrens erläutert werden: Bei einem regulären Verlauf möchte der Zahler nur Geld an eine bestimmte Person anweisen. Nach Absendung der Überweisungsdaten an das Rechenzentrum des Zahlungsdienstleisters wird dieses beim regulären Verlauf eine hierauf abgestimmte mTAN auf das Smartphone senden. Beim irregulären Verlauf manipuliert die Schadsoftware diese Daten. Die IBAN, die beim irregulären Verlauf am Rechenzentrum des Zahlungsdienstleisters ankommt, ist diejenige des Geldkuriers. Folgerichtig sendet nun das Rechenzentrum des Zahlungsdienstleisters auf die hinterlegte Mobilnummer eine mTAN für die vom Zahler nicht gewollte Überweisung an den Geldkurier. Ist es den Tätern gleichzeitig gelungen, den Datenverkehr mit dem Mobilfunkgerät des Zahlers zu manipulieren, gelangen sie nun in den Besitz der mTAN für die von den Tätern gewollte, aber vom Zahler nicht-autorisierte Zahlung an den Geldkurier. Die Angriffsformen auf das mTAN-Verfahren können somit durch ein Zusammenspiel der Schadprogramme auf dem PC und dem Smartphone in Echtzeit erfolgen. Darüber hinaus können die Täter, wenn sie zugleich auch das Mobiltelefon des Zahlers mittels einer Schadsoftware kontrollieren und dort eingehende SMS unterdrücken und an ihre eigene Mobilnummer weiterleiten können, unabhängig vom Computer des Zahlers agieren. Die Täter starten eine eigene Geldüberweisung. Die mTAN, die das Rechenzentrum des Zahlungsdienstleisters da-

5 Der Geldkurier hebt das Geld von seinem Konto ab und überweist es oft mittels Bargeldtransfer-Dienstleister (z.B. *WesternUnion* oder *MoneyGram*) ins Ausland. Die Anwerbung erfolgt meist nach einem ähnlich gelagerten Muster – entweder anonym über das Internet oder über Jobanzeigen. Exemplarisch zur Kontaktaufnahme s. *AG Neukölln* MMR 2010, 137 (Ls.); eingehend zur Rolle des Geldkuriers *Schulte am Hülse/Klabunde*, MMR 2010, 84, 85. Eher selten überweisen Täter auf Bankkonten, die zuvor mit Falschpersonalien eingerichtet worden sind (sog. „Bankdrops"), die über die Underground-Economy im Internet an Dritte verkauft werden.

6 Das *BKA* warnte erstmals mit PM v. 15.7.2011 vor Fällen des sog. Rücküberweisungs-Trojaners.

7 *LG Karlsruhe* BKR 2015, 86-88; zuvor bereits *AG Köln* MMR 2013, 819.

8 *LG Bonn* VuR 2015, 264; *AG Potsdam* MMR 2016, 394, Berufung anhängig beim *LG Potsdam* unter dem Az. 8 S 5/16. Nach der Legaldefinition des § 675j Abs. 1 Satz 1 BGB ist von der Zustimmung (Autorisierung) auszugehen, wenn die Erklärung des Einverständnisses mit dem Zahlungsvorgang als tatsächlichem Ereignis vorliegt.

raufhin an das Smartphone des Zahlers schickt, wird abgefangen und an die Täter übermittelt. Mit der abgefangenen mTAN wird die nicht-autorisierte Überweisung abgeschlossen.[9] Diese Angriffsform funktioniert unabhängig von der Fallgruppe der Rücküberweisungs-Trojaner.

3. Beispiele für Cyber-Attacken mit internationalem Bezug

Während in der rechtlichen Auseinandersetzung zwischen Zahler und Zahlungsdienstleister regelmäßig nur der Einzelfall eines Angriffs auf ein Konto mit einem oder mehreren Buchungsvorgängen im Vordergrund steht, steht dieser Einzelfall oft im Zusammenhang mit mehreren Schadensfällen mit weiteren Betroffenen. Die Täter begnügen sich oftmals nicht damit, nur ein einzelnes Konto anzugreifen, sondern sie bezwecken zur „Ertragssteigerung" die Schadensserie. Davon erfährt der Zahler allerdings oft erst, wenn er mithilfe eines Rechtsanwalts die Ermittlungsakte auswertet und wenn gleichgelagerte Schadensfälle zu diesem Zeitpunkt bereits zu einem Ermittlungsverfahren zusammengeführt worden sind.

