Internet und Recht 14

Michael Müller-Brockhausen

Haftung für den Missbrauch von Zugangsdaten im Internet

Nomos

Internet und Recht

Herausgegeben von

Prof. Dr. Georg Borges
Universität des Saarlandes

Band 14

Michael Müller-Brockhausen

Haftung für den Missbrauch von Zugangsdaten im Internet

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Marburg, Univ., Diss., 2014

ISBN 978-3-8487-1576-3 (Print)
ISBN 978-3-8452-5591-0 (ePDF)

1. Auflage 2014

Meiner Familie

Vorwort

Diese Arbeit wurde im Wintersemster 2013/2014 an der Philipps-Universität Marburg als Dissertation angenommen. Bei allen, die mich bei der Erstellung dieser Arbeit unterstützt haben, möchte ich mich an dieser Stelle herzlich bedanken.

Ein ganz besonderer Dank gebührt meinem Doktorvater Herrn Prof. Dr. Thomas Riehm. Ihm danke ich für exzellente Betreuung und die vielen hilfreichen Gespräche. Herrn Prof. Dr. Michael Kling bin ich dankbar für die zügige Erstellung des Zweitgutachtens. Für die Aufnahme in die Schriftenreihe möchte ich mich bei Herrn Prof. Dr. Georg Borges bedanken.

Herrn Dr. Matthias Schulz möchte ich herzlich danken für seine kritischen Gedanken zum Manuskript und die hilfreichen Diskussionen über juristische Probleme. Herrn Dr. Carsten Jungmann möchte ich neben seinen Anmerkungen zu einem Teil des Manuskripts insbesondere für alles danken, was ich von ihm gelernt habe.

Technisch habe ich die vorliegende Arbeit mit LaTeX umgesetzt. Dabei schrieb ich viele Zeilen Quelltext selbst, um das gewünschte Ergebnis zu erreichen. Einige hilfreiche Vorlagen haben diese Arbeit deutlich erleichtert. Für die Klasse `jurabook` möchte ich mich bei Herrn Dr. Axel Sodtalbers bedanken. Der verwendete Zitierstil basiert auf `biblatex-juradiss` von Herrn Dr. Tobias Schwan, dem ich danken möchte. Herrn Audrey Boruvka, Mitautor von `biblatex`, gebührt Dank für die technische Hilfe bei der Lösung meiner speziellen Wünsche.

Meiner Familie, der diese Arbeit gewidmet ist, bin ich unendlich dankbar. Vielen Dank für die uneingeschränkte Förderung meiner Ausbildung und die liebevolle Unterstützung bei der Anfertigung der vorliegenden Arbeit.

Hamburg, im Juni 2014 Michael Müller-Brockhausen

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.A.	Andere Ansicht
AcP	Archiv für die civilistische Praxis
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AGB/B	Allgemeine Geschäftsbedingungen der privaten Banken, AGB Banken
Anh	Anhang
Anm.	Anmerkung
AnwBl	Anwaltsblatt
API	Application Programming Interface, zu deutsch Programmierschnittstelle
APWG	Anti-Phishing Working Group
ARD	Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland
ARP	Address Resolution Protocol
Art.	Artikel
AT	Allgemeiner Teil
AO	Abgabenordnung
BAG	Bundesarbeitsgericht
BB	Betriebsberater
BDSG	Bundesdatenschutzgesetz
BeurkG	Beurkungdungsgesetz
BeckRS	Beck Rechtsprechung
Beil.	Beilage
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BKA	Bundeskriminalamt
BKR	Zeitschrift für Bank- und Kapitalmarktrecht
BPG	Bürgerportalgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)

BT	Bundestag / Besonderer Teil
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CD	Compact Disc
c.i.c.	*culpa in contrahendo*
CMS	Content Management System
CPU	Central Processing Unit
CR	Computer und Recht
c't	Magazin für Computertechnik
DIN	Deutsche Industrienorm
DJT	Deutscher Juristentag
DeMailG	Gesetz zur Regelung von De-Mail-Diensten (De-Mail-Gesetz)
Denic	Deutsches Network Information Center eG
DNA	deoxyribonucleic acid, deutsch Desoxyribonukleinsäure (DNS)
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DSL	Digital Subscriber Line
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DZWir	Deutsche Zeitschrift für Wirtschaftsrecht
ec	Electrnonic Cash
eCommerce	Electronic Commerce, auf Deutsch elektronischer Geschäftsverkehr
eG	Eingetragene Genossenschaft
eID	electronic identity
E-Mail	Electronical Mail, auf Deutsch elektronische Post
EG	Europäische Gemeinschaft
EWiR	Entscheidungen zum Wirtschaftsrecht
FG	Festgabe
FormAnpG	Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr (Formanpassungsgesetz)
FTP	File Transfer Protocol
FS	Festschrift
GG	Grundgesetz

GmbH	Gesellschaft mit beschränkter Haftung
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRUR-RR	Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report (Zeitschrift)
GSM	Global System for Mobile Communications
GUID	Global Unique Identifier
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten, (Geldwäschegesetz)
HBCI	Homebanking Computer Interface
HGB	Handelsgesetzbuch
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
i.e.S.	im engeren Sinn
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
iFrame	Inlineframe
IMAP	Internet Message Access Protocol
IMSI	International Mobile Subscriber Identity
Internet	Interconnected Networks
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
IT	Informationstechnik
ITR	IT-Recht
ITRB	Der IT-Rechtsberater
iTAN	Indizierte Transaktionsnummer
IuKDG	Informations- und Kommunikationsdienste-Gesetz
JA	Juristische Arbeitsblätter
JherJB	Jahrbücher für die Dogmatik des heutigen römischen und deutschen Rechts (Jhering-Jahrbücher)
JKomG	Justizkommunikationsgesetz
JR	Juristische Rundschau
Jura	Juristische Ausbildung
JurisPR	Juris-Praxisreport
JurPC	Internet-Zeitschrift für Rechtsinformatik und Informationsrecht
JuS	Juristische Schulung

JW	Juristische Wochenschrift
JZ	Juristenzeitung
Habil.	Habilitation
HTML	Hypertext Markup Language
KG	Kammergericht
K&R	Kommunikation und Recht
KOM	Kommission
LAN	Local Area Network
LG	Landgericht
lit.	Litera
LZ	Leipziger Zeitschrift für Deutsches Recht
LMK	Lindenmaier-Möhring – Kommentierte BGH-Rechtsprechung
Losebl.	Loseblatt-Sammlung
MarkenG	Markengesetz
MDR	Monatsschrift für Deutsches Recht
MittBayNot	Mitteilungen des Bayerischen Notarvereins, der Notarkasse und der Landesnotarkammer Bayern
MitM	Man-in-the-Middle
NK	NomosKommentar
MMR	Multimedia und Recht
mTAN	Mobile TAN
MUA	Mail User Agent, auch als E-Mail-Programm, E-Mail-Client bezeichnet
MüKo	Münchener Kommentar
MTA	Mail Transfer Agent
m.w.N.	mit weiteren Nachweisen
NIC	Network Information Center
NJ	Neue Justiz
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
NJW-CoR	Computerreport der Neuen Juristischen Wochenschrift
NJW-RR	Neue Juristische Wochenschrift, Rechtsprechungs-Report
nPA	neuer Personalausweis
NStZ	Neue Zeitschrift für Strafrecht
NZV	Neue Zeitschrift für Verkehrsrecht
OHG	Offene Handelsgesellschaft
OLG	Oberlandesgericht

OLG-NL	OLG-Rechtsprechung neue Länder
OLGZ	Entscheidungsammlung der Oberlandesgerichte in Zivilsachen einschließlich der freiwilligen Gerichtsbarkeit
PAuswG	Personalausweisgesetz
PAuswV	Personalausweisverordnung
PIN	Persönliche Identifikationsnummer
PGP	Pretty Good Privacy
PKI	Public-Key-Infrastruktur
POP3	Post Office Protocol, Version 3
POS	Point of Sale
PostIdent	Identifikationsverfahren als Dienstleitung der Deutschen Post AG
provet	Projektgruppe verfassungsverträgliche Technikgestaltung
RFC	Request for Comments, deutsch: Bitte um Kommentare
RFID	radio-frequency identification
RG	Reichtsgericht
RGRK	Reichsgerichtsräte-Kommentar
RGZ	Entscheidungen des Reichsgerichts in Zivilsachen
Rn.	Randnummer
RPfleger	Der Deutsche Rechtspfleger
SB	Sonderbedingungen
ScheckG	Scheckgesetz
Schr.	Schrift
Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung, mittlerweile als Schufa Holding AG tätig
1. SigÄndG	Erstes Gesetz zur Änderung des Signaturgesetzes
SigG	Signaturgesetz
SigV	Verordnung zur elektronischen Signatur
SIM	Subscriber Identity Module
SMG	Gesetz zur Modernisierung des Schuldrechts (Schuldrechtsmodernisierungsgegsetz)
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
SSO	Single Sign-on
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz

StVO	Straßenverkehrsordnung
SQL	Structured Query Language
TAN	Transaktionsnummer
TCP	Transmission Control Protocol
TKG	Telekommunikationsgesetz
TKV	Telekommunikations-Kundenschutzverordnung
TLD	Top-Level-Domain
u.d.T.	unter dem Titel
UFITA	Archiv für Urheber-, Film-, Funk- und Theaterrecht
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UMTS	Universal Mobile Telecommunications System
Univ.	Universität
URL	Uniform Resource Locator
USA	United States of America, deutsch Vereinigte Staaten von Amerika
USB	Universal Serial Bus
USD	US Dollar
UStG	Umsatzsteuergesetz
UStDV	Umsatzsteuer-Durchführungsverordnung
UrhG	Urhebergesetz
UWG	Unlautererwettbewerbsgesetz
VersR	Versicherungsrecht (Zeitschrift)
WechselG	Wechselgesetz
WRP	Wettbewerb in Recht und Praxis
WLAN	Wireless LAN
Web-Dok.	Web-Dokument
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WM	Wertpapier-Mitteilungen, Zeitschrift für Wirtschafts- und Bankrecht
WuM	Wohnungswirtschaft und Mietrecht, Zeitschrift
WWW	World Wide Web
XSS	Cross-Site-Scripting
ZAG	Zahlungsdiensteaufsichtsgesetz
ZD	Zeitschrift für Datenschutz
ZDF	Zweite Deutsche Fernsehen

ZDRL	Zahlungsdienste-Richtlinie, Richtlinie 2007/64/EG über Zahlungsdienste im Binnenmarkt
ZHR	Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht
ZIP	Zeitschrift für Wirtschaftsrecht, früher: Insolvenzrecht – Zeitschrift für die gesamte Insolvenzpraxis
ZPO	Zivilprozessordnung
ZUM	Zeitschrift für Urheber- und Medienrecht
ZZP	Zeitschrift für Zivilprozeß

§ 1 Einleitung

Das Internet gewinnt zunehmend an Bedeutung. Bereits Dreiviertel der Deutschen nutzen das Internet.[1] Durchschnittlich verbrachte im Jahr 2013 jeder Deutsche circa eineinhalb Stunden täglich mit der Nutzung des Internets.[2] Sogar der *BGH* hat mittlerweile festgestellt, dass das Internet von zentraler Bedeutung für die private Lebenshaltung ist.[3] Sobald die Nutzung des Internets darüber hinaus geht, sich Informationen zu beschaffen,[4] sich Videos anzuschauen[5] oder neue Software oder Updates herunterzuladen, benötigt der Nutzer häufig Zugangsdaten, um einen Dienst zu nutzen. Anhand eines durch Zugangsdaten gesicherten Accounts kann ein Dienst seine Benutzer wiedererkennen. Der E-Mail-Anbieter kann dem Account-Inhaber die E-Mail zustellen und ihn über seine Adresse E-Mails verschicken lassen.[6] Der Internetnutzer kann sich auf einem virtuellen Informationsportal oder Internet-Foren eine virtuelle Identität mit entsprechender Reputation erarbeiten. Online-Versandhändler können ihren Nutzern den Komfort bieten, dass die Lieferadresse und die Art der Zahlung zur beschleunigten Abwicklung vom Kunden gespeichert werden.[7] Zugangsdaten zu unterschiedlichsten Accounts sind im Internet omnipräsent. 1

1 *ARD/ZDF*, Online-Studie 2013, Onlinenutzung.

2 108 Minuten laut *ARD/ZDF*, Online-Studie 2013, Medienausstattung / -nutzung; 80 Minuten laut *TNS Infratest*.

3 *BGH*, Urteil v. 24. 1. 2013, III ZR 98/12 – NJW 2013, 1072, Rn. 17.

4 Beliebte Nutzung sind das Lesen von Zeitungen wie Spiegel online, Welt online oder ähnlichen sowie das Nachschlagen von Informationen in der Online-Enzyklopädie Wikipedia.

5 Neben dem Video-Portal YouTube, das von amüsanten über instruktiven bis hin zu kunstvollen Videos ein breites Spektrum bietet, ist das Anschauen von Fernsehsendungen wie Nachrichten oder Dokumentationen über die Mediatheken der Fernsehsender eine beliebte Anwendung.

6 Mit 76 % der Deutschen nutzt fast jeder, der das Internet nutzt, dieses zum Versand und zum Empfang von E-Mails, *Eurostat*.

7 Im Jahr 2012 hat der deutsche Handel circa € 30 Mrd. durch eCommerce umgesetzt, *HDE*.

I. Problemaufriss

2 Diese Zugangsdaten zu den unterschiedlichen Accounts im Internet sind in der Regel nur für die Nutzung durch den Account-Inhaber bestimmt. Er soll der einzige sein, der über den Account Handlungen vornimmt. Wenn ein Dritter in den Besitz der Zugangsdaten kommt, kann er den Account wie der Account-Inhaber nutzen und somit für seine Zwecke missbrauchen. Ein Missbrauch der Zugangsdaten ist in drei Konstellationen denkbar: nach Weitergabe durch den Account-Inhaber, ohne diese Weitergabe der Zugangsdaten und bei Erstellen des Accounts durch einen Dritten.

3 Viele Account-Inhaber teilen die Zugangsdaten zu ihren Accounts innerhalb der Familie oder der Arbeitsstätte. Ein passionierter Uhrensammler mag seine Ehefrau während seiner Geschäftsreise bitten, für ihn eine gewisse Uhr bei einer Internet-Auktion zu ersteigern. Ein Rechtsanwalt kann seiner Rechtsanwaltsfachangestellten seine Signatur-Karte samt PIN zur Erstellung qualifizierten elektronischer Signaturen überlassen, damit diese Schriftsätze an Gerichte im Namen des Anwalts verschicken kann. Die Gründe für dieses Überlassen der Zugangsdaten können mannigfaltig sein. Ein effizienter Arbeitsablauf kann vorsehen, dass die Assistentin nach dem Diktat das Dokument direkt signiert und verschickt. Der Vorgesetzte kann ebenso gut aus technischer Unwissenheit oder aus Bequemlichkeit die elektronische Signierung seiner Dokumente ausführen lassen. Das einvernehmliche Überlassen der Zugangsdaten ist allgegenwärtig.

4 Problematisch wird es, wenn derjenige, der die Zugangsdaten erhalten hat, sie nicht im Sinne des Account-Inhabers nutzt; wenn er Handlungen vornimmt, mit denen der Account-Inhaber nicht einverstanden ist. Dann stellt sich die Frage, ob die Handlungen dem Account-Inhaber zuzurechnen sind und er für sie einzustehen hat. Eine solche Situation kann dadurch entstehen, dass derjenige, dem der Account-Inhaber die Zugangsdaten überlassen hat, diese Zugangsdaten zu Handlungen nutzt, die der Account-Inhaber ihm untersagt hat. Die Ehefrau aus dem Beispiel des Uhrensammlers könnte die Uhr teurer ersteigern, als der Uhrensammler vorgegeben hat, oder sie könnte statt der vorgegebenen Uhr eine Kette für sich kaufen. Dann missbraucht die Ehefrau die Zugangsdaten des Account-Inhabers und es stellt sich die Frage nach seiner Einstandspflicht.

5 Häufig gelangen die handelnden Dritten jedoch ohne die Weitergabe des Account-Inhabers an die Zugangsdaten. Im *BGH*-Fall „VIP-Bareinrich-

tung“[8] nutzte der Verlobte der Account-Inhaberin deren eBay-Account ohne ihr Wissen um eine Bareinrichtung zu versteigern. Wie er an die Zugangsdaten gelangt ist, ließ sich nicht klären.[9] Um an die Zugangsdaten zu gelangen, können Angreifer die Zugangsdaten ausspähen. Der Weg über Phishing- und Pharming-Angriffe ist insbesondere beim Online-Banking weit verbreitet.[10] Aber auch Angriffe auf Accounts zu Social-Media-Plattformen wie Facebook und Twitter kommen vor.[11] Wegen der umfangreichen Handlungsmöglichkeiten, die die Zugangsdaten zu verschiedenen Accounts erlauben, ist der Angriff mit dem Ziel des Ausspähens für Kriminelle sehr attraktiv. Mit den Zugangsdaten zum Online-Banking oder zu einem Online-Bezahldienst kann sich ein Angreifer direkte finanzielle Vorteile verschaffen. Aber auch Zugangsdaten zu anderen Accounts können ihm mittelbare materielle Vorteile bringen. Mit den Zugangsdaten zu Accounts bei Social-Media-Plattformen können sich Fan-Seiten beispielsweise mehr Fans beschaffen, die das Ansehen der jeweiligen Seite steigern.[12] In einem solchen Fall der Benutzung des Accounts ohne Weitergabe der Zugangsdaten missbraucht der Dritte die Zugangsdaten.

Ein Dritter kann ebenfalls einen Account mit einer falschen Namensangabe erstellen. Bei vielen Accounts ist dies mangels Überprüfung der Identitätsbehauptung problemlos möglich. Nimmt der Dritte anschließend Handlungen über den Account vor, von denen der Namensträger nichts wusste oder mit denen er nicht einverstanden ist, missbraucht der Dritte die Zugangsdaten. 6

Jeder, der die Zugangsdaten zu einem Accounts hat, kann dieselben Handlungen vornehmen, wie der Account-Inhaber. Ein Dritter kann eine E-Mail im Namen des Account-Inhabers verschicken, in dessen Namen Bestellungen tätigen oder Angebote auf eine Internet-Auktionsplattform einstellen. Für den Empfänger der Nachricht ist nicht ersichtlich, ob der Account-Inhaber selbst oder ein Dritter gehandelt hat. Fälle, bei denen ein Dritter für den Account-Inhaber handelt, kommen häufig vor. 7

---

8 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346.

9 Ebd., Rn. 17.

10 Durch Phishing beim Online-Banking ist im Jahr 2011 ein Schaden in Höhe von € 25,7 Mio. entstanden, *BKA*, S. 12.

11 Siehe etwa den Angriff auf den Twitter-Account von Gizmodo, *Honan*, Wired v. 8. 6. 2012. Dazu unten Rn. 223.

12 Ein Facebook-Fan soll für eine Marke einen Wert von US$ 174,17 haben, dazu *Weck*, t3n v. 18. 4. 2013.

8 Juristisch stellt sich beim Missbrauch von Zugangsdaten das Problem der Haftung. Der Geschäftsgegner hat ein Interesse daran, dass er auf die scheinbar vom Account-Inhaber stammende Erklärung vertrauen darf und das Geschäft durchgeführt wird. Er möchte beispielsweise einen Imbiss-Anhänger gegen Zahlung des günstigen Kaufpreises erhalten.[13] Der Account-Inhaber hingegen hat ein Interesse daran, nicht dadurch verpflichtet zu werden und nicht dafür haften zu müssen, dass ein Dritter seine Zugangsdaten missbraucht. Er möchte beispielsweise seinen Imbiss-Anhänger, den er zum Betrieb seines Geschäfts benötigt, nicht übereignen müssen, weil ein Dritter den Anhänger, wahrscheinlich um einen Streich zu spielen, online zum Verkauf angeboten hat.[14] Juristisch interessant ist die Frage nach der Einstandspflicht in allen Konstellationen. Praktisch von großer Bedeutung ist die Frage nach der Einstandspflicht des Account-Inhabers, wenn kein Widerrufsrecht besteht, beispielsweise bei Verträgen zwischen zwei Verbrauchern oder zwischen zwei Unternehmern.

9 Für den Geschäftsgegner stellt sich juristisch eine weitere entscheidende Frage. Um einen Anspruch gegen den Account-Inhaber gerichtlich durchzusetzen, muss er beweisen, dass er eine Handlung über den Account vorgenommen hat oder wenigstens ein Dritter, dessen Verhalten dem Account-Inhaber zurechenbar ist. Dies stellt den Geschäftsgegner vor eine große Herausforderung. Er kann bei den zahlreichen Accounts im Internet, bei denen Handlungen weltweit über jeden Rechner vorgenommen werden können, kaum Angaben dazu machen, ob und wie der Account-Inhaber oder ein Dritter die Handlung vorgenommen hat. Diese Schwierigkeit, den Beweis zu führen, könnten Account-Inhaber für Schutzbehauptungen nutzen. Sie könnten wahrheitswidrig bestreiten, eine Willenserklärung über den Account abgegeben zu haben, um sich von einem unliebsamen Vertrag zu lösen. Juristisch stellt sich daher die Frage, ob ihm der schwierig zu führende Vollbeweis durch eine abweichende Beweisführung erleichtert wird.

10 Diese Arbeit beschäftigt sich mit diesen beiden, soeben aufgezeigten Bereichen. Zum einen wird die materielle Haftung des Account-Inhabers in den unterschiedlichen Konstellationen, in denen ein Missbrauch von Zugangsdaten im Internet häufig auftritt, untersucht. Ferner werden die Beweisprobleme sowie in Frage kommende Beweiserleichterungen behandelt.

---

13 So geschehen im Fall *LG Köln*, Urteil v. 27. 10. 2005, 8 O 15/05 – BeckRS 2006, 07259.

14 Siehe ebd.

Dazu nimmt diese Arbeit zunächst die seit gut einer Dekade geführte juristische Diskussion um die Haftung für den Missbrauch von Zugangsdaten im Internet auf, um den Stand der Forschung wiederzugeben und deren Ergebnisse zu analysieren und zu bewerten.

Dabei wird sich zeigen, dass die juristische Diskussion unter gewissen Defiziten leidet, die die folgenden Beispiele verdeutlichen sollen. Ob eine Person eine E-Mail versendet habe, könne über die „volle Einsicht in sein System einschließlich aller elektronischen Papierkörbe“ zuverlässig beurteilt werden.[15] Elektronische Papierkörbe kann der Nutzer jedoch genau so wie analoge Papierkörbe restlos leeren.[16] Ebenso verfehlt ist die Behauptung, mit den Verlaufsprotokollen sowie dem Cache des Internetbrowsers könne „noch relativ lange nachvollzogen werden, welche Internetseiten aufgesucht worden sind.“[17] Die meisten Browser speichern diese temporären Daten jedoch nicht lange und viele Nutzer deaktivieren die Speicherung vollständig.[18] Diese beiden Beispiele zeigen, dass der juristische Diskurs teilweise unter dem Defizit leidet, dass die technischen Abläufe nur oberflächlich behandelt werden oder mit falschen Annahmen operiert wird. Für die Beantwortung der juristischen Frage nach der Haftung für den Missbrauch von Zugangsdaten im Internet ist ein technischer Sachverstand über die Abläufe im Hintergrund jedoch entscheidend. Eine ausführliche Auseinandersetzung mit den technischen Grundlagen ist daher erforderlich, um die juristischen Fragestellungen überzeugend zu beantworten. 11

Die juristische Diskussion über die Haftung für den Missbrauch von Zugangsdaten leidet zusätzlich unter dem Defizit, dass gleiche Sachverhalte in verschiedenen Konstellationen unterschiedlich bewertet werden. Nach der unwidersprochenen herrschenden Meinung bei Weitergabe der Zugangsdaten haftet der Account-Inhaber dem Erklärungsempfänger.[19] Der Anspruch ergebe sich aus der Anwendung einer Form der Rechtsscheinhaftung.[20] Dazu wird bei der Weitergabe ein irgendwie gearteter Rechtsscheintatbestand bejaht. In Konstellationen ohne Weitergabe der Zugangsdaten lehnt die herr- 12

15 *Mankowski*, CR 2003, 44, 49.
16 Unten Rn. 842.
17 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261.
18 Unten Rn. 869.
19 Unten Rn. 293 ff.
20 Entweder in Form der Duldungsvollmacht, unten Rn. 297 ff., oder der analogen Anwendung des § 172 Abs. 1 BGB, unten Rn. 303 ff.

schende Meinung den Rechtsscheintatbestand hingegen ab.[21] Der für den Erklärungsempfänger wahrnehmbare Schein ist jedoch in beiden Fällen der Gleiche. Er kann nicht wahrnehmen, ob der Account-Inhaber die Zugangsdaten weitergeben hat oder nicht. Bezüglich des Rechtsscheintatbestandes besteht daher kein Unterschied, der eine abweichende juristische Wertung rechtfertigt. Die unwidersprochene herrschende Meinung zur Weitergabe steht somit im Widerspruch zur herrschenden Meinung ohne Weitergabe der Zugangsdaten.[22] Überzeugend kann dieser Widerspruch aufgelöst werden, indem der Rechtsscheintatbestand bei Anwendung der allgemeinen Rechtsscheingrundsätze vor dem Hintergrund der technischen Grundlagen differenziert nach der Art des verwendeten Accounts beurteilt wird.[23]

II. Zentrale Begriffe

13 Bereits der Problemaufriss verdeutlicht, dass eine Klärung des Verständnisses von zentralen Begriffen für eine überzeugende Behandlung der juristischen Probleme wichtig ist. Ohne auf die technischen Grundlagen einzugehen, soll daher nachfolgend zunächst das Verständnis von drei entscheidenden Begriffen, den Zugangsdaten, dem Missbrauch und der Haftung, geklärt werden.

1. Zugangsdaten

14 Zugangsdaten sind all diejenigen Komponenten, die jemand benötigt, um seine Berechtigung zur Vornahme von Handlungen über einen Account im Internet nachzuweisen. Dabei kann es sich ebenso um ein Passwort wie eine Chip-Karte für eine elektronische Signatur handeln. Die Arten der Accounts im Internet sind vielfältig. Im Rahmen dieser Arbeit werden Internetanschlüsse, E-Mail-Adressen, Benutzerkonten auf Internetseiten von Informationsportalen, Online-Händler und Internet-Auktionsplattformen, das Online-Banking, Online-Bezahldienste, elektronische Signaturen, der elektronische Identitätsnachweis im neuen Personalausweis sowie die De-Mail betrachtet.

---

21 Unten Rn. 371 ff.
22 Unten Rn. 667.
23 Unten Rn. 489 ff.

2. *Missbrauch*

Ein Missbrauch der Zugangsdaten liegt vor, wenn ein Dritter die Zugangsdaten in einer Weise verwendet, mit der der Account-Inhaber nicht einverstanden ist. Dies kann dadurch geschehen, dass ein Dritter, dem der Account-Inhaber die Zugangsdaten weitergegeben hat, sie umfänglicher nutzt, als vom Account-Inhaber gestattet. Ebenso kann ein Angreifer die Zugangsdaten vom Account-Inhaber ausspähen und sie anschließend gegen den mutmaßlichen Willen des Account-Inhabers einsetzen. Eine weitere Möglichkeit Zugangsdaten zu missbrauchen, besteht darin, dass der Dritte einen Account auf den Namen eines Anderen registriert und mit diesem Handlungen vornimmt, die den Eindruck erwecken, dass der Andere diese vorgenommen hat. Darüber hinaus existieren technische Möglichkeiten einen Account zu missbrauchen, ohne die Zugangsdaten vom Account-Inhaber zu erlangen. 15

3. *Haftung*

Der Begriff der Haftung wird in der Untersuchung im Sinne einer Einstandspflicht weit verstanden. Neben der deliktischen Jedermann-Haftung, die sich aus §§ 823 ff. BGB und zahlreichen Spezialgesetzen ergibt, ist darunter auch eine „vertragliche Haftung“[24] zu verstehen. Diese vertragliche Haftung meint nicht nur Sekundäransprüche wie Schadensersatz aus *culpa in contrahendo* oder § 122 BGB, sondern umfasst auch Primäransprüche, die auch als „Haftung auf Erfüllung“[25] oder „vertrauensrechtliche Erfüllungshaftung“[26] bezeichnet werden. Unter der rechtsgeschäftlichen Haftung wird sowohl eine Haftung auf das positive als auch auf das negative Interesse verstanden. Ein zentraler Gegenstand der Untersuchung ist somit, ob beim Missbrauch von Zugangsdaten im Internet ein Vertrag zwischen dem Erklärungsempfänger und dem Account-Inhaber zustande kommt. Die deliktische Haftung des Account-Inhabers wird nur am Rande betrachtet. Gegenstand der Untersuchung ist nur die zivilrechte Haftung. Die strafrechtliche Verantwortlichkeit im Sinne der Haftung für die Konsequenzen einer möglichen Straftat wird nicht betrachtet. 16

24 *Sonnentag*, WM 2012, 1614.
25 *Flume*[4], §49 4.
26 *Canaris*, in: FG 50 Jahre BGH, Bd. 1, 129, 132.

III. Gang der Darstellung

17 Der erste Teil der Arbeit befasst sich mit den technischen und juristischen Grundlagen der Haftung für den Missbrauch von Zugangsdaten im Internet. Die bisherige juristische Diskussion über das Thema der Haftung für den Missbrauch von Zugangsdaten leidet teilweise darunter, dass die technischen Grundlagen nicht ausreichend gewürdigt werden. Um diesem Defizit zu entgegnen, beginnt diese Untersuchung mit einer Darstellung der technischen Grundlagen (Rn. 20 ff.). Bei den juristischen Grundlagen wird zunächst die Rechtsscheinhaftung (Rn. 224 ff.) allgemein betrachtet, weil diese für viele Lösungswege relevant wird. Im Anschluss folgen kurze Ausführungen zu dem juristischen Rahmen des Vertragsschlusses im Internet (Rn. 271 ff.).

18 Der Hauptteil der Arbeit widmet sich den Einzelheiten der juristischen Frage nach der Haftung für den Missbrauch von Zugangsdaten im Internet. Die Frage nach der materiellen Haftung des Account-Inhabers orientiert sich an den verschiedenen Missbrauchsmöglichkeiten. Diese Darstellung bildet die juristische Diskussion ab, die die unterschiedlichen Missbrauchswege tendenziell getrennt behandelt und somit zu unterschiedlichen und sich widersprechenden Ergebnissen kommt. Die Haftung des Account-Inhabers für den Missbrauch nach Weitergabe der Zugangsdaten (Rn. 293 ff.) wird daher vor der Haftung für den Missbrauch ohne Weitergabe der Zugangsdaten (Rn. 370 ff.) betrachtet. Anschließend werden die Haftung des Account-Inhabers bei Erstellen des Accounts durch einen Dritten (Rn. 718 ff.) sowie die Haftung der anderen Beteiligten (Rn. 762 ff.) untersucht. Die deliktische Haftung des Account-Inhabers (Rn. 726 ff.) wird nur am Rande betrachtet, sofern sie für die Beurteilung der rechtsgeschäftlichen Haftung relevant ist. Prozessuale Fragen sind bei der Haftung des Account-Inhabers ebenso so wichtig wie die materielle Rechtslage. Daher wird im Anschluss an die Untersuchung der materiellen Rechtslage die Frage nach Beweiserleichterungen behandelt (Rn. 772 ff.).

19 Zum Schluss werden die gefundenen Ergebnisse auf die verschiedenen, untersuchten Account-Typen angewendet (Rn. 830 ff.). Zuletzt werden diese Ergebnisse zusammengefasst (Rn. 910 ff.).

Kapitel 1 Technische und juristische Grundlagen

§ 2 Technische Grundlagen

I. Internet

Internet, kurz für Interconnected Networks, ist ein weltweiter Verbund von Rechnern und Computernetzwerken.[1] Den Ursprung hat das Internet im Verlangen der USA im Kalten Krieg ein dezentrales Netzwerk zu schaffen, bei dem mehrere, voneinander entfernte Rechner auf unterschiedlichen Wegen miteinander kommunizieren können.[2] Die dezentrale Struktur des Netzwerkes sollte vor einer Zerstörung bei einer militärischen Auseinandersetzung, wie einem Atomangriff, schützen.[3] Ein unzerstörbares Netzwerk sollte geschaffen werden.[4] 20

Technisch basiert das Internet auf dem TCP/IP-Protokoll,[5] einem standardisierten Protokoll, das sich aus dem Transmission Control Protocol (TCP) und dem Internet Protocol (IP) zusammensetzt. Es ermöglicht den Austausch von Datenpaketen zwischen Rechnern, die über eine IP-Adresse erreichbar sind. Die Standards des Internets werden nicht zentral vorgegeben, sondern werden von verschiedenen informellen Gremien durch gegenseitige Zustimmung der Mitglieder geschaffen.[6] Die Internet Engineering Task Force (IETF) beispielsweise legt in den Requests for Comments (RFCs) zahlreiche Standards für gängige Protokolle fest.[7] 21

Das World Wide Web (WWW), oftmals synonym mit dem Begriff Internet verwendet, ist die häufigste Nutzungsweise des Internets.[8] Das WWW besteht aus in Hypertext Markup Language (HTML) gesetzten Internetseiten, die über Hyperlinks miteinander verbunden sind.[9] Zur Betrachtung ei- 22

---

1 *Borges*, Verträge, S. 9; *Jötten*, S. 11.
2 *S. Ott*, S. 39; *T. Stadler*, Haftung für Informationen[2], Rn. 1.
3 *Ufer*, S. 5; *Dennis Werner*, Verkehrspflichten, S. 21.
4 *Rieder*, S. 35.
5 Dazu ausführlich unten Rn. 38.
6 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.2.2.
7 Beispielsweise für IPv4: *IETF*, RFC 791.
8 *S. Ott*, S. 41.
9 *Sieber*, in: *Hoeren/Sieber/Holznagel*, Kap. 1 Rn. 3.

ner Internetseite benötigt der Nutzer ein spezielles Programm, das man als Browser bezeichnet,[10] sowie die Uniform Resource Locator (URL) der Seite, die der Webserver auf Anfrage per Hypertext Transfer Protocol (HTTP) überträgt.[11] Gegenstand der Untersuchung ist das Internet inklusive seiner Vielfalt von Nutzungsweisen. Diese Untersuchung beschränkt sich nicht auf das WWW, sondern betrachtet beispielsweise auch den E-Mail-Verkehr.

23 Während sich das Internet durch seine Offenheit auszeichnet, werden technisch gleich aufgebaute Netzwerke mit geschlossenen Benutzergruppen als Intranet bezeichnet.[12] Für diese Untersuchung ist der technische Unterschied zwischen offenen und geschlossenen Netzwerken nicht relevant, sodass fortan mit dem Begriff des Internets auch Intranets umfasst sind.

24 Zwar besteht im Internet durch seinen globalen Charakter ein rechtliches Durchsetzungsproblem.[13] Das Internet ist jedoch kein rechtsfreier Raum.[14] Im Internet agieren zahlreiche Akteure wie Content-Provider, Hostprovider und Access-Provider,[15] die Gegenstand nationaler Gesetzgebung sind. Zentraler Gegenstand dieser Untersuchung sind die Nutzer des Internets,[16] die das Internet für private oder geschäftliche Zwecke verwenden, ohne einer der oben genannten Provider zu sein.

II. Zugangsdaten

25 Zugangsdaten im Internet erlauben bestimmten im Internet angebotenen Diensten ihre Benutzer wiederzuerkennen. Sie erfüllen dabei eine doppelte Funktion. Sie dienen zum einen zur Identifizierung des Account-Inhabers und legitimieren den Handelnden gleichzeitig als Berechtigten. Bei Zugangsdaten im Internet sind Identifizierung und Legitimation untrennbar verbunden. Insbesondere bei der Begriffswahl zeigt sich, dass unterschiedliche Synonyme jeweils eine der Komponenten stärker betonen. Zugangs-

---

10 Gängige Browser sind Internet Explorer, Firefox, Safari, Chrome und Opera.
11 *Borges*, Verträge, S. 24 f.; *Rieder*, S. 36.
12 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.1; *Rieder*, S. 34 f.
13 *Haug*[2], Rn. 5.
14 *Hoeren*, NJW 2008, 2615, 2616; *Rieder*, S. 65; *Schapiro*, S. 4.
15 Zu den unterschiedlichen Akteuren *Hartmann*, S. 10 f.; *T. Stadler*, Haftung für Informationen[2], Rn. 9 ff.
16 *T. Stadler*, Haftung für Informationen[2], Rn. 13.

daten werden auch als Identifikationsmittel[17] oder als Legitimationsdaten[18] bezeichnet. Diese Untersuchung verwendet den Begriff der Zugangsdaten, weil er ihre Doppelfunktion sprachlich zum Ausdruck bringt.

Gegenstand dieser Untersuchung sind sämtliche Accounts. Dazu gehören Internetanschlüsse, E-Mail-Adressen, Benutzerkonten auf Internetseiten, elektronische Signaturen, der elektronische Identitätsnachweis sowie De-Mail-Accounts. Diese Untersuchung bezweckt allgemeine Grundsätze der Haftung für den Missbrauch von Zugangsdaten im Internet herauszuarbeiten. Accounts, bei denen die Haftung für den Missbrauch spezialgesetzlich geregelt ist, wie beim Online-Banking oder beim Telefonanschluss, werden dabei nur betrachtet, um rechtliche Schlüsse davon auf die gesetzlich nicht geregelten Missbrauchsfälle zu ziehen. 26

Um eine Person in Haftung[19] zu nehmen, reicht die virtuelle Identität eines Accounts nicht aus. Der Anspruchsteller muss den Anspruchsgegner nicht nur virtuell, sondern in der realen Welt identifizieren. Er muss dafür den vollen Namen sowie eine ladungsfähige Anschrift kennen. Diese Notwendigkeit ergibt sich zum einen daraus, dass bei der Erhebung der Klage der Klagegegner mit Name und Anschrift zu benennen ist (§ 130 Nr. 1 ZPO).[20] Zum anderen kann das Recht mittels Zwangsvollstreckung nur durchgesetzt werden, wenn die Person, gegen die vollstreckt werden soll, namentlich benannt ist (§ 750 Abs. 1 S. 1 ZPO).[21] Im Folgenden wird daher untersucht, inwiefern Accounts im Internet eine Identifikationsfunktion haben. 27

1. Identität

Identität im Gegensatz zur Gleichheit bezeichnet etwas Einzigartiges.[22] Identität liegt bei einer vollständigen oder totalen Gleichheit vor. Sprachlich vollzieht sich diese Unterscheidung durch die beiden Wörter *dasselbe* und *das Gleiche*.[23] *Das Gleiche* meint, dass zwei Objekte sich in ihren 28

17 *Holzbach/Süßenberger*, in: *Moritz/Dreier*[2], C Rn. 131.
18 *Hansen*, S. 5.
19 Zum Begriff der Haftung oben Rn. 16.
20 Vgl. dazu *A. Stadler*, in: *Musielak*[10], § 130 ZPO Rn. 3.
21 Dazu *Heßler*, in: MüKo-ZPO[4], § 750 Rn. 16.
22 *Höffe*, S. 2.
23 Siehe dazu auch *Baier*, S. 34; *J. Meyer*, Identität, S. 24.

Eigenschaften gleichen im Sinne von so etwas, Derartiges.[24] *Dasselbe* hingegen bezeichnet das eine, einzigartige Objekt im Sinne von dieses und kein anderes.[25]

29 Die Bedeutung des Begriffes Identität ist vielfältig.[26] Er wird unterschiedlich in der Gegenstandstheorie, in der Biologie, in der Sozialpsychologie sowie in der Theorie des Menschen verstanden.[27] Gegenstand dieser Arbeit ist das Verständnis der Gegenstandstheorie in Form der numerischen Identität. Ihre Funktion ist die Identifizierung einer Person durch die Abgrenzung und Unterscheidung von Anderen.[28] Die numerische Identität kann definiert werden als erkennbare Übereinstimmung von Daten mit einer einzigen Person.[29]

30 Die numerische Identität kann anhand verschiedener Identitätsdaten festgestellt werden, wie Personalien, Personenkennzeichen, biographische Daten sowie körperliche Merkmale.[30] Identifikationsmerkmale sind relativ. Reichen Identitätsdaten, z.B. in Form von personenbezogenen Daten (§ 3 Abs. 1 BDSG), für den einen Datenanwender aus, um eine Person zu identifizieren, kann ein anderer Datenanwender mit denselben Daten die Person nicht identifizieren.[31] Bei einer natürlichen Person wird die numerische Identität durch den vollen Namen, das Geburtsdatum und die Anschrift bestimmt. Die Ausweisnummer des Personalausweises oder Reisepasses kann bei gleichlautenden Namen zusätzlich zum Geburtsdatum bei der Unterscheidung zweier Personen behilflich sein.

31 Die numerische Identität einer juristischen Person bestimmt sich, sofern diese in einem Verzeichnis aufgeführt ist, durch die Angabe des Registerblattes und der zur Führung des Registers zuständigen Stelle. Beispielsweise lässt sich bei der GmbH die numerische Identität so durch die Angabe des Handelsregisterblatts und des zuständigen Registergerichts bestimmen.[32] Eine juristische Person kann nicht selbst, sondern nur durch natür-

---

24 Vgl. Duden[3], gleich, dergleichen.
25 Ebd., derselbe.
26 Eine Auflistung verschiedener Definitionen enthält *Borges/Schwenk/Stuckenberg/Wegener*, S. 1.
27 *Höffe*, S. 2.
28 *J. Meyer*, Identität, S. 24 f.
29 Ebd., S. 25.
30 Ebd., S. 26 ff.
31 *Roßnagel/Scholz*, MMR 2000, 721, 723.
32 Siehe dazu *Grunewald*[8], § 13 Rn. 32.

liche Personen handeln.[33] Die Frage, ob das Handeln der natürlichen Personen nur zugerechnet wird (Vertretertheorie) oder ein eigenes Handeln der juristischen Person darstellt (Organtheorie),[34] ist für diese Untersuchung irrelevant. Entscheidend ist, dass stets eine natürliche Person die Handlungen für eine juristische Person vornehmen muss. Für die Frage, ob eine Willenserklärung einer natürlichen oder juristischen Person vorliegt, bedarf es daher stets der Handlung einer natürlichen Person. Daher wird im Rahmen dieser Arbeit die numerische Identität von natürlichen Personen, nicht jedoch jene von juristischen Personen relevant.

32 Die virtuelle Identität, auch Online-Identiät, Cyber-Identität oder digitale Identität genannt,[35] hingegen bezeichnet die Wiedererkennbarkeit in einer virtuellen Welt. Die Wiedererkennbarkeit im Internet wird regelmäßig durch Accounts hergestellt. Der Account-Inhaber kann mit dem Account Handlungen vornehmen, die ihm zuzuordnen sind. Er kann somit eine umfangreiche virtuelle Persönlichkeit aufbauen. Die Zuordnung der virtuellen Identität zu einer numerischen Identität ist möglich, aber nicht notwendig. Vielmehr kann eine virtuelle Identität von mehreren Personen unterhalten werden. Ebenso ist möglich, dass die virtuelle Identität nur von einem Rechner gesteuert wird, der nach einem programmierten Muster Handlungen vornimmt.

33 Anonymität bedeutet, dass eine Person nicht identifiziert werden kann. Da das Gelingen des Identifikationsprozesses relativ davon abhängt, ob dem Identifizierenden die verfügbaren Daten reichen, ist die Anonymität ebenfalls relativ. Absolute Anonymität liegt nur vor, wenn ein Dritter nicht anhand von Merkmalen wie Verhaltensmuster oder sozialer Kategorisierung doch eine Identifizierung vornehmen kann.[36] Anonyme Daten lassen sich nicht, nicht mehr oder nur sehr unwahrscheinlich einer Person zuordnen.[37] Anonymität im Sinne von Unerkannt bleiben ist bei Handlungen außerhalb des Internets zunächst der Regelfall.[38]

---

33 *K. Schmidt*, Gesellschaftsrecht[4], S. 248; *Schöpflin*, in: *Bamberger/H. Roth*[3], § 21 BGB Rn. 14.

34 Dazu *K. Schmidt*, Gesellschaftsrecht[4], S. 250 ff. m.w.N.

35 *J. Meyer*, Identität, S. 52 m.w.N.; *ULD*, S. 23.

36 *Brunst*, Anonymität im Internet, S. 18.

37 *Roßnagel/Scholz*, MMR 2000, 721, 723.

38 *Brunst*, Anonymität im Internet, S. 9.

34 Von der Anonymität ist die Pseudonymität zu unterscheiden.[39] Pseudonym bedeutet ein fingierter Name oder ein Deckname.[40] Pseudonyme Daten lassen sich nur mit großem Aufwand einer Person zuordnen, im Notfall kann jedoch ein Dritter den Zuordnungsschlüssel erfragen und den Handelnden identifizieren.[41] Es gibt selbstgenerierte sowie von einem vertrauenswürdigen Dritten vergebene Pseudonyme.[42] Der vertrauenswürdige Dritte kann beispielsweise ein Online-Auktionshaus oder ein Internet-Provider sein. Kenner der Zuordnungsregel können die Pseudonymität aufheben.[43] Der Übergang von relativer Anonymität zur Pseudonymität ist graduell. Weil unterschiedliche Akteure zur Identifizierung einer Person unterschiedliche Informationen benötigen, können Daten, die eine Person einem Akteur gegenüber anonym erscheinen lassen, einer anderen Person gegenüber pseudonym sein.[44]

2. *Identifikationsfunktion von Accounts im Internet*

35 Die Identifikationsfunktion eines Accounts im Internet bedeutet zunächst nur, dass die Handlungen des Accounts einer Identität zugeordnet sind.[45] Grundsätzlich besitzen alle Accounts im Internet die Funktion, die Handlungen einer virtuellen Identität zuzuordnen. Da eine Haftung voraussetzt, dass eine Person mittels ihrer numerischen Identität identifiziert werden kann,[46] stellt sich die Frage, inwiefern die virtuelle Identität eines Accounts einer numerischen Identität zugeordnet ist. Grundsätzlich hat das Internet eine depersonalisierende Funktion.[47] Der Empfänger einer Erklärung kann mangels persönlichen Kontaktes nicht feststellen, ob derjenige von dem die Erklärung zu stammen scheint, auch derjenige ist, der sie abgegeben hat.[48]

---

39 *J. Meyer*, Identität, S. 34.
40 Brockhaus[21], Pseudonym.
41 *Roßnagel/Scholz*, MMR 2000, 721, 724.
42 *Brunst*, Anonymität im Internet, S. 28; *Roßnagel/Scholz*, MMR 2000, 721, 725.
43 *Scholz*, S. 189.
44 Vgl. *Federrath/Pfitzmann*, in: *U. Schneider/Dieter Werner*[7], 14.4.5.
45 *Klein*, MMR 2011, 450.
46 Siehe oben Rn. 27.
47 *Hoeren*, NJW 2008, 2615.
48 *Hoeren*, NJW 1998, 2849, 2854.

Eine Haftung für Handlungen von einem Account im Internet setzt somit zunächst voraus, dass der virtuellen Identität des Accounts eine numerische Identität zugeordnet sein soll. Um diese Zuordnung zu beurteilen, sollen zwei Eigenschaften einer für den Rechtsverkehr brauchbaren Identifikationsfunktion Maßstab sein. Zum einen muss die Identifikationsfunktion zuverlässig sein. Das bedeutet, dass der Rechtsverkehr sich darauf verlassen kann, dass der ausgewiesene Account-Inhaber auch derjenige ist, der die virtuelle Identität erstellt hat.[49] Die Zuverlässigkeit der Identifikationsfunktion kann insbesondere durch eine Überprüfung der Identität des Account-Inhabers beim Erstellen des Accounts erreicht werden. 36

Zum anderen muss die Identifikationsfunktion für den Rechtsverkehr nachvollziehbar sein. Das bedeutet, dass ein möglicher Anspruchsteller zur Verfolgung seiner Rechte in der Lage sein muss, eine eventuelle pseudonyme virtuelle Identität namentlich einer numerischen Identität mit allen für die Verfolgung von Rechten notwendigen Daten zuzuordnen. Eine Trusted Authority, ein vertrauenswürdiger Dritter, gegen die ein Auskunftsanspruch unter bestimmten Voraussetzungen besteht, kann eine solche Nachvollziehbarkeit der Identifikationsfunktion sicherstellen. Beispielsweise kann ein Auskunftsanspruch gegen die Trusted Authority bestehen, die numerische Identität hinter einem Pseudonym aufzudecken.[50] 37

a) Internetzugang – IP-Adresse

Zunächst stellt sich die Frage, ob ein Internetnutzer bei seinen Handlungen im Netz, z.B. dem Surfen auf einer Webseite, identifizierbar ist. Dazu soll zunächst die Funktionsweise des Internets mittels der Protokolle TCP/IP betrachtet werden. Jeder Rechner, der am Internet teilnimmt, hat eine IP-Adresse, über die er in gewissem Maße identifizierbar ist. Die IP-Adresse besteht in der Version 4 des Internet Protocol (IPv4)[51] aus 4 Byte.[52] In der sechsten Version (IPv6)[53] besteht die IP-Adresse aus 16 Byte, um den 38

49 Für Ausweissysteme wird dies auch als Verlässlichkeit bezeichnet, *Bohrer*, MittBayNot 2005, 460, 461.

50 Wie der Auskunftsanspruch gegen den De-Mail-Anbieter, unten Rn. 95.

51 Nach *IETF*, RFC 791.

52 *Löffler*, in: *U. Schneider/Dieter Werner*[7], 10.3.2.1; *Borges*, Verträge, S. 18.

53 Standardisiert durch *IETF*, RFC 2460.

gestiegenen Bedarf an zu vergebenden IP-Adressen zu decken.[54] Über eine Adressierung an eine IP-Adresse kann ein Datenpaket von der Quelle zum Ziel geschickt werden.[55] Zugang zum Internet und damit zu einer IP-Adresse erhält ein Nutzer über einen Internet Service Provider (ISP). Der Internetanschluss kann zum einen über eine feste Leitung, wie einem DSL-Anschluss[56] erfolgen, oder über ein mobiles Endgerät in einem Datenfunknetzwerk.[57]

aa) Internetanschluss

39 Zunächst stellt sich die Frage, ob ein Internetanschluss eine Identifikationsfunktion bezüglich einer numerischen Identität besitzt. Um einen eigenen Internetanschluss zu erhalten, muss der Anschlussinhaber regelmäßig mit einem ISP ein Dauerschuldverhältnis eingehen. Der ISP hat ein Interesse daran, bei diesem Dauerschuldverhältnis die Kreditwürdigkeit seines Vertragspartners zu überprüfen.[58] Bei der Anmeldung werden die Personalien des Geschäftspartners und späteren Anschlussinhabers daher überprüft. Ferner findet oft zur Bestimmung der Kreditwürdigkeit ein Abgleich mit den Daten der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) statt.[59] Dieses Verfahren ist gleich bei festen Internetanschlüssen in Haus und Wohnung sowie mobilen Anschlüssen über Mobiltelefone.

40 Bei einem festen Internetanschluss kommt ferner hinzu, dass der ISP eine physikalische Verbindung zu seinem Vertragspartner braucht.[60] Eine Verbindung zum Internet funktioniert über das Telefon- oder Kabelnetz nur, wenn der Anschlussinhaber physikalisch mit dem Netz des ISP verbunden ist. Über diese physikalische Verbindung ist sichergestellt, dass der ISP den Anschlussinhaber mittels häuslicher Adresse identifizieren kann. Häufig muss ein Internetanschluss vor der Anmeldung eingerichtet werden, wofür viele Kunden einen Techniker des ISP in Anspruch nehmen. In diesen Fällen kann der ISP sogar vor Ort die Identität des Anschlussinhabers ve-

54 *Freund/Schnabel*, MMR 2011, 495; *Sieber*, in: *Hoeren/Sieber/Holznagel*, Kap. 1 Rn. 57.
55 *Dennis Werner*, Verkehrspflichten, S. 34.
56 *Löffler*, in: *U. Schneider/Dieter Werner*[7], 10.2.6.4.
57 *Löffler*, in: *U. Schneider/Dieter Werner*[7], 10.2.7.5; *Tanenbaum/Wetherall*[5], S. 91 ff.
58 *Redeker*, in: *Hoeren/Sieber/Holznagel*, Kap. 12 Rn. 160.
59 Vgl. *Hoeren*, in: Verbraucherrecht, § 21 Rn. 211.
60 *Löffler*, in: *U. Schneider/Dieter Werner*[7], 10.2.6.4.

rifizieren. Internetanschlüsse sind daher mit der numerischen Identität des Anschlussinhabers verknüpft.

bb) WLAN

Typischerweise wird ein Internetanschluss mittlerweile nicht mehr nur über einen Rechner angesteuert, sondern die Verbindung wird mittels (W)LAN mit mehreren Rechnern geteilt.[61] Als Beispiel dafür soll das WLAN betrachtet werden. Dieses ermöglicht es, ein Netzwerk drahtlos ohne Verkabelung herzustellen, in dem beispielsweise die Internetverbindung eines ISP mit weiteren Mitnutzern geteilt werden kann.[62] 41

Um sich zu einem WLAN zu verbinden, benötigt der Rechner einen Access-Point, eine Basisstation, die die Möglichkeit des Verbindungsaufbaus zur Verfügung stellt.[63] Die Kommunikation zwischen dem Access-Point und dem Rechner ist durch den Standard IEEE 802.11 festgelegt.[64] Weil unverschlüsselte WLAN-Verbindungen mitgelesen werden können, sind viele WLAN mit den Verschlüsselungsprotokollen WEP oder WPA2 gesichert.[65] 42

cc) IP-Adresse

Sodann stellt sich die Frage, ob von der Identifikationsfunktion des Internetanschlusses bei dessen Benutzung mit einer bestimmten IP-Adresse eine Identifikationsfunktion der IP-Adresse abgeleitet werden kann. Jede öffentliche IP-Adresse wird weltweit nur einmal vergeben, sodass der Anschluss darüber identifizierbar ist.[66] Private IP-Adressen hingegen, die dazu dienen Rechner in lokalen Netzwerken anzusprechen, werden über das Internet nicht geroutet und können nur einmal pro Netzwerk, aber beliebig oft in verschiedenen Netzwerken vergeben werden.[67] Die Registrierungsstelle Internet Corporation for Assigned Names and Numbers (ICANN) und deren 43

61 Mit Beispielen *Eckert*[8], S. 892 f.
62 *Dennis Werner*, Verkehrspflichten, S. 29.
63 *Tanenbaum/Wetherall*[5], S. 97.
64 *Löffler*, in: *U. Schneider/Dieter Werner*[7], 10.2.7.3; *Eckert*[8], S. 893 f.
65 *Eckert*[8], S. 905 ff.; *Tanenbaum/Wetherall*[5], S. 99; *Dennis Werner*, Verkehrspflichten, S. 95.
66 *J. Meyer*, Identität, S. 36.
67 Vgl. *Sieber*, in: *Hoeren/Sieber/Holznagel*, Kap. 1 Rn. 56.

lokale Network Information Centers (NICs) vergeben die öffentlichen IP-Adressen.[68] So kann für jede IP-Adresse deren Inhaber bei der zuständigen Registrierungsstelle abgefragt werden.

44 Öffentliche IP-Adressen lassen sich in die Kategorien der dynamischen und statischen Adressen einteilen.[69] Rechner, die permanent und dauerhaft mit dem Internet verbunden sind, verwenden häufig statische IP-Adressen. Zahlreiche Firmen und Organisationen und nicht zuletzt Universitäten haben solche statischen IP-Adressen. Bei statischen IP-Adressen ist regelmäßig deren Benutzer als Inhaber eingetragen. Die Institution, von der die Anfrage kam, ist durch die statische IP-Adresse mittels einer Whois-Anfrage[70] beim zuständigen NIC identifizierbar.

45 Dynamische IP-Adressen sind häufig bei privaten Endanwendern im Einsatz, weil viele ISPs sie aus Effizienzgründen einsetzen. Der ISP registriert weniger IP-Adressen als er Internetanschlüsse vergibt und ordnet den Internetanschlüssen bei Bedarf eine IP-Adresse zu. Er kann somit das Verhältnis von IP-Adresse zu Kunden auf bis zu 1:20 absenken.[71] Der ISP ist dabei regelmäßig als Inhaber der IP-Adresse eingetragen. Er kann die Pseudonymität der dynamischen IP-Adresse auflösen und Auskunft darüber geben, zu welchem Zeitpunkt diese IP-Adresse welchem Anschlussinhaber zugeordnet war. An der Zuverlässigkeit der nachträglich ermittelten Zuordnung zweifeln einige Stimmen der Literatur.[72] Darüber hinaus sorgen Anonymisierungsdienste dafür, dass bei ihrem Nutzer die Zuordnung der IP-Adresse zum Nutzer des Anschlusses nicht möglich ist.[73] Diese Anonymisierungsdienste arbeiten über einen sog. Proxy-Server. Der unerkannt bleibende Nutzer schickt alle Anfragen an den zwischengeschalteten Proxy-Server, der diese an die anderen Server weiterleitet und die Antworten empfängt und dem Nutzer weitergibt.[74] Alle Anfragen über den Proxy-Server versendet dieser von der gleichen IP-Adresse.[75] Nur der Proxy-Server weiß, von

---

68 *Sieber*, in: *Hoeren/Sieber/Holznagel*, Kap. 1 Rn. 54, 63 f.

69 Ebd., Kap. 1 Rn. 55.

70 Mit einer Whois-Abfrage können die gespeicherten Bestandsdaten zu einer IP-Adresse oder Domain bei der zuständigen Registrierungsstelle abgefragt werden.

71 *M. Köhntopp/K. Köhntopp*, CR 2000, 248; *Grosskopf*, CR 2007, 122, 123.

72 *Alsbih*, DuD 2011, 482; *Grosskopf*, CR 2007, 122, 123; *Gietl/Mantz*, CR 2008, 810, 814 f.; *Hannemann/Solmecke*, MMR 2011, 398, 400.

73 *Brunst*, Anonymität im Internet, S. 130; *Dennis Werner*, Verkehrspflichten, S. 38; *Jandach*, in: FS Kilian, 443, 446.

74 *Brunst*, Anonymität im Internet, S. 133; *Gaycken*, S. 236.

75 *Brunst*, Anonymität im Internet, S. 133; *Jandach*, in: FS Kilian, 443, 446.

welchem konkreten Nutzer eine gewisse Anfrage stammt. Wenn er nach der Verbindung diese Daten löscht, wie es Anonymisierungsdienste tun, kann der Internetnutzer nicht mehr identifiziert werden.[76] Ferner ist es möglich, die Absender-Adresse bei einem versendeten Datenpaket zu fälschen (IP-Spoofing).[77] Zwar kann der Verwender der falschen IP-Adresse unter dieser nur Pakete verschicken und keine Datenpakete empfangen. Durch das IP-Spoofing können jedoch Datenpakete so versendet werden, dass diese, obwohl sie nicht aus dem Netz des Anschlussinhabers kommen, diesen Eindruck vortäuschen.

Kann anhand der IPv4-Adresse statisch oder dynamisch mit Hilfe des ISP der Anschlussinhaber ermittelt werden, so identifiziert die IP-Adresse nur einen Rechner, also den Server, Computer oder Router, der die Internetverbindung hergestellt hat. Die Internetverbindung muss jedoch noch nicht einmal auf einen konkreten Rechner hindeuten. Teilt sich der Anschlussinhaber, z.B. ein Haushalt oder eine Universität, einen Internetzugang auf verschiedene Rechner durch ein (W)LAN auf, kann durch die IP-Adresse noch nicht einmal auf einen konkreten Rechner geschlossen werden. Dadurch, dass mehrere Rechner sich eine IP-Adresse teilen können, lässt sie keinen Rückschluss auf den tatsächlich verwendeten Rechner zu.[78] 46

Darüber hinaus lassen sich selbst anhand eines konkreten Rechners keine Rückschlüsse auf die Person, die ihn benutzt hat, schließen. Mittels des Authentication-Headers bei IPv6[79] oder anderer Global Unique Identifier (GUID)[80] kann feststellt werden, von welchem Rechner eine bestimmte Internetkommunikation ausging. Ein Rechner kann von vielen Personen genutzt werden, sodass der Rechner keine Identifikationsfunktion bezüglich einer Person besitzt.[81] Anhand der IP-Adresse kann der Inhaber eines Internetanschlusses identifiziert werden. Dadurch kann jedoch nur in Erfahrung gebracht werden, dass der Handelnde einen Rechner, dem der Anschluss-Inhaber die Nutzung des Internetanschlusses gewährt oder der sich in das 47

76 *Brunst*, Anonymität im Internet, S. 133; *Gaycken*, S. 236.
77 *Eckert*[8], S. 119 f.
78 *R. Dietrich*, NJW 2006, 809, 811; *J. Meyer*, Identität, S. 36; *Dennis Werner*, Verkehrspflichten, S. 38.
79 Dazu *Federrath/Pfitzmann*, in: *Moritz/Dreier*[2], A Rn. 34; *Freund/Schnabel*, MMR 2011, 495, 496; *Tanenbaum/Wetherall*[5], S. 523 ff.
80 Dazu *Scholz*, S. 61 f.
81 *Bösing*, S. 17.

Netz des Anschluss-Inhabers eingeschlichen hat, nutzte. Ein Rückschluss auf den Handelnden ist über die IP-Adresse allein nicht möglich.[82]

b) E-Mail-Adresse

48 Electronical Mail (E-Mail) ist ein Dienst im Internet, der es den Nutzern ermöglicht, elektronische Nachrichten mit beliebigen Anhängen zu versenden.[83] Die E-Mail-Adresse bezieht sich auf ein Postfach, an das Nachrichten geschickt werden können. Sie besteht aus einem lokalen und einem globalen Teil, die durch ein @-Zeichen getrennt sind.[84] Der lokale Teil bezeichnet das Postfach, der globale Teil beinhaltet den Hostnamen, die Domain oder IP-Adresse des Servers, an den die E-Mail ausgeliefert werden soll. Eine E-Mail ist in zwei Teile aufgeteilt: den Header und den Body.[85] Im Header befinden sich die Informationen über die E-Mail selbst wie Absender- und Empfängeradresse sowie die Betreffzeile und andere Verwaltungsinformationen.[86] Im Body befindet sich der Text der E-Mail sowie etwaige Anhänge.[87]

49 Die beiden Enden der E-Mail-Kommunikation, das Absenden und das Empfangen, werden über zwei verschiedene Protokolle bewältigt. Das Versenden von E-Mails erfolgt über Simple Mail Transfer Protocol (SMTP).[88] Der SMTP-Server nimmt die E-Mails des Absenders entgegen und übermittelt sie an den Mailserver des Empfängers unter Einbeziehung verschiedener Mail Transfer Agents (MTAs).[89] Ein ständig erreichbarer Mailserver nimmt die E-Mails entgegen und speichert sie im Postfach des Nutzers.[90] Eine Authentisierung ist im Rahmen vom SMTP möglich und weit verbreitet, jedoch

82 So auch *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 15; *Sieber*, in: *Hoeren/Sieber/Holznagel*, Kap. 1 Rn. 54; *M. Köhler/Arndt/Fetzer*[7], Rn. 322; *J. Meyer*, Identität, S. 36.

83 *Wißner/Jäger*, in: Computerrechts-Handbuch, 300.

84 *Borges*, Verträge, S. 23; *Hoeren*, Internetrecht[2], S. 14 f.

85 Definiert durch *IETF*, RFC 2822.

86 *Dennis Werner*, Verkehrspflichten, S. 45.

87 *Borges*, Verträge, S. 23.

88 Nach dem Standard *IETF*, RFC 5321.

89 *F. A. Koch*, Internet-Recht[2], S. 30; *Pohlmann*, DuD 2010, 607, 608; *Dennis Werner*, Verkehrspflichten, S. 44.

90 *Sieber*, in: *Hoeren/Sieber/Holznagel*, Kap. 1 Rn. 113.

im Standard nicht als Voraussetzung definiert.[91] Ebenso wenig gehört eine Ende-zu-Ende-Verschlüsselung der Kommunikation zum Standard, ist aber über Secure Sockets Layer (SSL) möglich.[92]

Der Empfänger kann die E-Mail anschließend jederzeit von seinem Post- 50
fach abrufen. Dazu stehen ihm die Protokolle Post Office Protocol, Version 3 (POP3)[93] und Internet Message Access Protocol (IMAP)[94] zur Verfügung. Zum Abruf der E-Mails kann der Nutzer ein E-Mail-Programm,[95] ein sog. Mail User Agent (MUA), oder Webmail[96] verwenden. Beim Webmail braucht der Nutzer kein E-Mail-Programm auf seinem Rechner zu installieren, sondern kann mit seinem Browser auf seine E-Mails zugreifen. Die Webmail-Anwendung greift regelmäßig wie ein E-Mail-Programm per IMAP auf die Daten zu.

Für die Identifikationsfunktion von E-Mail-Adressen ist es entscheidend, 51
wie der Inhaber eine E-Mail-Adresse erstellen kann. Zunächst kann jeder Rechner als Mailserver fungieren und entsprechende Postfächer, die über eine oder mehrere E-Mail-Adressen erreichbar sind, einrichten. Um im Internet permanent erreichbar zu sein, braucht dieser Server eine globale IP-Adresse, die häufig zur Vereinfachung über eine Domain erreichbar ist. Über die IP-Adresse oder Domain kann deren Inhaber ermittelt werden und dieser kann gegebenenfalls Auskunft darüber geben, wem er das Postfach zugeordnet hat.

Die meisten E-Mail-Adressen werden von Firmen, Institutionen und Or- 52
ganisationen unter deren Domain vergeben. Häufig bekommen Mitarbeiter E-Mail-Adressen in der Form vorname.nachname@firma.de. Über die Domaininhaberschaft besteht theoretisch die Möglichkeit, nachzufragen, für wen ein E-Mail-Postfach eingerichtet wurde. Während im geschäftlichen Bereich bis zu einem gewissen Maße erwartet werden kann, dass Firmen und Institutionen E-Mail-Adressen nur nach Überprüfung der Identität vergeben und verwaiste E-Mail-Adressen zügig unerreichbar machen, kann im privaten Rechtsverkehr nicht davon ausgegangen werden.

---

91 *IETF*, RFC 5321, S. 75. Siehe auch *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.4.3; *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211.

92 *Dennis Werner*, Verkehrspflichten, S. 49 f.

93 Standardisiert durch *IETF*, RFC 1939.

94 Nach *IETF*, RFC 3501.

95 Gängige E-Mail-Programme sind Outlook, Mozilla Thunderbird, Windows Mail, OS X Mail sowie Mail-Programme von mobilen Betriebsystemen.

96 *Dennis Werner*, Verkehrspflichten, S. 49.

53 Private Personen nutzen häufig die Dienste von sog. Freemail-Anbietern.[97] Eine Überprüfung der Daten bei der Registrierung findet regelmäßig nicht statt.[98] Früher haben einige Anbieter einen Brief an die angegebene Adresse geschickt, um die Identität des Nutzers zu bestätigen. Diese Praxis haben die Anbieter mittlerweile nicht nur aus kostentechnischen sondern auch aus rechtlichen Gründen aufgegeben.[99] Lediglich eine Plausibilitätskontrolle der eingegebenen Daten findet statt, so muss z.B. eine existierende Straße mit zugehöriger Postleitzahl angegeben werden. Andere Anbieter lassen sogar eine komplett anonyme Erstellung eines E-Mail-Postfachs zu.[100] Das anonyme Anlegen einer kostenlosen E-Mail-Adresse ist daher problemlos möglich.

54 Andererseits kann die E-Mail-Adresse einen Namen enthalten und dadurch ein Identitätsdatum[101] oder sogar ein geschützter Name im Sinne des § 12 BGB sein.[102] Wird ein Name in einer E-Mail-Adresse verwendet, lässt dieser Name wegen Verwechselungsgefahr keinen Rückschluss auf eine Person in Form einer numerischen Identität zu.[103] Es können mehrere Personen mit dem gleichen Namen existieren, sodass z.B. die E-Mail-Adresse peter.meier@web.de wenig Aufschluss darüber gibt, wem sie gehört. Ferner kann der Name einer E-Mail-Adresse frei gewählt werden, ohne dass diese Angaben überprüft werden, sodass ein Rückschluss auf eine Person schwer möglich ist.

55 Scheinbar einfach zu ermitteln wäre der Inhaber einer E-Mail-Adresse, wenn eine Person sich eine Domain registriert und diese zum E-Mail-Versand verwendet. Registriert sich Max Mustermann die Domain mustermann.de und richtet sich eine E-Mail-Adresse max@mustermann.de ein, spricht zum einen die Bezeichnung in der E-Mail-Adresse, zum anderen die Inhaberinformationen der Domain dafür, dass dem als Domaininhaber bezeichneten Max Mustermann diese E-Mail-Adresse gehört. Eine Identifikationsfunktion bezüglich der numerischen Identität kann selbst bei diesem Fall nicht angenommen werden. Zum einen könnte der Domain-Inhaber die

---

97 Dazu gehören web.de, gmx.de, Google, Yahoo und Hotmail.

98 *Ernst*, MDR 2003, 1091; *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211; *Stöber*, JR 2012, 225, 229.

99 *Brunst*, Anonymität im Internet, S. 86.

100 Ebd., S. 87.

101 *J. Meyer*, Identität, S. 37.

102 *S. Münch*, S. 154.

103 Vgl. *LG Köln*, Urteil v. 3. 2. 2000, 14 O 322/99 (Maxem.de) – MMR 2000, 437, 438.

Domain über einen Domaintreuhänder registrieren.[104] Zum anderen prüft die Denic (Deutsches Network Information Center eG) bei der Registrierung der Domain lediglich, dass eine Adresse in Deutschland angegeben wurde.[105]

Eine Person kann mehrere E-Mail-Adressen besitzen. Dies hat jedoch keine Auswirkungen auf die Identifikationsfunktion der E-Mail-Adressen. Dafür entscheidend ist allein, ob die E-Mail-Adresse auf den Inhaber rückschließen lässt. Kann eine Person über mehrere E-Mail-Adressen eindeutig identifiziert werden, schadet die Vielzahl der E-Mail-Adressen nicht. Eine Person kann beispielsweise auch mehrere Bankkonten haben, ohne dass die Identifikationsfunktion der Bankkonten darunter leidet. 56

Gegen die Identifikationsfunktion bezüglich der numerischen Identität von E-Mail-Adressen spricht ferner, dass E-Mail-Adressen keiner natürlichen Person zugeordnet sein müssen. Zahlreiche Firmen verwenden beispielsweise E-Mail-Adressen in der Form info@firma.de oder mail@firma.de. Zwar kann man, mit der Zuverlässigkeit der Domain-Inhaberinformationen davon ausgehen, dass diese E-Mail-Adresse zu der domaininhabenden Firma gehört. Eine juristische Person kann jedoch als solche nicht handeln, sondern natürlichen Personen müssen die Handlungen für sie vornehmen.[106] Eine solche E-Mail-Adresse hat daher keine ausreichende Identifikationsfunktion bezüglich einer numerischen Identität einer natürlichen Person, die zum Handeln gebraucht wird. Anhand der E-Mail-Adresse lässt sich somit nicht auf deren Inhaber in Form einer numerischen Identität schließen.[107] 57

c) Passwortgeschützte Benutzerkonten auf Internetseiten

Benutzerkonten werden definiert als: „Zugangsberechtigung zu einem Computer oder Netzwerk. Setzt sich in der Regel aus Benutzername und Passwort zusammen. Beides muss vom Anwender zur Identifizierung eingegeben werden.“[108] Bei dieser Definition fehlt jedoch ein entscheidendes Merkmal der Benutzerkonten im Internet. Ein Benutzerkonto im Internet ent- 58

104 *P. Koch*, in: Computerrechts-Handbuch, Kap. 2 Rn. 347.
105 Vgl. *Denic*, §§ 2 Abs. 2, 3 Abs. 3. Dazu auch *Wien*[3], S. 21.
106 Dazu oben Rn. 31.
107 So auch *J. Meyer*, Identität, S. 37; *S. Münch*, S. 155; *Stöber*, JR 2012, 225, 229.
108 *Wißner/Jäger*, in: Computerrechts-Handbuch, 300.

steht durch die Registrierung. Diese Begrenzung auf eine Plattform führt dazu, dass ein Benutzerkonto kein allgemeines Identifizierungsinstrument ist.[109] Zwar kann ein Account-Inhaber gegebenenfalls mittels Single Sign-on (SSO)[110] das Benutzerkonto auf weiteren Internetseiten benutzen. Authentisieren kann sich der Inhaber des Benutzerkontos mit diesem jedoch nur gegenüber dem Betreiber der Internetseite, bei der er sich registriert hat. Andere Internetseiten, die sich dem SSO angeschlossen haben, erhalten nur das Ergebnis des Authentisierungsvorgangs, die Autorisierung.

59 Bei einem Benutzerkonto ist zwischen dem Konto selbst und dem Nutzerprofil zu unterscheiden.[111] Das Benutzerkonto ist das Verhältnis zum Betreiber der Internetseite oder Plattform. Mittels der Zugangsdaten zum Benutzerkonto kann sich der Inhaber gegenüber dem Plattformbetreiber authentisieren. In einfacher Form besteht das Nutzerkonto aus Login-Name, der nicht identisch mit dem Nutzernamen seines Nutzerprofils sein muss, sowie einem Passwort.[112] Das Nutzerprofil hingegen ermöglicht dem Account-Inhaber mit anderen Nutzern der Plattform zu kommunizieren. Nach erfolgreicher Authentifizierung gegenüber dem Plattformbetreiber autorisiert dieser den Nutzer, mit dem Nutzerprofil auf der Plattform zu kommunizieren. Jede Internetseite kann grundsätzlich technisch die Voraussetzungen schaffen, dass sich die Besucher dort ein Nutzerkonto einrichten können.[113] Wegen der unterschiedlichen Bedeutung dieser Nutzerkonten ist bezüglich der Identifikationsfunktion zu unterscheiden.[114]

aa) Informationsportale

60 Eine Kategorie Internetseiten, die typischerweise Nutzerkonten einsetzen, sind Informationsportale. Dazu gehören zum einen Meinungsforen, auf denen sich die Nutzer über allgemeine oder gewisse vorgegebene Themen austauschen können.[115] Zum anderen gehören auch gemeinsam erstellte Wissensdatenbanken wie *Wikipedia*[116] dazu. Die Angabe umfassender vali-

109 *Bösing*, S. 18.
110 Dazu *Wefel*, S. 21 ff.
111 *J. Meyer*, Identität, S. 32.
112 Ebd., S. 32.
113 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256 f.
114 So auch *Herresthal*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 29.
115 Dazu *Hartmann*, S. 21 f.; *Hollenders*, S. 36; *Schapiro*, S. 17 ff.
116 *Wikipedia*, Über Wikipedia.

der Daten, die eine Person identifizieren könnte, ist regelmäßig nicht erforderlich.[117] Teilweise wird noch nicht einmal die E-Mail-Adresse verifiziert. Bei *Wikipedia* ist die Angabe der E-Mail-Adresse optional.[118] Eine Identifikationsfunktion besitzt ein solcher Account daher nur in sehr geringem Umfang. Er identifiziert lediglich die virtuelle Identität des Accounts.

Andere Informationsportale verlangen häufig bei der Registrierung ei- 61
ne E-Mail-Adresse, bei der überprüft wird, dass der Account-Inhaber E-Mails unter dieser Adresse empfangen kann.[119] Nach Ausfüllen des Registrierungsformulars wird eine Aktivierungsmail an die E-Mail-Adresse geschickt. Diese E-Mail enthält einen Link und einen Aktivierungscode, die der Account-Inhaber zur Bestätigung seiner Identität aufrufen bzw. eingeben muss. Dieses Verfahren stellt sicher, dass der sich Registrierende Zugriff auf das E-Mail-Konto hat, dessen Inhaber er zu sein vorgibt. In diesem Fall ist der Inhaber des Accounts ebenso wenig zu identifizieren, wie der Inhaber der E-Mail-Adresse.[120] Speichert das Informationsportal bei der Registrierung des Accounts die IP-Adresse, kann über diese ebenfalls nicht der Handelnde, sondern nur der konkrete Rechner oder der Anschlussinhaber identifiziert werden.[121]

bb) eCommerce-Seiten, Online-Shops

eCommerce-Seiten zeichnen sich dadurch aus, dass sich ein Nutzer dort 62
registriert, um mit dem Betreiber der Seite Verträge abzuschließen. Ein Online-Versandhandel wie Amazon fällt z.B. in diese Kategorie. Eine (Waren-)Bestellung bei einem Online-(Versand-)Händler erfordert die Eingabe valider Daten, wie Name und Anschrift des Handelnden. Der Aussteller der Rechnung ist gesetzlich verpflichtet diese Daten zu erfragen, weil er sie regelmäßig auf der Rechnung aufführen muss.[122] Ferner bedarf es bei der Bestellung physikalischer Güter einer Anschrift, um diese an den Kunden liefern zu können. Accounts bei eCommerce-Internetseiten soll daher grund-

117 *Hartmann*, S. 21.
118 *Wikipedia*, Anmelden.
119 *Schapiro*, S. 18.
120 Zur Identifikationsfunktion von E-Mail-Adressen oben Rn. 48.
121 Oben Rn. 38.
122 Unten Rn. 596.

sätzlich eine Identifikationsfunktion bezüglich einer numerischen Identität zukommen.

63 Das primäre Interesse des Online-Händlers liegt nicht in der zuverlässigen Identifikation des Kunden, sondern in der Sicherstellung, dass er seine Leistung vergütet bekommt.[123] Darin ist der Grund zu sehen, warum E-Mail-Adressen bei einem Bestellvorgang regelmäßig nicht überprüft werden. Viele Online-Händler verlangen bei Bestellungen – manche nur bei der ersten Bestellung – eine Zahlungsweise, die dem Online-Händler die Zahlung garantiert. Dazu gehören klassische Kreditkarten oder Online-Bezahldienste wie PayPal. Durch eine garantierte Zahlung kann dem Online-Händler wie bei einem „Geschäft für den, den es angeht," die Identität des Vertragspartners von geringer Bedeutung sein.[124] Accounts bei Online-Händlern kommen somit grundsätzlich eine für den Händler nachvollziehbare Identifikationsfunktion zu. An der Zuverlässigkeit der Identifikationsfunktion sind jedoch Zweifel angebracht.

cc) Internet-Auktionsplattformen mit Reputationssystem

64 Bei Internet-Auktionsplattformen stellt der Betreiber der Plattform ein System bereit, das registrierten Nutzern erlaubt, nach festgelegten Regeln Verträge miteinander zu schließen.[125] Der Verkäufer einer Ware kann auf der Plattform ein Angebot freischalten,[126] auf das andere Nutzer anschließend bieten können. Der Anbieter der Ware legt einen Zeitraum fest, an dessen Ende ein Vertrag mit dem Höchstbietenden zustande kommen soll.[127] Beim weiteren Gang dieser Untersuchung wird häufig eBay als Beispiel für eine Internet-Auktionsplattform gewählt, da eBay Marktführer und Gegenstand zahlreicher Entscheidungen der Rechtsprechung sowie vielfältiger Diskussionen in der Literatur ist.

65 In die Integrität der Accounts bei Internet-Auktionsplattformen herrsche ein großes Vertrauen, weil der Plattformbetreiber in der Pflicht ist und ein Interesse daran hat, Missbrauch zu verhindern.[128] eBay führt eine Plausibi-

123 Vgl. dazu auch *M. Köhler/Arndt/Fetzer*[7], Rn. 172.
124 So auch ebd., Rn. 172.
125 *Hartmann*, S. 18; *Schapiro*, S. 14 f.
126 *Schapiro*, S. 15.
127 *Gurmann*, S. 6 f.; *Hartmann*, S. 19.
128 *Mankowski*, NJW 2002, 2822, 2824.

litätskontrolle der Daten bei der Registrierung durch und gleicht die eingegebenen Daten mit der Schufa ab.[129]

66 Ferner soll das Bewertungssystem Vertrauen in die korrekte Zuordnung der virtuellen Identität des Accounts zur numerischen Identität des benannten Account-Inhabers sicherstellen.[130] Bei dem Bewertungssystem oder auch Reputationssystem von Internet-Auktionsplattformen können Nutzer nach einer abgeschlossenen Transaktion den Geschäftspartner positiv, negativ oder neutral bewerten.[131] Die Anzahl der positiven abzüglich der negativen Bewertungen oder der Prozentanteil positiver Bewertungen wird bei manchen Plattformen hinter dem Nutzernamen angezeigt, sodass andere Nutzer einen Eindruck gewinnen können, wie zuverlässig der Account ist.[132] Dadurch schafft die Internet-Auktionsplattform eine explizite Reputation, die Nutzern anhand von Kennziffern ermöglicht, die Zuverlässigkeit des Gegenübers abschätzen zu können.[133] Dieses Bewertungssystem stärkt das Vertrauen in das Handeln durch das Verleihen einer Reputation für eine wiedererkennbare Online-Persönlichkeit.[134] Dabei funktioniert das Bewertungssystem wie Mundpropaganda in der Offline-Welt[135] mit dem Unterschied, dass die Bewertungen für jeden ständig erreichbar und abrufbar sind. Das Bewertungssystem dient dazu, die fehlende Möglichkeit, durch einen persönlichen Kontakt Vertrauen zu gewinnen, zu kompensieren.[136] Es erfüllt damit zugleich zwei Funktionen. Primär wird die Notwendigkeit der genauen Identifikation des Geschäftspartners dadurch abgeschwächt, dass dessen Zuverlässigkeit bescheinigt wird. Sekundär können positive Bewertungen auch darauf hindeuten, dass die Identitätsbehauptung im Account zutrifft.[137] Grundsätzlich kommt Accounts auf Internet-Auktionsplattformen somit eine Identifikationsfunktion zu.

---

129 *eBay*, Überprüfung durch die Schufa. Dazu auch *Hanau*, Handeln unter fremder Nummer, S. 209; *Hecht*, K&R 2009, 462, 464; *J. Meyer*, Identität, S. 32 Fn. 86; *Schapiro*, S. 14.

130 *OLG München*, Urteil v. 5. 2. 2004, 19 U 5114/03 – NJW 2004, 1328.

131 *ULD*, S. 171.

132 *LG Berlin*, Urteil v. 1. 10. 2003, 18 O 117/03 – NJW 2003, 3493, 3494; *Mankowski*, CR 2007, 606; *ders.*, CR 2011, 458.

133 *ULD*, S. 170.

134 *Baier*, S. 23; *M. Köhler/Arndt/Fetzer*[7], Rn. 323.

135 *ULD*, S. 169.

136 *Hoeren*, CR 2005, 498, 498 f.

137 Dazu ausführlich unten Rn. 620.

d) Online-Banking

67 Die Zuverlässigkeit der Identifikationsfunktion beim Online-Banking wird durch mehrere rechtliche Regelungen sichergestellt. Zur Teilnahme am Online-Banking benötigt der Bankkunde zunächst einen Zahlungsdiensterahmenvertrag wie einen Girovertrag und darüber hinaus eine besondere Vereinbarung über das Online-Banking.[138] Im ersten Schritt wird bei der Kontoeröffnung zur Wahrung der formellen Kontenwahrheit[139] aus steuerlichen Gründen die Identität des Bankkunden überprüft (§ 154 Abs. 1 AO).[140] Im Rahmen dieser Legitimationsprüfung (§ 154 Abs. 2 AO) muss die Bank regelmäßig einen amtlichen Ausweis kontrollieren.[141]

68 Eine Identifizierung mit amtlichen Dokumenten, die unter persönlicher Anwesenheit des Kontoinhabers zu erfolgen hat, ist darüber hinaus nach § 4 Abs. 1 S. 1 GwG erforderlich.[142] Zwar dient diese Vorschrift nur strafrechtlichen Zwecken,[143] die Zuverlässigkeit der Identifikationsfunktion stellt sie dadurch trotzdem sicher. Das GwG schreibt die Erhebung von mehr Daten als die AO vor, nämlich Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit und Anschrift (§ 4 Abs. 3 Nr. 1 GwG).[144] Die Überprüfung muss mittels eines amtlichen Ausweises stattfinden (§ 4 Abs. 4 S. 1 Nr. 1 GwG). Die Verpflichtung der Bank, die Identität eines Kunden bei Eröffnung zu überprüfen, soll sich jedoch auch ohne diese Vorschriften aus dem BGB ergeben, sodass sie Grundlage von einer Haftung der Bank sein kann.[145]

69 Sofern die Zusatzvereinbarung für das Online-Banking getroffen ist, erhält der Kunde die Zugangsdaten anschließend von der Bank. Beim einfachen TAN-Verfahren sowie beim iTAN-Verfahren schickt die Bank ihrem Kunden die persönliche Identifikationsnummer (PIN) und die Transaktions-

138 *Hanau*, Handeln unter fremder Nummer, S. 62; *Schwintowski*[3], § 9 Rn. 37; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 44.

139 *BGH*, Urteil v. 18. 10. 1994, XI ZR 237/93 – BGHZ 127, 229; *Joeres*, in: *Schimansky/Bunte/Lwowski*[4], § 31 Rn. 2.

140 *van Look*, in: *Claussen*[4], § 2 Rn. 8.

141 *van Look*, in: *Claussen*[4], § 2 Rn. 8; *Schwintowski*[3], § 5 Rn. 46; *Joeres*, in: *Schimansky/Bunte/Lwowski*[4], § 31 Rn. 16.

142 Dazu *van Look*, in: *Claussen*[4], § 2 Rn. 9; *Fischbeck*, in: *Schimansky/Bunte/Lwowski*[4], § 42 Rn. 151.

143 *Schwintowski*[3], § 5 Rn. 56.

144 Dazu *Fischbeck*, in: *Schimansky/Bunte/Lwowski*[4], § 42 Rn. 143.

145 *Schwintowski*[3], § 5 Rn. 52.

nummern (TANs) per Post zu.[146] Durch die anfängliche Überprüfung der Identität des Kunden hat ein Bankkonto, das über Online-Banking angesprochen wird, eine zuverlässige Identifikationsfunktion bezüglich der numerischen Identität des Kontoinhabers.

Die Nachvollziehbarkeit der Identifikationsfunktion ist Dritten gegenüber nur eingeschränkt gewährleistet. Das Bankgeheimnis verbietet der Bank Informationen über den Kunden weiterzugeben (§ 2 Abs. 1 AGB/B).[147] Sogar die Auskunft über das Bestehen einer Bankverbindung fällt unter dieses Bankgeheimnis,[148] sodass die Bank erst Recht nicht die Anschrift des Kunden preisgeben darf. Ausnahmen vom Bankgeheimnis bestehen gegenüber Strafverfolgungs- und Steuerbehörden[149] sowie vor Zivilgerichten zur Geltendmachung eigener Forderungen der Bank.[150] Im Zivilprozess zwischen Dritten ist das Bankgeheimnis durch das Zeugnisverweigerungsrecht nach § 383 Abs. 1 Nr. 1 ZPO geschützt.[151] Eine Bankauskunft, die Bankgeheimnisse offenbart, ist bei natürlichen Personen nur mit deren Einwilligung möglich.[152] Möchte ein Bankkunde die Identität eines Kontoinhabers herausfinden, beispielsweise bei einer Fehlüberweisung, kann er dies bei der Bank des Kontoinhabers nur mittels einer Anfrage seiner Bank, die zur Mithilfe verpflichtet ist (§ 675y Abs. 3 BGB).[153] 70

e) Online-Bezahldienste

Bei den Online-Bezahldiensten sind verschiedene Formen zu unterscheiden.[154] Es gibt anonyme Online-Bezahldienste, die Bezahlung mittels einer 71

146 *Hanau*, Handeln unter fremder Nummer, S. 62.
147 *Krepold*, in: *Schimansky/Bunte/Lwowski*[4], § 39 Rn. 2; *Claussen*, in: *Claussen*[4], § 3 Rn. 1.
148 *Krepold*, in: *Schimansky/Bunte/Lwowski*[4], § 39 Rn. 15; *Claussen*, in: *Claussen*[4], § 3 Rn. 8.
149 *Krepold*, in: *Schimansky/Bunte/Lwowski*[4], § 39 Rn. 102 ff., 231 ff.
150 Ebd., § 39 Rn. 97.
151 Ebd., § 39 Rn. 282.
152 *Bruchner/Krepold*, in: *Schimansky/Bunte/Lwowski*[4], § 40 Rn. 19; *Claussen*, in: *Claussen*[4], § 3 Rn. 16; *Schwintowski*[3], § 3 Rn. 58.
153 *Casper*, in: MüKo-BGB[6], § 675r Rn. 40 ff. m.w.N.
154 Dazu auch *Hossenfelder*, Pflichten von Internetnutzern, S. 218.

virtuelle Währung anbieten.[155] Diese haben keine Identifikationsfunktion bezüglich der numerischen Identität des Account-Inhabers.