Andere Erkenntnisse über größere Schadensereignisse ergeben sich aus der Presseberichterstattung, von denen nur exemplarisch wenige Einzelfälle herausgegriffen werden können. Im Februar 2015 berichteten die Medien von einem ungewöhnlich breiten Angriff von international agierenden Kriminellen, durch den rund 100 Zahlungsdienstleister in ca. 30 Ländern betroffen waren (darunter auch Deutschland) und bei denen Schäden von bis zu US$ 1 Mrd. entstanden sind. Die Kriminellen, die unter dem Namen „Carbanak" bekannt geworden sind, seien fast zwei Jahre lang aktiv gewesen und hätten sich in Computernetzwerke von Zahlungsdienstleistern gehackt, Informationen gesammelt und seien dadurch in die Lage versetzt worden, sich Geld zu überweisen oder bar auszahlen zu lassen.[10]

Die *Bundesanstalt für Finanzdienstleistungsaufsicht* (*BaFin*) und die *Europäische Zentralbank* (*EZB*) nahm u.a. einen erfolgreichen Hackerangriff im August 2014 auf die US-amerikanische Bank *J.P. Morgan Chase & Co.* zum Anlass, die Thematik „Risiken durch Cyber-Angriffe" verstärkt zum Thema für bankaufsichtsrechtliche Präventionsmaßnahmen auch in Deutschland zu machen.[11] Damals brachten die Täter eine eigens angefertigte Schadsoftware in die IT-Systeme der Bank ein, die es ihnen ermöglichte, die Systeme fernzusteuern. Sie nutzten dazu Sicherheitslücken, die bis dahin unbekannt waren, sog. Zero Day Vulnerabilities. Laut Pressberichten wurde der Angriff erst zwei Monate später entdeckt. Dabei sollen Daten von über 76 Mio. Privat- und 7 Mio. Firmenkunden abgegriffen worden sein.[12] Soweit bekannt, sollen die bis heute unbekannten Angreifer die damals abgegriffenen Daten nicht sofort für Erpressungen oder für Betrugszwecke genutzt haben, was darauf hindeutet, dass das Ziel des Angriffs vorerst nur die Ausspähung der Daten an sich war.[13]

Laut einem Medienbericht gelang es Tätern aus St. Petersburg im Jahr 2008, etwa 430 Internet-Knotenrechner in Deutschland zu scannen, die Kontozugangsdaten abzuphishen und durch nicht-autorisierte Überweisungen insgesamt knapp € 25 Mio. zu erbeuten. Da die Datenübertragung zwischen Zahlungsdienstleister und Zahler verschlüsselt war, konnten die Täter sie nicht direkt auslesen. Sie erfuhren jedoch, von welchem Anschluss die Daten an einen bestimmten Bankrechner gesandt werden sollten. Die Täter leiteten die Daten auf eine nachgeahmte und vertrauenserweckende Internetseite um, die derjenigen der eigenen Bank täuschend echt ähnlich sah. Mit den erbeuteten Daten meldeten die Täter sich dann unter der Identität des Bankkunden beim Rechner der kontoführenden Bank an und überwiesen Geld auf ein Konto in Südamerika.[14]

Die Liste dieser Fälle, die typisch sind für professionelle Cyber-Angriffe und Gemeinsamkeiten aufweisen, ließe sich fortsetzen. Die Täter agieren transnational und der Angriff erfolgt zielgerichtet in der Reihenfolge: Einschleusen von Schadsoftware, Abgreifen von zahlungsrelevanten Daten und der erst späten Entdeckung des Angriffs ggf. mit einer gesonderten Nutzung der abgegriffenen Daten zu einem späteren Zeitpunkt.

4. Problematik der Darlegungs- und Beweislast

An der rechtlichen Auseinandersetzung sind mangels bekannter Identität der Täter oftmals nur der Zahler und der Zahlungsdienstleister beteiligt. In einigen Fällen wird ggf. noch der Geldkurier in Anspruch genommen oder es ist eine Versicherung beteiligt. Der exakte Ablauf der Tathandlung bleibt im Zivilprozess oft im Dunkeln. Verkürzt gesagt wirft der Zahler dem Zahlungsdienstleister vor, eine nicht-autorisierte Zahlungsanweisung veranlasst zu haben. Demgegenüber ist das Bestreben des Zahlungsdienstleisters davon geprägt, die behauptete Nichtautorisierung durch den Zahler in Frage zu stellen oder dem Zahler wenigstens ein grob fahrlässiges Verhalten beim Schutz der personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff vorzuhalten. Eine wesentliche Kernfrage besteht darin, welcher Partei die Darlegungs- und Beweislast obliegt. Ist die Zustimmung (Autorisierung) des Zahlers zu einem Zahlungsvorgang strittig, hat der Zahlungsdienstleister nachzuweisen, dass das konkrete Online-Banking-Verfahren einschließlich seiner personalisierten Sicherheitsmerkmale genutzt und dies mithilfe eines Verfahrens überprüft worden ist. Dieser Nachweis genügt aber nicht notwendigerweise, um den dem Zahlungsdienstleister obliegenden Beweis der Autorisierung des Zahlungsvorgangs durch den Zahlungsdienstnutzer zu führen.

5. Beweiserleichterung durch einen Anscheinsbeweis im Online-Banking

Eine Kernfrage der Gerichtsverfahren der vergangenen Jahre war, ob dem Zahlungsdienstleister die jederzeit erschütterbare Beweiserleichterung eines Anscheinsbeweises zugute kommt.

a) Kein Anscheinsbeweis in Bezug auf grobe Fahrlässigkeit des Zahlers

Zu unterscheiden ist, worauf sich die Beweiserleichterung eines Anscheinsbeweises beziehen soll. Dazu hat der *BGH* seine Rechtsprechung zur Anwendbarkeit der Beweisgrundsätze des Anscheinsbeweises bei streitigen Zahlungsaufträgen durch U. v. 26.1.2016 fortentwickelt und deutlich einschränkende Grundsätze formuliert. Die Kritik der Literatur an der extensiven Anwendung des Anscheinsbeweises griff der *BGH* nunmehr zutreffend auf und lehnt einen Anscheinsbeweis gerichtet auf eine grob fahrlässige Pflichtverletzung des Zahlers für den Bereich des Online-Banking ab.[15]

b) Anscheinsbeweis im Hinblick auf die Autorisierung

Die ebenfalls umstrittene Frage der Anwendung der Grundsätze des Anscheinsbeweises im Hinblick auf die Autorisierung eines

9 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2014, S. 30.

10 Z.B. ZEIT ONLINE v. 15.2.2015, abrufbar unter: www.zeit.de/digital/internet/2015-02/banken-hackerangriff-cyberkriminalitaet unter Verw. auf einen Bericht der russischen IT-Sicherheitsfirma *Kaspersky*.

11 Dazu gehört auf Seiten der *EZB* das Vorhaben der Installation des Frühwarnsystems „Single Supervisory Mechanism" (Meldestelle für Cyber-Attacken), vgl. Handelsblatt Nr. 92 v. 13.-16.5.2016, S. 28 f.

12 Handelsblatt v. 3.10.2014, abrufbar unter: www.handelsblatt.com.

13 *Held*, Cyber-Angriffe: Risiken für Banken und Aktivitäten der Aufsicht, 2.2.2015, abrufbar unter: www.bafin.de.

14 *Welchering*, FAZ Nr. 196 v. 25.8.2009, „Motor und Technik", S. T1.

15 *BGH* MMR 2016, 382; krit. bereits *Spindler*, in: FS Nobbe, 2009, S. 215, 232; *Schulte am Hülse/Klabunde*, MMR 2010, 84, 87; a.A. *Borges*, BKR 2009, 85.

streitigen Zahlungsvorgangs durch den Zahler wurde vom *BGH* in seinem U. v. 26.1.2016 dahingehend aufgelöst, dass ein vom Zahler zu erschütternder Anscheinsbeweis nur dann in Betracht kommt, wenn das konkret eingesetzte Sicherungssystem im Zeitpunkt der Vornahme des strittigen Zahlungsvorgangs im Allgemeinen praktisch unüberwindbar gewesen sei, es im konkreten Einzelfall ordnungsgemäß angewendet worden ist und fehlerfrei funktioniert hat.[16] Damit hat sich die vereinzelt gebliebene Sichtweise, § 675w BGB enthalte neben einem Anscheinsbeweis zur Autorisierung gesondert eine gesetzliche Beweisvermutung, bei der allein anhand der „Transaktionsprotokolle" per se schon „alles dafür spricht, dass dem Zahlungsdienstnutzer zuzuordnende Autorisierungen der streitigen Zahlungsvorgänge vorliegen"[17], nicht durchgesetzt.