72 Andere Online-Bezahldienste verlangen Angaben zur Person,[156] sodass sie der Identifizierung des Account-Inhabers dienen sollen. Als Beispiel für einen solchen Dienst wird PayPal betrachtet. Dieser Dienst basiert darauf, dass der Account-Inhaber mittels seiner E-Mail-Adresse Geld versenden und empfangen kann.[157] Die E-Mail-Adresse wird zwar überprüft,[158] kann aber für den Account keine zuverlässige Identifikationsfunktion bewirken, weil sie eine solche selbst nicht besitzt.[159] Eine Identifizierung, wie sie ein Finanzdienstleister nach § 2 Abs. 1 GwG machen muss, wäre bei Online-Bezahldiensten nicht praktikabel.[160] Zur Einrichtung eines PayPal-Kontos ist mittlerweile jedoch die Verifizierung eines Zahlungsweges, entweder des Kontos oder der Kreditkarte erforderlich.[161] PayPal partizipiert damit an den Prüfpflichten der Bank aus § 154 Abs. 1 AO,[162] sodass davon abgeleitet die Zuverlässigkeit der Identifikationsfunktion hergestellt wird. Die Identifikationsfunktion ist jedoch nicht in gleichem Maße zuverlässig. Teilt der Kontoinhaber die Zugangsdaten zum Online-Banking sowie zu seiner E-Mail-Adresse mit einem Dritten, kann dieser Dritte ein PayPal-Konto unter dem Namen des Account-Inhabers anlegen und verifizieren lassen. Die Nachvollziehbarkeit der Identifikationsfunktion ist gegeben, wenn der Authentisierungsnehmer wie PayPal[163] bei berechtigtem Interesse die Identität des Account-Inhabers offenlegt.

f) Elektronische Signatur

73 Für eine elektronische Signatur bedarf es zwar keiner gesetzlichen Grundlage,[164] der deutsche Gesetzgeber hat sich jedoch dazu entschieden, einen

155 *Brunst*, Anonymität im Internet, S. 103; *Scholz*, S. 228 ff.
156 *Meder/Grabe*, BKR 2005, 467, 469; *Fiege*, CR 1998, 41, 43.
157 *Jehle*, S. 325; *Freitag*, in: *Leible/Sosnitza*, Rn. 446.
158 *Meder/Grabe*, BKR 2005, 467, 469.
159 Oben Rn. 48.
160 *Hoenike/Szodruch*, MMR 2006, 519, 525.
161 *PayPal*, Nutzungsbedingungen, 2.3; *Meder/Grabe*, BKR 2005, 467, 469; *Jehle*, S. 326; *Schöttle*, K&R 2007, 183, 186.
162 *Meder/Grabe*, BKR 2005, 467, 474.
163 *PayPal*, Datenschutzgrundsätze, Nr. 4.
164 *Rieder*, S. 52.

einheitlichen normativen Rahmen zu schaffen. Deutschland war eines der ersten Länder, das im Jahre 1997 im Rahmen des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) mit dem Signaturgesetz (SigG) eine gesetzliche Regelung von elektronischen Signaturen vorsah.[165] Auf europäischer Ebene wurde 1999 die Signaturrichtlinie (1999/93/EG) verabschiedet, die einen einheitlichen europäischen Rahmen schaffen soll.[166] Die Novellierung des SigG 2001 diente den beiden Zwecken, diese europäische Richtlinie umzusetzen und den Evaluierungsbericht der Bundesregierung[167] gesetzlich zu berücksichtigen.[168] Die elektronische Signatur soll – in ihren sicheren Formen – die eigenhändige Unterschrift ersetzen.[169]

aa) Formen der elektronischen Signatur

Seit der Novellierung des SigG 2001 sind unterschiedliche Formen der elektronischen Signatur vorgesehen, die mit jeder Stufe sicherer werden.[170] Die erste Form ist die einfache elektronische Signatur. Sie ist legaldefiniert als Daten in elektronischer Form, die der Authentifizierung dienen (§ 2 Nr. 1 SigG). Bei dieser Definition wählte der Gesetzgeber einen technologie-neutralen Ansatz.[171] Eine einfache elektronische Signatur ist beispielsweise die eingescannte Unterschrift, die der Verwender am Ende einer E-Mail platziert.[172] 74

Die zweite Form ist die fortgeschrittene elektronische Signatur (§ 2 Nr. 2 SigG), die die einfache elektronische Signatur um vier Merkmale erweitert.[173] Die Voraussetzungen der eindeutigen Identifizierung und Authentifizierung des Kommunikationspartners erreichen dabei eine größere Verlässlichkeit für den Rechtsverkehr.[174] Bei fortgeschrittenen elektronischen Signaturen kann es wegen der fehlenden Sicherstellung der Einmaligkeit 75

165 *Bösing*, S. 26.
166 Dazu *Steckler*[3], S. 254; *F. A. Koch*, Internet-Recht[2], S. 132.
167 Evaluierungsbericht IuKDG, BT-Drucks. 14/1191, S. 17 ff.
168 *M. Hoffmann*, S. 95.
169 Begr. SigG, BT-Drucks. 14/4662, S. 1, 14.
170 Dazu *Bergfelder*, S. 177 ff.; *Haug*[2], Rn. 770 ff.; *Roßnagel*, MMR 2002, 215; *Spiegelhalder*, S. 55 ff.
171 Begr. SigG, BT-Drucks. 14/4662, S. 18.
172 *F. A. Koch*, Internet-Recht[2], S. 134; *Spiegelhalder*, S. 55.
173 Dazu *Bergfelder*, S. 179; *M. Hoffmann*, S. 99.
174 *B. E. Brisch*/*K. M. Brisch*, in: *Hoeren*/*Sieber*/*Holznagel*, Kap. 13.3 Rn. 33.

von Signaturschlüsseln zu falschen Zuordnungen kommen, sodass sie nicht ausreichend sicher sind.[175] Sie erfüllen zwar ein mittleres Sicherungsniveau, was jedoch eine Gleichstellung mit der eigenhändigen Unterschrift nicht rechtfertigt.[176] Den technologie-neutralen Ansatz der einfachen elektronischen Signatur hat der Gesetzgeber bei dieser zweiten Stufe nicht durchgehalten. Das Gesetz fordert eine Signatur mit privatem und öffentlichem Schlüssel,[177] was eine Public-Key-Infrastruktur (PKI) im Rahmen einer asymmetrischen Verschlüsselung erfordert. Nach dem gesetzgeberischen Willen erfüllt beispielsweise die Software Pretty Good Privacy (PGP) die Anforderungen an eine fortgeschrittene elektronische Signatur.[178]

76 Die dritte Form der elektronischen Signatur ist die qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG), die das primäre Regelungssubjekt des SigG ist. Für sie sind zusätzlich zu den Merkmalen der fortgeschrittenen elektronischen Signatur ein qualifiziertes Zertifikat (§ 2 Nr. 7 SigG) sowie eine sichere Signaturerstellungseinheit (§ 2 Nr. 10 SigG) erforderlich.[179]

77 Die vierte Form der elektronischen Signatur ist die qualifizierte elektronische Signatur mit Anbieterakkreditierung (vgl. § 15 SigG).[180] Diese wird oft mit der qualifizierten elektronischen Signatur zusammen behandelt,[181] weil sich alle Anbieter akkreditieren haben lassen und eine rechtliche Unterscheidung bei den Rechtsfolgen nicht vorliegt.

bb) Asymmetrische Verschlüsselung

78 Auf das technische Verfahren der fortgeschrittenen und qualifizierten elektronischen Signatur mittels asymmetrischer Verschlüsselung soll kurz eingegangen werden. Die bekanntesten und ältesten kryptographischen Systeme beruhen auf einer symmetrischen Verschlüsselung, wobei der Versender für die Verschlüsselung denselben Schlüssel verwendet, wie der Empfänger bei der Entschlüsselung.[182] Bei einer elektronischen Signatur sind diese Ver-

175 *Roßnagel*, MMR 2003, 164, 165.
176 *B. E. Brisch/K. M. Brisch*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.3 Rn. 35.
177 *Haug*[2], Rn. 771.
178 Begr. SigG, BT-Drucks. 14/4662, S. 18.
179 Dazu *Reese*, S. 17.
180 Siehe *M. Hoffmann*, S. 104; *F. A. Koch*, Internet-Recht[2], S. 135.
181 *Roßnagel*, MMR 2003, 164.
182 *Baier*, S. 68; *Eckert*[8], S. 324; *Federrath/Pfitzmann*, in: *U. Schneider/Dieter Werner*[7], 14.3.1.1.

fahren ungeeignet, weil der Empfänger, der die Nachricht oder einen Teil davon entschlüsselt, ebenso eine Nachricht wie der Absender verschlüsseln könnte.[183]

Bei der asymmetrischen Verschlüsselung hingegen wird die Nachricht 79
oder Teile davon mit einem privaten Schlüssel, den nur der Absender kennt, verschlüsselt und mit einem öffentlichen Schlüssel, der auch dem Empfänger bekannt ist, entschlüsselt.[184] Bei der elektronischen Signatur verschlüsselt der Absender nicht die gesamte Nachricht, sondern nur eine Prüfsumme (Hash).[185] Der Absender verschlüsselt diesen aus dem Text der Nachricht gebildeten Hash mit seinem privaten Schlüssel und hängt ihn an die Nachricht an.[186] Der Empfänger bildet ebenfalls den Hash-Wert aus dem Text der Nachricht, entschlüsselt die elektronische Signatur des Absenders und vergleicht die beiden Hash-Werte.[187] Stimmen die beiden Werte überein, ist der Text unverändert angekommen. Hat ein Dritter den Text auf dem Weg verändert, ändert sich der Hash-Wert, den der Empfänger erzeugt, sodass er eine Abweichung des Textes bemerken kann.[188] Dadurch kann der Empfänger die Integrität der Nachricht überprüfen.

Bedeutsam für die Sicherheit der asymmetrischen Verschlüsselung ist, 80
dass ein Angreifer durch mathematische Methoden nicht mit Wissen des öffentlichen Schlüssels den privaten Schlüssel errechnen kann.[189] Das Schlüsselpaar wird anhand von zwei großen Primzahlen erstellt.[190] Dabei macht sich das Verfahren zu Nutze, dass die Faktorisierung von großen Zahlen mit einem sehr hohen Aufwand verbunden ist.[191] Die konstante Weiterentwicklung mathematischer Algorithmen sowie wachsende Rechnerpower,[192] die

183 Vgl. *Borges*, Verträge, S. 49.
184 *Baier*, S. 68; *Eckert*[8], S. 352 f.; *Federrath/Pfitzmann*, in: *U. Schneider/Dieter Werner*[7], 14.3.1.2.
185 *Borges*, Verträge, S. 50; *F. A. Koch*, Internet-Recht[2], S. 145.
186 *Eckert*[8], S. 400; *Rieder*, S. 52; *Tanenbaum/Wetherall*[5], S. 906.
187 *Eckert*[8], S. 400; *Tanenbaum/Wetherall*[5], S. 907; *Rieder*, S. 53.
188 *Bösing*, S. 23; *F. A. Koch*, Internet-Recht[2], S. 145; *Reese*, S. 12 f.
189 *Eckert*[8], S. 352; *Gassen*, S. 39.
190 *Eckert*[8], S. 358; *F. A. Koch*, Internet-Recht[2], S. 148.
191 *Eckert*[8], S. 354; *Gassen*, S. 39.
192 Nach dem mooreschen Gesetz verdoppelt sich die Anzahl der Transistoren auf einem Computerchip alle 12-24 Monate, *Moore*, Electronics 8/38 (1965), 114, 116. Bisher hat sich diese Vorhersage als zutreffend erwiesen, die Grenzen dürften jedoch bald erreicht sein, vgl. *Rojas*, Telepolis v. 4. 6. 2012.

ein Erraten mittels Brute-Force-Angriffen[193] einfacher machen, erfordern eine stetige Überprüfung der kryptographischen Sicherheit.[194]

cc) Der Zertifizierungsdiensteanbieter als Trusted Authority

81 Für die Identifikationsfunktion einer fortgeschritten oder qualifizierten elektronischen Signatur ist entscheidend, wie zuverlässig und nachvollziehbar diese ist. Wenn der Empfänger mittels des öffentlichen Schlüssels die Integrität der Nachricht überprüft hat, weiß er zunächst nur, dass diese mit dem privaten Schlüssel verschlüsselt wurde. Kennt der Empfänger den Absender und hat er den öffentlichen Schlüssel von diesem vorher erhalten, kann er sich dadurch vergewissern, dass der Schlüssel-Inhaber den privaten Schlüssel verwendet hat, solange der Schlüssel-Inhaber den Schlüssel nicht aus der Hand gegeben hat. In Systemen, in denen sich Benutzer nicht kennen, funktioniert dies nicht.[195] Erst mit Hilfe eines vertrauenswürdigen Dritten, der Trusted Authority oder Trusted Third Party,[196] kann der Empfänger dann wissen, von wem die Erklärung stammt. Diese Trusted Authority hat den öffentlichen Schlüssel gespeichert und kann diesen einer Person zuordnen, deren Identität sie zuvor überprüft hat. Die Rolle der Trusted Authority erfüllen die Zertifizierungsdiensteanbieter (§ 2 Nr. 8 SigG) bei der qualifizierten elektronischen Signatur. Dieser bestätigt die Identität des Absenders mittels eines qualifizierten Zertifikats (§ 2 Nr. 6 SigG). Das qualifizierte Zertifikat wird nur an natürliche Personen ausgegeben.[197] Da das Zertifikat auf einen Namensträger lautet, kommt der elektronischen Signatur eine Identifikationsfunktion zu. Die Zuverlässigkeit dieser Identifikationsfunktion soll durch die Überprüfung der Identität des Signaturschlüssel-Inhabers (§ 5 Abs. 1 S. 1 SigG) sichergestellt werden.

82 Die Nachvollziehbarkeit der Identifikationsfunktion stellt der Auskunftsanspruch in § 14 Abs. 2 S. 1 SigG nur teilweise her.[198] Da das Zertifikat nur den vollen Namen des Signaturschlüssel-Inhabers enthält (§ 7 Abs. 1

193 Dazu unten Rn. 181.
194 *Bösing*, S. 25.
195 *Reese*, S. 10.
196 *Borges*, Verträge, S. 51; *Gassen*, S. 47; *F. A. Koch*, Internet-Recht[2], S. 145; *Rieder*, S. 54.
197 *F. A. Koch*, Internet-Recht[2], S. 135; *Sanner*, S. 27.
198 Dazu *Roßnagel*, NJW 2005, 385, 387.

Nr. 1 SigG), bedarf es zur Identifizierung eventuell weitere Angaben wie Anschrift und Geburtsdatum. Jedoch können nur Behörden unter engen Voraussetzungen diese zusätzlichen Informationen abfragen.

dd) Die Akzeptanz der elektronischen Signatur

Obwohl die Hoffnung bestand, dass die elektronische Signatur eine schnelle und weite Verbreitung finden werde,[199] ist die praktische Relevanz der elektronischen Signatur gering.[200] *Hoeren* hat schon früh erkannt, dass die elektronische Signatur wegen der mangelnden Verständigung, wer die Finanzierungslast zu tragen habe, eine „Totgeburt" sei:[201] 83

> Der Kunde wird [die Kosten] nicht tragen, sofern er nicht in erheblichem Ausmaß kommerzielle Vorteile davon hat – denn warum sollte er für viel Geld Chip-Karte und Lesegerät kaufen, wenn sich daraus als einziger Effekt ergäbe, dass er an Verträge gebunden wäre, die er früher bestreiten konnte?

Das Akzeptanzproblem der elektronischen Signatur befindet sich in einem Teufelskreis mangels Erreichen der kritischen Masse.[202] Wenn die kritische Masse erreicht wird, sind die Vorteile für die Anwender größer und die Komponenten werden billiger. Der Einstieg Einzelner, die in der Summe zur kritischen Masse werden können, scheitert jedoch daran, dass das Verfahren wenig Vorteile bringt und die Komponenten zu teuer sind. Selbst die höchstrichterliche Entscheidung, dass ein Arbeitgeber von einem Arbeitnehmer verlangen kann, dass dieser für geschäftliche Zwecke eine elektronische Signatur beantragt und nutzt,[203] wird schwerlich bewirken können, dass die Verbreitung eine kritische Masse erreicht. Darüber hinaus verfolgt der Gesetzgeber keinen einheitlichen Ansatz. Für Erklärungen gegenüber dem Finanzamt gibt es andere Formen elektronischer Erklärungen,[204] was die Notwendigkeit der qualifizierten elektronischen Signatur beeinträchtigt. 84

199 *Wiebe*, MMR 2002, 257, 258.
200 *Borges*, Elektronischer Identitätsnachweis, S. 241; *Bösing*, S. 9; *Fox*, DuD 2009, 387; *Lapp*, DuD 2009, 651, 655.
201 *Hoeren*, CR 2002, 295, 296. Ähnlich *Spindler*, CR 2011, 309, Fn. 1.
202 *Hornung*, Die digitale Identität, S. 40.
203 *BAG*, Urteil v. 25. 9. 2013, 10 AZR 270/12.
204 Dazu *Roßnagel*, K&R 2003, 379.

85 Ferner hat die elektronische Signatur zwei praktische Unwägbarkeiten, die die weite Verbreitung beeinträchtigen. Zum einen ist das SigG für die Eigensignierung ausgelegt. Dokumente wie Rechnungen, die massenhaft verschickt werden, bereiten bei einer Signatur nach den strengen Voraussetzungen des SigG erheblichen Aufwand.[205] Es ist zwar möglich, selbst automatisiert Dokumente mit einer qualifizierten elektronischen Signatur zu versehen.[206] Die Signierung der Dokumente wird jedoch in der Praxis häufig ausgelagert. Das führt in Form der Fremdsignierung jedoch dazu, dass nach einer Ansicht keine qualifizierte elektronische Signatur mehr vorliegt.[207]

86 Zum anderen wird bezweifelt, dass ein Dokument mit qualifizierter elektronischer Signatur nach Jahren oder Jahrzehnten ebenso gut zur Beweisführung verwendet werden kann, wie ein handschriftlich unterschriebenes Dokument.[208] Die Zertifizierungsdiensteanbieter von qualifizierten elektronischen Signaturen müssen die Zertifikate nach Ablauf nur fünf weitere Jahre im Zertifikatsverzeichnis führen (§ 4 Abs. 1 SigV). Nur akkreditierte Zertifizierungsdiensteanbieter müssen die Zertifikate dreißig Jahre lang im Verzeichnis führen (§ 4 Abs. 2 SigV).[209] Damit kann nur bei elektronischen Signaturen von akkreditierten Zertifizierungsdiensteanbietern die vollen 30 Jahre lang, nach deren Ablauf spätestens durch Verjährung Rechtsfrieden eintritt (vgl. § 199 Abs. 2, Abs. 3 S. 1 Nr. 2, Abs. 3a BGB), auf das Zertifikatsverzeichnis des Zertifizierungsdiensteanbieters zugegriffen werden. Selbst bei ausreichend langer Aufbewahrung der Zertifikate besteht das Problem, dass durch die Verbesserung mathematischer Algorithmen und durch leistungsfähigere Rechner, nach dem derzeitigen Stand der Technik als sicher eingestufte Verfahren, möglicherweise einfach geknackt werden können.[210] Bei der Sicherheit der Verschlüsselungstechnik denkt man in Schritten von fünf Jahren.[211] Weiter als diese fünf Jahre kann die Sicherheit der Verschlüsselung nicht zuverlässig vorausgesehen werden. Darüber hinaus besteht das Problem der Archivierung durch die im Vergleich zu Papier geringe Haltbarkeit von Datenträgern. Bei Festplatten sowie selbstbeschriebe-

205 *Roßnagel*, MMR 2008, 22, 23.
206 *Roßnagel/Fischer-Dieskau*, MMR 2004, 133, 138.
207 *Roßnagel*, BB 2007, 1233, 1237; *ders.*, MMR 2008, 22, 28.
208 *F. A. Koch*, Internet-Recht[2], S. 133; *Wilke/Jandt/Löwe/Roßnagel*, CR 2008, 607.
209 Dazu *F. A. Koch*, Internet-Recht[2], S. 140.
210 *Knopp/Wilke/Hornung/Laue*, MMR 2008, 723, 727.
211 Vgl. *Stumpf/Sacher/Roßnagel/Eckert*, DuD 2007, 357, 359.

nen CDs sind die Daten nach fünf bzw. zehn Jahren nicht mehr lesbar, bei USB-Sticks schon nach drei Jahren.[212]

ee) Exkurs: Ausblick

Die EU-Kommission hat am 4.6.2012 einen Entwurf für eine „Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (KOM(2012) 238/2) vorgelegt. Neben einer Fortschreibung der Signaturrichtlinie enthält dieser Entwurf Regelungen zu Vertrauensdiensten.[213] Der Entwurf der Kommission soll durch die Pflicht zur Anerkennung ausländischer Identifizierungsmittel (Art. 5) Hindernisse im Binnenverkehr beseitigen (Erwägungsgrund 9). Stimmen in der Literatur kritisieren den Entwurf insbesondere dafür, dass die Sicherheitsstandards in der Verordnung nicht festgelegt sind, sondern nur die Kommission sie in davon unabhängigen, delegierten Rechtsakten festgelegen will.[214] Die gegenseitige Anerkennungspflicht erfolgt jedoch, ohne dass ein Sicherheitsstandard für die Dienste vorgeschrieben ist.[215] Dies führt zu bedenklichen Sicherheitslücken, wenn die Sicherheitsstandards in den Mitgliedsstaaten stark divergieren.[216] Darüber hinaus verbietet der Verordnungsentwurf einige Sicherheitsmerkmale deutscher Identifizierungsdienste, wie eine gegenseitige Authentisierung, bei der nicht nur der Authentisierungsnehmer die Identität des Authentisierungsgebers überprüft, sondern auch umgekehrt der Authentisierungsgeber den Authentisierungsnehmer überprüft.[217] Der neue Personalausweis[218] wäre daher nicht notifizierbar.[219] Bei der Regelungstechnik weicht die Kommission durch die Wahl einer Verordnung, die unmittelbar gilt und im Gegensatz zu den vorher verwendeten Richtlinien nicht mit Spielraum des Mitgliedsstaates umgesetzt

87

212 *Hoppen*, CR 2008, 674, 677.
213 Dazu *Hornung*, MMR 2012, 633, 634.
214 *Roßnagel*, MMR 2012, 781; *Roßnagel/Johannes*, ZD 2013, 65, 67.
215 *Spindler/Rockenbauch*, MMR 2013, 139, 141; *Roßnagel/Johannes*, ZD 2013, 65, 68.
216 *Spindler/Rockenbauch*, MMR 2013, 139, 142 f.
217 Ebd., 145.
218 Dazu unten Rn. 88.
219 *Hornung*, MMR 2012, 633, 634; *Spindler/Rockenbauch*, MMR 2013, 139, 145; *Quiring-Kock*, DuD 2013, 20, 21.

werden muss, ab.[220] Einige Stimmen in der Literatur betrachten dies als Kompetenzüberschreitung der Kommission, die den Grundsatz der Subsidiarität und Verhältnismäßigkeit nicht wahre.[221] Für die Akzeptanzprobleme der elektronischen Signatur[222] liefert der Entwurf jedoch keine Lösung.[223]

g) Elektronischer Identitätsnachweis im neuen Personalausweis (nPA)

88 Der neue, mit der Änderung des PAuswG zum 1.11.2010 eingeführte Personalausweis,[224] ermöglicht unter anderem einen elektronischen Identitätsnachweis. Gesetzgeberisches Ziel dabei ist, Diensteanbietern die zuverlässige Überprüfung der Identität des Ausweisinhabers zu ermöglichen.[225] Der elektronische Identitätsnachweis, auch electronic identity (eID) genannt,[226] erfolgt über einen RFID-Chip im Ausweis, in dem die Daten zur Online-Authentisierung abgelegt werden.[227] Die biometrischen Merkmale des Ausweisinhabers, die auf dem Personalausweis gespeichert sind, können nur Behörden abfragen, wohingegen die elektronische Authentisierung auch für den eCommerce geöffnet ist.[228]

89 Der Personalausweis ist als hoheitliches Ausweisdokument[229] das Modell für eine Identifikationsfunktion. Er ist das „klassische und universelle Authentisierungsmedium“[230] und „zentrales Instrument zum Nachweis der Identität einer natürlichen Person“[231]. Den Ausweis in seiner physischen Form kann der Ausweisinhaber im Internet nicht vorzeigen. Um trotzdem eine Identifikation zu ermöglichen hat der Gesetzgeber in § 18 PAuswG die Möglichkeit zum elektronischen Identitätsnachweis geschaf-

---

220 *Spindler/Rockenbauch*, MMR 2013, 139, 140; *Roßnagel/Johannes*, ZD 2013, 65, 67.
221 *Roßnagel*, MMR 2012, 781; *Roßnagel/Johannes*, ZD 2013, 65, 67.
222 Oben Rn. 83.
223 *Roßnagel/Johannes*, ZD 2013, 65, 72.
224 Dazu *Roßnagel/Hornung*, DÖV 2009, 301; *Borges*, NJW 2010, 3334; *ders.*, Elektronischer Identitätsnachweis, S. 36.
225 Begr. PAuswG, BT-Drucks. 16/10489, S. 20.
226 *Reisen*, DuD 2008, 164.
227 *Eckert*[8], S. 579.
228 *Reisen*, DuD 2008, 164.
229 *Borges*, NJW 2010, 3334.
230 *Borges*, Elektronischer Identitätsnachweis, S. 29.
231 *Borges/Schwenk/Stuckenberg/Wegener*, S. 188.

fen.[232] Der Vorteil des elektronischen Identitätsnachweises gegenüber klassischen Authentisierungen im Internet besteht darin, dass eine zuverlässige Erstauthentisierung möglich ist.[233] Eine sichere Identitätsfeststellung kann damit auch ohne Medienbruch wie bei PostIdent herbeigeführt werden.[234] Technisch sind für den Authentisierungsvorgang beidseitig Vorkehrungen zu treffen. Der Authentisierungsnehmer muss sich ein Berechtigungszertifikat (§ 2 Abs. 4 PAuswG) durch die Behörde ausstellen lassen (§ 18 Abs. 4 S. 1 PAuswG).[235] Der Ausweisinhaber benötigt neben seinem Rechner mit Internetverbindung als Hardware ein Kartenlesegerät und als Software die Ausweis-App.[236] Diese standardmäßig deaktivierte Funktion des neuen Personalausweises aktiviert die ausgebende Behörde auf Wunsch des Ausweisinhabers (§ 10 Abs. 1 S. 1 PAuswG).

Die Nachvollziehbarkeit der Identifikationsfunktion des Personalausweises wird zum einen dadurch begründet, dass jede natürliche Person nur einen Personalausweis hat und die primäre Funktion des Personalausweises die Identifikation des Namensträgers ist. Beim elektronischen Identitätsnachweis besteht jedoch die Möglichkeit, nur bestimmte Daten wie Alter oder Wohnort weiterzugeben (§ 18 Abs. 5 PAuswG).[237] In diesen Fällen wird der Ausweisinhaber anonymisiert, sodass keine nachvollziehbare Identifikation für den Authentisierungsnehmer möglich ist. Erhält der Authentisierungsnehmer jedoch zur Identifikation ausreichende Identitätsdaten wie Name und Anschrift, so entfaltet der elektronische Identitätsnachweis eine nachvollziehbare Identifikationsfunktion. **90**

Unabhängig von der Funktion des elektronischen Identitätsnachweises besteht optional die Möglichkeit, den neuen Personalausweis als Signaturerstellungseinheit zu verwenden, was standardmäßig deaktiviert ist (§ 22 PAuswG).[238] Für die Nutzung der Signatur ist jedoch eine zweite, unterschiedliche sechsstellige PIN erforderlich, deren Unterscheidung nur Fach- **91**

232 *Borges*, NJW 2010, 3334, 3335; *Schulz*, CR 2009, 267, 269.

233 *Borges*, Elektronischer Identitätsnachweis, S. 34; *Roßnagel/Hornung*, DÖV 2009, 301, 303.

234 *Borges*, NJW 2010, 3334, 3336.

235 Dazu *Roßnagel/Hornung*, DÖV 2009, 301, 303; *Roßnagel/Hornung/Schnabel*, DuD 2008, 168; *W. Müller/Redlich/Jeschke*, DuD 2011, 465; *Polenz*, MMR 2010, 671, 672.

236 *Eckert*[8], S. 581.

237 Dazu *Polenz*, MMR 2010, 671, 673 f.

238 *Engel*, DuD 2006, 207, 209; *Bender/Kügler/Margraf/Naumann*, DuD 2008, 173; *Roßnagel/Hornung*, DÖV 2009, 301, 302.

leuten einleuchtet und die schwer zu merken ist.[239] Wegen der Unabhängigkeit von eID- und Signaturfunktion muss der Ausweisinhaber im Falle eines Verlustes beide Funktionen getrennt sperren, wovon er eine Sperrung leicht vergessen kann.[240]

h) De-Mail

92 De-Mail ist ein Dienst, der wie eine E-Mail funktioniert, jedoch rechtssicher und nachweisbar sein soll. Die De-Mail war eine Gesetzesinitiative der Bundesregierung, die unter dem Namen Bürgerportal gestartet ist.[241] Nach einer Testphase in Friedrichshafen,[242] trat das Gesetz zur Regelung von De-Mail-Diensten (DeMailG) zum 3. Mai 2011 in Kraft.[243] Formuliertes Ziel des Gesetzes (§ 1 Abs. 1 DeMailG) ist, einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr zu etablieren.[244] Dazu bedient sich das Gesetz zweier Instrumente: der sicheren Authentisierung vor jeder Nutzung und der Identifizierung der Nutzer bei der Anmeldung.[245]

93 Den De-Mail-Adressen soll eine Identifikationsfunktion des Namensträger zukommen. Dies ist dadurch sichergestellt, dass die E-Mail-Adresse den Namen der Person enthält.[246] Bei natürlichen Personen muss der lokale Teil der E-Mail den Vor- und Nachnamen der Person enthalten (§ 5 Abs. 1 S. 2 Nr. 2 DeMailG). Bei juristischen Personen muss die Domain deren Bezeichnung enthalten (§ 5 Abs. 1 S. 2 Nr. 3 DeMailG).

94 Die auf Antrag durchzuführende Überprüfung der De-Mail-Anbieter (§§ 17 f. DeMailG) soll deren Zuverlässigkeit als Trusted Authority sicherstellen.[247] An der Zuverlässigkeit dieses Verfahrens wird teilweise

---

239 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 163.
240 *Borges*, NJW 2010, 3334, 3335.
241 *Dennis Werner*/*Wegener*, CR 2009, 310, 310.
242 Zu den Erfahrungen aus der Testphase *Gelzhäuser*, DuD 2010, 646.
243 *Roßnagel*, NJW 2011, 1473, 1474; *Rose*, K&R 2011, 439.
244 Dazu auch den „Vater" des Gesetzes: *Roßnagel*, NJW 2011, 1473; *ders.*, CR 2011, 23, 24.
245 *Roßnagel*, NJW 2011, 1473.
246 *Roßnagel*, NJW 2011, 1473, 1475; *ders.*, CR 2011, 23, 25; *Rose*, K&R 2011, 439, 440.
247 Dazu *Roßnagel*, NJW 2011, 1473, 1477; *ders.*, CR 2011, 23, 25; *Spindler*, CR 2011, 309, 310; *Roßnagel*/*Hornung*/*Knopp*/*Wilke*, DuD 2009, 728, 731 f.; *Dennis Werner*/*Wegener*, CR 2009, 310, 314; *Schumacher*, DuD 2010, 302; *Fechner*[14], Kap. 12 Rn. 188.

gezweifelt, weil private Dritte, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) nur überwacht, die Anbieter zertifizieren.[248] Die Überprüfung der De-Mail-Anbieter bezieht sich insbesondere darauf, dass diese neben den sicheren Authentisierungsverfahren auch eine ausreichend geschützte IT-Infrastruktur besitzen. Die Überzeugung des Gesetzgebers, dass der De-Mail-Adresse eine zuverlässige und nachvollziehbare Identifikationsfunktion zukommt, wird dadurch zum Ausdruck gebracht, dass Diensteanbieter Dritten einen Identitätsbestätigungsdienst anbieten können (§ 6 Abs. 1 DeMailG).[249]

Die Identifikationsfunktion einer De-Mail-Adresse ist darüber hinaus nachvollziehbar. Andere De-Mail-Nutzer können Auskunft über die gespeicherten Identitätsdaten unter den Voraussetzungen des § 16 Abs. 1 DeMailG vom Diensteanbieter verlangen.[250] Auch die pseudonyme Nutzung der De-Mail, die natürlichen Personen möglich ist (§ 5 Abs. 2 S. 1 DeMailG), steht der Zuverlässigkeit und der Nachvollziehbarkeit der Identifikationsfunktion nicht entgegen. Die pseudonymen Adressen sind als solche gekennzeichnet (§ 5 Abs. 2 S. 2 DeMailG), sodass der Kommunikationspartner kein Vertrauen darin entwickeln kann, dass der angezeigte Name den tatsächlichen Namen des Namensträgers widerspiegelt. Die Überprüfung der Identität des Nutzers findet ebenso wie bei allen anderen Accounts statt (§ 3 Abs. 2 DeMailG). Ferner können andere Nutzer Auskunft über Zuordnung des Pseudonyms vom Diensteanbieter verlangen (§ 16 Abs. 1 DeMailG). 95

Die De-Mail steht nicht in direkter Konkurrenz zur elektronischen Signatur. Sie ist vielmehr eine Ergänzung zur elektronischen Signatur. Während die elektronische Signatur die (Schrift-)Form von Willenserklärungen betrifft, betrifft die De-Mail die Übertragung von Willenserklärungen.[251] Die Verabschiedung des DeMailG werten Stimmen aus der Literatur daher posi- 96

248 *Spindler*, CR 2011, 309, 311.

249 Dazu *Roßnagel*, NJW 2011, 1473, 1476; *ders.*, CR 2011, 23, 28; *Rose*, K&R 2011, 439, 443 f.; *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 731.

250 Dazu *Roßnagel*, NJW 2011, 1473, 1477; *ders.*, CR 2011, 23, 28; *Spindler*, CR 2011, 309, 316; *Rose*, K&R 2011, 439, 444; *Warnecke*, MMR 2010, 227, 231 f.; Begr. DeMailG, BT-Drucks. 17/3630, S. 36.

251 Begr. DeMailG, BT-Drucks. 17/3630, S. 2, 19; *Roßnagel*, CR 2011, 23, 24; *Spindler*, CR 2011, 309; *Warnecke*, MMR 2010, 227, 230; *Berlit*, JurPC Web-Dok., 39/2011, Rn. 23.

tiv, weil der Gesetzgeber eine bisher fehlende Infrastruktur zum Nachweis des Zugangs elektronischer Willenserklärungen schaffe.[252]

97 Kritisch an der De-Mail merken Teile der Literatur an, dass keine Ende-zu-Ende-Verschlüsselung vorgeschrieben, sondern nur als Option möglich ist (§ 5 Abs. 3 S. 3 DeMailG).[253] De-Mails und E-Mails sind so einfach zu lesen wie eine Postkarte, weil sie in unverschlüsselter Form im Klartext durch zahlreiche Rechner transportiert werden.[254] Der Bundesrat forderte daher im Gesetzgebungsverfahren eine Ende-zu-Ende-Verschlüsselung.[255] Die Bundesregierung hingegen hat diesen Änderungswunsch abgelehnt, weil er auf Seiten der Nutzer einen technischen Mehraufwand bedeutet.[256] Von technischer Seite sei die De-Mail daher mit Anfängerfehlern behaftet.[257] Bei De-Mails sei weder die Vertraulichkeit noch Integrität sichergestellt.[258]

98 Zwar ist eine Bewertung der Akzeptanz der De-Mail zwei Jahre nach deren Einführung früh, es kann jedoch geprüft werden, ob die Gründe, die eine weite Verbreitung elektronischen Signatur verhinderten,[259] auch für die De-Mail zutreffen. Für Unternehmen und die Verwaltung bringt die De-Mail den großen Vorteil, dass sie nachweisbar Willenserklärungen zustellen lassen können.[260] Für Privatleute stellt die Nachweisbarkeit der Zustellung tendenziell einen Nachteil dar.[261] Insbesondere Personen, die wirksamen Zustellungen entgehen möchten, werden De-Mail nicht nutzen.[262] Der angeführte Vorteil für Privatpersonen, dass sie offizielle Kommunikation rund um die Uhr und weltweit digital abwickeln können, ist kein bedeutender Vorteil für Privatpersonen.[263] Diese können mit einem häufig anzutreffenden Verzicht auf Rechtssicherheit diese Kommunikation ebenso gut über E-

252 *Berlit*, JurPC Web-Dok., 39/2011, Rn. 35; *Roßnagel*, NJW 2011, 1473, 1478; *ders.*, CR 2011, 23, 29 f.; *Dennis Werner/Wegener*, CR 2009, 310, 316.
253 *Rose*, K&R 2011, 439, 442; *Lechtenbörger*, DuD 2011, 268; *Fechner*[14], Kap. 12 Rn. 190.
254 Begr. DeMailG, BT-Drucks. 17/3630, S. 1.
255 BT-Drucks. 17/4145, S. 2.
256 Ebd., S. 9.
257 *Lechtenbörger*, DuD 2011, 268, 269.
258 Ebd., 269.
259 Dazu oben Rn. 83.
260 *J. Dietrich/Keller-Herder*, DuD 2010, 299, 301.
261 *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 734; *Lapp*, DuD 2009, 651, 652.
262 *Lapp*, DuD 2009, 651, 652.
263 *Gelzhäuser*, DuD 2010, 646, 648.

Mail abwickeln. Erst wenn Behörden Dienste per De-Mail anbieten, die es ansonsten mangels Identifikationsfunktion nicht gibt, ergeben sich Vorteile für Privatpersonen.

Ebenso wie bei der elektronischen Signatur sind die Vorteile für Privat- 99
personen gering. Für Privatpersonen bestehen sogar tendenziell Nachteile beim Zugang von Willenserklärungen. Die Regeln des Zugangs sind strenger als bei sonstigen Kommunikationsformen.[264] Somit lässt sich die Erkenntnis von *Hoeren* bezüglich elektronischer Signaturen auch auf die De-Mail anwenden: Warum sollte ein Kunde Kosten aufwenden, um seinem Geschäftsgegner den rechtssicheren Nachweis von Rechtsgeschäften gegen ihn zu ermöglichen?[265] Gleichwohl herrscht Zuversicht, dass die De-Mail Verbreitung finden wird.[266] Eine Umfrage zeigt eine Bereitschaft von 60 % in der Bevölkerung, die De-Mail zu nutzen.[267] Andere Stimmen der Literatur zweifeln jedoch daran, dass die De-Mail Erfolg haben wird, weil die kritische Masse nicht zusammen kommen werde.[268] Der Versuch die missglückte Einführung der elektronischen Signatur mit der De-Mail zu retten, werde nicht funktionieren.[269] Insofern bietet die De-Mail ebenso wie die elektronische Signatur für Privatleute keine nennenswerten Vorteile.[270] Die Internationalität der De-Mail – wie der Name schon zeigt – ist nicht gegeben, weil die nationale Lösung keine Interoperabilität mit dem Ausland gewährleistet.[271]

Darüber hinaus besteht ein zusätzliches Problem für die Akzeptanz der 100
De-Mail. Zwar kann die De-Mail wegen der Umsetzung durch private Diensteanbieter nicht als „staatsgesteuerte Kommunikation“[272] angesehen werden.[273] Einige befürchten jedoch, dass der Staat Zugriff auf die im Postfach gespeicherten Daten erhalten könnte.[274] Diese Befürchtung könnte sogar auf im DeMailG einen Anhaltspunkt finden. Die zuständige Behörde hat die Ermächtigung, De-Mail-Konten sperren (§ 10 Abs. 2 S. 1 DeMailG)

---

264 *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 732 f.
265 Siehe *Hoeren*, CR 2002, 295, 296. Dazu oben Rn. 83.
266 *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 734.
267 *Gelzhäuser*, DuD 2010, 646, 647.
268 *Lapp*, DuD 2009, 651.
269 *Fox*, DuD 2009, 387.
270 *Lapp*, DuD 2009, 651, 655.
271 Ebd., 655.
272 *Heckmann*, JurisPR-ITR 3/2009, Anm. 1.
273 *Roßnagel*, NJW 2011, 1473, 1478.
274 *Schulz*, DuD 2009, 601, 604.

und auflösen (§ 10 Abs. 4 S. 2 DeMailG) zu lassen. Ein Zugriff auf diese gespeicherten Daten ist mit diesen Ermächtigungen jedoch nicht verbunden.

i) Zwischenergebnis zu den staatlichen Maßnahmen

101 Die staatlichen Versuche, rechtssichere und verlässliche elektronische Kommunikation zu ermöglichen, haben bisher kaum Akzeptanz gefunden. Beim neuen Personalausweis (nPA) und der De-Mail hat der Gesetzgeber versucht, durch niedrige technische Eintrittsbarrieren die Akzeptanz zu steigern. Beim neuen Personalausweis hat der Gesetzgeber auf das Erfordernis sicherer Kartenlesegeräte verzichtet, bei der De-Mail auf eine Ende-zu-Ende-Verschlüsselung. Bisher ist der bezweckte Erfolg noch nicht eingetreten. Vielmehr resultiert aus den niedrigen Eintrittsbarrieren ein Verzicht auf Sicherheit, der stark kritisiert wird. Diese mangelnde Sicherheit könnte sogar den gegenteiligen Effekt haben, nämlich, dass die neuen Möglichkeiten wegen der unzureichenden Sicherheit keine Akzeptanz finden. Demnach ist der Aussage zuzustimmen, dass sich der Gesetzgeber Regelungen von technischen Entwicklungen – wie auch negative Beispiele in der Vergangenheit gezeigt haben –, gut überlegen und eher zurückhaltend agieren soll.[275]

3. Authentisierung, Authentifizierung und Autorisierung

102 Bei einem Authentifizierungsvorgang gibt es drei entscheidende Schritte: Authentisierung, Authentifizierung und Autorisierung. Diese drei Schritte sollen nachfolgend betrachtet werden.

103 Authentisierung beschreibt das Vorlegen von Authentisierungsmitteln zum Nachweis einer Identitätsbehauptung aus der Perspektive desjenigen, der die Identität behauptet.[276] Der die Identität Behauptende wird dabei als Authentisierungsgeber bezeichnet. Die behauptete virtuelle Identität, beispielsweise die Benutzerkennung, ist der Identifikator.[277] Beim Missbrauch von Zugangsdaten im Internet ist der Authentisierungsgeber derjenige, der versucht den Account mit den Zugangsdaten zu verwenden. Dies kann

275 *Rieder*, S. 86.
276 *J. Meyer*, Identität, S. 43; *Wefel*, S. 7.
277 *W. Müller/Redlich/Jeschke*, DuD 2011, 465.

der Account-Inhaber, ein Dritter, der die Zugangsdaten vom Account-Inhaber erhalten hat, oder ein Angreifer, der versucht Handelungen über den Account vorzunehmen, sein.