6. Kriterium der Unüberwindbarkeit

Ist das maßgebliche Kriterium für die Anwendbarkeit der Beweisgrundsätze des Anscheinsbeweises im Hinblick auf die Autorisierung nach dem *BGH* die „allgemeine praktische Unüberwindbarkeit" des konkret eingesetzten Sicherungssystems auf der Grundlage aktueller Erkenntnisse und der Beachtung des konkret eingesetzten Sicherungsverfahrens im konkreten Einzelfall, stellt die Darlegungs- und Beweislast für den Zahlungsdienstleister bei einem ausgefeilten „Man-in-the-Middle"-Angriff eine hohe Hürde dar.

Aus der Auswertung der Tathandlungen der vergangenen Jahre lässt sich das Phänomen eines ständigen Auf und Ab innerhalb kurzer Zeiträume zwischen der Einführung neuer Sicherheitsmerkmale durch den Systemanbieter Bank und der Innovationsfähigkeit der Täter, die professionell, arbeitsteilig und international agieren, ableiten.[18] Außerdem verändern sich nicht nur Tathandlungen, sondern auch Online-Banking-Systeme. Ein bestimmtes Banking-Verfahren kann sich sowohl von Zahlungsdienstleister zu Zahlungsdienstleister als auch in zeitlicher Hinsicht, da es fortentwickelt wird, unterscheiden. Der Erkenntnisgewinn aus Sachverständigengutachten, die einige Jahre zurückreichen, sind deshalb oftmals gering, weil sie zu einem Sachverhalt ergangen sind, der mit den Fällen der Gegenwart nicht vergleichbar ist und sich die Methodik der Täter inzwischen fortentwickelt hat.

Das Kriterium der „Unüberwindbarkeit" verweist in die bereits 1989/90 von der damaligen *Zentralstelle für Sicherheit in der Informationstechnik* (*BSI*) für die Bewertung und Zertifizierung von Computersystemen und Software erarbeiteten IT-Sicherheitskriterien.[19] Demnach wird bei der Bewertung der Vertrauenswürdigkeit eines Computersystems in der Regel zwischen der Wirksamkeit der Methode und der Korrektheit der Implementierung unterschieden. Die Wirksamkeit der Methode bezeichnet hierbei die Widerstandsfähigkeit eines Schutzmechanismus gegen Umgehungsversuche, die anhand der IT-Sicherheitskriterien seinerzeit in eine sechsstufige Bewertungsskala eingeteilt worden sind. Davon ausgehend beschreibt der Begriff „nicht überwindbar" die höchste Qualitätsklasse. Während bereits für die direkt darunterliegende Stufe gilt, dass sie nach dem Stand der Technik nur mit äußerstem Aufwand zu überwinden sein darf, muss dies bei der Klasse „nicht überwindbar" im Zeitpunkt der Tathandlung allgemein und praktisch ausgeschlossen sein.

Dies macht eine Einzelfallbetrachtung des jeweils bei einer Tathandlung konkret eingesetzten Online-Banking-Systems erforderlich und setzt die Kenntnis der permanent im Fluss befindlichen Kriminalitätsentwicklung im Zeitpunkt der Tathandlung voraus. Angesichts der rasanten Veränderungen im Online-Banking vermag dieser Beitrag allenfalls eine Momentaufnahme darzustellen und es ist auch zukünftig damit zu rechnen, dass sich die Frage der Unüberwindbarkeit im Zeitpunkt zukünftiger Tathandlungen immer wieder neu stellen wird.

a) Allgemeine Einordnung des iTAN-Verfahrens

Nachdem die Täter die Sicherheitsmerkmale des ursprünglich nichtindizierten TAN-Verfahrens vergleichsweise leicht überwunden hatten, brachte rückwirkend betrachtet das indizierte TAN-Verfahren (iTAN) eine zeitweise Verbesserung. Nachdem ab dem Jahr 2009 die Fallzahlen jedoch wieder anstiegen, gelten die Sicherheitsmerkmale des iTAN-Verfahrens inzwischen als leichte Hürde für technisch versierte Täter.[20] Von einer allgemeinen Unüberwindbarkeit kann bereits seit dem Jahr 2009 nicht mehr gesprochen werden.

b) Allgemeine Einordnung des mTAN-Verfahrens

Historisch betrachtet ergab sich aus der Einführung des mTAN-Verfahrens im Jahr 2012, dokumentiert durch sinkende Fallzahlen, eine Verbesserung im Vergleich zum iTAN-Verfahren, weil die Autorisierung nun über zwei unabhängig voneinander existierende Kommunikationswege stattfand. Inzwischen liegen Erkenntnisse darüber vor, dass es den Tätern auch beim mTAN-Verfahren gelungen ist, die Sicherheitsmerkmale zu umzugehen. Bereits 2013 wurde in Untergrundforen Schadsoftware zur Überwachung und Manipulation von Android-Smartphones angeboten, die u.a. für Angriffe auf das mTAN-Verfahren verwendet worden sind. In der damaligen Variante wurde der PC des Zahlers mit einem Schadprogramm infiziert. Bei der darauffolgenden Anmeldung zum Online-Banking manipuliert das Schadprogramm die Webseite des Zahlungsdienstleisters und fordert Informationen zum Mobiltelefon des Zahlers an. Der Zahler erhielt daraufhin eine SMS mit einem Link zu einer infizierten App und wurde dazu gebracht, diese App auf seinem Smartphone zu installieren. Der Angriff auf das Online-Banking erfolgte damals durch das Zusammenspiel der Schadprogramme auf dem PC und dem Smartphone in Echtzeit.[21]

---

16 *BGH* MMR 2016, 382.

17 *Beesch*, in: NK-BGB, Bd. 2/2, 2. Aufl. 2012, §§ 675v, 675w Rdnr. 27. Diese zu weitgehende Sichtweise lässt sich ersichtlich nicht mit § 675w Satz 3 BGB in Einklang bringen, in dem es heißt: „Wurde der Zahlungsvorgang (...) ausgelöst, reicht die Aufzeichnung der Nutzung des Zahlungsauthentifizierungsinstruments einschließlich der Authentifizierung durch den Zahlungsdienstleister allein nicht notwendigerweise aus, um nachzuweisen, dass der Zahler den Zahlungsvorgang autorisiert (...) hat". Krit. zu dieser Literaturansicht *AG Berlin-Mitte* MMR 2016, 391 (zum iTAN-Verfahren): „Dabei ist nach § 675w BGB zu berücksichtigen, dass die Eingabe von PIN und TAN nicht notwendigerweise das einwandfreie Funktionieren des Autorisierungssystems oder gar die Autorisierung an sich belegen".

18 Soweit die Polizeiliche Kriminalstatistik (PKS) bzgl. der Anzahl der auf Cybercrime entfallenden Straftaten für das Jahr 2014 ggü. den Vorjahren einen deutlichen Rückgang enthält, sind diese statistischen Aussagen auf veränderte Erfassungsmodalitäten zurückzuführen: Bis einschließlich 2013 erfasste die Mehrzahl der Länder Cybercrime-Delikte mit einem Schadensereignis in Deutschland (z.B. mit Schadsoftware befallene Rechner oder Betrugsopfer in Deutschland), auch wenn unbekannt war, ob sich die kriminelle Handlung im In- oder Ausland ereignet hatte. Für das Jahr 2014 wurde damit begonnen, Cybercrime-Delikte bundeseinheitlich nur noch in der PKS zu erfassen, wenn konkrete Anhaltspunkte für eine Tathandlung innerhalb Deutschlands vorliegen. Die Zahlen der PKS des Jahres 2014 bilden insofern keinen Vergleichsmaßstab für die zurückliegenden Jahre, vgl. PKS 2014, 62. Ausg., Vorbem. S. 4.

19 IT-Sicherheitskriterien, 1. Version 1989, S. 16, abrufbar unter: https://www.bsi.bund.de: „nicht überwindbar: Der Mechanismus bietet einen z.Zt. nicht überwindbaren Schutz bei absichtlichen Verstößen gegen die Sicherheitsanforderungen. Zur Aufrechterhaltung seiner Stärke werden höchstens solche organisatorische Maßnahmen eingesetzt, die durch systeminterne Überwachungsfunktionen praktisch vollständig gegen Fehler abgesichert sind. Alle diese Kontrollfunktionen müssen Bestandteil der zu evaluierenden Software sein." Während die nationalen IT-Sicherheitskriterien 6 Qualitätsklassen von ungeeignet, schwach, mittelstark, stark, sehr stark bis zur höchsten Stufe von nicht überwindbar unterscheiden, kennt die Information Technology Security Evaluation Criteria (ITSEC) als europäischer Standard nur drei Kriterien zur Daten- und Informationssicherheit von Computersystemen: niedrig, mittel und stark.