Authentifizierung hingegen beschreibt den Vorgang der Überprüfung dieser Authentisierungsmittel aus der Perspektive desjenigen, dem gegenüber die Identität behauptet wird. Authentifizierung kann somit als die Überprüfung der Identitätsbehauptung definiert werden.[278] Demjenigen, dem gegenüber die Identität behauptet wird, ist der Authentisierungsnehmer. Beim Missbrauch von Zugangsdaten im Internet ist der Authentisierungsnehmer beispielsweise der Diensteanbieter oder der Plattformbetreiber. 104

Im Englischen werden die Begriffe Authentisierung und Authentifizierung durch das einheitliche Wort *authentication* ausgedrückt.[279] Eine Trennung wie in der deutschen Sprache findet dabei nicht statt, sodass die Begriffe daher manchmal verwechselt werden. 105

Autorisierung bezeichnet den Vorgang nach einer erfolgreichen Authentifizierung. Hat der Authentisierungsnehmer den Authentisierungsgeber authentifiziert, räumt er ihm gewisse Rechte ein.[280] Beim Missbrauch von Zugangsdaten im Internet räumt der Authentisierungsnehmer dem Account-Inhaber je nach Art des Accounts die entsprechenden Rechte ein. Auf einer Internet-Auktionsplattform kann der Handelnde nach der Autorisierung beispielsweise Gebote abgeben oder Gegenstände versteigern. Beim elektronischen Identitätsnachweis bestätigt der Authentisierungsnehmer einem Dritten die Identität und autorisiert den Ausweisinhaber dadurch, sich Dritten gegenüber auszuweisen. Diese technische Definition der Autorisierung weicht von der Legaldefinition der Autorisierung in § 675j Abs. 1 S. 1 BGB ab, die die Zustimmung zu einem Rechtsgeschäft beschreibt. 106

278 *Baier*, S. 58; *BSI*, E-Government-Handbuch, S. 6; *Eckert*[8], S. 8; *J. Meyer*, Identität, S. 42 f.; *Wefel*, S. 7.

279 *BSI*, E-Government-Handbuch, S. 6 ff.; *J. Meyer*, Identität, S. 42 Fn. 141. Vgl. auch *Tanenbaum/Wetherall*[5], S. 60.

280 *Federrath/Pfitzmann*, in: *U. Schneider/Dieter Werner*[7], 14.2.3; *BSI*, E-Government-Handbuch, S. 7; *Eckert*[8], S. 5; *Tanenbaum/Wetherall*[5], S. 935; *Wefel*, S. 7; *Kent/Millet*, S. 20.

a) Authentisierungsmittel

107 Zentral für einen Authentisierungsvorgang sind die Zugangsdaten zu dem entsprechenden Account. Bei diesen Zugangsdaten handelt es sich um die Informationen und Gegenstände, die der Account-Inhaber bei der Authentisierung dem Authentisierungsnehmer zur Behauptung der Identität gibt. Diese Zugangsdaten überprüft der Authentisierungsnehmer im Rahmen der Authentifizierung anschließend. Um Zugangsdaten zu Accounts im Internet zu realisieren, stehen drei verschiedene Kategorien von Authentisierungsmitteln bereit. Der Authentisierungsvorgang kann aus einer Komponente oder aus einer Kombination mehrerer Komponenten gleicher oder unterschiedlicher Art bestehen. Mögliche Komponenten bei der Authentisierung sind Wissen, Besitz und Sein.[281]

108 Bevor auf die drei Arten der Authentisierungsmittel eingegangen wird, soll kurz erläutert werden, warum der Begriff des Authentisierungsmittels verwendet wird. Zunächst ist zu erwägen, gesetzliche Begriffe wie das Zahlungsauthentifizierungsinstrument aufzugreifen und statt von Authentisierungsmitteln von Authentifizierungsinstrumenten zu sprechen. Das Zahlungsauthentifizierungsinstrument beschreibt nach der im Bürgerlichen Recht anzuwendenden (§ 675c Abs. 3 BGB) Legaldefinition des § 1 Abs. 5 ZAG genau das, was im Rahmen dieser Untersuchung als Authentisierungsmittel bezeichnet wird. Beide Teile des Begriffes Zahlungsauthentifizierungsinstrument hat der Gesetzgeber jedoch unglücklich gewählt. Der Begriff, wie er in § 675k Abs. 1 BGB steht, stammt aus der Zahlungsdienste-Richtlinie (ZDRL) und ist das Ergebnis einer schlechten Übersetzung.[282] Das englische Wort *authentication*, wie es in Art. 4 Nr. 19 ZDRL definiert ist, hat im Deutschen zwei Bedeutungen: Authentisierung und Authentifizierung. Die sprachliche Differenzierung der Perspektive, die durch diese beiden Begriffe möglich ist, wird im Englischen nicht vollzogen[283] und wurde bei der Übersetzung anscheinend auch nicht vollzogen. Der englische Begriff *instrument* hat eine vom deutschen stark abweichende Bedeutung. Im Deutschen hat das Instrument primär die Bedeutung des Gerätes oder

281 *Albrecht*, S. 32 f.; *Federrath/Pfitzmann*, in: *U. Schneider/Dieter Werner*[7], 14.2.2; *dies.*, in: *Moritz/Dreier*[2], F Rn. 26; *Hornung*, Die digitale Identität, S. 29; *J. Meyer*, Identität, S. 43; *W. Müller/Redlich/Jeschke*, DuD 2011, 465; *Schneier*, S. 43; *Wefel*, S. 31.

282 Ähnlich *Oechsler*, WM 2010, 1381: „ungeschickte Lehnübersetzung".

283 Oben Rn. 105.

Werkzeugs.[284] Diese Bezeichnung umfasst sprachlich nur die Besitz-Komponenten einer Authentisierung, Wissen- oder Sein-Komponenten können nur schwerlich darunter verstanden werden. Das *payment instrument*, das in Art. 55 ZDRL beschrieben ist, hat eine andere Bedeutung als die deutsche Übersetzung der Richtlinie mit dem Begriff des Zahlungsinstruments zum Ausdruck bringt. Das englische Wort *instrument* hat auch die Bedeutung von Urkunde oder Beweisstück.[285] Diese Bedeutung hatte das deutsche Wort Instrument im 18. und 19. Jahrhundert zwar auch, sie ist jedoch nicht mehr Teil des kontemporären Sprachgebrauchs.[286] Eine zeitgemäße Übersetzung von *payment instrument* ist Zahlungsmittel.[287] Daher lehnt sich diese Arbeit nicht an den ungenauen, gesetzlichen Begriff von Authentifizierungsinstrumenten an, sondern spricht von Authentisierungsmitteln.

aa) Wissen

Eine Wissen-Komponente bei der Authentisierung setzt darauf, dass der Au- 109
thentisierungsgeber Kenntnis von einer gewissen Information hat.[288] Bei einer wissensbasierten Authentisierung fragt der Authentisierungsnehmer z.B. Passwörter, PINs oder Antworten auf Fragen ab.[289] Das Wissen um die Information ist dann ein taugliches Mittel zur Authentisierung, wenn es sich um eine geheime Information handelt. Hätte jeder die Information, könnte jeder sich erfolgreich als Berechtigter ausweisen. Für die Sicherheit wissensbasierten Authentisierungen spielt daher die Geheimhaltung der abgefragten Information eine entscheidende Rolle.

Vorteile einer wissensbasierten Authentisierung ist ihre Einfachheit. Au- 110
thentisierungsnehmer und -geber müssen lediglich eine nur diesen beiden bekannte Information teilen. Wiederholt der Authentisierungsgeber die Information anschließend gegenüber dem Authentisierungsgeber kann er sich dadurch ausweisen. Für den Authentisierungsgeber hat eine wissensbasierte Authentisierung den Vorteil, dass er diese weltweit durchführen kann,

284 Duden[3], Instrument.
285 *Romain/Bader/Byrd*[5], instrument; *v. Beseler/Jacobs-Wüstefeld*[4], instrument.
286 Vgl. Duden[3], Instrument.
287 *Romain/Bader/Byrd*[5], instrument, ∼ of payment; *v. Beseler/Jacobs-Wüstefeld*[4], instrument, ∼ of payment.
288 *Eckert*[8], S. 468; *Wefel*, S. 31.
289 *Borges/Schwenk/Stuckenberg/Wegener*, S. 6; *Federrath/Pfitzmann*, in: *U. Schneider/Dieter Werner*[7], 14.2.2; *dies.*, in: *Moritz/Dreier*[2], F Rn. 26; *Schneier*, S. 136.

ohne etwas bei sich führen zu müssen. Die Kosten für eine wissensbasierte Authentisierung sind daher sehr gering. Weder der Authentisierungsgeber noch der Authentisierungsnehmer müssen Geld für eine materielle Besitz-Komponente aufwenden. Teure Technik zur Überprüfung von Besitz- oder Sein-Komponenten fallen nicht an. Es muss weder Geld für eine materielle Besitz-Komponente aufgewendet werden, noch teure Technik zur Überprüfung von Besitz- oder Sein-Komponenten angeschafft werden.

111 Die Vorteile der Einfachheit der wissensbasierten Authentisierung korrelieren jedoch auch mit entscheidenden Nachteilen. Zwar kann sich der Authentisierungsgeber weltweit durch das Wissen ausweisen. Das geheime Wissen kann er jedoch nur begrenzt kontrollieren, weil Wissen unendlich teilbar ist. Sobald ein Dritter an die geheime Information gelangt – ob durch Weitergabe, List oder Erraten –, kann er sich mittels dieses Wissens authentisieren. Die wissensbasierte Authentisierung bietet somit keinen hohen Schutz.[290] Darüber hinaus besteht die Gefahr, dass der Authentisierungsgeber die geheime Information vergisst. Zwar kann er mangels Körperlichkeit diese nicht wie eine Besitz-Komponente vergessen im Sinne von liegen lassen. Er kann sie jedoch vergessen im Sinne von sich nicht mehr daran erinnern. Angesichts der Tatsache, dass das menschliche Gehirn nur eine begrenzte Aufnahmefähigkeit hat, stellt dies Authentisierungsgeber vor eine Herausforderung. Um die geheimen zur Authentisierung dienenden Informationen nicht zu vergessen, notieren viele Authentisierungsgeber sich diese, was eine Geheimhaltung dieser Notiz erfordert, um die Sicherheit des Vorgangs nicht zu gefährden.

bb) Besitz

112 Eine besitzbasierte Authentisierung setzt darauf, dass der Authentisierungsgeber etwas besitzt, das er vorlegen oder anwenden kann.[291] Mögliche Besitz-Komponenten sind Papierdokumente, Metallschlüssel, Magnetstreifen- und Chip-Karten.[292] Bei einem Verfahren mittels mobiler Transaktionsnummer (mTAN) stellt die SIM-Karte des Mobiltelefons die Besitz-Komponente dar. Eine Authentisierung, die den Besitz einer Sache überprüft, muss zur

290 *J. Meyer*, Identität, S. 44 Fn 153.
291 *Wefel*, S. 31.
292 *Federrath/Pfitzmann*, in: *U. Schneider/Dieter Werner*[7], 14.2.2; *dies.*, in: *Moritz/Dreier*[2], F Rn. 26; *Schneier*, S. 145.

Sicherheit den Besitz einer physisch einmaligen Sache überprüfen. Kann man den Gegenstand, dessen Besitz der Authentisierungsnehmer überprüft, beliebig kopieren, wäre die Authentisierung so unsicher wie eine wissensbasierte Authentisierung mit öffentlich verfügbaren Informationen. Im Internet stellt sich das Problem, dass der Authentisierungsnehmer den Besitz mangels räumlicher Nähe zum Authentisierungsnehmer nicht wie in der analogen Welt überprüfen kann. Für eine elektronische Überprüfung des Besitzes muss der Besitz daher digitalisiert werden, weil ein Authentisierungsgeber den Besitz elektronisch nicht übertragen kann.[293] Die digitale Überprüfung des Besitzes geschieht mittels eines Datensatzes, der nur durch Verwendung einer besonderen Sache (Token) gebildet werden kann.[294] Zur Herstellung einer physisch einmaligen Besitz-Komponente darf dieser Token nur auf der Besitz-Komponente gespeichert sein. Ferner darf die Besitz-Komponente nicht kopierbar sein[295] und ein Angreifer darf den Token nicht auslesen können.

Der Vorteil von Besitz-Komponenten bei der Authentisierung ist, dass der 113
Authentisierungsgeber die physische Kontrolle über das Authentisierungsmittel hat. Ein Diebstahl ist ebenso wie das Ausspähen einer Wissen-Komponenten möglich, der Authentisierungsgeber kann jedoch seinen fehlenden Besitz am Authentisierungsmittel leicht bemerken. Bemerkt der Authentisierungsgeber den Verlust der Besitz-Komponente kann er bei entsprechenden Vorrichtungen des Authentisierungsgebers die Komponente sperren lassen und somit Authentisierungen durch unberechtigte Dritte verhindern. Ein weiterer Vorteil der Besitz-Komponente ist, dass der Authentisierungsgeber diese Komponente nicht vergessen, im Sinne von sich nicht daran erinnern, kann. Vergessen im Sinne von liegen lassen, kann er diese jedoch sehr wohl. Der Nachteil von Besitz-Komponenten besteht in dem mit ihnen verbundenen hohen Aufwand. Für die Besitz-Komponente entstehen Kosten bei der Herstellung der einmaligen, physischen Sache. Ferner bedarf es zur Digitalisierung des Besitzes technischer Komponenten, deren Anschaffungspreis nicht zu vernachlässigen ist. Ein Nachteil für den Authentisierungsgeber besteht darin, dass er die Besitz-Komponenten bei sich führen muss, um sich zu authentisieren.

293 *Wefel*, S. 34.
294 *Borges*, Elektronischer Identitätsnachweis, S. 30.
295 Magnetstreifenkarten z.B. lassen sich einfach kopieren, *Wefel*, S. 34.

cc) Sein

114 Bei einer Sein-Komponente oder auch biometrischen Komponente wird ein individuelles Merkmal des Authentisierungsgebers überprüft. Für eine zuverlässige Authentisierung muss jede Person das Merkmal besitzen und das Merkmal muss für jede Person einmalig sowie unveränderlich sein.[296] Sein-Merkmale sind die Handgeometrie, der Fingerabdruck, das Aussehen, die Handschrift, das Netzhaut-Muster, die Stimme oder DNA-Muster.[297] Die zuverlässige, digitalisierte Überprüfung von Sein-Komponenten ist schwer zu realisieren. Bei der digitalen Überprüfung einer Sein-Komponente gleicht der Authentisierungsnehmer ein aus den individuellen Merkmalen des Authentisierungsgebers erhobenes digitalisiertes Muster mit Referenzdaten ab.[298] Dies führt zu zwei Problemen. Zum einen muss bei der Übereinstimmung mit den Referenzdaten ein Schwellenwert gefunden werden, ab dessen Grad an Übereinstimmung die Authentifizierung als erfolgreich angesehen wird. Dies führt zu einer Abwägung zwischen dem Zurückweisen berechtigter Authentisierungen (False Rejection Rate) und dem Annehmen unberechtigter Authentisierungen (False Acceptance Rate).[299] Ferner muss bei einer Sein-Authentisierung im Internet der aus den biometrischen Daten generierte Datensatz zum Authentisierungsgeber übertragen werden. Dabei handelt es sich jedoch um eine Information, vergleichbar mit einer Wissen-Komponente, die ein Angreifer ausspähen kann.[300] Eine sichere Authentisierung mit Sein-Komponenten ist somit nur bei lokalen Authentisierungen bei der Übertragung über kontrollierte, sichere Kanäle möglich.[301]

115 Einen Vorteil der Sein-Komponenten teilt sie mit der Wissen-Komponente. Der Authentisierungsgeber braucht sie im Gegensatz zu einer Besitz-Komponente nicht separat bei sich führen. Er kann sich weltweit authentisieren. Darüber hinaus kann der Authentisierungsgeber die Sein-Kom-

296 *Eckert*[8], S. 496.

297 *Federrath/Pfitzmann*, in: *U. Schneider/Dieter Werner*[7], 14.2.2; *dies.*, in: *Moritz/Dreier*[2], F Rn. 26; *Weichert*, CR 1997, 369, 370 ff.

298 *Borges/Schwenk/Stuckenberg/Wegener*, S. 42; *Heibey/Quiring-Kock*, DuD 2010, 332; *Hornung*, Die digitale Identität, S. 80.

299 *Albrecht*, S. 53 ff.; *Eckert*[8], S. 502; *Heibey/Quiring-Kock*, DuD 2010, 332; *Hornung*, Die digitale Identität, S. 80; *Schneier*, S. 142 f.

300 *Borges/Schwenk/Stuckenberg/Wegener*, S. 41; *J. Meyer*, Identität, S. 46 f.; *Schneier*, S. 143.

301 *Borges/Schwenk/Stuckenberg/Wegener*, S. 41.

ponente weder vergessen im Sinne von liegen lassen, noch vergessen, im Sinne von sich nicht mehr daran erinnern. Denn es besteht eine untrennbare Bindung zwischen dem Merkmal und der Person.[302] Die Nachteile von Sein-Komponenten bestehen darin, dass sie über das Internet nicht sicher zu realisieren sind. Ferner entstehen für eine Authentisierung mit einer Sein-Komponente hohe Kosten,[303] weil technische Geräte zur Überprüfung des Sein-Merkmals, wie ein Iris-Scanner, vorhanden sein müssen. Ein gravierender Nachteil von Sein-Komponenten ist, dass der Authentisierungsgeber sie nach einer Kompromittierung nicht ersetzen kann.[304] Bei einer Wissen-Komponente kann der Authentisierungsgeber beispielsweise das Passwort ändern, wenn ein Dritter es kennt. Die Besitz-Komponente kann der Authentisierungsgeber sperren lassen und sich eine Neue beschaffen, wenn diese gestohlen wurde. Hat hingegen ein Angreifer ein Modell eines Fingerabdrucks vom Authentisierungsgeber erlangt und gelingt damit die Authentisierung, kann der Authentisierungsnehmer zwar die Authentisierung mit diesem Fingerabdruck sperren. Der Authentisierungsgeber kann jedoch anschließend nicht seinen Fingerabdruck ändern, sodass ihm die Möglichkeit der Authentisierung mit der entsprechenden Sein-Komponente verwehrt ist.[305] Insgesamt bieten Sein-Komponenten, die bei einer Authentisierung über das Internet eingesetzt werden, zur Zeit noch nicht die Sicherheit der anderen Komponenten.[306]

Wegen der zahlreichen Vergleiche von Zugangsdaten im Internet mit einem Brief, dessen Briefkopf und der Unterschrift,[307] soll auf die Natur der Unterschrift eingegangen werden. Die Unterschrift als Teil der Handschrift ist ein Sein-Merkmal.[308] Die Handschrift lässt sich auf Grund ihrer individuellen Merkmale auf Echtheit überprüfen. Bei einer Unterschrift ist die Schriftprobe so gering, dass eine zuverlässige Überprüfung eventuell nicht möglich ist.[309] Aus diesem Grund muss z.B. das eigenhändige Tes- **116**

302 *Hornung*, Die digitale Identität, S. 85.
303 *Eckert*[8], S. 496.
304 *Albrecht*, S. 51.
305 Zu anderen Problemen der Unveränderlichkeit *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 41 f.; *Heibey*/*Quiring-Kock*, DuD 2010, 332.
306 *Stumpf*/*Sacher*/*Roßnagel*/*Eckert*, DuD 2007, 357, 360.
307 Dazu unten Rn. 490 ff.
308 *Federrath*/*Pfitzmann*, in: *Moritz*/*Dreier*[2], F Rn. 26; *Hornung*, Die digitale Identität, S. 76; *Jandt*, K&R 2009, 548, 551 f.; *Roßnagel*, MMR 2008, 22, 25; *Schneier*, S. 142.
309 *Hecker*, Forensische Handschriftenuntersuchung, S. 252.

tament (§ 2247 Abs. 1 BGB) nicht nur eigenhändig unterschrieben, sondern der gesamte Text muss vom Erblasser eigenhändig geschrieben sein, um die zuverlässige Echtheitsüberprüfung zu gewährleisten.[310] Der *BGH* begründet dieses Erfordernis damit, dass das Testament „von ihm in der ihm eigenen Schrift geschrieben und damit in einer Art und Weise errichtet worden ist, welche die Nachprüfung der Echtheit des Testaments auf Grund der individuellen Züge, die die Handschrift jedes Menschen aufweist, gestattet."[311] Die Echtheit einer Handschrift und damit einer Unterschrift kann mittels Schriftvergleich festgestellt werden. Handschrift ist zwar nicht absolut stabil und nicht unveränderlich, aber ein verlässliches Personenmerkmal.[312] Die Veränderbarkeit eines Sein-Merkmals schadet grundsätzlich nicht. Auch ein Fingerabdruck ist beispielsweise durch Verletzungen veränderbar. Der Authentizitätswert einer Unterschrift bei einem Erstkontakt wird jedoch teilweise bezweifelt.[313]

b) Zwei- und Mehr-Faktor-Authentisierung

117 Neben der Möglichkeit eine Authentisierung auf eine der Komponenten oder auf mehrere Komponenten einer Art zu stützten, besteht die Möglichkeit einer Zwei-Faktor-Authentisierung, auch Mehr-Faktor-Authentisierung genannt. Weit verbreitet ist die Zwei-Faktor-Authentisierung in Form einer Kombination aus Wissen und Besitz. Die ec-Karte beispielsweise verbindet durch ihren Besitz und der nötigen Kenntnis der PIN diese zwei Faktoren.[314] Ebenso setzen SmartCards, die den auf ihnen gespeicherten Token nur nach Eingabe eines PINs freigeben, auf diese Zwei-Faktor-Authentifizierung. Dazu gehören Chip-Karten der qualifizierten elektronischen Signatur sowie der elektronische Identitätsnachweis.

118 Ebenso ist das mTAN-Verfahren eine Zwei-Faktor-Authentisierung, die auf eine Kombination von Wissen und Besitz setzt. Regelmäßig muss der Account-Inhaber sich mittels Kenntnis seines Benutzerkontos sowie des dazugehörigen Passworts authentisieren. Möchte er eine Transaktion durchführen, bekommt er auf sein Mobiltelefon eine einmalig zu verwendende

310 *Hagena*, in: MüKo-BGB[6], § 2247 Rn. 14; *Lange/Kuchinke*[5], S. 376 f.
311 *BGH*, Beschluss v. 3. 2. 1967, III ZB 14/66 – BGHZ 47, 68, 70.
312 *Hecker*, NStZ 1990, 463, 463 f.; *ders.*, in: *Widmaier*, § 76 Rn. 9.
313 *Mankowski*, NJW 2002, 2822, 2824.
314 *Wefel*, S. 47.

TAN geschickt. Der Besitz der SIM-Karte im Mobiltelefon des Account-Inhabers wird dadurch überprüft, dass die SMS mit der einmaligen TAN nur den Besitzer der SIM-Karte erreichen kann.

Den Besitzes einer Sache kann der Authentisierungsgeber im elektroni- 119
schen Verkehr nicht gleichermaßen wie in der Offline-Welt nachweisen. Daher muss der Besitz digitalisiert werden, um ihn elektronisch nachweisbar zu machen. Eine Methode besteht darin, ein Einmal-Passwort auf ein Mobiltelefon zu schicken. Dadurch soll nachgewiesen werden, dass derjenige, der das Einmal-Passwort eingibt, im Besitz des Mobiltelefons ist. Bei einer anderen Methode wird auf einer Chip-Karte ein sog. Token gespeichert. Der Besitz dieses Tokens wird elektronisch nachgewiesen werden.[315] Der Token muss ausreichend vor dem Zugriff geschützt werden. Denn wenn er dies nicht ist, erfolgt die Authentisierung lediglich mittels des Wissens um den Token. Um den Token zu schützen werden mehrere Vorkehrungen getroffen. Zum einen ist der Token nur auf der Chip-Karte gespeichert. Der Aussteller der Chip-Karte muss den Token nach dessen Erstellen löschen.[316] Ferner darf der Token nicht auslesbar sein. Würde der Authentisierungsgeber den Token an sich übertragen, würde der Authentisierungsnehmer Kenntnis von diesem erlangen und eine besitzbasierte Authentisierung läge nicht mehr vor. Damit der Authentisierungsgeber den Token nicht übertragen muss und der Authentisierungsnehmer ihn dennoch überprüfen kann, basiert die Überprüfung auf einem asymmetrischen Verschlüsselungsverfahren.[317] Der Account-Inhaber verschlüsselt mittels seines Private-Key, der als Token auf der Chip-Karte gespeichert ist, einen Kontrollhash, den der Authentisierungsnehmer mittels des öffentlichen Schlüssels entschlüsselt und überprüft.[318] Damit ein Angreifer den Token nicht von der Chip-Karte auslesen kann, muss diese dagegen geschützt sein. Dies geschieht regelmäßig durch einen sechsstelligen PIN, ohne die der Zugriff auf den Token verwehrt wird.[319]

315 *Borges*, Elektronischer Identitätsnachweis, S. 30.
316 Dazu unten Rn. 883.
317 Zur asymmetrischen Verschlüsselung oben Rn. 78.
318 Dazu oben Rn. 79.
319 *Eckert*[8], S. 547 f.

4. Besondere Merkmale von Zugangsdaten im Internet

120 Die wesentliche Besonderheit von Zugangsdaten im Internet besteht darin, dass der Kommunikationspartner keine Möglichkeit hat zu überprüfen, ob der Account-Inhaber oder ein Dritter handelt. An der elektronischen Erklärung oder Handlung kann der Kommunikationspartner nur die virtuelle Identität des Accounts erkennen. Welche reale Person – wenn überhaupt eine gehandelt hat – handelte, wird anhand der übertragenen Daten nicht ersichtlich. Beim Einsatz von Wissen- oder Besitz-Komponenten besteht somit stets die Möglichkeit, dass ein anderer als der Account-Inhaber gehandelt hat. Der Dritte kann entweder durch eine Weitergabe der Zugangsdaten durch den Account-Inhaber an diese kommen oder diese stehlen, also eine Wissen-Komponente ausspähen oder den Besitz einer Besitz-Komponente an sich nehmen.

121 Bei einem Authentisierungsvorgang wird die Identität des Handelnden anhand vorhandener Daten mittels Authentisierungsmitteln überprüft. Als Ergebnis des Authentifizierungsvorgangs folgt bei erfolgreicher Authentifizierung die Autorisierung des Handelnden. Die Authentifizierung verbindet zwei in der Offline-Welt getrennte Vorgänge, nämlich die Identifikation und die Überprüfung der Legitimation. Zugangsdaten im Internet vermitteln somit zweierlei gleichzeitig: Identität und Legitimation. Weil der Kommunikationspartner nicht erkennen kann, ob der Account-Inhaber gehandelt hat, kann keine Trennung zwischen der Identität des Handelnden und seiner Legitimation stattfinden. Die Identität sowie die Befugnis Handlungen vorzunehmen werden beide durch die Zugangsdaten überprüft. Ein Dritter, der den Account verwendet, hat ohne Einschränkungen stets die gleichen Möglichkeiten wie der Account-Inhaber selbst. Lediglich bei Attribut-Zertifikaten nach § 7 Abs. 2 SigG[320] kommt eine Trennung von Identität und Legitimation in Betracht, wobei auch die Legitimation, die Vollmacht zu verwenden, nicht von der Identität des Vertreters getrennt werden kann.

122 Diese verknüpfte Möglichkeit von Identität und Legitimation ist vor unbefugtem Zugang durch die Authentisierungsmittel geschützt. Die weit verbreitete rein wissensbasierte Authentisierung schützt die virtuelle Identität durch einen Benutzernamen und ein Passwort. Ersterer ist häufig öffentlich. Nur das Wissen des Passworts, das häufig aus nicht mehr als acht Zeichen

320 Zu Attribut-Zertifikaten *Gramlich*, in: *Spindler/F. Schuster*[2], § 7 SigG Rn. 9; *Reese*, S. 19.

besteht, identifiziert und legitimiert damit eine Person. Die kombinierten Zugangsdaten aus Benutzername und Passwort haben häufig nicht mehr als 30 Zeichen. Ihre Kenntnis eröffnet jedoch umfangreiche Handlungsmöglichkeiten. Der Kommunikationspartner hat dabei das Vertrauen darin, dass die Zugangsdaten geschützt waren. Wegen der zahlreichen Möglichkeiten an die Zugangsdaten zu gelangen,[321] vertraut der Kommunikationspartner dabei anhand von teilweise öffentlich bekannten 30 Zeichen der Zugangsdaten darauf, dass der Account-Inhaber handelt.

Bei einem klassischen Identitätsdiebstahl ist eine räumliche Nähe zwischen Opfer und Täter erforderlich.[322] Der Täter muss beispielsweise den Personalausweis aus dem Portemonnaie des Opfers stehlen oder eine Kopie dessen ec-Karte anfertigen. Im Internet kann ein Angreifer die Zugangsdaten auch ohne räumliche Nähe zum Account-Inhaber ausspähen. Eine Phishing-Mail oder ein Software-Keylogger[323] können weltweit verschickt bzw. eingesetzt werden. Die physikalische Nähe zwischen Täter und Opfer ist nicht erforderlich. 123

III. Missbrauch

Der Missbrauch von Zugangsdaten kann durch verschiedene Wege erfolgen. Der Account-Inhaber kann dem Dritten die Zugangsdaten weitergeben. Der Dritte kann die Zugangsdaten jedoch auch ohne eine Weitergabe vom oder ohne den Account-Inhaber ausspähen. Ebenfalls unter den Missbrauch von Zugangsdaten fällt, wenn ein Dritter unter falschem Namen einen Account anlegt. 124

1. Missbrauch nach bewusster Weitergabe der Zugangsdaten

Eine erste Möglichkeit Zugangsdaten zu missbrauchen, besteht darin, dass ein Dritter nach der Weitergabe der Zugangsdaten durch den Account-Inhaber seine Befugnisse überschreitet. Es kommt häufig vor, dass eine Familie sich einen Account bei einem Online-Shop oder Internetauktions-Haus 125

321 Dazu unten Rn. 124 ff.
322 *BSI*, Lagebericht 2011, S. 22.
323 Dazu unten Rn. 142 bzw. 166.

teilt.[324] Ebenso besitzen Assistenten häufig die Zugangsdaten ihrer Vorgesetzten, um für diese Erklärungen abgeben zu können. Manche Nutzer teilen sich gemeinsam einen Account (Account-Sharing), was bei Zugängen, für die eine monatliche Gebühr zu entrichten ist, ein so weit verbreitetes Phänomen ist, dass viele Anbieter es in den AGB untersagen. Der Account-Inhaber kann sowohl die Passwörter einer rein wissensbasierten Authentisierung als auch die Chip-Karte mit zugehöriger PIN bei einer Zwei-Faktor-Authentisierung weitergeben. Eine Umfrage hat gezeigt, dass 40 % der Deutschen Ihre Passwörter gelegentlich weitergeben.[325] Mit der Überlassung eines eBay-Accounts kann der Account-Inhaber sogar Geld verdienen.[326] Eine Weitergabe liegt auch vor, wenn der Account-Inhaber einem Diensteanbieter zur Ausführung einer Überweisung im Rahmen des Online-Bankings die Zugangsdaten offenbart.[327] Benutzt der Dritte, dem der Account-Inhaber die Zugangsdaten weitergeben hat, diese Zugangsdaten anschließend in einer Weise, mit der der Account-Inhaber nicht einverstanden ist, liegt ein Missbrauch vor.[328]

2. *Missbrauch ohne bewusste Weitergabe der Zugangsdaten*

126 Auch ohne die bewusste Weitergabe der Zugangsdaten kann ein Dritter an diese gelangen. Identitätsdiebstähle kommen häufig vor, dabei arbeiten Angreifer jedoch neuerlich nicht mehr nur mit Phishing sondern auch mit Trojanern.[329] Unter dem engeren Begriff des Identitätsdiebstahls wird die Verwendung von personenbezogenen Daten zur Begehung einer Straftat verstanden.[330] Wenn hier von Identitätsdiebstahl gesprochen wird, geschieht dies nicht mit der einschränkenden Bedingung, dass das Ziel die Begehung einer Straftat sein muss. Die Unwissenheit vieler Internetnutzer birgt die Gefahr, dass sie unbewusst Daten preisgeben, die sie nicht preisgeben möch-

---

324 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 175.
325 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 118.
326 Vgl. *LG Bonn*, Urteil v. 7. 12. 2004, 11 O 48/04 – WRP 2005, 640; *AG Neumünster*, Urteil v. 3. 4. 2007, 31 C 1338/06 – NJW-RR 2007, 1544.
327 Beispielsweise bei sofortueberweisung.de.
328 Beispielsweise geschehen bei *LG Aachen*, Urteil v. 15. 12. 2006, 5 S 184/06 – NJW-RR 2007, 565.
329 *BSI*, Lagebericht 2011, S. 23.
330 *EG-Kommission*; *J. Meyer*, Identität, S. 38.

ten.[331] Gefährlich beim Missbrauch der Zugangsdaten ist, dass das Opfer den Angriff oder das Ausspähen der Zugangsdaten häufig gar nicht erkennt oder bemerkt.[332] Dass die Zugangsdaten einem Dritten bekannt sind, fällt den Opfern häufig erst auf, wenn der Dritte die Zugangsdaten das erste Mal missbraucht. Dieser Missbrauch erfolgt teilweise zeitversetzt, Monate oder Jahre nach dem Abgreifen der Zugangsdaten.[333]

Wenn behauptet wird, dass das Ausspähen eines Passworts unwahrscheinlich sei,[334] oder das Diebstahlrisiko der Zugangsdaten gering sei,[335] kann dem nicht zugestimmt werden. Die Gefahr, dass Angreifer Zugangsdaten abgreifen, ist unverändert hoch.[336] Die meisten Angriffe wenden sich gegen den Endanwender als schwächstes Glied in der Kette der IT-Sicherheit.[337] Bei den Angriffsarten ist zwischen zwei verschiedenen Angriffstypen zu unterscheiden. Passive Angriffe beschränken sich darauf, vertrauliche Daten mitzulesen und unautorisiert Informationen zu gewinnen.[338] Aktive Angriffe hingegen manipulieren Anwendung oder Internet-Verbindungen, um in Echtzeit mit Hilfe der Zugangsdaten abgegebenen Erklärungen zu manipulieren.[339] 127

Teilweise wird behauptet, dass das Ausspähen der Zugangsdaten nur mit besonderen Fachkenntnissen möglich sei.[340] Dies solle dafür sprechen, dass das Ausspähen der Daten unwahrscheinlich sei. Dagegen spricht jedoch, dass ein potentieller Angreifer sich Methoden die Zugangsdaten auszuspähen mit frei verfügbaren Informationen im Internet anlesen kann,[341] was dazu führt, dass auch sog. Script-Kiddies an Zugangsdaten gelangen. Zum anderen lässt die Underground Economy zu, dass sich technisch wenig versierte Kriminelle den Sachverstand einkaufen können.[342] Für Viren existieren beispielsweise einfach zu bedienende Baukästen, bei denen der Nutzer mit 128

331 *Baier*, S. 17.
332 *BKA*, S. 9.
333 *Schulte am Hülse/Welchering*, NJW 2012, 1262, 1264.
334 *Sonnentag*, WM 2012, 1614, 1617.
335 *Mankowski*, CR 2011, 458.
336 *BKA*, S. 18.
337 *Borges/Schwenk/Stuckenberg/Wegener*, S. 50.
338 *Eckert*[8], S. 19; *Schwenk/Gajek*, in: Internet-Auktion, 180, 181.
339 *Eckert*[8], S. 19; *Schwenk/Gajek*, in: Internet-Auktion, 180, 181.
340 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 176; *Mankowski*, CR 2011, 458.
341 *Armgardt/Spalka*, K&R 2007, 26, 29.
342 *BKA*, S. 18.

wenigen Klicks einen Virus zusammenstellen kann.[343] Für die besonders gefährlichen Drive-By-Exploits sind sog. Exploit-Kits käuflich zu erwerben, die für einen Preis 200 bis 4000 USD gehandelt werden.[344] Neben Informationen über Zero-Day-Exploits kann ein Angreifer auch die Kontrolle über ein Bot-Netz mieten oder sich Zugangsdaten einkaufen.[345] Die Zugangsdaten werden in einer sog. Dropzone gesammelt und können dort erworben werden.[346] Für Webmailer, Handelsplattformen, Online-Shops, Soziale Netzwerke sowie fürs Online-Banking existieren dort zahlreiche Datensätze von Deutschen.[347]

129 Auf der Seite der Angreifer agieren unterschiedliche Arten mit verschiedensten Intentionen. Als Hacker werden technisch sehr versierte Menschen bezeichnet, die Sicherheitslücken in IT-Systemen aufspüren.[348] Die Motivation der Hacker liegt jedoch regelmäßig nicht darin einen finanziellen Vorteil durch die aufgefundene Sicherheitslücke zu erhalten, sondern vielmehr darin, die Öffentlichkeit auf die Schwachstellen aufmerksam zu machen.[349] Cracker, auch als Black-Hat-Hacker bezeichnet,[350] hingegen halten sich nicht an die Hacker-Ethik, sondern nutzen ihren technischen Sachverstand, um die Lücken von IT-System zu ihrem finanziellen Vorteil zu nutzen.[351] Bei Script-Kiddies handelt es sich um junge Menschen, die viel Zeit, jedoch häufig nur rudimentären Sachverstand haben, mit dem sie bekannte Exploits, eher aus einem Spieltrieb oder Neugierde heraus oder um Ruhm zu erlangen, ausnutzen.[352] Die Intention, Schaden anzurichten beziehungsweise einen finanziellen Vorteil zu erhalten, ist somit nur bei Crackern nicht aber bei Hackern oder Script-Kiddies Hauptmotivation.

130 Folgend werden zahlreiche Wege aufgeführt, wie ein Angreifer an die Zugangsdaten des Account-Inhabers gelangen kann. Im Nachhinein lässt

343 *BSI*, Lagebericht 2011, S. 25; *Dennis Werner*, Verkehrspflichten, S. 60; *Pierrot*, in: *Ernst*, Rn. 96.
344 *BSI*, Lagebericht 2011, S. 12.
345 *Gaycken*, S. 229; *Sieber*, Gutachten zum 69. DJT, S. C 23.
346 *Schulte am Hülse/Welchering*, NJW 2012, 1262, 1264.
347 *BSI*, Lagebericht 2011, S. 23.
348 *Holznagel*, § 3 Rn. 27; *Schneier*, S. 43.
349 *Eckert*[8], S. 22; *Pierrot*, in: *Ernst*, Rn. 9.
350 *Gaycken*, S. 49.
351 *Eckert*[8], S. 22; *Holznagel*, § 3 Rn. 27; *Schneier*, S. 43.
352 *Eckert*[8], S. 22; *Holznagel*, § 3 Rn. 27; *Gaycken*, S. 50; *Pierrot*, in: *Ernst*, Rn. 9.

sich häufig nicht mehr feststellen, auf welche Art und Weise der Angreifer an die Zugangsdaten gelangt ist.[353]

a) Wege, um an die Zugangsdaten zu gelangen

Möchte ein Angreifer an die Zugangsdaten des Account-Inhabers gelangen, stehen ihm dafür zahlreiche Möglichkeiten zur Verfügung. Diese setzen zum überwiegenden Teil eine Mitwirkung des Account-Inhabers voraus. Dies ist jedoch nicht zwingend. 131

aa) Physikalischer Zugriff auf die Zugangsdaten

Der einfachste Weg für einen Datendieb an die Zugangsdaten zu gelangen ist, wenn sich der Account-Inhaber die Zugangsdaten auf einem Zettel oder einem anderen körperlichen Gegenstand notiert hat. Häufig notieren sich die Account-Inhaber Passwörter auf einem Zettel[354] oder ec-Karten-Inhaber die PIN auf einem Papier im Portemonnaie in der Nähe der Karte.[355] Eine Speicherung auf einem elektronischen Datenträger kommt ebenso vor.[356] Unter den physikalischen Zugriff auf die Zugangsdaten fällt auch der Fall, dass der Account-Inhaber die Zugangsdaten so eingibt, dass ein Dritter sie bei der Eingabe mitlesen kann.[357] Insbesondere bei längeren oder komplizierten Passwörtern besteht wegen der Schwierigkeit sich das Passwort zu merken, ein Bedarf, das Passwort zu notieren.[358] Im Rahmen der Pflichten des Kunden beim Online-Banking wird diskutiert, dass dieses Aufschreiben erlaubt sein muss, weil dem Bankkunden nicht zuzumuten ist, sich so viele Passwörter zu merken.[359] 132

353 Vgl. *OLG Bremen*, Beschluss v. 21. 6. 2012, 3 U 1/12 – MMR 2012, 593, insoweit nicht abgedruckt Rn. 25; *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813; *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255.

354 *Spindler*, CR 2003, 534.

355 *Schulte am Hülse/Welchering*, NJW 2012, 1262, 1263 f.

356 Beispielsweise bei *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 180 f.

357 Vgl. dazu *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06 – NJW 2007, 611, 611 f.

358 *Pierrot*, in: *Ernst*, Rn. 38.

359 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 115. Zur ec-Karte *Borges*, Verträge, S. 498.

133 Die Account-Inhaber versuchen ihre Zugangsdaten häufig vor einem Zugriff auf die Materialisierung in Form des Zettels zu schützen. Während einige Account-Inhaber so nachlässig sind und einen Klebezettel am Monitor anbringen, machen andere Nutzer sich die Mühe den Zettel gut zu verstecken. Da es übliche Verstecke für Zugangsdaten gibt, sind diese teilweise recht schnell ausfindig zu machen.[360]

134 Die zweite Methode besteht darin, dass die Zugangsdaten zwar notiert werden, sie jedoch in gewisser Weise chiffriert oder verschlüsselt werden. Eine häufige Methode besteht darin, die Geheimziffer wie die PIN in Form einer Telefonnummer in das Adressbuch zu schreiben.[361] Weil diese Methode Angreifern bekannt ist, können als Telefonnummern getarnte Geheimziffern häufig schnell ausfindig gemacht werden.

bb) Zugriff zu gespeicherten Zugangsdaten

135 Wie die Notiz des Passworts in der analogen Welt, funktioniert die Schlüsselbund-Verwaltung eines Betriebssystems, eines Browsers oder eines Cloud-Anbieters. In einem Passwort-Speicher können zahlreiche kryptische, sich schwer zu merkende Passwörter so gespeichert werden, dass sie bei Bedarf im Authentisierungsvorgang automatisch eingegeben werden.[362] Wenn in einem auf dem Rechner gespeicherten Passwort-Speicher Zugangsdaten ungeschützt abgelegt sind und ein Dritter Zugriff auf den Rechner hat, kann er den mit den Zugangsdaten geschützten Account verwenden.[363] Den Passwort-Speicher eines Rechners kann ein Angreifer bei einem infizierten[364] Rechner auslesen, wenn der Passwort-Speicher nicht oder nicht ausreichend verschlüsselt ist.

136 Das zunehmende Angebot von Cloud-Anbietern an Online-Passwort-Speichern bereitet ähnliche Zugriffsmöglichkeiten. Dienste wie Apples iCloud Keychain oder die in Google Chrome integrierte Anmeldung mit Cloud-Anbindung, ermöglichen es den Nutzer die Passwörter nicht ausschließlich auf seinem eigenen Rechner abzuspeichern, sondern zusätzlich

360 *Pierrot*, in: *Ernst*, Rn. 38.
361 Dazu *BGH*, Urteil v. 17. 10. 2000, XI ZR 42/00 – BGHZ 145, 337, 338.
362 *Baier*, S. 52 f.
363 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 176. So geschehen bei *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 519.
364 Unten Rn. 182 ff.

online bei den als Cloud bezeichneten Servern[365] des jeweiligen Anbieters zu hinterlegen. Sollte es einem Angreifer gelingen, auf die beim Cloud-Anbieter hinterlegten Daten zuzugreifen,[366] ist es möglich, dass er diese Zugangsdaten zur missbräuchlichen Verwendung von Accounts einsetzt. Selbst wenn der Dritte beim Angriff nur Zugriff auf die verschlüsselten Daten[367] der vom Cloud-Anbieter für die Nutzer gespeicherten Zugangsdaten erhält, ist es theoretisch möglich, dass er diese entschlüsselt und missbräuchlich verwenden kann.

Darüber hinaus besteht beim Zugriff eines Dritten auf den Rechner die 137
Gefahr, dass dieser den mittels der Zugangsdaten geschützten Account deswegen verwenden kann, weil der Account-Inhaber den Logout vergessen hat[368] oder der Account-Inhaber mittels Cookies dauerhaft eingeloggt ist. In solchen Fällen kann ein Dritter, der den Rechner benutzt, mangels Notwendigkeit zur Wiederholung des Authentisierungsvorgangs den Account missbrauchen, ohne die Zugangsdaten zu besitzen.

cc) Phishing

Phishing wird als Oberbegriff für internetbasierte Angriffe verwendet, die 138
das Ziel haben vertrauliche Daten, insbesondere Zugangsdaten, vom Account-Inhaber zu erlangen.[369] Für den etymologischen Ursprung des Phishings gibt es zwei Erklärungsversuche. Häufig wird behauptet, Phishing sei eine englische Zusammenfassung der Wörter Passwort und Angeln (to fish).[370] Dieser Erklärungsversuch vermag das h in dem Wort Phishing nicht zu erklären. Wahrscheinlicher ist daher der zweite Erklärungsversuch des Ursprungs. In der Hackersprache ist es üblich, dass das f durch ph ersetzt wird. Phishing sei daher lediglich das in Hackersprache geschriebene Fis-

365 Zur Definition der Cloud *M. Lehmann/Giedke*, CR 2013, 608, 610 f.; *Schulz/Boseßky/C. Hoffmann*, DuD 2013, 95.

366 Worüber zahlreiche Fällen bekannt werden, *Kalabis/Kunz/R. Wolf*, DuD 2013, 512.

367 Regelmäßig werden die Daten vom Anbieter in der Cloud verschlüsselt, ebd., 513.

368 *Ernst*, MDR 2003, 1091, 1093.

369 *Hansen*, S. 11; *Eckert*[8], S. 23; *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.7.2; *J. Meyer*, Identität, S. 45; *Wien*[3], S. 193; *Marberth-Kubicki*[2], Rn. 118.

370 *Hilgendorf/Valerius*[2], Rn. 760; *BSI*, IT-Grundschutz-Kataloge, G 5.157; *Eckert*[8], S. 23; *Popp*, NJW 2004, 3517; *Recknagel*, S. 51; *Schwenk/Gajek*, in: Internet-Auktion, 180, 184; *Wien*[3], S. 193; *Bachfeld*, c't 22/2005, 148.

hing.[371] Das metaphorische Angeln beim Phishing beschreibt den Versuch der Angreifer im großen Meer des Internets nach wertvollen Zugangsdaten zu angeln, bis ein Account-Inhaber an ihrer Angel anbeißt und seine Zugangsdaten preisgibt.

139 Der Vorgang des Phishing ist in zwei Phasen eingeteilt.[372] In der ersten Phase lockt der Angreifer den Account-Inhaber auf seine Internetseite. Bei den Methoden, wie der Angreifer den Account-Inhaber auf seine Seite locken kann, unterscheidet man zwischen dem klassischen Phishing, Pharming und Social-Engineering. In der zweiten Phase befindet sich der Account-Inhaber auf dieser Seite, gibt seine Zugangsdaten ein und sendet sie damit an den Angreifer. Für Phishing ist daher charakteristisch, dass das Opfer aufgefordert wird seine Zugangsdaten einzugeben, wobei die Aufforderung scheinbar vom Authentisierungsnehmer kommt, in Wahrheit aber ein Dritter dahinter steckt.[373]

140 Eine bewusste Weitergabe der Zugangsdaten durch das Opfer an den Angreifer liegt beim Phishing nicht vor. Das Opfer gibt die Zugangsdaten nämlich nicht weiter, sondern nur ein. Diese bewusste Eingabe der Zugangsdaten erfolgt beim Phishing im Glauben, diese wie gewöhnlich zur Authentisierung gegenüber dem Authentisierungsnehmer zu verwenden. Zwar gelangen die Zugangsdaten dabei an den sich als Authentisierungsnehmer gerierenden Angreifer. Dem Opfer des Phishing-Angriffs ist jedoch nicht bewusst, dass ein Dritter die Daten von ihm erhält. Er geht bei der Eingabe der Zugangsdaten nicht davon aus, dass anschließend ein Dritter seinen Account wie nach einer bewussten Weitergabe verwenden kann.

141 Hat der Angreifer auf diese Art und Weise Kenntnis der Zugangsdaten des Account-Inhabers erlangt, kann er diese missbrauchen. Bei Zugangsdaten zum Online-Banking werden die Daten häufig genutzt, um Geld vom Konto des Account-Inhabers auf ein eigenes Konto oder ein Konto eines Geldkuriers zu überweisen. Mit den Zugangsdaten zu Accounts bei Online-Shops oder Internet-Auktionsplattformen kann der gesamte Account übernommen werden (Account-Takeover).[374]

---

371 *APWG*; *Gercke*, CR 2005, 606; *Hansen*, S. 12.

372 *Schwenk/Gajek*, in: Internet-Auktion, 180, 186; *Schwenk/Gajek/Wegener*, DuD 2005, 639, 640.

373 *Hilgendorf/Valerius*[2], Rn. 760; *Borges*, NJW 2005, 3313; *Recknagel*, S. 51.

374 *Gercke*, CR 2005, 606, 607.

aaa) Klassisches Phishing

Beim klassischen Phishing schreiben die Angreifer ihre potentiellen Opfer mit einer massenhaften verschickten E-Mail an.[375] Die E-Mail enthält die Aufforderung auf einen Link zu klicken, der zur Internetseite des Angreifers führt.[376] Den Adressaten der E-Mail wird ein Vorwand vorgegeben, der sie dazu bringen soll, auf den Link zu klicken, um dort die Zugangsdaten einzugeben.[377] Beispielsweise wird behauptet, eine Bank habe technische Probleme mit dem Online-Banking oder habe das Verfahren des Online-Bankings angepasst, sodass es erforderlich sei, dass der Kunde seine Daten erneut eingibt.[378] 142

Die Angreifer nutzen verschiedene Methoden, um die E-Mail glaubwürdig erscheinen zu lassen. Zum einen passen sie die E-Mail an die Corporate Identitiy des Authentisierungsnehmers an und übernehmen Logo, Schriftart, Schriftgröße und Farbe des Unternehmens.[379] Darüber hinaus geben die Angreifer Hyperlinks in HTML-Mails im Beschreibungstext mit der originalen Domain an. Klickt das Opfer auf den Link, wird es jedoch zu einer anderen als in der Beschreibung angegebenen URL geleitet.[380] Der Empfänger der E-Mail meint beispielsweise, er klicke gerade auf einen Link, der ihn z.B. auf http://www.deutsche-bank.de leitet, in Wahrheit gelangt er jedoch auf die Seite des Angreifers. 143

Um den Absender der E-Mail vertrauenswürdig erscheinen zu lassen, wählen Angreifer entweder einen Absender, der dem Original ähnelt, oder sie fälschen den Absender. Die Ähnlichkeit mit dem originalen Absender erreichen sie dadurch, dass sie eine Domain wählen, die das Opfer leicht verwechseln kann.[381] Bei einer Bank wird teilweise die Bank als banc.de 144

375 *Hansen*, S. 13; *Gercke*, CR 2005, 606; *Schwenk/Gajek/Wegener*, DuD 2005, 639, 640.

376 *BSI*, IT-Grundschutz-Kataloge, G 5.157; *Erfurth*, WM 2006, 2198, 2200; *Hansen*, S. 11; *J. Meyer*, Identität, S. 45; *Recknagel*, S. 51; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 30.

377 *BSI*, IT-Grundschutz-Kataloge, G 5.157; *Erfurth*, WM 2006, 2198, 2200; *Hansen*, S. 14 f. *Knupfer*, MMR 2004, 641; *Recknagel*, S. 51.

378 *Knupfer*, MMR 2004, 641.

379 *Hansen*, S. 14; *Recknagel*, S. 51; *Schwenk/Gajek*, in: Internet-Auktion, 180, 186.

380 *Erfurth*, WM 2006, 2198, 2200; *Schwenk/Gajek*, in: Internet-Auktion, 180, 187; *Schwenk/Gajek/Wegener*, DuD 2005, 639, 640.

381 *Tanenbaum/Wetherall*[5], S. 38; *Gercke*, CR 2005, 606.

geschrieben oder das a mit einem kyrillischen a dargestellt.[382] Verwenden die Angreifer beim Absender als frei wählbare Header-Information[383] eine bestehende, ihnen nicht gehörende E-Mail-Adresse,[384] kann der Nutzer mit den standardmäßig angezeigten Informationen in E-Mail-Programmen nicht feststellen, dass die E-Mail vom Angreifer und nicht vom vermeintlichen Absender stammt.

145 Trotz der zahlreichen Versuche, die E-Mail möglichst echt aussehen zu lassen, befinden sich in vielen Phishing-Mails Schwachstellen. Als in der Anfangszeit des Phishings die Methoden aus den USA nach Deutschland kamen, haben die Angreifer die E-Mails noch mittels automatischer Übersetzungsprogrammen ins Deutsche übersetzt und die Mails waren folglich mit offensichtlichen Rechtschreib- oder Grammatikfehlern durchsäht.[385] Diese Fehler begehen viele Angreifer jedoch nicht mehr. Die Glaubwürdigkeit von klassischen Phishing-Mails leidet darüber hinaus auch unter dem massenhaften Versenden der Mails. Die E-Mails werden an eine lange Liste von Empfängern versendet, sodass ein Streuverlust eintritt und Empfänger angeschrieben werden, die keinen Account beim Authentisierungsnehmer unterhalten.[386]

146 Das klassische Phishing kann lediglich eine einfache wissensbasierte Authentisierung überwinden. Bereits das iTAN-Verfahren kann ein Angreifer mittels Phishings praktisch nur schwer umgehen.[387] Dazu ist die Eingabe des gesamten TAN-Blocks erforderlich, wozu sich jedoch unerfahrene Nutzer durchaus verleiten lassen.[388] Ebenso können Authentisierungsverfahren mit Besitzkomponente wie das mTAN-Verfahren oder SmartCard-Einsätze nicht mittels klassischen Phishings angegriffen werden.[389] Diese Verfahren können nur von Echtzeitmanipulationen, wie einem Man-in-the-Middle-Angriff überwunden werden.[390] Das klassische Phishing sei deswegen praktisch nicht mehr feststellbar.[391]

---

382 *Hansen*, S. 15.
383 Die sich einfach fälschen lässt, dazu unten Rn. 212.
384 *Schwenk/Gajek*, in: Internet-Auktion, 180, 187.
385 *Gercke*, CR 2005, 606.
386 *Bachfeld*, c't 22/2005, 148; *Hansen*, S. 1; *Schwenk/Gajek*, in: Internet-Auktion, 180, 187.
387 *Hansen*, S. 20; *Herresthal*, in: *Langenbucher/Bliesener/Spindler*, Kap. 5 Rn. 62.
388 So bei *OLG München*, Urteil v. 23. 1. 2012, 17 U 3527/11 – MMR 2013, 163.
389 *Hansen*, S. 20.
390 *BKA*, S. 12. Dazu unten Rn. 168.
391 *BSI*, Lagebericht 2011, S. 23.

bbb) Pharming

Beim Pharming[392] wird in der ersten Phase keine E-Mail an das Opfer verschickt, um ihn auf die Seite zu leiten. Vielmehr manipuliert der Angreifer die DNS-Zuordnungstabelle, damit das Opfer auf seine Internetseite gelangt.[393] Etymologisch ist nicht vollständig geklärt, woher der Begriff stammt. Im illegalen Kontext bezeichnen Angreifer ihre Ansammlung von Servern häufig mit dem englischen Begriff für Bauernhof farm, weil sie so viele Server kontrollieren, wie es Tiere auf einem Bauernhof gibt.[394] In der Hackersprache ist dann das f durch das ph ersetzt worden, sodass dadurch möglicherweise die Bezeichnung Pharming entstand. 147

Domain Name System (DNS) ist ein System, das Domainnamen in IP-Adressen auflöst.[395] Menschen können sich schwer IP-Adressen merken, die in IPv4 aus vier Byte bestehen[396] und als vier Zahlenblöcke aus je bis zu dreistelligen Ziffern dargestellt werden (z.B. 173.194.44.87). Anwenderfreundlicher sind Domainnamen (z.B. google.de), die der DNS-Nameserver anschließend in die dazugehörige IP-Adresse umwandelt.[397] 148

Beim Pharming greift der Angreifer in diesen automatischen Prozess der Auflösung von Domainnamen in IP-Adressen ein. Der Nutzer wird an Stelle der korrekten Weiterleitung an die IP-Adresse des Servers des Authentisierungsnehmers an die IP-Adresse des Angreifers geleitet.[398] Die Auflösung der Domain-Namen läuft automatisch im Hintergrund, also ohne Mitwirkung des Nutzers ab.[399] Das macht Pharming besonders gefährlich.[400] Unbemerkt vom Account-Inhaber wird dieser auf die Seite des Angreifers geleitet.[401] Der Prozess der Domain-Auflösung durch einen Nameserver ist vielschichtig, sodass fürs Pharming vier Angriffspunkte bestehen: die lokale Hosts-Datei, der DNS-Cache, der Router des Accounts-Inhabers sowie der zentrale Nameserver. 149

---

392 Auch als technischen Phishing bezeichnet *Hansen*, S. 12.
393 *BSI*, IT-Grundschutz-Kataloge, G 5.157; *J. Meyer*, Identität, S. 45.
394 *Popp*, MMR 2006, 84.
395 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.3.3; *Tanenbaum/Wetherall*[5], S. 703 ff.
396 Dazu oben Rn. 38.
397 *Eckert*[8], S. 107.
398 *Gaycken*, S. 235.
399 *Schwenk/Gajek/Wegener*, DuD 2005, 639, 641.
400 *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08 – MMR 2008, 626, 628; *Borges*, NJW 2005, 3313, 3314; *J. Meyer*, Identität, S. 45.
401 *Schwenk/Gajek*, in: Internet-Auktion, 180, 187.

150 Die erste Methode des Pharming setzt beim Betriebssystem des Account-Inhabers an. Die lokale hosts-Datei des Betriebssystems sorgt dafür, dass eine Anfrage an einen Nameserver nur dann geschickt wird, wenn kein Eintrag in der lokalen hosts-Datei vorhanden ist.[402] Dadurch können eigene Domains für jeden Rechner festgelegt werden. Ein typischer Eintrag ist beispielsweise, dass die Domain localhost auf IP-Adresse 127.0.0.1 zeigt. Bei einem infizierten[403] Rechner kann ein Wurm oder ein Trojaner diese hosts-Datei so verändern, dass für gewisse Domains keine Anfrage an einen Nameserver geschickt wird, sondern der Nutzer direkt auf die Seite des Angreifers geschickt wird.[404] Ebenso kann der Angreifer beim infizierten Rechner des Nutzers die Einstellungen des Betriebssystems so verändern, dass alle DNS-Anfragen an einen vom ihm kontrollierten Nameserver geleitet werden und dadurch den gleichen Effekt erzielen.

151 Die zweite Methode setzt ebenfalls in der Sphäre des Account-Inhabers an. Nicht nur der Rechner des Account-Inhabers ist an der Domain-Auflösung beteiligt. Regelmäßig stellen Nutzer die Internet-Verbindung über einen Router her. Den Nameserver, den der Router nach der Auflösung fragt, kann der Nutzer frei wählen. Gelingt einem Angreifer der Zugriff auf den Router des Account-Inhabers, kann er alle DNS-Anfragen an seinen eigenen Nameserver leiten und damit beliebig viele verfälschte DNS-Auskünfte dem Router und damit dem Rechner des Account-Inhabers mitteilen.[405] Dieser Angriff wird als Drive-By-Pharming bezeichnet.[406]

152 Die dritte Methode des Pharming greift den für die Domain zuständigen Nameserver an. Der Angreifer nutzt Schwachstellen im Betriebsystem des Nameservers, um Kontrolle über diesen zu erlangen.[407] Hat er die Kontrolle, kann er DNS-Einträge in der Datenbank verändern, sodass nachfragende

402 *Eckert*[8], S. 121.

403 Zu den Infektionswegen unten Rn. 182 ff.

404 *BSI*, IT-Grundschutz-Kataloge, G 5.157; *Borges*, NJW 2005, 3313, 3314; *Erfurth*, WM 2006, 2198, 2199; *J. Meyer*, Identität, S. 45; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 30; *Popp*, MMR 2006, 84.

405 *BSI*, IT-Grundschutz-Kataloge, G 5.157; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 31.

406 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 31.

407 *BSI*, IT-Grundschutz-Kataloge, G 5.78, 5.157; *Schwenk/Gajek*, in: Internet-Auktion, 180, 188; *Schwenk/Gajek/Wegener*, DuD 2005, 639, 641.

Nutzer bei den ausgewählten Domains auf die Internetseite des Angreifers geleitet werden.[408] Dieser Angriff wird als DNS-Poisoning bezeichnet.[409]

153 Die vierte Methode des Pharming manipuliert den DNS-Cache eines Nameservers, der nicht den zu manipulierenden Eintrag kontrolliert. Die Root-Nameserver sind in zahlreiche Zonen aufgeteilt.[410] Lokale Nameserver fragen bei dem Root-Nameserver an, der den DNS-Eintrag kontrolliert, und speichern die Ergebnisse in ihrem Cache für 24 oder 48 Stunden, sodass die lokalen Server nicht bei jedem Domain-Aufruf eine neue Anfrage an den Root-Server schicken müssen.[411] Der Cache des lokalen Nameservers, den der Account-Inhaber primär befragt, kann mit verfälschten Einträgen gefüllt werden, sodass der Account-Inhaber auf die Seite des Angreifers geschickt wird.[412] Dazu muss der Angreifer weder den lokalen Nameserver, auf den der Account-Inhaber zugreift, noch den den Eintrag kontrollierenden Root-Nameserver kontrollieren. Es reicht aus, dass der Angreifer einen Nameserver kontrolliert, bei dem eine Domain abgefragt wird, für die der Nameserver des Angreifers gefragt wird. Neben der Auskunft für die angefragte Domain, sendet der Angreifer mit seinem Nameserver ebenfalls einen ungefragten Eintrag, den der Nameserver des Angreifers nicht kontrolliert, mit verfälschter Adresse zurück.[413] Diesen nicht angefragten Eintrag übernimmt der lokale Nameserver des Account-Inhabers häufig ungeprüft,[414] sodass der Account-Inhaber auf die Seite des Angreifers geleitet wird. Diese Methode wird als DNS-Cache-Poisoning bezeichnet.[415] Durch den zunehmenden Einsatz von Domain Name System Security Extensions (DNSSEC), also einer Überprüfung der DNS-Einträge, ist DNS-Cache-Poisoning bei

---

408 *Borges*, NJW 2005, 3313, 3314; *Erfurth*, WM 2006, 2198, 2199; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 31.

409 *Popp*, MMR 2006, 84.

410 *Tanenbaum/Wetherall*[5], S. 703 f.

411 *BSI*, IT-Grundschutz-Kataloge, 5.78; *Gaycken*, S. 236; *Tanenbaum/Wetherall*[5], S. 705.

412 *BSI*, IT-Grundschutz-Kataloge, G 5.157; *Schwenk/Gajek*, in: Internet-Auktion, 180, 187.

413 *Eckert*[8], S. 138; *Gaycken*, S. 236; *Schwenk*[3], S. 203; *Biallaß/Borges/Dienstbach* u. a., in: Innovationsmotor IT-Sicherheit, 495, 498.

414 *Sieber*, in: *Hoeren/Sieber/Holznagel*, Kap. 1 Rn. 60; *Schneier*, S. 180.

415 *BSI*, IT-Grundschutz-Kataloge, G 5.157; *Gaycken*, S. 235; *Schwenk/Gajek*, in: Internet-Auktion, 180, 187; *Tanenbaum/Wetherall*[5], S. 956; *Dennis Werner*, Verkehrspflichten, S. 72.

vielen Top-Level-Domains (TLDs) nicht mehr möglich.[416] Oberbegriff für DNS-Poisoning und DNS-Cache-Poisoning ist DNS-Spoofing.[417]

154 Das DNS-Cache-Poisoning kann ein Angreifer recht einfach erreichen. Einen Nameserver kann der Angreifer selbst aufsetzen. Für jede einzelne Domain kann angegeben werden, welcher Nameserver sie auflöst. Der Angreifer kann daher eine beliebige Domain registrieren und somit einen Nameserver im Internet platzieren.[418] Erreicht er, dass ein Nutzer die registrierte Domain auflöst, kann er zusätzliche manipulierte Einträge unterbringen. Das Auflösen der vom Angreifer registrierten Domain kann er bereits dadurch erreichen, dass ein Bild, das auf der Domain gehostet ist und das beispielsweise als Werbung auf einem gut frequentieren Blog geschaltet ist, aufgerufen wird. Wenn der Angreifer es schafft, den DNS-Cache des ISP zu verfälschen, muss noch nicht einmal das Opfer die Domain besuchen. Es reicht vielmehr aus, dass ein Kunde des ISP die Domain auflöst.[419]

155 Nach dem erfolgreichen Pharming eines verfälschten DNS-Eintrages, der den Account-Inhaber erreicht, wird er beim Aufruf der manipulierten Domain auf den Server des Angreifers geleitet. In seiner Adresszeile erscheint die gewünschte URL, eine Manipulation kann der Nutzer nicht erkennen. Dieses Ergebnis wird als URL-Spoofing bezeichnet.[420]

156 Im Gegensatz zum Phishing hat das Pharming den großen Vorteil, dass kein Streuverlust eintritt. Selbst wenn einem Nicht-Kunden ein falscher DNS-Eintrag untergeschoben wird, bemerkt er diesen nicht. Nur Nutzer, die die Seite besuchen und ihre Zugangsdaten dort eingeben möchten, werden auf die Seite des Angreifers geleitet.

157 Ein weiterer Unterschied zum Phishing liegt darin, dass das Risiko des Pharming nicht komplett in der Sphäre des Account-Inhabers liegt. Beim Phishing kann der Betroffene anhand verschiedener Merkmale wie Fehler im Text, der Browser-Adresszeile oder Verhalten der Seite die Echtheit der Seite widerlegen. Nutzer, die trotzdem ihre Zugangsdaten eingeben, haben sich vom Angreifer täuschen lassen, was dem Nutzer eventuell vorwerfbar ist. Beim Pharming richtet sich nur bei den ersten beiden Methoden ein möglicher Vorwurf gegen den Nutzer, er habe seinen Rechner oder seinen

---

416 *BSI*, Lagebericht 2011, S. 32.
417 *BSI*, IT-Grundschutz-Kataloge, G 5.78; *Erfurth*, WM 2006, 2198, 2199; *Recknagel*, S. 49.
418 *Tanenbaum/Wetherall*[5], S. 957.
419 Ebd., S. 957.
420 *Popp*, MMR 2006, 84.

Router nicht ausreichend geschützt. Beim DNS-Spoofing und beim DNS-Cache-Poisoning stammt die Möglichkeit zur Veränderung des DNS-Eintrages nicht aus der Sphäre des Account-Inhabers.[421] Er hat keine effektive Möglichkeit, sich gegen diese Angriffe zu wehren.

Ein Antiviren-Programm kann nicht erkennen, dass der DNS-Eintrag manipuliert wurde.[422] Die einzige Möglichkeit wäre, die Zuordnung der IP-Adresse, in die die Domain aufgelöst wurde, mittels einer Whois-Abfrage zu klären. Diese Lösung wäre jedoch nicht praktikabel und der Sachverstand kann vom Durchschnittsnutzer nicht erwartet werden.[423] 158

ccc) Zweite Phase: die Internetseite des Angreifers

In der zweiten Phase des Angriffs befindet sich das potentielle Opfer auf der Internetseite des Angreifers. Diese beinhaltet ein Formular zur Eingabe der Zugangsdaten, das täuschend echt aussieht.[424] Das Nachbilden einer Seite, die echt aussieht, ist ohne großen Aufwand möglich.[425] 159

Beim klassischen Phishing kann der Nutzer an der Adresszeile seines Browsers erkennen, dass die Domain nicht mit der Domain des Authentisierungsnehmers übereinstimmt.[426] Viele Nutzer schenken der Adresszeile jedoch kaum Beachtung, sodass es ihnen nicht auffällt, wenn dort eine andere Domain steht.[427] Zumal die Angreifer die Domains so wählen, dass ein Nutzer sie mit der wahren Domain leicht verwechseln kann.[428] Teilweise kaufen die Angreifer für die Webformulare sogar SSL-Zertifikate.[429] Diese stammen zwar von vertrauensunwürdigen Stellen. Nach einem kurzen 160

421 *Dennis Werner*, Verkehrspflichten, S. 73.
422 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 31.
423 Ebd., § 55 Rn. 31.
424 *BSI*, IT-Grundschutz-Kataloge, G 5.157; *Borges*, NJW 2005, 3313; *Erfurth*, WM 2006, 2198, 2200.
425 *Erfurth*, WM 2006, 2198, 2200; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 30; *Pohlmann*, DuD 2010, 607, 611.
426 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 30.
427 *Knupfer*, MMR 2004, 641, 642.
428 *Hansen*, S. 15.
429 *Schwenk/Gajek/Wegener*, DuD 2005, 639, 640.

Warnhinweis, den manche Nutzer als unbedeutende Fehlermeldung abtun, erscheint ihnen die Verbindung dann jedoch sicher.[430]

161 An zwei Stellen können die Nutzer jedoch erkennen, dass die Seite nicht die Echte des Authentisierungsnehmers ist. Zum einen kann die Seite zwar auf die Eingabe des Nutzers reagieren, indem sie eine Erfolgs- oder Fehlermeldung ausgibt. Da der Dritte die Zugangsdaten jedoch abgreifen möchte und sie noch nicht hat, kann er nicht wissen, welche Zugangsdaten echt sind. Nutzer können daher falsche Daten eingeben und wenn eine Erfolgsmeldung angezeigt wird, kann der Nutzer daran erkennen, dass die Seite nicht echt ist. Ferner fragen die Seiten der Angreifer regelmäßig mehr Informationen ab, als zu einem Login beim Authentisierungsnehmer erforderlich sind. Nutzer von Online-Banking z.B. werden bereits für den Login nach TAN-Nummern gefragt, was gänzlich unüblich für Banken ist.[431]

dd) Social Engineering

162 Als Social Engineering bezeichnet man den Angriff auf den Menschen als Schwachstelle.[432] Social Engineering setzt darauf an die Zugangsdaten eines Account-Inhabers zu gelangen, indem der Angreifer sein Vertrauen erschleicht.[433] Unter einem Vorwand wird nach den Zugangsdaten gefragt.[434] Das Opfer gibt beim Social Engineering im guten Glauben die geheimen Informationen preis.[435] Der Fokus beim Social Engineering liegt dabei auf dem Erlangen von sensiblen Informationen mittels nicht-technischer Methoden.[436] Gleichwohl können technische Methoden zur Unterstützung des Social Engineerings dienen.

163 Die Ursprünge hat das Social Engineering in den 1980er Jahren, als Angreifer ihre Opfer anriefen, sich als Systemadministratoren ausgaben und somit an die Passwörter der Account-Inhaber gelangten.[437] Um das Vertrauen der Opfer zu erlangen, versuchen die Angreifer möglichst viele Infor-

430 *BSI*, IT-Grundschutz-Kataloge, G 5.143; *Schwenk/Gajek*, in: Internet-Auktion, 180, 188.
431 *Borges*, NJW 2005, 3313.
432 *Lipski*, S. 7.
433 *Fox*, DuD 2013, 5; *Pierrot*, in: *Ernst*, Rn. 39; *Lardschneider*, DuD 2008, 574, 576.
434 *Pierrot*, in: *Ernst*, Rn. 40.
435 *Eckert*[8], S. 26.
436 *Schwenk/Gajek*, in: Internet-Auktion, 180, 185.
437 *BSI*, IT-Grundschutz-Kataloge, G 5.42; *Hansen*, S. 16.

mationen über ihre Opfer zu sammeln.[438] Mittlerweile bedienen sie sich dazu der öffentlichen Informationen aus sozialen Netzwerken[439] oder aus öffentlich verfügbaren Telefon- oder Mitarbeiterlisten.[440] Andere Angreifer durchwühlen den Müll potentieller Opfer, um an Informationen zu kommen (Dumpster Diving).[441] Die Angreifer verwenden sämtliche Tricks, um das Opfer zur Preisgabe der Informationen zu bewegen, wie Mitleid, Humor oder Autorität.[442]

Die Anfänge des Social Engineerings liegen daher vor dem Phishing. Das klassische Phishing zeichnet sich durch den massenhaften Versand von E-Mails aus und setzt dabei auch auf die Schwachstelle Mensch. Im Gegensatz zum Social Engineering, wird jedoch kein besonderes Vertrauen in die E-Mail gesetzt. Social Engineering kann jedoch zum Phishing verwendet werden. Der Angreifer kann dem Opfer eine persönliche E-Mail schicken und dadurch die Erfolgschancen erhöhen.[443] Diese Verbindung aus Social Engineering und Phishing wird als Spear-Infection oder Spear-Phishing bezeichnet, abgeleitet vom englischen Wort für Speer, das die Zielgenauigkeit des Angriffs ausdrücken soll.[444] 164

Durch das erlangte Vertrauen erreicht der Angreifer, dass das Opfer eine gewisse Handlung vollzieht. Während beim klassischen Social Engineering das Opfer die Zugangsdaten noch telefonisch weitergab, werden mittlerweile technische Mittel eingesetzt, die jedoch auf die Mitwirkung des Opfers setzen. Das kann zum einen eine Phishing-Seite des Angreifers sein, auf der das Opfer ähnlich wie am Telefon die Zugangsdaten eingibt. Andererseits können die Opfer auch dazu bewogen werden, Programme zu öffnen, die Malware enthalten,[445] oder Links zu öffnen, die den Computer mittels einer Drive-By-Infection infizieren.[446] Social-Engineering-Angriffe sind schwer 165

438 *Gaycken*, S. 242; *Schneier*, S. 266.
439 *BSI*, IT-Grundschutz-Kataloge, G 5.158.
440 *Schimmer*, DuD 2008, 569, 570.
441 *Borges/Schwenk/Stuckenberg/Wegener*, S. 97; *Lipski*, S. 18.
442 *Pierrot*, in: *Ernst*, Rn. 42; *Lardschneider*, DuD 2008, 574, 576; *Gaycken*, S. 243.
443 *BSI*, IT-Grundschutz-Kataloge, G 5.157; *Fox*, DuD 2013, 5; *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.7.2; *Biallaß/Borges/Dienstbach* u. a., in: Innovationsmotor IT-Sicherheit, 495, 496.
444 *BKA*, S. 12; *Höhmann*, heise online v. 9. 7. 2012; *Gaycken*, S. 52; *Sieber*, Gutachten zum 69. DJT, S. C 20; *Biallaß/Borges/Dienstbach* u. a., in: Innovationsmotor IT-Sicherheit, 495, 496.
445 *BKA*, S. 9.
446 Zu den Infektionswegen unten Rn. 182 ff.

abzuwehren.[447] Der Mensch ist das schwächste Glied in der IT-Sicherheitskette.[448]

ee) Keylogger

166 Ein Keylogger zeichnet die gesamte Tastatureingabe eines Rechners auf.[449] Das Wort Keylogger setzt sich zusammen aus dem englischen to log (protokollieren) und key (Taste auf einer Tastatur). Es gibt unterschiedliche Arten von Keyloggern. Zum einen existieren physische Keylogger, die als Adapter zwischen Tastatur und den Anschluss am Rechner gesteckt werden.[450] Die andere Art physikalische Keylogger wird beim Ausspähen der PIN bei ec-Karten verwendet. Auf ein PIN-Eingabefeld eines Bankautomaten wird beispielsweise ein zweite Tastatur geklebt, die die Eingabe mitprotokolliert.[451] Ein physischer Keylogger kann jedoch auch eine Wärmebildkamera über diesem Eingabefeld sein, die anhand der Bewegung der Hand die eingegebene PIN erkennen kann.[452]

167 Eine andere Art von Keyloggern ist der softwarebasierte Keylogger. Eine Keylogger-Software nistet sich im Betriebssystem ein, überwacht alle Eingaben auf der Tastatur und protokolliert sie.[453] Der Keylogger kann zum einen auf einem Rechner installiert sein, der öffentlich zugänglich ist, beispielsweise in einem Internetcafé.[454] Andererseits können infizierte Rechner[455] mittels eines Trojaners den Keylogger aufgespielt bekommen.[456] Die Nutzer merken regelmäßig nicht, dass ein Keylogger ihr System überwacht, weil er im Hintergrund abläuft.[457] Das macht Keylogger besonders gefährlich. Die Informationen, die der Keylogger gesammelt hat, werden anschlie-

---

447 *Weßelmann*, DuD 2008, 601.
448 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 96.
449 *Sodtalbers*, Rn. 129; *Hansen*, S. 25; *Schmidl*, in: *Hauschka*[2], § 29 Rn. 307.
450 *Pierrot*, in: *Ernst*, Rn. 49; *Schimmer*, DuD 2008, 569, 572.
451 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 56; *Schulte am Hülse*/*Welchering*, NJW 2012, 1262, 1265.
452 *Schulte am Hülse*/*Welchering*, NJW 2012, 1262, 1265.
453 *Kossel*/*Kötter*, c't 2/2007, 76; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 25.
454 *Ernst*, MDR 2003, 1091, 1094.
455 Zu den Infektionswegen unten Rn. 182 ff.
456 *Borges*, NJW 2005, 3313, 3314; *J. Meyer*, Identität, S. 46; *Dennis Werner*, Verkehrspflichten, S. 62.
457 *LG Bonn*, Urteil v. 7. 7. 2009, 7 KLs 01/09, Rn. 41.

ßend an den Angreifer übermittelt.[458] Dieser kann die Daten danach auswerten und Zugangsdaten aus dem Protokoll aller Eingaben herausfiltern.

ff) Man-in-the-Middle-Angriff (MitM-Angriff)

Bei einem Man-in-the-Middle-Angriff stellt sich der Angreifer zwischen sein Opfer und dessen Kommunikationspartner.[459] Das führt zum einen dazu, dass der Angreifer die komplette Kommunikation zwischen dem Opfer und dessen Kommunikationspartner mitlesen kann.[460] Technisch kann der Angreifer den kompletten Informationsfluss über sich laufen lassen, was auch bei verschlüsselter Kommunikation funktioniert.[461] Darüber hinaus hat der Angreifer die Möglichkeit, in den Kommunikationsvorgang einzugreifen. Er kann Kommunikation vortäuschen oder manipulieren.[462] 168

Ein Angriff, der die gesamte Kommunikation auf den Angreifer umleitet, kann mittels drei Möglichkeiten erfolgen.[463] Bei diesen Möglichkeiten unterscheidet man zwischen einem physikalischen und einem logischen Vorgehen.[464] Die erste Möglichkeit besteht darin mittels ARP-[465] oder DNS-Spoofing[466] alle Daten-Pakete physikalisch auf den Rechner des Angreifers zu leiten.[467] Dazu kann zunächst in die zentrale Netzinfrastruktur eingegriffen werden.[468] Obwohl dies möglich ist, erfolgt ein solcher Eingriff nur selten, weil er für einen Angreifer schwer zu realisieren ist.[469] 169

458 *Hansen*, S. 26.
459 *J. Meyer*, Identität, S. 47; *Wefel*, S. 117; *BSI*, IT-Grundschutz-Kataloge, G 5.143; *Borges*, NJW 2005, 3313, 3314; *Sieber*, Gutachten zum 69. DJT, S. C 19; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 32.
460 *BSI*, IT-Grundschutz-Kataloge, G 5.143; *Sieber*, Gutachten zum 69. DJT, S. C 19.
461 *Eckert*[8], S. 440; *Tanenbaum/Wetherall*[5], S. 942.
462 *J. Meyer*, Identität, S. 47; *BSI*, IT-Grundschutz-Kataloge, G 5.143; *Borges*, NJW 2005, 3313, 3314; *Sieber*, Gutachten zum 69. DJT, S. C 19.
463 *Schulte am Hülse/Klabunde*, MMR 2010, 84, 85.
464 *BKA*, S. 12; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 32.
465 *Gaycken*, S. 231 f. ARP ist die Abkürzung für Address Resolution Protocol.
466 Dazu oben Rn. 152.
467 *BSI*, IT-Grundschutz-Kataloge, G 5.143; *Sieber*, Gutachten zum 69. DJT, S. C 19; *Schulte am Hülse/Klabunde*, MMR 2010, 84, 85.
468 Zum DNS-Poisoning und DNS-Cache-Poisoning oben Rn. 152.
469 *Borges/Schwenk/Stuckenberg/Wegener*, S. 48.

170 Eine zweite, ebenfalls physikalische Möglichkeit ist, den Verkehr eines WLAN-Netzwerkes auf den Angreifer umzuleiten.[470] Dazu richtet der Angreifer einen WLAN-Hotspot ein, der einen bestehenden kopiert (Evil Twin). Ist das Sendesignal des Hotspots des Angreifers stärker als das Signal des eigentlichen Hotspots, verbindet sich der Rechner des Opfers mit dem Evil Twin. Somit kann der Angreifer den kompletten WLAN-Verkehr mitlesen. Mit dieser Methode ist auch das Abhören einer Mobilfunk-Verbindung möglich. Eine GSM-Basisstation kann ebenfalls als Evil Twin beispielsweise mittels eines Evil Twins erstellt werden,[471] weil eine Authentisierung im GSM-Standard nur einseitig stattfindet.[472] Ein IMSI-Catcher ist ein Gerät, das sich gegenüber in der Nähe befindlichen Mobilfunk-Teilnehmern als Basis-Station ausgibt.[473] Weil sich Mobiltelefone immer automatisch in die Basisstation mit dem besten Signal einbinden, verbinden sich in der Nähe befindliche Mobiltelefone unbemerkt mit dem IMSI-Catcher.[474] Durch diese Schwachstelle kann ein Angreifer beispielsweise Gespräche und SMS mithören.[475] Für diese Methoden muss der Angreifer jedoch in räumlicher Nähe zum Opfer sein und zusätzlich seinen Hotspot nah am Opfer positionieren.

171 Die dritte Möglichkeit den Informationsfluss zwischen Opfer und dessen Kommunikationspartner auf den Angreifer umzuleiten, besteht in der Infektion[476] des Rechners des Opfers. Mittels eines Trojaners kann die lokale DNS-Zuordnungstabelle geändert werden, sodass die gesamte Kommunikation mit einer gewissen Domain auf den Angreifer umgeleitet werden kann.[477]

172 Ein komplettes physikalisches Umleiten der Kommunikation zwischen Opfer und dessen Partner ist jedoch nicht erforderlich. Der Angreifer kann, mit Hilfe eines Trojaners[478] auf dem infizierten Rechner des Opfers, die Kommunikation mitlesen. Dies geschieht häufig dadurch, dass die Funktionsweise des Browsers durch den Einsatz des Trojaners verändert wird,

---

470 *BSI*, IT-Grundschutz-Kataloge, G 5.143; *Eckert*[8], S. 927.
471 *BSI*, Lagebericht 2011, S. 36.
472 *Eckert*[8], S. 877.
473 *Eckert*[8], S. 877; *Schwenk*[3], S. 191.
474 *Eckert*[8], S. 877.
475 *Schwenk*[3], S. 191.
476 Zu den Infektionswegen unten Rn. 182 ff.
477 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 33; *Borges/Schwenk/Stuckenberg/Wegener*, S. 50. Im Zusammenhang mit Pharming, oben Rn. 150.
478 Dazu unten Rn. 193.

weswegen diese Angriffe als Man-in-the-Browser-Angriffe bezeichnet werden.[479] Die Manipulation läuft in Echtzeit ab, sodass das Opfer nicht bemerkt, dass die Kommunikation verändert wurde.[480] Es existieren Trojaner, die nicht nur im Rahmen der Überweisung eine gefälschte Erfolgsseite anzeigen, sondern um eine Entdeckung zu verhindern, auch die Umsatzanzeige beim Online-Banking verändern.

Bei Man-in-the-Middle-Angriffen kann ein Angreifer mittels eines passi- 173
ven oder aktiven Angriffs vorgehen. Ein passiver Angriff beschränkt sich darauf, die Kommunikation zwischen Opfer und dessen Partner mitzulesen, um die geheimen Informationen wie die Zugangsdaten zu erlangen.[481] Erst später werden die Zugangsdaten dann missbräuchlich eingesetzt.

Bei einem aktiven Eingriff verändert der Angreifer die Kommunikation 174
zwischen Opfer und dessen Partner in Echtzeit.[482] Bei aktiven Angriffen können mit Phishing nicht zu überlistende Sicherheitsverfahren wie iTAN umgangen werden.[483] Sogar das mTAN-Verfahren, das auf eine Zwei-Faktor-Authentisierung mit Wissen der PIN und Besitz der SIM-Karte setzt, lässt sich mittels eines Man-in-the-Middle-Angriffs überwinden.[484] Beim mTAN-Verfahren wird eine einmalig zu verwendende TAN an das Mobiltelefon des Bankkunden geschickt, die dieser anschließend zur Durchführung der Transaktion eingibt.[485] Zwar sind Angriffe gegen diese Methode wegen der Zwei-Faktor-Authentisierung schwierig,[486] sie sind jedoch möglich und tatsächlich passiert.[487]

Zwei Methoden des Angriffs sind dabei möglich. Zum einen kann ein 175
Trojaner den Rechner des Opfers infiziert haben, sodass die Bankseite in Echtzeit manipuliert wird. An die Bank werden andere Transaktionsdaten gesendet, als der Kunde eingegeben hat. Die Bank schickt dem Kunden anschließend die SMS, die bei einem sicheren Verfahren diese Transakti-

479 *BKA*, S. 12; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 51.
480 *Maihold*, in: *Schimansky*/*Bunte*/*Lwowski*[4], § 55 Rn. 36.
481 *Borges*, NJW 2005, 3313, 3314.
482 *Borges*, NJW 2005, 3313, 3314; *Maihold*, in: *Schimansky*/*Bunte*/*Lwowski*[4], § 55 Rn. 32.
483 *Borges*, NJW 2005, 3313, 3314; *Hansen*, S. 21.
484 *BKA*, S. 12.
485 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 36; *Schwenk*/*Gajek*/*Wegener*, DuD 2005, 639, 642.
486 *Biallaß*/*Borges*/*Dienstbach* u. a., in: Innovationsmotor IT-Sicherheit, 495, 500.
487 *Maihold*, in: *Schimansky*/*Bunte*/*Lwowski*[4], § 55 Rn. 37.

onsdaten wie Zielkonto und Betrag enthält.[488] Nur wenn der Kunde nicht bemerkt, dass in der SMS andere Daten eingetragen sind, wird der Angriff erfolgreich verlaufen.

176 Eine zweite Methode ist, die an das Mobiltelefon geschickte SMS abzufangen. Dies geschieht entweder durch Abhören des Mobilfunks, wozu der Täter in räumlicher Nähe zum Opfer sein muss,[489] oder über die Infektion des Mobiltelefons mit einem Trojaner. Auch Mobiltelefone werden mittlerweile mit Schadsoftware wie Trojanern infiziert.[490] Dies geschieht mittels Social Engineering[491] oder nach Infektion des Rechners des Opfers einen Hinweis, der auf einer Webseite des Angreifers platziert ist.[492] Diese durch den Trojaner im Rechner des Opfers manipulierte Internetseite fordert das Opfer auf, ein vermeintliches Sicherheitsupdate für sein Mobiltelefon zu installieren, das jedoch Schadsoftware enthält.[493] Bei einem infizierten Mobiltelefon können die SMS mitgelesen, verändert oder unterdrückt werden.