20 Der Ablauf zur Überwindung des iTAN-Verfahrens i.R.e. Echtzeitangriffs ist beschrieben bei *Schulte am Hülse/Klabunde*, MMR 2010, 84, 85, Fußn. 6.

21 *BSI*, Die Lage der IT-Sicherheit in Deutschland 2014, S. 30.

Über einen modus operandi beim Abgreifen von Bankzugangsdaten beim mTAN-Verfahren berichtete die Süddeutsche Zeitung. Demzufolge sollen sich die Täter mithilfe einer Spähsoftware in den PC eingehackt und sich durch Ausspähen von Daten zugleich die Mobilfunknummer des Zahlers beschafft haben. In einem weiteren Schritt sollen sie sich gegenüber dem Mobilfunkanbieter des Zahlers als „Mitarbeiter eines Mobilfunk-Shops" ausgegeben und „den angeblichen Verlust der Sim-Karte" gemeldet haben. Man wolle „eine Ersatzkarte aktivieren", bei der es sich offenbar um eine gestohlene Sim-Karte gehandelt haben soll. Auf diese Weise konnte das Umleiten der mTAN auf das Handy der Täter veranlasst werden, die damit eine nicht-autorisierte Zahlungsanweisung in Gang setzten. Der Mobilfunkanbieter musste daraufhin die „Maßnahmen zur Händleridentifikation verschärfen".[22]

Nun gelangten Fälle vor Gericht, bei dem die Autorisierung durch den Zahler am Beispiel des mTAN-Verfahren gerade nicht feststand und die Täter ohne Mitwirkung des Zahlers möglicherweise den gesamten Datenverkehr kurzzeitig übernommen hatten. Einen solchen Fall hatte das *LG Oldenburg* 2016 zu beurteilen. Das *Gericht* legte anhand des Einzelfalls dar, dass sich die Täter möglicherweise gleichzeitig Zugriff auf die beiden für eine erfolgreiche Überweisung im mobilen TAN-Verfahren notwendigen Systeme verschafft haben könnten (den PC des Zahlers und sein Mobilfunkgerät), werteten hierzu die beigezogene Ermittlungsakte aus und gelangte zu der Auffassung, dass die insgesamt 44 Überweisungen ohne das kausale Zutun des Zahlers erfolgt sein könnten.[23] Im Ergebnis ist die Autorisierung eine Frage des Einzelfalls, die sich jeder schematischen Betrachtungsweise entzieht. Der Anscheinsbeweis als reine Beweiserleichterung findet hierbei auf das mTAN-Verfahren mangels Unüberwindbarkeit ersichtlich keine Anwendung.

7. Kriterien bei anderen Verfahren

Neben dem iTAN- und dem mTAN-Verfahren existieren zahlreiche weitere unterschiedliche Online-Banking-Verfahren, die je nach Anbieter verschiedene Namen tragen (eTAN, eTAN plus, Sm@rt-TAN plus, Sm@rt-TAN optic, photoTAN, chipkartenbasiertes Online-Banking wie z.B. HBCI Banking, Websign etc.).

Bei der Beurteilung des Kriteriums der Unüberwindbarkeit ist es geboten, sich sachlich und mit einem kritischen Bewusstsein für die Kreativität der Täter stets von neuem der sachverständigen Frage zu nähern, ob die Tathandlung nur möglich war, indem der Zahler mit den bei ihm vorhandenen personalisierten Sicherheitsmerkmalen in den Autorisierungsvorgang eingebunden gewesen sein musste. Dies ist naturgemäß eine abstrakte und hypothetische Frage, da sie sich nur stellt, wenn der konkrete Ablauf der Tathandlung streitig ist. Nur wenn das Kriterium der Unüberwindbarkeit aus der allgemeinen Lebenserfahrung heraus sicher anzunehmen ist, darf dem Zahlungsdienstleister die Beweiserleichterung des Anscheinsbeweises zugebilligt werden. Andernfalls bleibt es bei der herkömmlichen Beweislastverteilung, wonach der Zahlungsdienstleister die streitige Autorisierung des Zahlers darzulegen und zu beweisen hat und, wenn ihm dies nicht gelingt, er im Zivilprozess beweisfällig bleibt.