Selbst sichere Zwei-Faktor-Authentisierungen lassen sich mittels Echtzeitmanipulationen beim Man-in-the-Middle-Angriff überlisten.

gg) Sniffing: Mitlesen des Datenverkehrs

177 Sniffing bezeichnet das Abhören des Netzverkehrs mit dem Ziel geheime Informationen wie Zugangsdaten zu erlangen.[494] Jeder Server, der an dem langen Übertragungsweg beteiligt ist, hat grundsätzlich die Möglichkeit das Datenpaket auszulesen.[495]

178 Angreifer verwenden dazu Programme, die den Netzverkehr nicht nur automatisch aufzeichnen, sondern auch nach den geheimen Informationen filtern.[496] Das Auslesen ist bei unverschlüsselten Verbindungen einfach mög-

488 *Borges/Schwenk/Stuckenberg/Wegener*, S. 36; *Biallaß/Borges/Dienstbach* u. a., in: Innovationsmotor IT-Sicherheit, 495, 500.
489 Dazu unten Rn. 179.
490 *BKA*, S. 16; *BSI*, Lagebericht 2011, S. 36.
491 *BKA*, S. 16.
492 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 37.
493 Ebd., § 55 Rn. 37.
494 *Gaycken*, S. 223; *Dennis Werner*, Verkehrspflichten, S. 74.
495 *Recknagel*, S. 49.
496 *BSI*, IT-Grundschutz-Kataloge, G 5.7; *Graf*, in: MüKo-StGB[2], § 202a Rn. 71; *Recknagel*, S. 49; *Dennis Werner*, Verkehrspflichten, S. 74.

lich.[497] Denn der Geheimnisschutz bei unverschlüsselt durchs Internet übertragenen Informationen entspricht dem einer Postkarte.[498] Früher wurden Informationen im Internet wegen des kleinen Teilnehmerkreises stets unverschlüsselt übertragen, was als Konzeptionsfehler betrachtet wird.[499] Ein häufiges Angriffsziel sind dabei WLAN-Verbindungen.[500]

Der Mobilfunk ist je nach eingesetzter Technologie anfällig für das Mit- 179
lesen des Datenverkehrs. Das verschlüsselte GSM-Netz kann mittels Entschlüsselungstools abgehört werden.[501] Neue Technologien wie UMTS sind davon nicht betroffen.[502] Ferner werden SMS im GSM-Netz unverschlüsselt versendet.[503] Befindet sich der Angreifer in räumlicher Nähe zum Opfer können somit SMS mitgelesen werden. Ein Angreifer kann ebenfalls eine SIM-Karte klonen, um die Mobilfunk-Kommunikation abzufangen. Solche Angriffe werden jedoch von der Basisstation entdeckt, die merkt, wenn zwei SIM-Karten mit der gleichen IMSI im Netz sind.[504]

hh) Erraten der Zugangsdaten durch Ausprobieren bekannter Daten oder durch Brute-Force-Angriffe

Ein Angreifer kann die Zugangsdaten unter Umständen erraten. Dafür 180
gibt es zwei gewöhnliche Möglichkeiten. Die erste Möglichkeit besteht darin, dass bekannte Zugangsdaten, die bei einem Authentisierungsnehmer funktionieren, bei einem anderen Authentisierungsnehmer ausprobiert werden.[505] Diese Methoden funktionieren deswegen, weil Nutzer häufig dasselbe Kennwort bei unterschiedlichen Authentisierungsnehmern verwenden.[506] Studien zeigen, dass zwei Drittel der Anwender nur weniger als drei Passwörter nutzen, ein Drittel sogar stets dasselbe Passwort.[507] Um

497 *Borges/Schwenk/Stuckenberg/Wegener*, S. 26; *Dennis Werner*, Verkehrspflichten, S. 74.
498 *Roßnagel*, MMR 2002, 67, 68.
499 *Fuhrberg*, K&R 1999, 20, 22.
500 *BSI*, IT-Grundschutz-Kataloge, G 5.139; *Gaycken*, S. 224.
501 *BSI*, Lagebericht 2011, S. 35; *Schwenk*[3], S. 189; *Eckert*[8], S. 879.
502 *BSI*, Lagebericht 2011, S. 35; *Schwenk*[3], S. 191 ff.; *Eckert*[8], S. 884, 891.
503 *Eckert*[8], S. 880.
504 Ebd., S. 879.
505 *B. Lorenz*, DuD 2013, 220, 222.
506 *Spindler*, CR 2003, 534.
507 *Wefel*, S. 3.

an die Zugangsdaten eines Authentisierungsnehmers zu kommen, kann der Angreifer diese ausspähen oder beispielsweise in einer Dropzone erwerben. Oder er macht sich selbst zum Authentisierungsnehmer und veranlasst Nutzer dazu, einen Account mit Zugangsdaten bei ihm anzulegen. Dazu werden häufig Profile von Prominenten gefälscht. Über diese Profile wird aufgerufen, sich auf der Seite des Angreifers zu registrieren. Alternativ kann der Angreifer ein vermeintliches Gewinnspiel veranstaltet, um Nutzer dazu zu bewegen, Zugangsdaten bei ihm anzulegen.

181 Die zweite Methode nennt sich Brute-Force-Angriff. Wie der englische Begriff der rohen Gewalt erkennen lässt, geht es bei dieser Angriffsform darum, Zugangsdaten so lange auszuprobieren, bis eine Kombination passt.[508] Der erste Teil der Zugangsdaten, nämlich der Benutzername ist leicht herauszubekommen. Er kann bei Online-Plattformen öffentlich einsehbar sein. Bei anderen Seiten wird häufig die E-Mail-Adresse verwendet, die ebenfalls leicht herauszubekommen ist. Bei den E-Mail-Adressen werden dann Passwörter durchprobiert. Dazu kann der Angreifer zum einen jede mögliche Kombination ausprobieren oder eine Liste häufiger Passwörter verwenden.[509] In dieser Liste befinden sich Wörter aus dem Wörterbuch, Vornamen und andere häufig gewählte Kennwörter.[510] Wenn der Angreifer Informationen über den Account-Inhaber hat oder diese mittels öffentlich verfügbarer Daten gesammelt hat, kann er das Passwort gezielter erraten.[511] Im Rahmen einer asymmetrischen Verschlüsselung kann mit einem Brute-Force-Angriff versucht werden, anhand der Kenntnis des öffentlichen Schlüssel und dessen Zusammenhang mit dem geheimen Schlüssel durch Primzahlen den geheimen Schlüssel herauszufinden.[512]

508 *BSI*, IT-Grundschutz-Kataloge, G 5.18; *Ernst*, MDR 2003, 1091, 1094; *Pierrot*, in: *Ernst*, Rn. 46.

509 *BSI*, IT-Grundschutz-Kataloge, G 5.18; *Pierrot*, in: *Ernst*, Rn. 46.

510 *Eckert*[8], S. 469; *Schneier*, S. 137.

511 *Pierrot*, in: *Ernst*, Rn. 43 ff.

512 Oben Rn. 80 sowie *Gassen*, S. 72.

b) Infektionswege

Malware sind bösartige Computerprogramme, die dazu dienen, Schaden am System auszuüben oder Zugangsdaten auszuspähen.[513] Das Wort Malware setzt sich zusammen aus dem englischen *malicious*, was böswillig oder bösartig meint, und dem Wort Software.[514] Im Volksmund werden sämtliche Formen der Malware als Viren bezeichnet.[515] Das zeigt sich z.B. dadurch, dass der Virenschutz durch das Anti-Virenprogramm vor Viren, Würmern, Trojanern und ähnlichem schützen soll. Eine trennscharfe Abgrenzung zwischen den einzelnen Kategorien der Malware ist möglich, viele Schadprogramme vereinen jedoch die Charakteristiken mehrerer Arten.[516] **182**

Während Schadprogramme sich früher in Massen verbreitet haben, gestalten Angreifer diese mittlerweile individueller, sodass sie schwerer zu entdecken sind.[517] Oftmals befällt ein Schadprogramm mittlerweile nur 20 Rechner oder weniger.[518] Während früher ein Schadprogramm mehrere Monate genutzt werden konnte, wird es heute schon nach wenigen Tagen von einer Nachfolgeversion abgelöst.[519] Ein Virenprogramm kann nicht mit hundert prozentiger Sicherheit vor Schadprogramm schützen.[520] Bei dem zeitgleichen Einsatz von drei unterschiedlichen Virenprogrammen wurden nur über 90 Prozent infizierter Dokumente als schädlich identifiziert.[521] **183**

aa) Sicherheitslücken in Programmen, Zero-Day-Exploits

Programmierfehler, sog. Bugs, können von Angreifern in aktiven Angriffen genutzt werden, um das System zu kompromittieren.[522] Das Ausnutzen **184**

513 *Schwenk/Gajek*, in: Internet-Auktion, 180, 183; *Gaycken*, S. 238; *Schneier*, S. 151; *Dennis Werner*, Verkehrspflichten, S. 57. Vgl. auch die Legaldefinition von Schadprogrammen in § 2 Abs. 5 BSIG.

514 *BKA*, S. 9; *Gaycken*, S. 238.

515 *Ernst*, CR 2006, 590, 591; *Frank*, in: Informationsstrafrecht, 23, 24.

516 *Ernst*, CR 2006, 590, 591; *Mantz*, offene Netze, S. 39; *Dennis Werner*, Verkehrspflichten, S. 58.

517 *BSI*, Lagebericht 2011, S. 25.

518 Ebd., S. 25; *Höhmann*, heise online v. 9. 7. 2012.

519 *BSI*, Lagebericht 2011, S. 25.

520 Unten Rn. 202.

521 *BSI*, Lagebericht 2011, S. 26.

522 *Graf*, in: MüKo-StGB^2, § 202a Rn. 66. Allgemein zu Programmierfehlern *Taeger*, S. 47 ff.

von Sicherheitslöchern bezeichnet man mit dem englischen Begriff Exploiting.[523] Kommerzielle Standardprogramme weisen zwischen 15 bis 50 solcher Fehler pro tausend Zeilen Code auf.[524] Es existieren zahlreiche Kategorien von Sicherheitslücken.

185 Ein Weg Sicherheitslücken auszunutzen ist das Erzeugen eines Buffer-Overflows[525] an einem Port, der mittels Port-Scanning ermittelt wurde. Beim Port-Scanning überprüft der Angreifer sämtliche Ports des Zielrechners.[526] Er erforscht damit, auf welchen Ports Dienste laufen, die angegriffen werden können.[527] Durch das übermäßige Senden von Daten an einen Port kann dieser Dienst angegriffen werden. Enthält die Software Programmierfehler, kann es zu einem Buffer-Overflow kommen.[528] Dabei werden große Datenmengen in einen kleinen dafür reservierten Speicherplatz geschrieben, wodurch ein Angreifer den Speicherplatz im dahinter liegenden Speicherbereich überschreiben kann.[529]

186 Manche Entwickler bauen bewusst Sicherheitslücken in ihre Software ein, sog. Trapdoors oder Backdoors,[530] die ihnen ermöglichen in das System des Nutzers einzudringen.[531] Sobald Angreifer diese Trapdoors aufspüren, können sie sie nutzen, um fremde Rechner zu infizieren.

187 Besonders gefährlich sind sog. Zero-Day-Exploits.[532] Als solche werden Sicherheitslücken und Bugs in Programmen bezeichnet, die noch nicht, also null Tage lang, öffentlich bekannt sind.[533] Weil sie noch nicht bekannt sind, werden sie von Anti-Virenprogrammen regelmäßig nicht erkannt.[534] Und auch der Hersteller der Software kann mangels Kenntnis die Sicherheitslücke nicht mittels Update schließen.

188 Die Anzahl an Schwachstellen, die eine Infektion erlauben, hat in den vergangen Jahren zugenommen.[535] Insbesondere bei Browser-Plug-ins wie

---

523 *Gaycken*, S. 56; *Pierrot*, in: *Ernst*, Rn. 51.
524 *Gaycken*, S. 54 m.w.N.
525 Dazu *Gaycken*, S. 230; *Schneier*, S. 207.
526 *Gaycken*, S. 225; *Pierrot*, in: *Ernst*, Rn. 58.
527 *Recknagel*, S. 50.
528 *Eckert*[8], S. 47 f.
529 Ebd., S. 51.
530 *Gaycken*, S. 53 f.
531 *Pierrot*, in: *Ernst*, Rn. 62.
532 *Gaycken*, S. 56; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 34.
533 *Gaycken*, S. 57.
534 Unten Rn. 203.
535 *BSI*, Lagebericht 2011, S. 9 f.

Flash und Java werden zahlreichen Sicherheitslücken aufgedeckt[536], die wegen der hohen Verbreitung oft ausgenutzt werden. Es lassen sich Angriffe auf sämtliche Plattformen verzeichnen.[537] Der Angreifer kann durch das Ausnutzen einer Schwachstelle einen beliebigen Code auf dem Zielrechner ausführen und diesen dadurch steuern.[538]

bb) Computervirus

Der Computervirus wurde nach dem biologischen Mirko-Organismus Virus benannt, der sich dadurch auszeichnet, dass er auf eine lebende Wirtszelle angewiesen ist, keinen eigenen Stoffwechsel besitzt und fähig ist, sich zu reproduzieren.[539] Viren sind unselbständige Programmroutinen, die sich als Bestandteil von Anwendungsdaten installieren.[540] Beim Ausführen der Anwendung kann der Virus weitere Wirtsprogramme durch Reproduktion von sich selbst infizieren.[541] 189

Viren können sich nur passiv dadurch vermehren, dass der Benutzer einen Code ausführt.[542] Viren verbreiten sich dabei zum Beispiel über Datenträger, wie früher Disketten und heute USB-Sticks, oder über E-Mail-Anhänge.[543] Ein Virus kann wie die anderen Schadprogramme einen beliebigen schädlichen Code auf dem Rechner des Opfers ausführen. 190

cc) Computerwurm

Ein Computerwurm ist ein ablauffähiges Programm, das sich selbst reproduzieren kann, indem es über ein Netzwerk an anderen Computern Veränderungen vornimmt.[544] Während der Computervirus innerhalb eines Compu- 191

536 *Borges/Schwenk/Stuckenberg/Wegener*, S. 50.
537 Ebd., S. 111.
538 *Eckert*[8], S. 52 f.; *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.7.1.
539 *Eckert*[8], S. 56; *Tanenbaum/Wetherall*[5], S. 986; *Frank*, in: Informationsstrafrecht, 23, 24; *Pierrot*, in: *Ernst*, Rn. 81; *Schneier*, S. 152; *Schwenk*[3], S. 243.
540 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.7.1; *Dennis Werner*, Verkehrspflichten, S. 59; *Wien*[3], S. 195; *Wißner/Jäger*, in: Computerrechts-Handbuch, 300.
541 *Eckert*[8], S. 56; *Mantz*, offene Netze, S. 37; *Sodtalbers*, Rn. 119.
542 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.7.1.
543 *Eckert*[8], S. 58, 61; *Gaycken*, S. 239 f.
544 *Eckert*[8], S. 68; *Frank*, in: Informationsstrafrecht, 23, 25; *Gaycken*, S. 241; *Dennis Werner*, Verkehrspflichten, S. 60; *Holznagel*, § 3 Rn. 17; *Schneier*, S. 155.

ters Programme mit Schadcode infiziert, versucht ein Computerwurm möglichst viele Rechner in einem Netzwerk zu infizieren.[545] Ebenso unterscheidet ihn vom Computervirus, dass der Computerwurm kein Wirtsprogramm braucht, sondern selbstständig ausführbar ist.[546]

192 Zahlreiche Computerwürmer verbreiten sich per E-Mail, indem sie den schädlichen Anhang als etwas Interessantes tarnen.[547] Solche Würmer verbreiten sich häufig dadurch, dass sie sich selbst an alle Empfänger des Adressbuchs des befallenen Rechners verschicken, wodurch der Absender vertrauenswürdig wirkt.[548] Ein weiterer Verbreitungsweg besteht darin, im Netzwerk die anderen Rechner mit Hilfe eines Buffer-Overflows[549] zu infizieren.[550]

dd) Trojanisches Pferd, Trojaner

193 Am häufigsten werden die Zugangsdaten mittlerweile mittels eines Trojaners ausgespäht.[551] Das Trojanische Pferd oder Trojaner bekommt seinen Namen von der Sage um den Kampf der Stadt Troja.[552] Als Trojaner wird daran angelehnt eine Software bezeichnet, die nur scheinbar ein nützliches Programm ist, in Wirklichkeit aber Schadcode enthält.[553] Wie die nach einem 10-jährigen Kampf scheinbar kampfesmüden Griechen den Bewohnern der Stadt Troja ein großes hölzernes Pferd, in dem sie ihre Soldaten versteckten, schenkten, offeriert der Angreifer seinem Opfer ein scheinbar nützliches Programm. Dieses Programm nützt dem Opfer nicht nur, sondern schadet ihm auch, wie die griechischen Soldaten, die, nachdem die Bewohner der Stadt Troja das Pferd in das Innere ihrer Stadtmauern schie-

545 *Erfurth*, WM 2006, 2198, 2199; *Sodtalbers*, Rn. 123; *Dennis Werner*, Verkehrspflichten, S. 60; *Pierrot*, in: *Ernst*, Rn. 109.

546 *Mantz*, offene Netze, S. 38; *Dennis Werner*, Verkehrspflichten, S. 61; *Wien*[3], S. 195.

547 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.7.1; *Dennis Werner*, Verkehrspflichten, S. 61. So der ILOVEYOU-Wurm, dazu *Eckert*[8], S. 70; *Frank*, in: Informationsstrafrecht, 23.

548 *Dennis Werner*, Verkehrspflichten, S. 61.

549 Dazu oben Rn. 185.

550 *Eckert*[8], S. 68.

551 *BSI*, Lagebericht 2011, S. 23.

552 *Eckert*[8], S. 73; *Holznagel*, § 3 Rn. 13; *Schneier*, S. 155.

553 *BSI*, IT-Grundschutz-Kataloge, G 5.21; *Frank*, in: Informationsstrafrecht, 23, 26; *Gaycken*, S. 241; *Sodtalbers*, Rn. 127; *Dennis Werner*, Verkehrspflichten, S. 62; *Graf*, in: MüKo-StGB[2], § 202a Rn. 64; *Schneier*, S. 155; *Schwenk*[3], S. 243.

ben ließen, in der Nacht aus dem Inneren des Pferdes heraus kamen und die Stadt Troja einnahmen.

Technisch lässt sich der Trojaner als Programm definieren, bei dem die implementierte Ist-Funktionalität nicht mit der angegebenen Soll-Funktionalität übereinstimmt.[554] Sie bestehen daher aus einem dem Anwender bekannten nützlichen Teil und dem verborgenen, schädlichen Teil.[555] Trojaner nisten sich häufig so im System ein, dass sie bei jedem Systemstart wieder ausgeführt werden.[556] 194

Im Gegensatz zu Computerwürmern ist für Trojaner charakteristisch, dass sie keine eigenen Verbreitungsroutinen enthalten.[557] Häufig werden Schadprogramme jedoch so zusammengewürfelt, dass sie die Funktionalitäten eines Trojaners haben, sich aber auch wie ein Computerwurm selbstständig verbreiten können.[558] Während Computerviren und -würmer darauf angelegt sind, dem System zu schaden, dienen Trojaner regelmäßig dazu, Informationen zu beschaffen (Sniffer) und das System zu übernehmen (Backdoor).[559] Trojaner können darüber hinaus so konzipiert werden, dass sie sich aus dem Internet mittels eines Updates neue Funktionalitäten herunterladen können.[560] 195

Aus dem Einsatz von Staatstrojanern[561] lassen sich zwei Schlussfolgerungen ziehen. Zum einen sind Computer anfällig gegenüber Schadprogrammen, die Informationen wie Zugangsdaten ausspionieren. Zum anderen besteht ein staatliches Interesse daran, einige Türen aufrecht zu erhalten, die die Infizierung eines Computersystems durch ein Schadprogramm erlauben. 196

554 *Eckert*[8], S. 43; *Skistims*/*Roßnagel*, ZD 2012, 3.

555 *Dennis Werner*, Verkehrspflichten, S. 62; *R. Koch*, NJW 2004, 801, 802.

556 *Dennis Werner*, Verkehrspflichten, S. 63.

557 *BSI*, IT-Grundschutz-Kataloge, G 5.21; *Dennis Werner*, Verkehrspflichten, S. 62.

558 *Ernst*, CR 2006, 590, 591.

559 *Eckert*[8], S. 75; *Ernst*, CR 2006, 590, 591; *Henning*, in: *U. Schneider*/*Dieter Werner*[7], 11.7.1; *J. Meyer*, Identität, S. 45; *Dennis Werner*, Verkehrspflichten, S. 62.

560 *Eckert*[8], S. 75.

561 Zu deren Zulässigkeit *BVerfG*, Urteil v. 27. 2. 2008, 1 BvR 370/07, 1 BvR 595/07 (Online-Durchsuchung) – BVerfGE 120, 274; *Braun*/*Roggenkamp*, K&R 2011, 681; *Hoffmann-Riem*, JZ 2008, 1009, 1015 ff.; *Popp*, ZD 2012, 51; *Skistims*/*Roßnagel*, ZD 2012, 3.

ee) Rootkits

197 Rootkits sind Schadsoftware, die versuchen sich mit einer maximalen Berechtigung im Zielsystem zu verankern.[562] Sie sind darauf angelegt die maximalen Berechtigungen dauerhaft und heimlich zu erhalten, um dem Dritten zu ermöglichen, das System zu einem beliebigen Zeitpunkt zu steuern.[563] Rootkits selbst sind keine Angriffswerkzeuge, sondern werden von Computerviren, -würmern und Trojanern verwendet, um deren Eindringen zu verschleiern.[564]

198 Wegen des Verwischens der Spuren durch das Rootkit können sie nur schwer von Antiviren-Programmen entdeckt werden und auch erfahrenen Systemadministratoren bereitet die Entdeckung und Entfernung von Rootkits Schwierigkeiten.[565] Ein Rootkit kann sogar eine komplette Neuinstallation des Systems überleben.[566] Der Angriff mittels eines Rootkits erfolgt so schnell, dass er praktisch nicht beobachtet, geschweige denn verhindert werden kann.[567]

ff) Drive-By-Infection

199 Regelmäßig sind Viren, Würmer und Trojaner auf eine Mitwirkung des Benutzers in Form einer Interaktion angewiesen.[568] Der Nutzer muss z.B. ein heruntergeladenes Programm ausführen oder einen E-Mail-Anhang öffnen. Es gibt jedoch Wege, bei denen – eine entsprechend unsichere Konfiguration der Programme und des Systems vorausgesetzt – eine Infizierung ohne eine nennenswerte Interaktion des Nutzers möglich ist, sog. Drive-By-Infection oder Drive-By-Exploit.[569] Zur Infektion erforderlich ist nur, dass

562 *Dennis Werner*, Verkehrspflichten, S. 68; *Dolle/Wegener*, DuD 2006, 471; *Kühnhauser*, DuD 2003, 218.
563 *Dennis Werner*, Verkehrspflichten, S. 68; *Grosskopf*, CR 2007, 122, 123.
564 *Gaycken*, S. 233; *Dennis Werner*, Verkehrspflichten, S. 68; *Dolle/Wegener*, DuD 2006, 471, 472.
565 *Grosskopf*, CR 2007, 122, 123; *Dennis Werner*, Verkehrspflichten, S. 69; *Kühnhauser*, DuD 2003, 218.
566 *J. Schmidt*, c't 2/2007, 86.
567 *Kühnhauser*, DuD 2003, 218.
568 *Dennis Werner*, Verkehrspflichten, S. 58, 63.
569 *BSI*, Lagebericht 2011, S. 11; *Dennis Werner*, Verkehrspflichten, S. 58, 63; *Borges/Schwenk/Stuckenberg/Wegener*, S. 92; *Sieber*, Gutachten zum 69. DJT, S. C 19.

der Rechner ein gewisses Bild oder Dokument anzeigt, beispielsweise beim Betrachten einer Webseite.[570] Der Nutzer muss dieses Bild, das eventuell als Werbeeinblendung auf einer eigentlich vertrauenswürdigen Internetseite erscheint, noch nicht einmal anklicken.

Während früher zur Infektion eine Spam-Mail mit dem anzuklickenden Link das Opfer auf eine Webseite verwiesen wurde, die ihn im „Vorbeisurfen“[571] infizierte, werden heute gängige Internetseiten übernommen und der Drive-By-Exploit durch ein möglicherweise unsichtbares iFrame durchgeführt. Dazu verwenden die Angreifer ausgespähte FTP-Zugangsdaten oder Sicherheitslücken im verwendeten Content Management System (CMS) oder der verwendeten Serversoftware.[572] Eine Drive-By-Infection kann auch dadurch entstehen, dass im E-Mail-Programm des Opfers, dem Mail User Agent (MUA), eine E-Mail mit einem eingebundenen Bild angezeigt wird.[573] 200

c) Schutz gegen Infektionen des Rechners

Gegen die zahlreichen Infektionsmöglichkeiten von Rechnern haben sich einige Schutzmöglichkeiten entwickelt. Neben den regelmäßigen Updates von Betriebssystem und Anwendungen[574] gehören dazu Antiviren-Programme sowie Firewalls. Die beiden letzten Methoden sollen nachfolgend vorgestellt und auf deren Wirksamkeit gegen Infektionen untersucht werden. 201

aa) Antiviren-Programm

Ein Antiviren-Programm, auch Virenscanner[575] oder Malwareschutzprogramm[576] genannt, ist eine Software, die Malware aufspürt, blockiert und gegebenenfalls beseitigt.[577] Zwar deutet der Name des Anti*viren*-Pro- 202

570 *BKA*, S. 11; *Eckert*[8], S. 164; *Erfurth*, WM 2006, 2198, 2202.
571 *BSI*, Lagebericht 2011, S. 11.
572 Ebd., S. 11.
573 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.4.3, 11.7.1; *R. Koch*, NJW 2004, 801.
574 *Dennis Werner*, Verkehrspflichten, S. 87.
575 *Eckert*[8], S. 67; *Dennis Werner*, Verkehrspflichten, S. 75.
576 *Hossenfelder*, Pflichten von Internetnutzern, S. 125.
577 *Dennis Werner*, Verkehrspflichten, S. 75.

gramms darauf hin, dass es nur Computerviren[578] schützen soll. Die Bezeichnung greift jedoch das verbreitete Verständnis von Viren als sämtliche Formen der Malware auf.[579] Ein Antiviren-Programm läuft im Hintergrund und scannt regelmäßig den gesamten Internet-Verkehr sowie Dateien vor deren Zugriff auf Virenbefall.[580] Erkennt ein Antiviren-Programm Malware, kann es versuchen den schadhaften Teil abzutrennen. Falls dies nicht gelingt, kann es die Datei zerstören oder isolieren und nicht mehr verwenden.[581] Um die Effektivität von Antiviren-Programmen zu beurteilen sollen folgend gängige Erkennungsverfahren untersucht werden.

203 Das Erkennungsverfahren, das auf einer ersten Stufe Antiviren-Programmen zu Grunde liegt, ist die Signaturerkennung.[582] Dabei werden bekannte, schadhafte Byte-Folgen oder Codesquenzen mit der untersuchten Datei verglichen.[583] Durch den Vergleich mit bekannten schadhaften Quellcode-Teilen kann die Signaturerkennung nur bekannte Viren identifizieren.[584] Darin liegt die größte Schwäche dieses Verfahren. Das Antiviren-Programm muss daher durch Updates stets auf dem aktuellen Stand gehalten werden.[585] Die Antiviren-Definitionen sollten täglich aktualisiert werden.[586] Selbst mit aktuellem Antiviren-Schutz sind Rechner in der Zeit vom Bekanntwerden der Malware bis zur Aufnahme in die Liste der Signaturen durch den Antiviren-Programm-Hersteller bis zur Auslieferung der Signaturdatenbank ungeschützt.[587] Darüber hinaus stößt die Signaturerkennung an ihre Grenzen, wenn Malware Verschleierungsmechanismen einsetzt. Durch eine Komprimierung oder Verschlüsselung des Quelltextes ändert sich die Byte-Folge,[588] sodass die Signatur der unkomprimierten oder unverschlüsselten Version nicht mit der geänderten Version übereinstimmt. Ferner verändert sich manche Malware bei jeder Verbreitung im Rahmen einer polymor-

578 Oben Rn. 189.
579 Oben Rn. 182.
580 *BSI*, IT-Grundschutz-Kataloge, M 4.3; *Dennis Werner*, Verkehrspflichten, S. 76.
581 *Dennis Werner*, Verkehrspflichten, S. 75.
582 *BSI*, IT-Grundschutz-Kataloge, M 2.157; *Dennis Werner*, Verkehrspflichten, S. 77.
583 *Eckert*[8], S. 66; *Kaspersky*, S. 86; *Lehner/Hermann*, DuD 2006, 768, 769; *Dennis Werner*, Verkehrspflichten, S. 77.
584 *Eckert*[8], S. 66; *Kaspersky*, S. 86.
585 *Dennis Werner*, Verkehrspflichten, S. 75.
586 *BSI*, IT-Grundschutz-Kataloge, M 2.157.
587 *BSI*, IT-Grundschutz-Kataloge, M 2.157; *Dennis Werner*, Verkehrspflichten, S. 78.
588 *Lehner/Hermann*, DuD 2006, 768.

phen Selbstmutation,[589] was beim Verfahren der Signaturerkennung nicht zur Entdeckung der Malware führt.

Um diese Schwächen der Signaturerkennung auszugleichen, wird zusätz- 204
lich die heuristische Analyse verwendet, um unbekannte Viren oder Abwandlungen bekannter Viren zu erkennen.[590] Dabei wird Malware auf auffällige Merkmale wie Komprimierungen, Verschlüsselung oder sich selbst modifizierenden Programmcode untersucht.[591] Bei der heuristischen Analyse gibt es zwei Vorgehensweisen. Zum einen können im Rahmen einer statischen heuristischen Analyse bestimmte Strukturen mit bekannten Bytefolgen verglichen werden, wobei wie bei der Signaturerkennung nur der Struktur nach bekannte Malware erkannt wird.[592] Zum anderen kann bei einer dynamischen heuristischen Analyse die betroffene Anwendung in einer sicheren Umgebung ausgeführt werden, um die Funktionsweise zu beobachten.[593] Vorteil dieser Methode ist, dass sich dadurch Verschlüsselungen und polymorphe Veränderungen erkennen lassen.[594] Entscheidender Nachteil ist jedoch, dass diese dynamische heuristische Analyse erhebliche Rechenleistung beansprucht und deswegen zeitintensiv ist.[595] Insgesamt funktioniert die heuristische Analyse noch nicht ausreichend zuverlässig.[596]

Antiviren-Programme leiden daher unter der Schwäche, dass sie häu- 205
fig nur bekannte Viren zuverlässig identifizieren können. Eine weitere Schwäche von Antiviren-Programmen besteht bei der Erkennung von Trojanern.[597] Da Trojaner[598] zum einem Teil nützliche und nur zum anderen Teil schädliche Programme sind, fällt es Antiviren-Programmen schwer, diese schädlichen Teile zuverlässig zu identifizieren. Ferner sind Antiviren-Programme gegen Rootkits[599] häufig machtlos.[600] Rootkits laufen häufig

589 *Gaycken*, S. 239; *Lehner/Hermann*, DuD 2006, 768, 771.
590 *BSI*, IT-Grundschutz-Kataloge, M 2.157; *Eckert*[8], S. 66.
591 *Lehner/Hermann*, DuD 2006, 768; *Dennis Werner*, Verkehrspflichten, S. 78.
592 *Lehner/Hermann*, DuD 2006, 768, 769 f.
593 Ebd., 770.
594 Ebd., 770.
595 Ebd., 770.
596 *Eckert*[8], S. 67; *Lehner/Hermann*, DuD 2006, 768, 772; *Kaspersky*, S. 87; *Dennis Werner*, Verkehrspflichten, S. 78.
597 *Dennis Werner*, Verkehrspflichten, S. 77.
598 Oben Rn. 193.
599 Oben Rn. 197.
600 *Dolle/Wegener*, DuD 2006, 471, 472; *Dennis Werner*, Verkehrspflichten, S. 79; *Grosskopf*, CR 2007, 122, 123.

auf dem nullten Ring der Central Processing Unit (CPU) im Kernel-Mode, sodass die auf dem dritten Ring der CPU im User-Mode ausgeführten Antiviren-Programme diese nicht entdecken können.[601] Ebenso können Bootsektor-Viren durch Antiviren-Programme nicht erkannt werden, weil diese das System infizieren, bevor das Antiviren-Programm gestartet wird.[602]

206 Zusammenfassend zeigt die Untersuchung der Antiviren-Programme, dass sie nicht gegen alle Arten von Malware schützen. Mit Trojanern und Rootkits gibt es Kategorien, die Antiviren-Programme nur schwer bis gar nicht erkennen können. Bei Computerviren und -würmern erkennen Antiviren-Programme häufig nur bekannte Varianten wieder. Auch ein ständig aktualisiertes Antiviren-Programm kann somit eine Infektion mit einer neuartigen Schadsoftware nicht komplett ausschließen.[603] Nur circa 95 % der Schadsoftware wird von Antiviren-Programmen erkannt.[604] Das Infektionsrisiko eines Rechners kann mit einem Antiviren-Programm somit zwar verringert, jedoch nicht ausgeschlossen werden.

bb) Firewall

207 Eine Firewall ist ein weiterer Baustein im Sicherheitskonzept, um sich gegen die Infektion eines Rechners zu schützen. Der Begriff Firewall stammt vom englischen Wort für Brandschutzmauern und soll metaphorisch aufgreifen, dass die Ausbreitung eines Brandes vom einen auf den anderen Gebäudeteil übergreift.[605] Eine Firewall kontrolliert und filtert den Netzverkehr von einem in ein anderes Netzwerk, sodass bedrohliche Datenpakete gestoppt werden.[606] Die Firewall stellt damit ein organisatorisches und technisches Konzept zur Trennung von Netzbereich dar, das eine (teilweise) Abschottung nach Außen erreicht.[607] Durch die Überwachung des Datenverkehrs zwischen einem lokalen Netzwerk und einem anderen Netzwerk, häufig dem Internet, kann eine Firewall vor unberechtigten Zugriffen schüt-

601 *Dolle/Wegener*, DuD 2006, 471, 472.
602 *Gaycken*, S. 240.
603 *Dennis Werner*, Verkehrspflichten, S. 80.
604 *BSI*, IT-Grundschutz-Kataloge, M 2.157. Vgl. auch *Lehner/Hermann*, DuD 2006, 768, 772.
605 *Eckert*[8], S. 714.
606 *IETF*, RFC 2828, S. 73; *Eckert*[8], S. 714; *Fritsch/Gundel*[2], S. 33.
607 *Federrath/Pfitzmann*, in: *Moritz/Dreier*[2], F Rn. 54; *Eckert*[8], S. 715; *Dennis Werner*, Verkehrspflichten, S. 80.

zen.[608] Dabei kann eine Firewall sowohl softwarebasiert als Anwendung auf einem Betriebssystem als auch hardwarebasiert eine eigene physikalische Komponente in einem Netzwerk sein.[609]

Eine Firewall funktioniert so, dass nach festgelegten Regeln Datenpakete durchgelassen oder blockiert werden.[610] Dazu hat die Firewall drei Möglichkeiten. Sie kann zum einen Datenpakete nach bestimmten Formalkriterien filtern.[611] Sie kann zum anderen ganze Ports sperren[612] und dadurch gewisse Interaktionen von Anfang an blockieren. Ferner kann eine Firewall den Inhalt des Netzverkehrs kontrollieren und mit einem Content-Filter nur bestimmte als sicher eingestufte Inhalte durchlassen.[613] Diese drei Möglichkeiten lassen sich auch kombinieren.[614] 208

Die größten Probleme einer Firewall bestehen zum einen darin, dass eine Konfiguration sehr schwer ist. Nur sehr erfahrene Anwender können eine Firewall so konfigurieren, dass sie möglichst viel unerwünschte Angriffe abwehrt, jedoch möglichst wenig von gewollter Interaktion verbietet.[615] Darüber hinaus ist die Möglichkeit einer Firewall Schadsoftware zu stoppen begrenzt.[616] Häufig verbreitet sich solche Malware über das World Wide Web oder E-Mails, welche durch eine Firewall regelmäßig als gewollte Verbindungen angesehen werden und nicht blockiert sind.[617] Ohne ein solches Offenlassen von WWW- und E-Mail-Verbindungen wäre ein vernünftiges Arbeiten unmöglich.[618] Auch der Einsatz einer Firewall kann somit nicht verhindern, dass ein Rechner mit Schadsoftware infiziert wird. 209

608 *IETF*, RFC 2828, S. 74; *Eckert*[8], S. 715; *Dennis Werner*, Verkehrspflichten, S. 80; *Schneier*, S. 189.
609 *Eckert*[8], S. 715; *Dennis Werner*, Verkehrspflichten, S. 81.
610 *IETF*, RFC 2828, S. 74; *Dennis Werner*, Verkehrspflichten, S. 81.
611 *Fritsch/Gundel*[2], S. 38; *Zahedani/Obert*, DuD 2006, 627, 630.
612 *Eckert*[8], S. 717; *Fritsch/Gundel*[2], S. 38; *Federrath/Pfitzmann*, in: *Moritz/Dreier*[2], F Rn. 55.
613 *Eckert*[8], S. 717; *Dennis Werner*, Verkehrspflichten, S. 82.
614 *Fritsch/Gundel*[2], S. 54; *Dennis Werner*, Verkehrspflichten, S. 82.
615 *Eckert*[8], S. 743.
616 *Eckert*[8], S. 745; *Dennis Werner*, Verkehrspflichten, S. 86.
617 *Eckert*[8], S. 745; *Dennis Werner*, Verkehrspflichten, S. 86.
618 *Federrath/Pfitzmann*, in: *Moritz/Dreier*[2], F Rn. 57.

3. Missbrauch durch Erstellen eines Accounts unter falschem Namen

210 Eine Möglichkeit des Missbrauchs von Zugangsdaten im Internet besteht darin, einen Account unter falschem Namen anzulegen. Wenn die Identitätsbehauptung nicht überprüft wird, kann dies durch die einfache Angabe von Personendaten des Namensträgers geschehen.[619] Wird die Identitätsbehauptung überprüft, kann diese möglicherweise durch eine beglaubigte Kopie vom Personalausweis des Namensträgers erfolgen.[620]

4. Missbrauch ohne Erlangen der Zugangsdaten vom Account-Inhaber

211 Ein Missbrauch des Accounts ist möglich, ohne dass die Zugangsdaten vom Account-Inhaber erlangt werden. Das ist einmal der Fall, wenn wie beim Mail-Spoofing eine Authentisierung nicht erfolgt. Zum anderen kann durch mangelnde IT-Sicherheit beim Authentisierungsnehmer eine Person als Account-Inhaber authentifiziert werden, die gar nicht der Account-Inhaber ist.

a) Mail-Spoofing

212 Beim Mail-Spoofing[621] oder Maskerade-Angriff[622] wird eine E-Mail unter falscher Absenderangabe verschickt. Wenn behauptet wird, dass die Fälschung des E-Mail-Absenders schwer sei,[623] ist dem zu widersprechen. Wegen der fehlenden Authentifizierung und der Tatsache, dass der Absender lediglich eine Header-Information ist, lässt sich der Absender einer E-Mail leicht fälschen.[624] Wie der Absender auf einer Postkarte oder einem Brief kann der Versender einer E-Mail den Absender frei wählen. Die Einfachheit der Fälschung des Absenders wird sogar in der Definition des SMTP-Protokolls gesehen.[625]

---

619 Siehe *BGH*, Urteil v. 10. 4. 2008, I ZR 227/05 (Namensklau im Internet) – NJW 2008, 3714; *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676.
620 Siehe *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08.
621 *IETF*, RFC 5321, S. 75; *Eckert*[8], S. 153.
622 *Damker/Federrath/M. J. Schneider*, DuD 1996, 286.
623 *Mankowski*, NJW 2002, 2822, 2825.
624 *BSI*, IT-Grundschutz-Kataloge, G 5.73; *Ernst*, MDR 2003, 1091, 1092; *Dennis Werner*, Verkehrspflichten, S. 49; *Sieber*, in: *Hoeren/Sieber/Holznagel*, Kap. 1 Rn. 114.
625 *IETF*, RFC 5321, S. 75.

Zum einen ist der Absender einer E-Mail nur eine frei wählbare Header-Information.[626] Der Header „From“ wird nicht überprüft, sodass er von einem beliebigen Server versendet werden kann.[627] Zwar könnte der Empfänger anhand der IP-Adresse erkennen, dass die E-Mail von einem anderen Server stammt.[628] Diese Informationen werden von E-Mail-Programmen jedoch weder angezeigt noch überprüft.[629] Die meisten E-Mail-Programme, Mail User Agents (MUAs), zeigen nur einen verkürzten Header an, der Absender, Titel und weitere Empfänger offenbart.[630] Der durchschnittliche Nutzer würde daher nicht bemerken, dass die E-Mail von einem anderen SMTP-Server versendet wurde.[631] Ferner könnte der Angreifer auch die IP-Adresse des SMTP-Server so vortäuschen, dass die Fälschung nicht auffällt.[632] 213

Zum anderen funktionieren manche SMTP-Server ohne eine Authentisierung. SMTP bietet ohne entsprechende Konfiguration keine Sicherheitsfunktionalitäten.[633] Der Versand einer E-Mail über einen SMTP-Server kann ohne ein Passwort möglich sein.[634] Manche SMTP-Server überprüfen, dass die IP-Adresse aus dem passenden Subnetz kommt.[635] Wenn der SMTP-Server keine Authentifikation vornimmt, können durch eine falsche Absenderangabe E-Mails unter fremder E-Mail-Adresse verschickt werden.[636] Selbst eine Authentisierung hilft in Fällen nicht weiter, in denen der Angreifer einen Account auf dem SMTP-Server des Namensträgers hat,[637] weil SMTP-Server die Absenderadressen regelmäßig nicht prüfen.[638] Ferner besteht in der store&forward-Verteilung der E-Mails das Problem, dass 214

626 *Schwenk*[3], S. 59; *Dennis Werner*, Verkehrspflichten, S. 49; *Tanenbaum/Wetherall*[5], S. 717.
627 *Schwenk/Gajek*, in: Internet-Auktion, 180, 184; *Fuhrberg*, K&R 1999, 20, 23.
628 *Damker/Federrath/M. J. Schneider*, DuD 1996, 286, 291.
629 *BSI*, IT-Grundschutz-Kataloge, G 5.73; *Damker/Federrath/M. J. Schneider*, DuD 1996, 286, 291.
630 *Sosnitza/Gey*, K&R 2004, 465, 467.
631 *Dennis Werner*, Verkehrspflichten, S. 49; *Sosnitza/Gey*, K&R 2004, 465, 467.
632 *Sosnitza/Gey*, K&R 2004, 465, 467.
633 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.4.3; *Eckert*[8], S. 153.
634 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211; *Pohlmann*, DuD 2010, 607, 609.
635 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211; *Damker/Federrath/M. J. Schneider*, DuD 1996, 286.
636 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211. Siehe dazu das Beispiel bei *Fox*, c't 9/1995, 184.
637 *Damker/Federrath/M. J. Schneider*, DuD 1996, 286, 291.
638 *Gaycken*, S. 235.

jeder SMTP-Server auf dem langen Weg durch die MTAs der E-Mail diese verändern kann, ohne dass dies bemerkbar ist.[639]

b) Schwachstellen beim Authentisierungsnehmer

215 Schwachstellen oder ungenügende Sicherheitsanforderungen können dazu führen, dass der Angreifer den Account missbrauchen kann, ohne die Zugangsdaten auszuspähen oder auszuprobieren.

aa) SQL-Injection

216 SQL-Injections sind ein häufiges Einfallstor, um den Webserver oder die Datenbank eines Authentisierungsnehmers zu kompromittieren. Eine SQL-Injection wird durch unsaubere Programmierung der Webanwendung des Authentisierungsnehmers ermöglicht. Bei einer SQL-Injection nutzt der Angreifer eine Eingabemöglichkeit, um eine Datenbank-Abfrage, die in der Structured Query Language (SQL) geschrieben ist, zu manipulieren und seinen Sachcode zu injizieren.[640] Wird die Eingabe des Nutzers nicht ausreichend überprüft oder maskiert, kann er die SQL-Abfrage beliebig manipulieren.[641] Der Angreifer kann die Abfrage durch Verwendung von Sonderzeichen so abändern, dass statt der eigentlich von der Anwendung intendierten Datenbank-Abfrage beliebige weitere Anfragen gestellt werden.[642] Er kann Datensätze auslesen, erstellen, verändern oder löschen.[643]

---

639 *Damker*/*Federrath*/*M. J. Schneider*, DuD 1996, 286, 293; *Damker*/*Günter Müller*, DuD 1997, 24, 25; *Dennis Werner*, Verkehrspflichten, S. 49; *Eckert*[8], S. 153; Begr. FormAnpG, BT-Drucks. 14/4987, S. 10.

640 *BSI*, IT-Grundschutz-Kataloge, G 5.131; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 137; *Eckert*[8], S. 181.

641 *BSI*, IT-Grundschutz-Kataloge, G 5.131; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 85; *Eckert*[8], S. 179.

642 *BSI*, IT-Grundschutz-Kataloge, G 5.131; *Eckert*[8], S. 180.

643 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 85; *Eckert*[8], S. 180.

bb) Cross-Site-Scripting (XSS)

Cross-Site-Scripting (XSS) bezeichnet eine Angriffsform, bei der durch das Ausnutzen einer Sicherheitslücke in einer Webanwendung Informationen aus einem nicht vertrauenswürdigen Kontext in einen anderen Kontext eingefügt werden, wo sie als vertrauenswürdig gelten.[644] Nachgeladener Inhalt auf der Webseite des Authentisierungsnehmers wird durch den Angreifer geliefert, sodass er auf der vertrauenswürdigen Seite ausgeführt wird.[645] Dadurch können beispielsweise Zugangsdaten ausspioniert werden.[646] 217

Voraussetzung für Cross-Site-Scripting ist eine schlechte Implementierung der Webanwendung.[647] Das Cross-Site-Scripting kann zum einen persistent durch Eindringen in den Server des Authentisierungsnehmers und Platzieren des Codes in dessen Datenbank oder nicht persistent durch einen Link, den das Opfer anklicken muss, erfolgen.[648] XSS-Schwachstellen sind auf Internetseiten weit verbreitet, weil deren Gefährdungspotential vielfach unterschätzt wird.[649] Nutzer einer Internetseite haben keine wirksame Schutzmöglichkeit gegen XSS.[650] Den Schutz vor XSS-Angriffen müssen die Betreiber der Internetseiten sicherstellen. 218

cc) Schwachstellen in der IT-Infrastruktur

Der Authentisierungsnehmer muss einen Server betreiben, mit dem er die Authentifizierung vornimmt. Auf dem Server befindet sich eine Datenbank, die die Informationen über Accounts und Authentisierungsmittel wie Passwörter enthält. Zum einen kann im Rahmen eines aktiven Angriffs ein gesamter Server übernommen und kompromittiert werden.[651] 219

644 *Borges/Schwenk/Stuckenberg/Wegener*, S. 101; *Fox*, DuD 2012, 840; *Gaycken*, S. 231.

645 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 35; *Schwenk/Gajek*, in: Internet-Auktion, 180, 184; *J. Schmidt*, c't 22/2010, 42.

646 *J. Schmidt*, c't 4/2011, 35.

647 *Schwenk/Gajek*, in: Internet-Auktion, 180, 184; *Fox*, DuD 2012, 840.

648 *Borges/Schwenk/Stuckenberg/Wegener*, S. 102.

649 *Borges/Schwenk/Stuckenberg/Wegener*, S. 104; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 35; *J. Schmidt*, c't 4/2011, 35.

650 *Fox*, DuD 2012, 840.

651 Dazu ein Beispiel bei *Damker/Günter Müller*, DuD 1997, 24, 25.

220 Zum anderen kann nach einem Eindringen in die Server im Rahmen eines passiven Angriffs die Datenbank mit den Zugangsdaten ausgelesen werden.[652] Diese Datenbank enthält neben den Benutzernamen auch Passwörter, die mittels einer kryptologischen Hashfunktion in eine Richtung verschlüsselt sind. Mittels dieser Hash-Werte der Passwörter können diese durch einen Brute-Force-Angriff[653] herausgefunden werden. Diesen kann der Authentisierungsnehmer technisch durch eine Verzögerung von Login-Versuchen nicht mehr verlangsamen. Ist der Password-Hash nicht mittels des Salting-Verfahrens gesichert, kann das verschlüsselte Passwort mittels einer Rainbow-Table schnell entschlüsselt werden. Eine Rainbow-Table wird mit allen möglichen Werten, die mit einer One-Way-Hash-Funktion generiert werden können, gefüllt. Dadurch kann von einem Hash auf das Passwort im Klartext geschlossen werden. Verschlüsselt der Authentisierungsnehmer das Passwort jedoch nicht im Klartext, sondern hängt eine Zeichenkette vorne oder hinten an, was als Salting bezeichnet wird, kommt ein anderer Hash heraus, der mittels der Rainbow-Table nicht der unverschlüsselten Zeichenkette zugeordnet werden kann.

dd) Unbefugte Weitergabe der Zugangsdaten

221 Die Zugangsdaten zu einem Account kann ein Angreifer ferner dadurch erlangen, dass der Authentisierungsnehmer die Zugangsdaten unbefugt an einen Dritten weitergibt. Zum einen bietet die Passwort-Vergessen-Funktion, die regelmäßig angeboten wird, einen häufigen Angriffspunkt, um unbefugt an die Zugangsdaten zu gelangen.

222 Dabei kann die Passwort-Vergessen-Funktion technisch überlistet werden. Bei Skype war es beispielsweise bis November 2012 möglich, mittels der Passwort-Zurücksetzen-Funktion fremde Accounts zu übernehmen.[654] Bei Skype konnte sich ein Angreifer mit einer fremden E-Mail-Adresse einen Account anlegen. Über die Passwort-Zurücksetzen-Funktion wurde anschließend der Link zum Zurücksetzen des ersten Accounts per Skype-Nachricht an den zweiten Account geschickt. Der Dritte konnte damit einen Skype-Account übernehmen, sobald die E-Mail-Adresse bekannt war. Ei-

652 *B. Lorenz*, DuD 2013, 220, 225. Dies ist beispielsweise dem Internet-Auktionshaus eBay im Mai 2014 passiert, dazu *Briegleb*, heise online v. 22. 5. 2014.

653 Dazu oben Rn. 181.

654 Zu dieser Sicherheitslücke: *Ries*, heise online v. 14. 11. 2012.

ne ähnliche Sicherheitslücke war bei Google trotz der Zwei-Faktor-Authentisierung sieben Monate lang vorhanden, wurde jedoch Anfang 2013 geschlossen. Eine App, die Zugriff auf die API hatte, konnte das Passwort eines Google-Kontos ändern, ohne dass der Account-Inhaber dies über die Authentisierungskomponente des Besitzes bestätigen musste.[655]

Eine andere Methode, die Passwort-Zurücksetzen-Funktion zu überwin- 223
den, besteht im Social-Engineering. Beispielsweise wurde auf diese Weise ein Apple-iCloud-Account im Sommer 2012 von einem Hacker übernommen.[656] Die Apple-Hotline hat dem Angreifer ein temporäres Passwort zugewiesen, obwohl er die Sicherheitsfrage nicht beantworten konnte. Die E-Mail-Adresse, die Rechnungsadresse und die letzten vier Ziffern der Kreditkarte reichten der Hotline aus, um das temporäre Passwort auszustellen. Die letzten vier Zahlen der Kreditkartennummer haben die Angreifer über Amazon herausgefunden, wofür die Rechnungsadresse und einige Schritte notwendig sind. Durch den Zugriff auf die Apple-ID, den Account beim Authentisierungsnehmer Apple, und damit auf die iCloud, dem Cloud-Dienst von Apple, konnte der Angreifer sämtliche Daten von Handy, Tablet und Laptop mittels remote wipe löschen. Mit der E-Mail-Adresse haben die Angreifer anschließend den Google-Account übernommen und gelöscht sowie den Twitter-Account übernommen und missbraucht.

655 *Eickenberg*, heise online v. 26. 2. 2013.

656 Dazu der Bericht des Opfers *Honan*, Wired v. 8. 6. 2012.

§ 3 Rechtsscheinhaftung

Bei der Haftung für den Missbrauch von Zugangsdaten im Internet rekurrieren viele Lösungen auf die Rechtsscheinhaftung in unterschiedlichen Formen. Um diese Lösungen einordnen und bewerten zu können, wird zunächst die Rechtsscheinhaftung allgemein sowie in den Formen der Duldungs- und Anscheinsvollmacht abstrakt, losgelöst von den Besonderheiten des Missbrauchs von Zugangsdaten im Internet, behandelt. 224

Die Rechtsscheinhaftung schützt das Vertrauen eines objektiven Beobachters in das Vorliegen einer scheinbar gegebenen Rechtslage. Sie ist nicht allgemein gesetzlich kodifiziert, sondern wurde von Literatur und Rechtsprechung anhand bestehender spezieller Rechtsscheintatbestände entwickelt.[1] Die Rechtsscheinhaftung umfasst als Teil der Vertrauenshaftung im Wesentlichen das Vertrauen in die Register, die Rechtsscheinvollmachten, den gutgläubigen Erwerb, den Scheinkaufmann, die Scheinvollmachten, die Scheingesellschaft, die Scheingesellschafter sowie die wertpapierrechtliche Rechtsscheinhaftung.[2] Sie bezweckt den Schutz des Vertrauens des Empfängers im Sinne des Verkehrsschutzes.[3] Die Rechtsscheinhaftung ist ein Unterfall der Lehre von der Vertrauenshaftung,[4] deren dogmatische Grundlage umstritten ist.[5] 225

I. Voraussetzungen einer Rechtsscheinhaftung

Die allgemeinen Voraussetzungen der Rechtsscheinhaftung sind nicht gesetzlich kodifiziert, wurden jedoch anhand der Gemeinsamkeiten gesetzlicher Rechtsscheintatbestände, wie der §§ 170 ff. BGB,[6] entwickelt. Die vier Voraussetzungen der Rechtsscheinhaftung sind ein Rechtsscheintatbe- 226

1 *Rieder*, S. 90; *Schnell*, S. 123. Monographisch zur Entstehungsgeschichte *Selter*, S. 17 ff.
2 *Canaris*, in: FG 50 Jahre BGH, Bd. 1, 129, 132 f.
3 *Canaris*, Vertrauenshaftung, S. 526; *Borges*, NJW 2011, 2400, 2401.
4 *Canaris*, in: FG 50 Jahre BGH, Bd. 1, 129, 132 f.; *Rieder*, S. 90.
5 *Borges*, Elektronischer Identitätsnachweis, S. 133; *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 32.
6 Dazu *Conrad*, S. 25 ff.; *Faust*, BGB AT[3], § 26 Rn. 20 ff.

stand, dessen zurechenbares Hervorrufen, die Gutgläubigkeit des Dritten sowie dessen kausale Disposition.[7]

1. Rechtsscheintatbestand

227 Als Rechtsscheintatbestand qualifiziert sich „grundsätzlich jeder Sachverhalt, der Vertrauen erweckt."[8] Es muss sich um eine objektive Vertrauensgrundlage handeln, ein „blindes" Vertrauen reicht nicht aus.[9] Die Rechtsscheinhaftung umfasst in der Rechtsfolge mit der Gewährung von Erfüllungsansprüchen den Ersatz des positiven Interesses[10] und belastet den In-Anspruch-Genommenen somit stark. Wegen dieser Härte muss ein Sachverhalt für die Anerkennung als Rechtsscheintatbestand strenge Anforderungen erfüllen.[11] Ein starker Vertrauenstatbestand sowie ein erhöhtes Verkehrsschutzbedürfnis erfüllen diese Anforderungen.[12] Ein erhöhtes Verkehrsschutzbedürfnis besteht beispielsweise bei Wertpapieren, deren notwendige Umlauffähigkeit durch geringere Anforderungen hergestellt wird. Im Gegensatz zu anderen abhandengekommenen Sachen kann daher an abhandengekommenen Wertpapieren gutgläubig Eigentum erworben werden (§ 935 Abs. 2 BGB). Bei Rechtsscheintatbeständen ist zwischen künstlichen, durch das Gesetz geschaffenen, und natürlichen äußeren Tatbeständen zu unterscheiden.[13] Die künstlichen Tatbestände umfassen das Vertrauen in die Richtigkeit von Registereintragungen wie das Handels- oder Grundbuchregister.[14] Ihre Voraussetzungen und der Umfang des durch sie geschützten Vertrauens ist gesetzlich vorgegeben.[15]

---

7 *Conrad*, S. 38 ff.; *Faust*, BGB AT[3], § 26 Rn. 18; *Larenz/M. Wolf*[9], § 48 Rn. 32. Auf drei Voraussetzungen reduzierend *M. Wolf/Neuner*[10], § 10 Rn. 83.

8 *Canaris*, Vertrauenshaftung, S. 495. Dazu auch *Rieder*, S. 91.

9 *Bork*[3], Rn. 1539; *Canaris*, Vertrauenshaftung, S. 491; *Spiegelhalder*, S. 128.

10 Unten Rn. 256.

11 *Canaris*, Vertrauenshaftung, S. 527; *Rieder*, S. 91.

12 *Canaris*, Vertrauenshaftung, S. 533 Fn. 43a; *Reese*, S. 50; *Rieder*, S. 91 f.

13 *Canaris*, Vertrauenshaftung, S. 492; *Rieder*, S. 92. Diese Unterscheidung geht zurück auf *Wellspacher*, S. 22 ff.

14 *Canaris*, Vertrauenshaftung, S. 492.

15 Eintragungspflichtige Tatsachen im Handelsregisters sind beispielsweise in ihrer negativen Publizität geschützt (§ 15 Abs. 1 HGB), dazu etwa *Hopt*, in: *Baumbach/Hopt*[35], § 15 HGB Rn. 4.

Bei natürlichen äußeren Rechtsscheintatbeständen wird anhand einer Ge- 228
samtbewertung des Einzelfalls abgewogen, ob der gegebene Sachverhalt von einem durchschnittlichen Dritten aus dem betroffenen Verkehrskreis nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte in der von dem Vertrauenden gedeuteten Weise verstanden werden durfte.[16] Bei dieser Bestimmung werden die Grundsätze der objektiven Auslegung von Willenserklärungen (§§ 133, 157 BGB) entsprechend herangezogen.[17] Entscheidende Voraussetzung für die Anerkennung eines Rechtsscheintatbestandes ist die Stärke des Scheins. Er muss unter regelmäßigen Umständen den sicheren Schluss auf die angenommene Lage aufgrund der äußeren Umstände zulassen.[18] Nur vernünftige und nachvollziehbare Anhaltspunkte reichen dafür aus.[19] Eine Formalisierung der Voraussetzung verbietet sich, sodass für jeden Rechtsscheintatbestand von Fall zu Fall eine Gesamtabwägung erfolgen muss.[20] Bei gesetzlichen Rechtsscheintatbeständen ist die Stärke des Scheins durch die physische Einmaligkeit des Besitzes oder durch verschiedene Formen menschlichen Verhaltens wie mündliche oder schriftliche Erklärungen begründet.[21]

Einzelne Stimmen in der Literatur versuchen, wenngleich erfolglos, den 229
Rechtsscheintatbestand durch eine negative Abgrenzung zu bestimmen. Ein Rechtsscheintatbestand scheide demnach aus, wenn der Vertrauende die wahre Lage kennt oder sich wegen diverser Anhaltspunkte ihrer vergewissern muss.[22] Bei fehlender Erkenntnisfahrlässigkeit sei eine hinreichende Wahrscheinlichkeit für einen Rechtsscheintatbestand gegeben.[23] Dementsprechend sei eine Voraussetzung für einen Rechtsscheintatbestand, dass weitergehende Vergewisserungen unzumutbar seien.[24] Diese negative Abgrenzung überzeugt nicht. Wenn der Vertrauende die wahre Lage kennt, scheidet seine Schutzwürdigkeit aus, was eine der Voraussetzungen der

16 *Canaris*, Vertrauenshaftung, S. 494; *Kuhn*, S. 215; *Spiegelhalder*, S. 128; *Rieder*, S. 92.
17 *Canaris*, Vertrauenshaftung, S. 494; *Kuhn*, S. 215; *Spiegelhalder*, S. 129; **a.A.** wohl *AG Berlin Mitte*, Urteil v. 28. 7. 2008, 12 C 52/08 – MMR 2008, 696.
18 *Reese*, S. 50.
19 *Brückner*, S. 86.
20 *Canaris*, Vertrauenshaftung, S. 493; *Rieder*, S. 92.
21 *Canaris*, Vertrauenshaftung, S. 492; *Rieder*, S. 92.
22 *Schnell*, S. 129.
23 Ebd., S. 137.
24 Ebd., S. 137 f.; *v. Craushaar*, AcP 174 (1974), 2, 11.

Rechtsscheinhaftung ist.[25] Beim Abstellen auf die Schutzwürdigkeit bei der Anerkennung des Rechtsscheintatbestandes hätte die Stärke des Rechtsscheintatbestandes keine eigene Bedeutung.

230 Ein Sachverhalt, der die notwendige Stärke aufweist, muss einige weitere Voraussetzungen erfüllen, um als Rechtsscheintatbestand anerkannt zu werden. Eine wichtige Voraussetzung dabei ist, dass sich der Rechtsscheintatbestand auf ein Verhalten desjenigen beziehen muss, dessen Einstandspflicht begründet werden soll.[26] Diese Anforderung setzt vor der Zurechnung an, die die zweite Voraussetzung einer Rechtsscheinhaftung ist.[27] Eine Person kann durch ihr Verhalten eine Rechtsscheinhaftung eines Dritten ebenso wenig begründen, wie sie Verträge zu seinen Lasten abschließen kann.[28] Das Verhalten einer Person kann daher nur gegen diese Person eine Rechtsscheinhaftung begründen.[29] Eine bewegliche Sache muss beim gutgläubigen Erwerb vom Eigentümer willentlich übergeben worden sein (vgl. § 935 Abs. 1 BGB), eine besondere Mitteilung der Vollmacht (§ 171 Abs. 1 BGB) muss der Vertretene kundgeben, um als Rechtsschein gegen diesen anerkannt zu werden. Nur einige gesetzliche Vertrauenstatbestände in die Richtigkeit einer Registereintragung verlangen keine Rückkopplung an das Verhalten desjenigen, der in Anspruch genommen wird. Für den gutgläubigen Erwerb eines Grundstückes kommt es beispielsweise nicht darauf an, ob der Eigentümer die Eintragung veranlasst hat.[30]

231 Weitere Voraussetzung ist, dass sich der Inhalt des Rechtsscheintatbestandes auf eine gegenwärtige, bereits bestehende Lage beziehen muss.[31] Das Vertrauen in ein künftiges Ereignis verdient keinen Schutz. Zum einen ergibt sich dies daraus, dass die Zukunft ungewiss ist und dies allgemein bekannt ist.[32] Zum anderen erlaubt die Vertragsfreiheit den Parteien, künftiges Verhalten zu vereinbaren. Im Umkehrschluss ist ohne eine vertragliche Vereinbarung das Vertrauen in das künftige Verhalten der anderen Partei nicht schutzwürdig.[33] Darüber hinaus muss sich der Scheintatbestand auf eine

25 Unten Rn. 252.
26 *Canaris*, Vertrauenshaftung, S. 497.
27 Unten Rn. 233.
28 Zur Unzulässigkeit des Vertrags zu Lasten Dritten *Gottwald*, in: MüKo-BGB[6], § 328 Rn. 250 m.w.N.
29 *Canaris*, Vertrauenshaftung, S. 93.
30 *Kohler*, in: MüKo-BGB[6], § 892 Rn. 2 m.w.N.
31 *Canaris*, Vertrauenshaftung, S. 495; *Rieder*, S. 92.
32 *Hildebrandt*, S. 215.
33 *Canaris*, Vertrauenshaftung, S. 352 f.

rechtsgeschäftliche Handlung beziehen. Ein Rechtsscheintatbestand liegt somit bei Unterschriften auf Autogrammkarten oder bei Vorlage eines privaten Briefes als Vollmachtsurkunde nicht vor.[34]

Ferner muss sich der Rechtsscheintatbestand auf eine rechtlich mögli- 232
che Lage beziehen.[35] Diese Anforderung ergibt sich daraus, dass es für einen objektiven Dritten aus den Umständen selbst ersichtlich ist, dass diese scheinbare Lage rechtlich unmöglich ist. Ein Vertrauen darin kann somit nicht gebildet werden. Darüber hinaus ist nur das Vertrauen in eine bestimmte Rechtslage, nicht in eine bestimmte Tatsachenlage schützenswert.[36] Der Name *Rechts*schein suggeriert bereits, dass das Vertrauen in scheinbar vorliegende Tatsachen nicht geschützt ist.[37] Der Tatsachenschein sei dem geltendem Recht fremd.[38]

2. *Zurechenbarkeit*

Zweite Voraussetzung der Rechtsscheinhaftung ist, dass der Rechtsschein- 233
tatbestand zurechenbar gesetzt wurde. Diese Voraussetzung ist ein zwingendes Erfordernis, weil eine Haftung nur gerechtfertigt ist, wenn sie ein Ausdruck der Selbstverantwortung der Person ist.[39] Insbesondere bei natürlichen äußeren Rechtsscheintatbeständen ist das Erfordernis der Zurechenbarkeit entscheidend. Bei den künstlichen Rechtsscheintatbeständen hat der Gesetzgeber selbst offensichtlich oder versteckt Zurechnungskriterien festgelegt oder ganz auf die Zurechnung verzichtet.[40] Für das Prinzip, nach dem bei der Rechtsscheinhaftung zugerechnet wird, haben sich unterschiedliche Ansichten herausgebildet.[41]

---

34 *Canaris*, Vertrauenshaftung, S. 443.
35 Ebd., S. 495 f.; *Rieder*, S. 93.
36 *Canaris*, Vertrauenshaftung, S. 496; *Rieder*, S. 93.
37 *Canaris*, Vertrauenshaftung, S. 496 f.; *Rieder*, S. 93.
38 *Canaris*, Vertrauenshaftung, S. 496.
39 Ebd., S. 468; *Reese*, S. 61; *Rieder*, S. 96.
40 Zum reinen Rechtsscheinprinzip im Rahmen von §§ 892, 935 Abs. 2 BGB *Rieder*, S. 96.
41 Übersichten bei *Kuhn*, S. 227 ff.; *Reese*, S. 62 ff.; *Spiegelhalder*, S. 142 ff.

a) Veranlassungsprinzip

234 Früher wurde in der Literatur überwiegend vertreten, dass für die Zurechnung des Rechtsscheins lediglich eine Veranlassung des Anspruchsgegners erforderlich sei.[42] Eine Verursachung des Rechtsscheintatbestandes reiche demnach aus.[43] Dabei findet der Rechtsgedanke Anwendung, dass der Urheber eines Schadens ihn zu bessern habe.[44] Auf ein Verschulden komme es nicht an, allein entscheidend sei, ob nach Treu und Glauben (§ 242 BGB) ein Dritter aufgrund des Verhaltens des Geschäftsherren auf den Rechtsscheintatbestand vertrauen durfte.[45] Die objektive Möglichkeit den Rechtsschein zu verhindern, reiche zur Zurechnung aus.[46]

235 Gegen das Veranlassungsprinzip spricht, dass es sich lediglich um Kausalitätserwägungen in einem anderen Gewand handelt.[47] Das Abstellen auf die reine Kausalität würde jedoch dazu führen, dass auf ein Zurechnungskriterium vollständig verzichtet wird.[48] Das Verhalten des in Haftung Genommenen muss Ausgangspunkt des Rechtsscheins sein.[49] Weil dieses schon Voraussetzung des Rechtsscheintatbestandes ist, wäre nach dem Veranlassungsprinzip daher der Rechtsscheintatbestand stets zurechenbar.

236 Ferner kann das Veranlassungsprinzip beim Unterlassen keine Begründung zur Zurechnung sein.[50] Ein Unterlassen kann nicht kausal für das Entstehen eines Rechtsscheintatbestandes im Sinne der *conditio-sine-qua-non*-Formel sein.[51] Vertreter des Veranlassungsprinzips versuchen das Unterlassen mit dem Bestehen einer Rechtspflicht zu begründen, die verletzt wurde.[52] Dabei handelt es sich jedoch um Verschuldenserwägungen, nicht mehr um eine reine Veranlassung. Dies zeigt, dass selbst Vertreter des Veranlassungsprinzips teilweise auf Risiko- oder Verschuldenserwägungen zu-

---

42 *Enneccerus/Nipperdey*[15], § 184 II 3 c); *Hubmann*, AcP 155 (1956), 85, 120 ff.; *Jacobi*, JherJB 70 (1921), 300, 325 f.; *H. Meyer*, ZHR 81 (1918), 365, 387 ff.; *Oertmann*, ZHR 95 (1930), 443, 466; *Stoll*, AcP 135 (1932), 89, 104 ff.

43 *Stoll*, AcP 135 (1932), 89, 105.

44 Ebd., 105.

45 *Enneccerus/Nipperdey*[15], § 184 II 3 c).

46 Ebd., § 184 II 3 c).

47 *Canaris*, Vertrauenshaftung, S. 474; *Rieder*, S. 96; *Spiegelhalder*, S. 142.

48 *Canaris*, Vertrauenshaftung, S. 474.

49 Oben Rn. 230.

50 *Canaris*, Vertrauenshaftung, S. 474 f.; *Reese*, S. 63; *Spiegelhalder*, S. 142.

51 *Canaris*, Vertrauenshaftung, S. 475.

52 *Stoll*, AcP 135 (1932), 89, 108.

rückgreifen und somit belegen, dass allein die Veranlassung kein sinnvolles Kriterium für die Zurechnung ist.[53]

b) Verschuldensprinzip

Die überwiegende Rechtsprechung[54] und Literatur[55] lösen die Zurechnung des Rechtsscheintatbestandes über das Verschuldensprinzip. Der Rechtsscheintatbestand sei demnach dann zuzurechnen, wenn er bei pflichtgemäßer Sorgfalt hätte erkannt werden müssen und verhindert werden können.[56] Die überwiegende Ansicht lässt eine einfache Fahrlässigkeit dafür ausreichen.[57] Einzelne Stimmen der Literatur entgegnen dem, dass nur bei grober Fahrlässigkeit die Haftung auf das positive Interesse gerechtfertigt sei.[58] 237

Gegen das Verschuldensprinzip spricht, dass ein Verschulden im Sinne des § 276 BGB mangels rechtsgeschäftlichen Kontaktes nicht in Betracht komme.[59] Mangels dieser Verbindung ist daher eine Pflichtverletzung nicht möglich.[60] Denn Sorgfaltspflichten, das Vermögen einer anderen Person zu schützen, kommen nur im Rahmen von Sonderverbindungen in Betracht (vgl. §§ 241 Abs. 2, 311 Abs. 2 BGB). Gegenüber der Allgemeinheit bestehen diese Sorgfaltspflichten nicht. Diesen Bedenken wird mit unterschied- 238

53 Ein weiteres Beispiel behandelt *Reese*, S. 63.

54 *BGH*, Urteil v. 12. 2. 1952, I ZR 96/51 – BGHZ 5, 111, 116; Urteil v. 12. 3. 1981, III ZR 60/80 – NJW 1981, 1727, 1728; Urteil v. 5. 3. 1998, III ZR 183/96 – NJW 1998, 1854, 1855; Urteil v. 21. 6. 2005, XI ZR 88/04 – NJW 2005, 2985, 2987; Urteil v. 10. 1. 2007, VIII ZR 380/04 – NJW 2007, 987, Rn. 25; *OLG Frankfurt*, Urteil v. 15. 1. 1998, 16 U 223/95 – WM 1999, 791, 794; *OLG Düsseldorf*, Beschluss v. 24. 7. 2009, 24 U 67/08 – NJOZ 2010, 139, 140; *OLG Hamm*, Urteil v. 20. 7. 2010, 28 U 2/10, I-28 U 2/10, Rn. 47; *LG Duisburg*, Urteil v. 10. 12. 2003, 11 S 111/02 – NJOZ 2004, 554, 555; *LG Flensburg*, Urteil v. 16. 9. 2005, 7 S 18/05 – MMR 2006, 47.

55 *Ellenberger*, in: *Palandt*[73], § 172 BGB Rn. 11; *Hübner*[2], Rn. 1286; *Leptien*, in: *Soergel*[13], § 167 BGB Rn. 22; *Maier-Reimer*, in: *Erman*[13], § 167 BGB Rn. 19; *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 40; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 59; *Valenthin*, in: *Bamberger/H. Roth*[3], § 167 BGB Rn. 16.

56 *BGH*, Urteil v. 10. 1. 2007, VIII ZR 380/04 – NJW 2007, 987, Rn. 25.

57 Explizit *Leptien*, in: *Soergel*[13], § 167 BGB Rn. 22, implizit *BGH*, Urteil v. 10. 1. 2007, VIII ZR 380/04 – NJW 2007, 987, Rn. 25; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 59.

58 *Hübner*[2], Rn. 1289.

59 *Canaris*, Vertrauenshaftung, S. 477 f.; *Reese*, S. 64; *Spiegelhalder*, S. 144.

60 *Canaris*, Vertrauenshaftung, S. 447 f.

lichen Konstruktionen begegnet. Bei einer Konstruktion solle Verschulden sich nicht auf eine Pflicht- sondern auf eine Obliegenheitsverletzung beziehen.[61] Diese Konstruktion weist jedoch das gleiche Problem auf. Obliegenheiten werden im Interesse eines Anderen im Rahmen von Sonderverbindungen auferlegt.[62] Bei einer anderen Konstruktion stelle das Verschulden ein Verschulden gegen sich selbst dar, bei der die Sorgfalt in eigenen Angelegenheiten zu beachten ist.[63] Dabei hafte der Geschäftsherr für Organisationsmängel in der eigenen Rechtssphäre.[64] Die Anwendung eines „Verschuldens gegen sich selbst" überzeugt jedoch ebenfalls nicht, weil der Geschäftsherr bei der Schaffung eines Rechtsscheintatbestandes nicht schuldhaft handelt.[65]

239 Ebenfalls spreche gegen das Verschuldensprinzip, dass das Ziel des Verkehrsschutzes der Rechtsscheinhaftung durch ein Verschuldenserfordernis vereitelt werde.[66] Der Vertrauende könne nicht überprüfen, ob der Geschäftsherr den Rechtsschein zu vertreten habe, sodass eine nicht hinzunehmende Rechtsunsicherheit entstehe. Das überzeugt nicht. Der Verkehrsschutz wird nicht grenzenlos gewährt, sondern findet seine Grenze dort, wo jemand ohne ein privatautonomes Handeln verpflichtet werden soll. Dies zeigt sich systematisch beispielsweise in der Regelung des § 935 Abs. 1 S. 1 BGB. Der Besitz ist ein Rechtsscheinträger (§ 1006 Abs. 1 S. 1 BGB), aufgrund dessen gutgläubig Eigentum erworben werden kann (§§ 929 S. 1, 932 Abs. 1 S. 1 BGB). Der Verkehrsschutz überwiegt die Interessen des Eigentümers jedoch nicht, wenn diesem die Sache abhandengekommen ist (§ 935 Abs. 1 S. 1 BGB). Der gutgläubig Erwerbende ist dadurch ebenfalls mit der Rechtsunsicherheit belastet, dass die Sache abhandengekommen ist. Der Vollmachtsurkunde (§ 172 Abs. 1 BGB) kann der Vertrauende ebenfalls nicht ansehen, ob sie willentlich übergeben wurde oder abhandengekommen ist. Der Verkehrsschutz gebietet keinen absoluten Schutz, sodass eine Rechtsunsicherheit durch das Verschuldensprinzip nicht gegen dieses spricht.

---

61 *Leptien*, in: *Soergel*[13], § 167 BGB Rn. 22.

62 *Reese*, S. 64.

63 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 61; *Maier-Reimer*, in: *Erman*[13], § 167 BGB Rn. 19.

64 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 61.

65 *Canaris*, Vertrauenshaftung, S. 478; vgl. auch *Kuhn*, S. 228.

66 *Canaris*, Vertrauenshaftung, S. 477; *Kuhn*, S. 228; *Reese*, S. 64; *Spiegelhalder*, S. 144; *v. Craushaar*, AcP 174 (1974), 2, 20.

Ferner spricht gegen das Verschuldensprinzip, dass die gesetzlichen Rechtsscheintatbestände kein Verschulden voraussetzen.[67] Eine Haftung für einen fahrlässig verursachten Rechtsschein ist dem Bürgerlichen Recht im Gegensatz zum Handelsrecht fremd.[68] Die zahlreichen gesetzlichen Normen der Rechtsscheinhaftung setzen die willentliche Schaffung des Rechtsscheintatbestandes voraus.[69] Diese willentliche Schaffung kann jedoch nicht mit dem Vorsatz eines Verschuldens gleichgesetzt werden. Fahrlässiges Handeln setzt das Außer-Acht-Lassen der im Verkehr erforderlichen Sorgfalt voraus. Wer eine Vollmacht kundgibt (§ 171 Abs. 1 BGB) oder eine Vollmachtsurkunde ausstellt (§ 172 Abs. 1 BGB), handelt nicht fahrlässig oder vorsätzlich. Er beteiligt sich nur willentlich am Geschäftsverkehr. Da die Schaffung des Rechtsscheintatbestandes nicht gegen die im Verkehr erforderliche Sorgfalt verstößt, kann ein Verschulden nicht daran anknüpfen.[70] Anknüpfungspunkt für das Verschulden kann nur sein, dass der Geschäftsherr die Wirkungen des Rechtsscheins nicht verhindert hat. Das Verschuldensprinzip liefert dabei keine überzeugenden Ergebnisse, wenn kein Verschulden vorliegt, eine Haftung des Geschäftsherren wegen des Nutzens, den seine Handlungen für ihn bringen, jedoch geboten erscheint.[71] Übergibt ein Geschäftsherr einem stets zuverlässigen Mitarbeiter eine Vollmachtsurkunde, die dieser missbraucht, ist eine Haftung für den Rechtsschein angemessen, nach dem Verschuldensprinzip jedoch nicht zu erreichen.[72] 240

Ferner spreche gegen das Verschuldensprinzip, dass ein Verschulden in der deutschen Rechtsordnung lediglich Schadensersatzansprüche und keine Erfüllungshaftung begründe.[73] Dieses Argument erschüttert das Verschuldensprinzip als solches nicht, sondern beschränkt den Umfang auf Rechtsfolgenseite. Darüber hinaus ist diese Argumentation zirkulär. Nach überwiegender Ansicht hat der Erklärende bei fehlendem Erklärungsbewusstsein für seine scheinbare Willenserklärung einzustehen, wenn er erklärungsfahrlässig handelt.[74] Nur mit einer anschließend möglichen Anfechtung 241

67 *Canaris*, Vertrauenshaftung, S. 479; *Rieder*, S. 97; *Spiegelhalder*, S. 143.
68 *Canaris*, Vertrauenshaftung, S. 39, 478 f.
69 Ebd., S. 29.
70 A.A. wohl *BGH*, Urteil v. 21. 6. 2005, XI ZR 88/04 – NJW 2005, 2985, 2986.
71 *Reese*, S. 64.
72 Ebd., S. 64.
73 *Langenbucher*, S. 25; *Reese*, S. 64.
74 Unten Rn. 472.

kann er seine Einstandspflicht analog zu § 122 BGB auf den Schadensersatz in Höhe des negativen Interesses beschränken. Je nach vertretener Ansicht kann ein Verschulden sehr wohl die Erfüllungshaftung zur Folge haben.

242 Mit dem Verschuldensprinzip lässt sich die Zurechnung des Rechtsscheintatbestandes somit nicht überzeugend lösen. Nachfolgend wird die Zurechnung jedoch auch nach dem Verschuldensprinzip untersucht, um dem Umstand Rechnung zu tragen, dass die herrschende Meinung nach Verschuldensgesichtspunkten den Rechtsscheintatbestand zurechnet.

c) Risikoprinzip

243 Die Zurechnung des Rechtsscheintatbestandes lässt sich überzeugend durch das Risikoprinzip lösen.[75] Das Prinzip hinter diesem Zurechnungskriterium ist die Selbstverantwortung der Person für ihr Verhalten und ihren Geschäftskreis.[76] Demnach haftet der Geschäftsherr für das Risiko von Mängeln und Gefahren, die seiner Sphäre entstammen. Kritiker wenden gegen das Risikoprinzip insbesondere ein, dass es zu einer zu weitreichenden Haftung führt.[77] Dass sogar der *BGH* das Risikoprinzip in einer Entscheidung als Grundlage der Rechtsscheinhaftung betrachtet,[78] zeigt jedoch, dass die Eingrenzung der Risikosphäre durchaus bei der Konstruktion einer angemessen weitreichenden Haftung hilfreich ist.

244 Eine Zurechnung kommt nach dem Risikoprinzip nur in Betracht, wenn der Geschäftsherr ein erhöhtes Risiko setzt, das er abstrakt eher beherrscht als der andere Teil.[79] Dabei begründet nicht schon jede rechtsgeschäftliche Erklärung an sich ein Risiko, denn der Empfänger setzt sich mit seinem Vertrauen diesem Risiko freiwillig aus (allgemeines Erklärungsrisiko).[80] Entscheidende Frage beim Risikoprinzip ist, welche Risiken einem Geschäftsherren aufgebürdet werden. Für vermeidbare Gefahren soll der Beherrscher

---

75 *Canaris*, Vertrauenshaftung, S. 479 ff.; *ders.*, in: FG 50 Jahre BGH, Bd. 1, 129, 157 f.; *Bork*[3], Rn. 1555, 1564; *Frensch*, in: *Prütting/Wegen/Weinreich*[8], § 167 BGB Rn. 43; *Kuhn*, S. 228 f.; *Koller*, WM 1981, 210; *Reese*, S. 65 ff.; *Rieder*, S. 97; *Spiegelhalder*, S. 153 f.; *Steffen*, in: RGRK[12], § 167 BGB Rn. 12; *v. Craushaar*, AcP 174 (1974), 2, 20 f.; *Wiebe*, Elektronische Willenserklärung, S. 159 ff., 223 ff.

76 *Canaris*, Vertrauenshaftung, S. 468; *Rieder*, S. 96.

77 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 61; *Hübner*[2], Rn. 1286.

78 *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 19.

79 *Canaris*, Vertrauenshaftung, S. 482; *Reese*, S. 70; *Rieder*, S. 97.

80 *Canaris*, Vertrauenshaftung, S. 481.

der Risikosphäre einstehen, wenn die Teilnehmer im Rechtsverkehr schützenswert vertrauen.[81] Von jedem Teilnehmer am Rechtsverkehr kann erwartet werden, dass er seinen Bereich sorgfältig organisiert.[82] Zur Bestimmung des Risikobereichs hilft die Abgrenzung der Sphären der Beteiligten.[83] Der räumlich-gegenständliche Bereich des Geschäftsherren fällt regelmäßig in seinen Risikobereich.[84]

d) Voraussetzungen und Fälle der Zurechnung

Nachfolgend werden erst allgemeine Voraussetzungen der Zurechnung dargestellt, um anschließend einzelne Fälle der Zurechnung nach dem Risikoprinzip und dem Verschuldensprinzip zu untersuchen. Dabei zeigt sich, dass die Behauptung, die praktischen Unterschiede zwischen den beiden Ansichten seien gering,[85] nicht zutrifft. 245

Zentrale Voraussetzung der Zurechenbarkeit ist, dass der potentiell Haftende eine Möglichkeit hat, den Rechtsschein zu verhindern beziehungsweise einen vorhandenen Rechtsschein zu zerstören.[86] Da eine Haftung stets auf eine Handlung als Ausdruck der Selbstbestimmung zurückzuführen sein soll und unbeherrschbare Risiken nicht durch eine Handlung beeinflusst werden können, gebietet die Selbstbestimmung, dass eine Zurechnung dann nicht in Betracht kommt. Ansonsten würde die Rechtsscheinhaftung für den Geschäftsherren wie eine Gefährdungshaftung wirken. Eine solche lässt sich jedoch nur durch eine besondere gesetzgeberische Entscheidung begründen, wie beispielsweise bei § 833 S. 1 BGB oder § 7 Abs. 1 StVG. Dabei kommt es nicht darauf an, ob der Rechtsscheintatbestand durch Handeln oder Unterlassen geschaffen wurde. Das Unterlassen kann zur Zurechnung ebenso führen wie ein Handeln.[87] Beim Unterlassen ist jedoch ebenso zu beachten, dass die gebotene Handlung den Rechtsschein hätte verhindern können.[88] 246

81 *Reese*, S. 66.
82 *Bork*[3], Rn. 1564.
83 *Spiegelhalder*, S. 153.
84 *Reese*, S. 70.
85 *Faust*, BGB AT[3], § 26 Rn. 34.
86 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 63; *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 42; *Canaris*, Vertrauenshaftung, S. 498; *Rieder*, S. 93.
87 *Rieder*, S. 100.
88 *Canaris*, Vertrauenshaftung, S. 490.

247 Aus der Tatsache, dass sich die Haftung nur für Handlungen, die Ausdruck von Selbstbestimmung sind, rechtfertigt, folgen zwei Fälle, bei denen nicht zugerechnet werden kann. Ein Rechtsscheintatbestand kann nur einem insoweit Geschäftsfähigen zugerechnet werden.[89] Somit kann einem Geschäftsunfähigen kein Rechtsscheintatbestand zugerechnet werden. Dem beschränkt Geschäftsfähigen hingegen kann der Rechtsschein nur dann zugerechnet werden, wenn er ein solches Geschäft abschließen kann. Des Weiteren folgt aus der Selbstbestimmung, dass bei *vis absoluta* eine Zurechnung nicht stattfindet.[90]

248 Bei Handlungen Dritter hingegen kann wieder in dem Ziel die Selbstverantwortung zum Ausdruck zu bringen, festgestellt werden, dass die Handlungen Dritter grundsätzlich nicht zurechenbar sind. Etwas anderes ergibt sich nur, wenn der Dritte mit Vertretungsmacht handelt.[91] Ein eindeutiger Fall des Handelns Dritter ist die Fälschung. Wird der Rechtsscheinträger von einem Dritten gefälscht, so kann dies dem Geschäftsherren nicht zugerechnet werden.[92] Fälschung und Verfälschungen sind nicht nur wegen der fehlenden Selbstverantwortung auszuschließen, sondern nach dem Risikoprinzip ebenso, weil der Erklärungsempfänger das Fälschungsrisiko genau so wenig wie der Geschäftsherr beherrschen kann.

249 Eine Zurechnung ist stets gegeben, wenn der Anspruchsgegner den Rechtsschein willentlich geschaffen hat.[93] Das zeigt sich durch die Betrachtung der gesetzlichen Rechtsscheintatbestände. § 171 Abs. 1 BGB setzt beispielsweise die willentliche Mitteilung einer Vollmacht, § 172 Abs. 1 BGB die willentliche Übergabe einer Vollmachtsurkunde voraus. Ferner ist im Rahmen des Verschuldensprinzips mit der willentlichen Schaffung ein vorsätzliches Handeln gegeben, das die stärkste Form des Verschuldens darstellt.

250 Unterhalb der Schwelle der willentlichen Schaffung ist das Richtigkeitsrisiko. Die bewusste Kundgabe bei Unkenntnis der Unrichtigkeit des Erklärten trägt grundsätzlich nicht der Erklärende.[94] Nur bei drittgerichteten Rechtstatsachen trägt der Erklärende das Richtigkeitsrisiko ausnahmswei-

---

89 *Bork*[3], Rn. 1542; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 52; *Reese*, S. 62; *Rieder*, S. 100.

90 *Canaris*, Vertrauenshaftung, S. 468 f.; *Rieder*, S. 96; *Reese*, S. 62.

91 *Rieder*, S. 99; *Reese*, S. 62.

92 *Canaris*, Vertrauenshaftung, S. 487 f.; *Rieder*, S. 99.

93 *Bork*[3], Rn. 1542; *Canaris*, Vertrauenshaftung, S. 29; *Rieder*, S. 97.

94 *Canaris*, Vertrauenshaftung, S. 484; *Rieder*, S. 97.

se.[95] Dabei ergeben sich keine Unterschiede zwischen Risiko- und Verschuldensprinzip.