Nach dem gegenwärtigen Stand, der sich in der Zukunft verändern kann, stellen jedenfalls derzeit Angriffe auf Authentifizierungsverfahren im Online-Banking dann für Täter eine kaum zu überwindende Hürde dar, wenn

- die Authentifizierungsverfahren im Online-Banking von einer Kompromittierung des eingesetzten Geräts nicht berührt werden,
- ein Zugriff Unberechtigter auf den Übertragungsweg ausgeschlossen ist,
- die – dynamische – TAN stets an einen konkreten Zahlungsvorgang gebunden und zeitlich beschränkt ist und
- zudem das Verfahren dem Zahler vor einer Freigabe die Überprüfung des vollständigen, unverfälschten Zahlungsauftrags inklusive der IBAN und der Höhe des Geldbetrags ermöglicht und
- auch eine Innentäterattacke anhand nachgewiesener Sicherheitsstandards ausgeschlossen werden kann.[24]

a) Möglichkeit der Innentäterattacke

Bei der Prüfung dieser Fragestellung ist zu berücksichtigen, dass i.R.d. Innentäterszenarios insbesondere unternehmenssensible Daten und Informationen abfließen können. Der Innentäter, der durch sein Wissen über internes Know-how und Ressourcen etablierte Schutzmaßnahmen über einen langen Zeitraum analysieren und diese somit leichter überwinden kann als ein externer Täter, nutzt darüber hinaus das entgegengebrachte Vertrauen in der eigenen Organisation aus. Neben Mitarbeitern können auch externe Dienstleister zu Innentätern werden, die durch ihre Tätigkeit Einfluss oder direkten Zugang zu internen Prozessabläufen haben.

b) Möglichkeit der Schadsoftware auf dem PC des Zahlers

Daneben installieren Täter für „Man in the Middle"- und „Man in the Browser"-Angriffe Schadsoftware („trojanisches Pferd") auf dem PC und/oder dem Mobilfunkgerät des Zahlers.[25]

c) Möglichkeit des Scannens der Internet-Knotenrechner

Schließlich wird man zur Anwendbarkeit der Grundsätze des Anscheinsbeweises den Ausschluss fordern müssen, dass es Tätern im Tatzeitpunkt nicht gelingen konnte, sich durch das Scannen der Internet-Knotenrechner in die Datenverbindung zwischen dem PC des Zahlers und dem Rechenzentrum des Zahlungsdienstleisters dazwischenzuschalten, und es ihnen nicht gelingen konnte, auf diesem Weg eine Zahlungsanweisung zu manipulieren.

III. Notwendigkeit der Aktualisierung angreifbarer Online-Banking-Systeme

Gelangt man zu der Annahme, dass dem Zahler zwar einerseits auf Grund einer nicht-autorisierten Zahlungsanweisung gem. § 675u BGB ein Berichtigungsanspruch des fehlerhaft ausgewiesenen Kontostands gegen den Zahlungsdienstleister zukommt, der Zahlungsdienstleister dem Anspruch des Zahlers andererseits aber einen Schadensersatzanspruch nach § 675v Abs. 2 BGB entgegenhalten kann, so stellt sich abschließend die Frage, ob ein Verschulden des Zahlungsdienstleisters zum Schaden beigetragen hat. Dann ist dies in Höhe des Verursachungsanteils gem. § 254 Abs. 1 BGB berücksichtigungsfähig.

Ein Mitverschulden des Zahlungsdienstleisters kann sich aus einer ungenügenden technischen Aktualisierung des Online-Banking-Systems ergeben. Grundsätzlich ergeben sich aus dem Girokontovertrag wechselseitige Pflichten zur Rücksichtnahme. Bietet ein Zahlungsdienstleister ein offenkundig leicht angreifbares Online-Banking-Verfahren an, so potenziert sich das Manipulationsrisiko. Die Täter fokussieren ihre Angriffe nämlich auf Online-Banking-Verfahren, bei denen sie sich die meisten Erfolgschancen ausrechnen.

Erstmals hat sich im Jahr 2008 das *LG Nürnberg-Fürth* i.R.e. obiter dictum mit der Frage befasst, ob ein Zahlungsdienstleister im Jahr 2005 verpflichtet gewesen sei, das noch nicht indizierte, einfache TAN-Verfahren durch das damals modernere iTAN-Ver-

22 *Freiberger*, Süddeutsche Zeitung v. 20.10.2015, abrufbar unter: www.sueddeutsche.de.
23 *LG Oldenburg* MMR 2016, 450 – in diesem Heft.
24 Eigene Ergänzung der Kriterien nach *BGH* MMR 2016, 382.
25 Vgl. *Welchering*, FAZ Nr. 208 v. 8.9.2009, „Motor und Technik", S. T2.

fahren zu ersetzen. Das *Gericht* legte dar, dass ein Zahlungsdienstleister verpflichtet sei, „die Möglichkeiten des Missbrauchs im Rahmen des technisch Machbaren und wirtschaftlich Zumutbaren zu minimieren". Im Ergebnis blieb die Frage des anteiligen Schadensersatzes jedoch offen.[26] In einer Entscheidung aus dem Jahr 2009 hat dann das *KG* die vom *LG Nürnberg-Fürth* offengelassene Frage bejaht und einem Zahlungsdienstleister ein Mitverschulden von 70% auferlegt. Die Sorgfaltspflichtverletzung sei darin zu sehen, dass der Zahlungsdienstleister noch zu einem Zeitpunkt (im Jahr 2008) das nicht-indizierte TAN System verwendete, „als die von den Tätern gewählte Angriffsmethode des Abfragens mehrere TAN-Nummern bereits hinlänglich bekannt war und in Form des neueren iTAN-Systems damals ein wirksameres System zur Abwehr dieser Angriffe existierte".[27] Danach, nachdem sich die Angriffsformen auf das Online-Banking weiterentwickelt haben, hat der *BGH* in seinem U. v. 24.4.2012 die Ansicht der Vorinstanz bestätigt, wonach unter dem Gesichtspunkt des Mitverschuldens zumindest im Jahr 2008 noch kein Anlass für einen Zahlungsdienstleister bestanden habe, das zwischenzeitlich ebenfalls angreifbare iTAN-Verfahren durch ein moderneres und weniger sicherheitsanfälliges zu ersetzen.[28] Angesichts der fortschreitenden Kriminalitätsentwicklung und der neuen auf dem Markt befindlichen Online-Banking-Systeme bleibt die Diskussion um das Mitverschulden weiterhin offen. Zahlungsdienstleistern ist anzuraten, sich von sicherheitsanfälligen Online-Banking-Systemen nicht zu spät wieder zu trennen.

IV. Zusammenfassung und Ausblick

Die modernen Fälle des Abgreifens von Zugangsdaten zum Online-Banking spielen sich auch im Bereich von Echtzeitmanipulationen ab. Die frühere Streitfrage, inwiefern das Preisgeben von einzelnen oder mehreren Transaktionsnummern (TAN) eine grobe Fahrlässigkeit auf Seiten des Zahlers begründet, spielt bei diesen Angriffsszenarien keine Rolle mehr, da das Preisgeben von TAN bei ausgereiften Angriffsszenarien nicht erforderlich ist.

Die Entwicklung der Fallzahlen und die damit verbundenen Erfahrungswerte belegen, dass sich die Risiken von Manipulationen beim Online-Banking auf technischer Ebene minimieren lassen, wenn Zahlungsdienstleister ihre Systeme kontinuierlich weiterentwickeln und dem Stand der (Angriffs-)Technik anpassen.

Der *BGH* hat mit seinem U. v. 26.1.2016 eine bis dahin umstrittene Frage zum Anwendungsbereich des Anscheinsbeweises zutreffend geklärt und verlangt Zahlungsdienstleistern für zukünftige Streitfälle erhebliche Anforderungen an die Darlegungs- und Beweislast ab, die eine Kenntnis der aktuellen Kriminalitätsentwicklung und der Funktionsweise des konkreten Online-Banking-Systems voraussetzt.

Dr. Ulrich Schulte am Hülse
ist Fachanwalt für Bank- und Kapitalmarktrecht und Gründungspartner von ilex Rechtsanwälte, Berlin und Potsdam.

Mag. rer. publ. Michael Kraus
ist Kriminaloberrat beim Bundeskriminalamt.

Der Beitrag gibt ausschließlich die Meinung der Verfasser wieder.

26 *LG Nürnberg-Fürth*, U. v. 28.4.2008 – 10 O 11391/07.
27 *KG* MMR 2011, 338.
28 *BGH* MMR 2012, 484.

Dr. Ulrich Schulte am Hülse
ilex Rechtsanwälte
Kanzlei in der ehem. Garde-Ulanen-Kaserne
Voltaireweg 4
14469 Potsdam