Das Abhandenkommen durch den Diebstahl eines Dritten kann kein Anknüpfungspunkt für die Zurechnung sein.[96] Das ergibt sich zum einen aus der gesetzlichen Wertung der §§ 935 Abs. 1 S. 1, 172 Abs. 1 BGB sowie daraus, dass das Handeln des Dritten der Selbstverantwortung des Geschäftsherren nicht zuzurechnen ist. Eine Ausnahme kann jedoch für Umlaufpapiere gemacht werden, bei denen der erhöhte Verkehrsschutz eine Ausnahme rechtfertigt (vgl. § 935 Abs. 2 S. 1 BGB).[97] Das Verhalten des Geschäftsherren hingegen, dass er ein Abhandenkommen ermöglicht, kann hingegen im Rahmen der Selbstverantwortung als Grundlage der Zurechnung herangezogen werden.[98] Trüge der Geschäftsherr nach dem Risikoprinzip jedoch das Diebstahlrisiko,[99] bestünde ein erheblicher Unterschied zum Verschuldensprinzip. 251

3. Schutzwürdigkeit des Geschäftsgegners

Der Geschäftsgegner muss schutzwürdig sein.[100] Dazu gehört zum einen, dass er gutgläubig ist. Ihm schadet jedenfalls Kenntnis und häufig auch vorwerfbare Unkenntnis.[101] Je nach Grad der Stärke des Rechtsscheins sehen gesetzliche Regelungen vor, dass nur positive Kenntnis (bei Registern), grob fahrlässige Unkenntnis (bei § 932 Abs. 2 BGB) oder sogar leicht fahrlässige Unkenntnis schadet.[102] Im Rahmen von Rechtsscheinvollmachten wird das Gutgläubigkeitserfordernis aus § 173 BGB übertragen, sodass in diesem Zusammenhang leicht fahrlässige Unkenntnis schadet.[103] Selbst wenn vorwerfbare Unkenntnis schadet, besteht keine allgemeine Prüfungsoblie- 252

95 *Canaris*, Vertrauenshaftung, S. 485.
96 *Rieder*, S. 99; *v. Craushaar*, AcP 174 (1974), 2, 22; **a.A.** *Canaris*, Vertrauenshaftung, S. 487.
97 *Rieder*, S. 99.
98 Vgl. dazu *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13, 15.
99 So *Canaris*, Vertrauenshaftung, S. 487.
100 Ebd., S. 516.
101 *Bork*[3], Rn. 1543; *Börner*, S. 77.
102 *Bork*[3], Rn. 1543.
103 *Faust*, BGB AT[3], § 26 Rn. 36; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 70; *Spiegelhalder*, S. 166.

genheit.[104] Lediglich bei Zweifeln muss sich der Geschäftsgegner erkundigen.[105]

253 Zum anderen gehört zur Schutzwürdigkeit, dass es sich um ein Verkehrsgeschäft handelt, also aus dem Kontext deutlich wird, dass die Tatsachen, die den Rechtsschein begründen, auch rechtsgeschäftlichen Charakter haben.[106] Dies ist der Fall, wenn der geltend gemachte Anspruch nicht aus einer rechtsgeschäftlichen Beziehung zwischen den beiden Parteien stammt, sondern etwas auf einer deliktischen Handlung beruht oder es an einem Verkehrsgeschäft fehlt.[107]

4. Disposition im Vertrauen auf den Rechtsschein

254 Der Geschäftsgegner ist nur schutzwürdig, wenn er im Vertrauen auf den Rechtsscheintatbestand eine Disposition getroffen hat. Dazu ist zunächst erforderlich, dass er den Rechtsscheintatbestand kannte.[108] Ansonsten stellt sich aus dessen Sicht der Rechtsscheintatbestand als ein glücklicher Zufall dar, auf den er „blind" vertraut hat.[109] Nur bei den künstlichen Rechtsscheintatbeständen, beispielsweise dem Handelsregister, kommt es in der gesetzlichen Ausformung auf die Kenntnis des Registerinhalts beim Vertrauenden nicht an.[110]

255 Ferner muss eine Vertrauensdisposition in Form der Vornahme des Rechtsgeschäftes erfolgen.[111] Für diese Disposition muss das Vertrauen in den Rechtsscheintatbestand kausal gewesen sein.[112] Dies ist nicht der Fall, wenn das Rechtsgeschäft auch ohne den Rechtsscheintatbestand vorgenommen worden wäre.[113]

---

104 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 70.
105 *Faust*, BGB AT[3], § 26 Rn. 24.
106 *Canaris*, Vertrauenshaftung, S. 516.
107 Ebd., S. 516.
108 *Bork*[3], Rn. 1544; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 66; *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 43.
109 *Canaris*, Vertrauenshaftung, S. 507.
110 *Bork*[3], Rn. 1544; *Canaris*, Vertrauenshaftung, S. 507.
111 *Canaris*, Vertrauenshaftung, S. 511; *Rieder*, S. 95.
112 *Canaris*, Vertrauenshaftung, S. 514 f. *Spiegelhalder*, S. 167; *Bork*[3], Rn. 1544.
113 *Leptien*, in: *Soergel*[13], § 167 BGB Rn. 23.

II. Rechtsfolge der Rechtsscheinhaftung

Als Rechtsfolge der Rechtsscheinhaftung kommt sowohl die Erfüllung des positiven als auch des negativen Interesses in Betracht.[114] Das Gesetz gewährt teilweise in Fällen der bewussten Setzung des Rechtsscheintatbestandes positiven Vertrauensschutz, wie bei §§ 171 f. BGB, in anderen Fällen negativen Vertrauensschutz, beispielsweise bei § 122 BGB. 256

1. Positives Interesse

Beim positiven Vertrauensschutz erhält der Vertrauende das, was seinem Vertrauen entspricht.[115] Ein Scheinkaufmann wird beispielsweise wie ein richtiger Kaufmann behandelt.[116] Bei der Rechtsscheinvollmacht wird das Vertrauen in das Bestehen einer Vollmacht geschützt, sodass der Geschäftsgegner sich darauf berufen kann.[117] Die Rechtsscheinhaftung wirkt jedoch nur einseitig zu Gunsten des Vertrauenden.[118] 257

2. Anfechtung des Rechtsscheins: negatives Interesse

Wenn der Geschäftsherr die Möglichkeit hat, den Rechtsschein analog zu §§ 116 ff. BGB zu vernichten, kann er somit seine Haftung auf das negative Interesse beschränken (vgl. § 122 Abs. 1 BGB). Dadurch kann, wenn die Rechtsfolge des Ersatzes des positiven Interesses nicht angemessen ist, durch die Gewährung des negativen Interesses dennoch der Vertrauende geschützt werden.[119] 258

Die Möglichkeit, die Haftung auf das negative Interesse zu beschränken, steht dem Geschäftsherren nach herrschender Ansicht beim fehlenden Er- 259

114 *Canaris*, Vertrauenshaftung, S. 518; *ders.*, in: FG 50 Jahre BGH, Bd. 1, 129, 132.
115 *Canaris*, Vertrauenshaftung, S. 521; *ders.*, Handelsrecht[24], § 6 Rn. 80.
116 *K. Schmidt*, Handelsrecht[5], S. 330 f.
117 *Canaris*, Handelsrecht[24], § 14 Rn. 17; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 46.
118 *Canaris*, Vertrauenshaftung, S. 518; *Reese*, S. 49.
119 *Gerd Müller*, AcP 181 (1981), 515, 536.

klärungsbewusstsein zu.[120] Bei den Rechtsscheinvollmachten hat er diese Möglichkeit nach überwiegender Ansicht jedoch nicht.[121]

3. Wahlrecht zwischen Schein und Wirklichkeit

260 Bei jeder Form der Rechtsscheinhaftung stellt sich die Frage, ob der Vertrauende ein Wahlrecht zwischen dem Schein und der Wirklichkeit hat. Vereinzelt wird vertreten, dass der Vertrauende grundsätzlich die Wahl habe.[122] Bei den Rechtsscheinvollmachten steht dem Vertrauenden nach überwiegender Meinung jedoch kein Wahlrecht zu.[123] Beim Handelsregister[124] sowie beim Scheinkaufmann[125] hat der Vertrauende nach herrschender Ansicht die Wahl zwischen Schein und Wirklichkeit. Es ist daher für jeden Rechtsscheintatbestand gesondert zu überlegen, ob ein Wahlrecht besteht.

III. Beispiele für Rechtsscheinhaftung

261 Als Beispiel für die Rechtsscheinhaftung sollen die beiden richterrechtlich entwickelten Formen der Rechtsscheinvollmacht, die Duldungs- und die Anscheinsvollmacht, betrachtet werden. Diese beiden Formen der Rechtsscheinvollmacht werden nach einer Ansicht zur Lösung des Problems der Haftung für den Missbrauch von Zugangsdaten herangezogen. Um diese Meinungen besser einordnen zu können, werden diese beiden Formen hier allgemein betrachtet. Weitere Beispiele wie der Scheinkaufmann oder -gesellschafter werden hier nicht behandelt.[126]

---

120 Unten Rn. 472.

121 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 53; *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 45; *Leptien*, in: *Soergel*[13], § 167 BGB Rn. 22; **a.A.** *Kindl*, S. 117 f.

122 *Canaris*, Vertrauenshaftung, S. 519.

123 *BGH*, Urteil v. 20. 1. 1983, VII ZR 32/82 – BGHZ 86, 273; *Leptien*, in: *Soergel*[13], § 167 BGB Rn. 24; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 76; **a.A.** *M. Wolf/Neuner*[10], § 50 Rn. 112.

124 *Canaris*, Handelsrecht[24], § 15 Rn. 23; *W. Roth*, in: *Koller/W. Roth/Morck*[7], § 15 HGB Rn. 15 m.w.N.; **a.A.** *K. Schmidt*, Handelsrecht[5], S. 399.

125 *Joost*, in: *Ebenroth/Boujong/Joost/Strohn*[2], § 343 HGB Rn. 8; *Lettl*[2], § 2 Rn. 83.

126 Dazu *K. Schmidt*, Handelsrecht[5], S. 323 ff.; *Jung*[9], Kap. 2 Rn. 36 ff. jeweils m.w.N.

1. Duldungsvollmacht

Der nicht gesetzlich vorkommende Begriff Duldungsvollmacht muss zu- 262
nächst definiert werden.[127] Eine Bevollmächtigung durch konkludente Willenserklärung des Vertretenen ist nicht gemeint. Ist das Verhalten des Vertretenen nach dem objektiven Empfängerhorizont (§§ 133, 157 BGB) als Bevollmächtigung auszulegen, bedarf es keines Rückgriffs auf die Rechtsscheinhaftung.[128] Häufig wird die Auslegung am objektiven Empfängerhorizont (§§ 133, 157 BGB) jedoch ergeben, dass mangels Erklärungswillen keine Willenserklärung vorliegt. Dann bedarf es der Rechtsscheinhaftung, um eine Einstandspflicht des Vertretenen zu begründen. Bei der Duldungsvollmacht wird nämlich durch das Verhalten des Geschäftsherren nur der Eindruck erweckt, er habe dem Vertreter bereits in der Vergangenheit Vollmacht erteilt, nicht darauf, dass er durch die Handlung die Vollmacht erteilt.[129]

Die Duldungsvollmacht setzt voraus, dass „der Vertretene es [...] zu[lässt], 263
dass ein anderer ohne eine Bevollmächtigung als sein Vertreter auftritt, so dass Dritte daraus berechtigterweise auf das Bestehen einer Vollmacht schließen können."[130] Im Rahmen des Rechtsscheins ist ein für den Geschäftsgegner erkennbares Dulden des Auftretens eines Drittens als Vertreter erforderlich.[131] Dieses Auftreten erweckt insbesondere dann den Rechtsschein, wenn es von gewisser Dauer und Häufigkeit geprägt ist.[132] Ein einmaliges Auftreten kann jedoch ausreichen.[133]

Als Zurechnungsgrund für den Rechtsscheintatbestand kommt bei der 264
Duldungsvollmacht nur die willentliche Schaffung in Betracht.[134] Schreitet der Geschäftsherr nicht gegen das Auftreten des Dritten als Vertreter ein, ist ihm der Rechtsscheintatbestand zurechenbar.[135] Die Gutgläubigkeit so-

---

127 Zum unterschiedlichen Verständnis *Conrad*, S. 34; *Faust*, BGB AT[3], § 26 Rn. 40.
128 *Bork*[3], Rn. 1556.
129 *Canaris*, in: FG 50 Jahre BGH, Bd. 1, 129, 154; *M. Wolf/Neuner*[10], § 50 Rn. 86.
130 *BGH*, Urteil v. 21. 6. 2005, XI ZR 88/04 – NJW 2005, 2985, 2987.
131 *Bork*[3], Rn. 1550.
132 *Kindl*, S. 90; *M. Wolf/Neuner*[10], § 50 Rn. 87.
133 *OLG Karlsruhe*, Urteil v. 20. 1. 2004, 17 U 53/03 – WM 2004, 1135, 1137; *OLG Frankfurt*, Beschluss v. 16. 5. 2006, 9 U 37/05 – WM 2006, 2207, 2208; *Bork*[3], Rn. 1550; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 46.
134 *Bork*[3], Rn. 1554.
135 *M. Wolf/Neuner*[10], § 50 Rn. 88.

wie die kausale Disposition im Vertrauen auf den Rechtsscheintatbestand[136] sind wie immer erforderlich.[137]

265 Die Behauptung, dass die Duldungsvollmacht keine dogmatische Begründung habe,[138] kann nicht bestätigt werden. Zwar ist eine Herleitung aus einer analogen Anwendung der §§ 170-173 BGB[139] wegen der fehlenden Drittgerichtetheit des Verhaltens wenig überzeugend. Aus dem allgemeinen Rechtsprinzip Rechtsscheinhaftung kann die Duldungsvollmacht jedoch überzeugend hergeleitet werden.

2. *Anscheinsvollmacht*

266 Die Anscheinsvollmacht unterscheidet sich von der Duldungsvollmacht in den Voraussetzungen nur im Rahmen der Zurechnung.[140] Sie setzt nach der herrschenden Meinung[141] voraus, dass „der Vertretene das Handeln des Scheinvertreters nicht kennt, er es aber bei pflichtgemäßer Sorgfalt hätte erkennen und verhindern können."[142]

267 Gegen diese Form der Anscheinsvollmacht formiert sich vielfach Widerstand. Zahlreich wird diese Form der Anscheinsvollmacht nur für den kaufmännischen Verkehr anerkannt.[143] Daneben wird teilweise versucht durch eine Herleitung über die *culpa in contrahendo* die Haftung auf das negative Interesse zu beschränken.[144] Trotz der zahlreichen Streite rund um dogmatische Herleitung, Umfang und Anwendungsbereich der Anscheinsvollmacht, besteht grundsätzlich Einigkeit darin, dass der Geschäftsherr für das Auftreten des Scheinvertreters einzustehen hat, wenn ihm dieses zurechenbar ist.

---

136 Zu diesen allgemeinen Voraussetzungen oben Rn. 252 ff.
137 *M. Wolf/Neuner*[10], § 50 Rn. 93.
138 *Börner*, S. 70.
139 So *Schramm*, in: MüKo-BGB[6], § 167 Rn. 51.
140 *Bork*[3], Rn. 1560; *Kindl*, S. 83.
141 *BGH*, Urteil v. 12. 2. 1952, I ZR 96/51 – BGHZ 5, 111, 116; Urteil v. 5. 3. 1998, III ZR 183/96 – NJW 1998, 1854, 1855; Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 17; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 56; *H. Köhler*, BGB AT[37], § 11 Rn. 44.
142 *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 17.
143 *Canaris*, Vertrauenshaftung, S. 52; *ders.*, Handelsrecht[24], § 14 Rn. 17; *ders.*, JZ 1976, 132, 133; *ders.*, in: FG 50 Jahre BGH, Bd. 1, 129, 158; *Medicus*[10], Rn. 972; *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 31; *M. Wolf/Neuner*[10], § 50 Rn. 98.
144 *Flume*[4], § 49 4; *Medicus*[10], Rn. 971.

Der Rechtsscheintatbestand muss sich auf ein Verhalten des Vertretenen 268
beziehen. Ein Handeln des Scheinvertreters allein reicht nicht aus.[145] Das Verhalten des Vertretenen muss sich als objektiv wahrnehmbares Signal einer schon früher erteilten Vollmacht deuten lassen.[146] Es beschränkt sich häufig darauf, dass der Geschäftsherr nicht eingreift, sondern den Scheinvertreter Rechtsgeschäfte abschließen lässt, die er erfüllt.[147] Das Auftreten des Vertreters muss von gewisser Dauer und Häufigkeit sein,[148] damit sich ein schützenswertes Vertrauen des Geschäftsgegners bilden kann.

Die Zurechnung des Rechtsscheintatbestandes der Anscheinsvollmacht 269
erfolgt nach dem jeweilig vertretenen Prinzip.[149] Nach dem herrschenden Verschuldensprinzip kommt es auf das schuldhafte Nicht-Eingreifen an.[150] Der Geschäftsherr muss jedoch die Möglichkeit gehabt haben, den Rechtsschein zu zerstören.[151] Die allgemeinen Voraussetzungen der Gutgläubigkeit sowie der kausalen Disposition im Vertrauen auf den Rechtsscheintatbestand[152] sind ebenfalls erforderlich.[153]

Auf der Rechtsfolgenseite ist umstritten, welches Interesse dem Vertrau- 270
enden ersetzt wird. Überwiegend wird ihm das positive Interesse zugestanden.[154] Eine Haftung des vermeintlich Vertretenen auf das negative Interesse kommt nach zwei Ansichten in Betracht. Einer Ansicht nach, seien Konstellationen der Anscheinsvollmacht über die *culpa in contrahendo* zu lösen.[155] Eine andere Ansicht lässt die Anfechtung des Rechtsscheins bei der Anscheinsvollmacht zu.[156]

---

145 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 57.
146 *Faust*, BGB AT[3], § 26 Rn. 33.
147 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 58.
148 *M. Wolf/Neuner*[10], § 50 Rn. 96; *Hübner*[2], Rn. 1285.
149 *Conrad*, S. 37; *Faust*, BGB AT[3], § 26 Rn. 34; *Schramm*, in: MüKo-BGB[6], § 167 Rn. 59.
150 *Bork*[3], Rn. 1560.
151 *Leptien*, in: *Soergel*[13], § 167 BGB Rn. 22.
152 Dazu oben Rn. 252 ff.
153 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 66 ff.
154 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 74; *Canaris*, Vertrauenshaftung, S. 518; *Spiegelhalder*, S. 168. Nur bei grober Fahrlässigkeit *Hübner*[2], Rn. 1289.
155 So *Flume*[4], § 49 4; *Medicus*[10], Rn. 971; *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 31.
156 So *Kindl*, S. 117 f.

Missbraucht ein Dritter die Zugangsdaten des Account-Inhabers im Internet, stellt sich die Frage, ob dieser dafür in Form einer Erfüllungshaftung oder von Schadensersatz einzustehen hat. Im Folgenden soll zunächst an das Problem der Haftungsfrage herangeführt werden, um anschließend für die unterschiedlichen Formen des Missbrauchs nach einer Lösung für die rechtliche Frage der Haftung zu suchen. 271

Wird eine Willenserklärung elektronisch übermittelt, erscheint es dem Erklärungsempfänger so, als habe der Account-Inhaber sie abgegeben. Für den Erklärungsempfänger besteht keine Möglichkeit, den Handelnden, der die Willenserklärung tatsächlich abgegeben hat, zu identifizieren. Für ihn stellen sich daher die Fragen, ob ein Vertrag zustande kommt, wer sein Vertragspartner ist und ob dieser wirksam verpflichtet wurde. 272

Hat der Account-Inhaber selbst gehandelt, wird er verpflichtet. Hier werden Fälle betrachtet, bei denen die Willenserklärung nicht vom Account-Inhaber abgegeben wurde. Tritt der Dritte als Bote auf und gibt z.B. nur eine vom Account-Inhaber formulierte Willenserklärung in elektronischer Form weiter, handelt er mit Botenmacht. Der Namensträger wird dadurch rechtsgeschäftlich verpflichtet.[1] Ebenso kann er im Namen des Account-Inhabers mit Vollmacht für diesen eine Willenserklärung im Rahmen seiner Befugnisse abgeben. Beispielsweise kann ein Account-Inhaber einem Dritten seine Zugangsdaten zu einer Internet-Auktionsplattform überlassen und ihn bitten, einen Gegenstand zu ersteigern, bei dessen Auktionsende der Account-Inhaber keine Zeit hat, selbst die Gebote abzugeben. Auch in diesem Fall wird der Namensträger rechtsgeschäftlich verpflichtet.[2] Gegenstand dieser Untersuchung sind Fälle, bei denen ein Dritter die Zugangsdaten missbraucht. Das bedeutet, dass der Dritte keine oder keine so weitreichende Befugnis hatte, die Willenserklärung über den Account abzugeben. 273

Für den Geschäftsgegner sieht es auch in diesen Fällen so aus, als ob die Erklärung vom Account-Inhaber stammt. Er hat ein Interesse daran, mit diesem zu kontrahieren. Dieses Interesse verstärkt sich dadurch, dass der handelnde Dritte häufig nicht identifizierbar ist. Der Geschäftsgegner 274

1 Vgl. *Bork*[3], Rn. 1361; *M. Wolf/Neuner*[10], § 41 Rn. 40.

2 *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 6.

möchte sich daher an den ihm namentlich bekannten Account-Inhaber halten. Dieser hingegen hat die Willenserklärung weder abgegeben noch ist er mit ihrem Inhalt einverstanden. Er möchte eine Bindung vermeiden.

I. Vertragsschluss im Internet

275 Der Vertragsschluss im Internet erfolgt nach den gleichen Regeln, wie ein Vertragsschluss ohne Verwendung des Internets. Regelmäßig kommt ein Vertrag durch Angebot und Annahme (§§ 145 ff. BGB) zustande. Bei der Kommunikation mit E-Mails oder Formularen in Online-Shops im Internet ergeben sich keine Unterschiede zum klassischen Vertragsschluss, etwa durch den Austausch von Briefen.[3] Sogar eine automatische Willenserklärung, die ein Computerprogramm oder ein Automat nach einer vorher definierten Logik abgibt, ist eine vollwertige Willenserklärung im Sinne der Rechtsgeschäftslehre.[4]

276 In zahlreichen Fällen des Missbrauchs von Zugangsdaten im Internet, die die Rechtsprechung zu entscheiden hatte, erfolgte der Vertragsschluss über eine Internet-Auktionsplattform. Selbst bei diesen kommt der Vertrag ohne Abweichungen von der Grundregel durch Angebot und Annahme zustande. Eine Anwendung des § 156 BGB, der den Vertragsschluss bei Versteigerungen regelt, liegt zunächst wegen des Namens der Internet-Auktion nahe. Diese dispositive[5] Vorschrift kann in den AGB des Internetauktionshauses abbedungen sein. Selbst ohne diesen Ausschluss der Anwendung, ist sie nicht einschlägig. Es fehlt an der typischen Auktionssituation, sodass § 156 BGB nicht den Vertragsschluss herbeiführen kann.[6] Bei § 156 BGB erfolgt der Vertragsschluss durch Gebot des Bieters sowie durch den Zuschlag des Auktionators, der eine Willenserklärung ist.[7] Bei Internetauktionen wird die Auktion durch Zeitablauf beendet, was jedoch keine Willenserklärung ist.[8] Die Regelungen des § 156 BGB findet daher keine Anwendung bei dem Vertragsschluss bei Internetauktionshäusern.[9]

---

3 Dazu auch *Borges*, Verträge, S. 40 ff.
4 *H. Köhler*, AcP 182 (1982), 126, 133 f.
5 *Ellenberger*, in: *Palandt*[73], § 156 BGB Rn. 1.
6 *BGH*, Urteil v. 7. 11. 2001, VIII ZR 13/01 (ricardo.de) – BGHZ 149, 129, 133.
7 *Busche*, in: MüKo-BGB[6], § 156 Rn. 4.
8 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 139 f.; *Biallaß*, in: Internet-Auktion, 11, 22; *Striepling*, S. 6.
9 A.A.: *Wiebe/Neubauer*, in: *Hoeren/Sieber/Holznagel*, Kap. 15 Rn. 18.

Vielmehr wird der Vertrag nach den allgemeinen Regeln der §§ 145 ff. BGB geschlossen.[10] Die Ausgestaltung des Vertragsschlusses hängt von den jeweiligen AGB des Internetauktionshauses ab.[11] Diese finden zwar keine direkte Anwendung im Verhältnis zwischen den Auktionsteilnehmern, sind jedoch ausschlaggebend für die Bestimmung des Inhalts der Willenserklärungen im Rahmen der Auslegung.[12] Bei einer Ausgestaltung stellt das Freischalten der Angebotsseite das Angebot und das Höchstgebot die Annahme dar.[13] Alle Gebote werden mit der auflösenden Bedingung (§ 158 Abs. 2 BGB) versehen, dass sie erlöschen, wenn vor Auktionsende ein höheres Gebot abgegeben wird. Bei anderer Gestaltung der AGB kann das Einstellen der Angebotsseite die antizipierte Annahme späterer (An-)Gebote der Bieter sein.[14] 277

Wenn das Internetauktionshaus die Möglichkeit bietet, das Angebot vorzeitig zu beenden, ändert dies nichts an der Verbindlichkeit des Angebotes. Nur eine berechtigte Rücknahme, z.B. eine Anfechtung der Willenserklärung bei der Einstellung des Angebotes, verhindert einen Vertragsschluss mit dem Höchstbietenden.[15] Beendet der Verkäufer das Angebot zu Unrecht frühzeitig, kommt ein Vertrag mit den zu diesem Zeitpunkt Höchstbietenden zustande.[16] 278

10 *BGH*, Urteil v. 7. 11. 2001, VIII ZR 13/01 (ricardo.de) – BGHZ 149, 129, 133.

11 *OLG Nürnberg*, Urteil v. 26. 2. 2014, 12 U 336/13 – CR 2014, 316, 317; *Biallaß*, in: Internet-Auktion, 11, 23. Ausführlich zu den AGB eines Internetauktionshauses unten Rn. 405.

12 *OLG Hamm*, Urteil v. 14. 12. 2000, 2 U 58/00 – MMR 2001, 105, 107; *LG Corburg*, Urteil v. 6. 7. 2004, 22 O 43/04 – MMR 2005, 330, 331; *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 149. Zu den abweichenden Meinung unten Rn. 407.

13 *BGH*, Urteil v. 3. 11. 2004, VIII ZR 375/03 – NJW 2005, 53, 54 zu den eBay-AGB. So auch *OLG Hamm*, Urteil v. 14. 12. 2000, 2 U 58/00 – MMR 2001, 105, 107.

14 *LG Hof*, Urteil v. 26. 4. 2002, 22 S 10/02 – CR 2002, 844; *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 152. Dagegen *T. Wagner/Zenger*, MMR 2013, 343, 344.

15 *BGH*, Urteil v. 8. 6. 2011, VIII ZR 305/10 – NJW 2011, 2643, Rn. 18. Kritisch zu den Rücknahmegründen *T. Wagner/Zenger*, MMR 2013, 343, 347 f.

16 *KG Berlin*, Beschluss v. 25. 1. 2005, 17 U 72/04 – NJW 2005, 1053, 1054; *OLG Oldenburg*, Urteil v. 28. 7. 2005, 8 U 93/05 – NJW 2005, 2556, 2557. Dies geschah auch bei *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 1; *LG Dortmund*, Urteil v. 23. 12. 2008, 3 O 508/08, Rn. 5.

II. Handeln unter fremdem Namen

279 Nachdem gezeigt wurde, dass sich der Vertragsschluss im Internet nicht von anderen Vertragsschlüssen unterscheidet, soll für das Handeln unter fremdem Namen das Gleiche erfolgen. Dazu wird zunächst allgemein auf das Handeln unter fremdem Namen eingegangen, um anschließend dessen Anwendung im Internet aufzuzeigen.

1. Allgemein

280 Der Geschäftspartner hat ein schützenswertes Interesse daran zu wissen, mit wem er kontrahiert. Das Offenheitsprinzip[17] der Stellvertretung stellt dies sicher. Dieses Offenkundigkeitsprinzip führt zu zwei unterschiedlichen Fallvarianten beim Handeln unter fremdem Namen (i.w.S.).

281 Die erste Fallvariante ist das Handeln unter falscher Namensangabe. Dabei möchte der Handelnde selbst Vertragspartner werden, gibt jedoch einen falschen Namen an, was der Erklärungsempfänger auch so versteht.[18] Ist dem Erklärungsempfänger der willkürliche Name des Handelnden gleichgültig, so kommt dabei ein Eigengeschäft des Handelnden zustande. Nach dem Grundsatz *falsa demonstratio non nocet*[19] schadet die falsche Bezeichnung des Vertragspartners nicht. Ein Beispiel für dieses Handeln unter falscher Namensangabe ist der Ehemann, der unter falscher Namensbezeichnung ein im Voraus bar bezahltes Hotelzimmer für einen Seitensprung mietet.[20]

282 Die zweite Fallvariante ist das Handeln unter fremdem Namen (i.e.S.). Dabei kommt es dem Geschäftspartner entscheidend darauf an, dass der wirkliche Namensträger Vertragspartner wird.[21] Dies ist insbesondere bei Dauerschuldverhältnissen oder kreditgewährenden Geschäften der Fall. Ein Vertreter kann z.B. das Schreiben mit dem Namen des Vertretenen unter-

---

17 Das Offenheitsprinzip, auch als Offenkundigkeitsprinzip bezeichnet, ergibt sich aus dem Wortlaut des § 164 Abs. 1 BGB: „im Namen des Vertretenen". Dazu *Faust*, BGB AT[3], § 25 Rn. 1 ff.; *Bork*[3], Rn. 1377 ff. jeweils m.w.N.

18 *BGH*, Urteil v. 8. 12. 2005, III ZR 99/05 – NJW-RR 2006, 701, Rn. 12; *Medicus*[10], Rn. 907.

19 Dazu *H. Köhler*, BGB AT[37], § 9 Rn. 13 m.w.N.

20 Vgl. auch das Beispiel von *Brox/Walker*, BGB AT[37], Rn. 529.

21 *Faust*, BGB AT[3], § 25 Rn. 7.

schreiben.[22] Im Folgenden wird der Begriff Handeln unter fremdem Namen in dem engeren Sinne der zweiten Fallgruppe verwendet. Beim Handeln unter fremdem Namen finden die Stellvertretungsregeln (§§ 164 ff. BGB) entsprechend Anwendung.[23]

2. *Im Internet*

Im Internet können sich im Bezug auf das Handeln unter fremdem Namen 283
die gleichen Konstellationen abspielen wie ohne Einsatz des Internets. Das Handeln in sowie unter fremdem Namen ist ebenso möglich wie das Handeln unter falscher Namensbezeichnung oder unter fremdem Namen (i.e.S.). Das Handeln unter fremder Namensbezeichnung ist zwar mangels des persönlichen Kontaktes schwerer, aber möglich. Beispielsweise bestehen für einen Nutzer von Angeboten der Erwachsenenunterhaltung auch im Internet Möglichkeiten, die Angebote zu nutzen, ohne namentlich identifiziert zu werden. In der Offline-Welt erlaubt der persönliche Kontakt den unmittelbaren Austausch von Leistungen, wobei sich die Vertragspartner durch ihre physikalische Präsenz identifizieren können. Das Feststellen der Identität kann dabei ausbleiben, sodass ein Vertragspartner oder beide anonym bleiben können. Bei Geschäftsabschlüssen über das Internet ist ein direkter Leistungsaustausch wegen des fehlenden persönlichen Kontaktes schwerer möglich. Soll ein Besteller materielle Güter erhalten, muss er diese abholen oder sie müssen ihm zugeschickt werden, wofür eine Adresse notwendig ist. Bei virtuellen Gütern oder Dienstleistungen hingegen kann die numerische Identität des Account-Inhabers bei einem anonym angelegten Account geheim bleiben. Die zweite Hürde ist der anonyme Zahlungsvorgang, der wegen der gesetzlichen Verpflichtung von Banken die Inhaber von Konten zu identifizieren[24] möglich, aber schwer zu realisieren ist. Über einen anonymen Online-Bezahldienst[25] ist dies auch bei mangelndem persönlichen Kontakt möglich. Schaffen es die Vertragspartner unter Aufrechterhaltung von

22 Siehe *BGH*, Urteil v. 3. 3. 1966, II ZR 18/64 – BGHZ 45, 193.

23 Ebd., 195 sowie schon *RG*, Urteil v. 6. 7. 1934, II 73/34 – RGZ 145, 87. Für eine direkte Anwendung in den überwiegenden Fallkonstellationen: *Flume*[4], § 44 IV; *Pawlowski*, BGB AT[7], Rn. 708.

24 Oben Rn. 67.

25 Oben Rn. 71.

Anonymität ein Rechtsgeschäft abzuwickeln, ist das Handeln unter fremder Namensbezeichnung im Internet möglich.

284 Das Handeln unter fremdem Namen ist im Internet ebenso möglich wie in anderen Konstellationen. Schreibt ein Dritter unter Verwendung der E-Mail-Adresse eines Anderen eine Nachricht oder verwendet ein Dritter einen fremden Account zur Abgabe von Willenserklärungen, kann dieser unter dem Namen des Account-Inhabers handeln.

285 In Drei-Personen-Konstellationen, wie Internet-Auktionsplattformen, erscheinen die Accounts gegenüber den anderen Teilnehmern häufig nur als Pseudonym. Erst nach einem Vertragsschluss teilt der Authentisierungsnehmer den Vertragspartnern die Identität des jeweils anderen mit. Bei diesen pseudonymen Accounts handelt es sich ebenfalls um eine Situation des Handelns unter fremdem Namen (i.e.S.), bei der der Account-Inhaber verpflichtet werden soll. Darüber herrscht Einigkeit in Rechtsprechung[26] und Literatur.[27] Bei Accounts im Internet kann der Geschäftspartner nicht erkennen, wer handelt. Er bekommt eine elektronische Willenserklärung, die als Absender den Account-Inhaber ausweist. Im Gegensatz zu einem persönlichen Kontakt, bei dem das Handeln unter fremdem Namen auffallen könnte, hat der Geschäftsgegner im Internet unter Benutzung des gleichen Kommunikationskanals keine Möglichkeit den Handelnden zu identifizieren. Der Geschäftspartner hat daher ein Interesse daran, den Account-Inhaber zu verpflichten. Dieses Interesse verstärkt sich bei Internetauktionshäusern mit Reputationssystem. Dort können Nutzer nach abgeschlossenen Transaktionen den Geschäftspartner bewerten.[28] Sammelt ein Nutzer unter seinem Pseudonym zahlreiche positive Bewertungen, wirkt er vertrauenswürdig ge-

---

26 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 10; *OLG München*, Urteil v. 5. 2. 2004, 19 U 5114/03 – NJW 2004, 1328; *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 141; *LG Aachen*, Urteil v. 15. 12. 2006, 5 S 184/06 – NJW-RR 2007, 565; *AG Saarbrücken*, Urteil v. 15. 2. 2008, 37 C 1251/06; **a.A.** *LG Kassel*, Urteil v. 15. 4. 2008, 9 O 2539/06 – NJW-RR 2009, 781.

27 *Ellenberger*, in: *Palandt*[73], § 172 BGB Rn. 18; *Faust*, JuS 2011, 1027, 1028; *Herresthal*, K&R 2008, 705; *ders.*, in: *Taeger/Wiebe*, 21, 24; *ders.*, JZ 2011, 1171, 1172; *Kuhn*, S. 194; *Schinkels*, LMK 2011, 320461, 2 a; *Schramm*, in: MüKo-BGB[6], § 164 Rn. 45a; *Oechsler*, AcP 208 (2008), 565, 566; *Valenthin*, in: *Bamberger/H. Roth*[3], § 167 BGB Rn. 33; *Dennis Werner*, K&R 2011, 499.

28 Oben Rn. 66.

genüber neuen Geschäftspartnern. Der Geschäftsgegner hat daher ein schützenswertes Interesse, mit dem Account-Inhaber zu kontrahieren.[29]

Dieses Interesse ist nicht deswegen schutzunwürdig, weil der Account- **286**
Inhaber ein Pseudonym verwendet, das häufig ein Phantasiename ist. In der älteren Literatur wird betont, dass ein Kontrahieren mit dem Namensträger ausscheidet, wenn Phantasienamen eingesetzt werden.[30] Grund dafür sei, dass sich der Geschäftsgegner eine Vorstellung vom Namensträger machen können muss.[31] Wenn bei Internetauktionshäusern alle Nutzer grundsätzlich unter einem eindeutigen Pseudonym verkehren, kann sich der Geschäftsgegner, z.B. anhand der erhaltenen Bewertungen, eine Vorstellung vom Account-Inhaber machen.

Dieses Interesse ist schutzwürdig, soweit der objektive Empfänger davon **287**
ausgehen darf, dass er mit dem Account-Inhaber kontrahiert. Eine klare Mitteilung im Angebotstext, dass der Handelnde Vertragspartner werden soll, könnte dies hervorrufen. Nicht ausreichend hingegen ist, dass der Handelnde seine E-Mail-Adresse und Mobilfunknummer angibt.[32] Der objektive Empfänger fasst dies als Mitteilung der Kontaktdaten auf, nicht als Benennung des Vertragspartners. Er kann eine mögliche Diskrepanz zwischen dem Namensträger und dem Handelnden anhand der Kontaktdaten nicht erkennen. Denn die Identitätsdaten des Account-Inhabers werden erst nach Abschluss des Vertrags vom Plattformbetreiber offengelegt. Selbst wenn eine E-Mail-Adresse mit vollem Vor- und Nachnamen angegeben ist,[33] kann der Geschäftsgegner erst nach Vertragsschluss und somit zu spät erkennen, dass diese vom Account-Inhaber abweicht.

Darüber hinaus ist zu beachten, dass der Geschäftsgegner nur in dem **288**
Interesse, mit der als Account-Inhaber ausgewiesenen Person zu kontrahieren, geschützt ist, soweit der Account dessen Inhaber identifiziert.[34] Fallen Account-Inhaber und Namensträger auseinander, kontrahiert der Geschäfts-

---

29 *OLG München*, Urteil v. 5. 2. 2004, 19 U 5114/03 – NJW 2004, 1328; *LG Aachen*, Urteil v. 15. 12. 2006, 5 S 184/06 – NJW-RR 2007, 565; *LG Berlin*, Urteil v. 1. 10. 2003, 18 O 117/03 – NJW 2003, 3493, 3494; *LG Köln*, Urteil v. 27. 10. 2005, 8 O 15/05 – BeckRS 2006, 07259; *Oechsler*, AcP 208 (2008), 565, 567.

30 *Larenz*, in: FS Lehmann, Bd. 1, 234, 236 f.; *Lieb*, JuS 1967, 107, 108.

31 *Larenz*, in: FS Lehmann, Bd. 1, 234, 236 f.

32 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 10; **a.A.**: *LG Dortmund*, Urteil v. 23. 12. 2008, 3 O 508/08, Rn. 39.

33 Wie bei *LG Dortmund*, Urteil v. 23. 12. 2008, 3 O 508/08, Rn. 39; *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346.

34 Zur Identifikationsfunktion von Accounts im Internet, unten Rn. 595.

gegner nicht mit der Person, die im Account namentlich benannt wird, sondern mit dem Account-Inhaber, also der Person, die hinter dem Account steht.[35] Darüber hinaus weisen die AGB von Internet-Auktionsplattformen darauf hin, dass mit dem Account-Inhaber ein Vertrag geschlossen wird.[36] Diese gebieten die Geheimhaltung der Zugangsdaten und verbieten deren Weitergabe. Die Vermutung des Geschäftsgegners, dass der Account-Inhaber handelt, ist daher schützenswert.

289 Ferner wird argumentiert, dass die Erfüllung gesetzlicher Informationspflichten aus §§ 312b, 312e BGB nur gegenüber dem Account-Inhaber möglich ist.[37] Deswegen könne der Geschäftsgegner auf ein Handeln des Account-Inhabers vertrauen. Dieses Argument ist nicht zwingend. Bestellt der Handelnde über den Account des Inhabers, so werde ihn, wenn er berechtigt handelt, regelmäßig auch die an den Account-Inhaber gerichteten E-Mails mit diesen Informationen erreichen. Denkbar ist, dass er selbst Zugriff auf diese E-Mails hat oder der Account-Inhaber ihm diese weiterleitet. Ferner kann erwogen werden, dass durch das Verwenden des fremden Accounts, also auch einer fremden Anschrift (egal ob in Form von E-Mail- oder Postadresse) der Account-Inhaber als Empfangsvertreter oder -bote eingesetzt wird.

290 Sowohl das Handeln im als auch unter fremdem Namen ist in vielfältigen Konstellationen möglich. Die Verwendung eines Pseudonyms verhindert nicht die Anwendung der Grundsätze des Handelns unter fremdem Namen, wenn dem Account eine Identifikationsfunktion zukommt.

291 *Hanau* hat versucht, für Konstellationen des Handelns unter fremdem Namen mit Zugangsdaten den Begriff „Handeln unter fremder Nummer“ zu etablieren.[38] Die Begriffswahl begründet *Hanau* mit Persönliche Identifikationsnummer (PIN) bei der ec-Karte.[39] Bei diesem Beispiel wäre sogar das Handeln unter fremder Nummer noch ein zutreffender Begriff. Denn mit der ec-Karte handelt der Verwender unter einer fremden Kontonummer. In anderen Fällen ist die Bezeichnung jedoch unangebracht. Zum einen kann es auf das Authentisierungsmittel wie die PIN nicht ankommen. Das Authentisierungsmittel sieht der Geschäftsgegner nicht. Sein schützenswertes

35 *LG Kassel*, Urteil v. 15. 4. 2008, 9 O 2539/06 – NJW-RR 2009, 781.
36 *LG Aachen*, Urteil v. 15. 12. 2006, 5 S 184/06 – NJW-RR 2007, 565; *Oechsler*, AcP 208 (2008), 565, 568.
37 *Oechsler*, AcP 208 (2008), 565, 567.
38 *Hanau*, Handeln unter fremder Nummer; *ders.*, VersR 2005, 1215.
39 *Hanau*, Handeln unter fremder Nummer, S. 1, 18.

Interesse bezieht sich auf die Identität, nicht auf die Authentisierungsmethode.[40] Auf dieses kann sich daher kein Rechtsschein beziehen. Zum anderen kann das Authentisierungsmittel neben einer Nummer, ein aus Buchstaben bestehendes Passwort oder lediglich ein Gegenstand sein, dessen Besitz überprüft wird. Schon bei den von *Hanau* gewählten Beispielen wird die Ungeeignetheit des Begriffs klar. Bei einem eBay-Account[41] erfolgt die Authentisierung mittels E-Mail-Adresse und Passwort, wobei beide zwar Nummern enthalten können, Buchstaben jedoch regelmäßig im Vordergrund stehen. Entscheidend für das Vertrauen des Rechtsverkehrs ist dabei jedoch das Pseudonym des Account-Inhabers. Dieses ist jedoch keine Nummer, sondern ein frei gewählter Name. Der Begriff des „Handeln unter fremder Nummer" hat sich daher zu Recht nicht durchgesetzt.

III. Zwei- und Drei-Personen-Konstellationen

Beim Vertragsschluss über das Internet existieren unterschiedliche Konstellationen, die nachfolgend untersucht werden. Häufig authentisiert sich der Account-Inhaber gegenüber dem Authentisierungsnehmer, der gleichzeitig sein Geschäftsgegner ist. Dies ist insbesondere bei Online-Versandhändlern der Fall. Ebenso häufig fallen jedoch Authentisierungsnehmer und Geschäftsgegner auseinander. Dies ist beispielsweise bei Internet-Auktionsplattformen, der elektronischen Signatur, dem elektronischen Identitätsnachweis im neuen Personalausweis und der De-Mail der Fall. Bei der Suche nach einer überzeugenden Lösung der Haftung für den Missbrauch von Zugangsdaten im Internet wird sich zeigen, dass manche Lösungsansätze nur eine der beiden Konstellationen betrifft, andere Lösungswege hingegen sowohl für Zwei- als auch für Drei-Personen-Konstellationen Antworten liefern. **292**

40 Diesen Unterschied übersieht anscheinend auch *Oechsler*, AcP 208 (2008), 565, 566.

41 Dazu *Hanau*, Handeln unter fremder Nummer, S. 209 ff.

Kapitel 2 Die Haftung für den Missbrauch von Zugangsdaten im Internet in unterschiedlichen Konstellationen

§ 5 Haftung des Account-Inhabers bei bewusster Weitergabe der Zugangsdaten

Durch die Weitergabe der Zugangsdaten wird ein Dritter willentlich in die Position gebracht, unter dem Namen des Account-Inhabers Willenserklärungen abzugeben.[1] Diese willentliche Weitergabe begründet die Zurechnung eines etwaigen Rechtsscheins.[2] Dementsprechend existieren einige Lösungsansätze, den Account-Inhaber auf das positive Interesse des Geschäftspartners haften zu lassen, wenn er die Zugangsdaten weitergegeben hat. In der dogmatischen Begründung unterscheiden sich die Ansichten jedoch. 293

Beim Handeln über fremde Accounts im Internet finden die Stellvertretungsregeln wie beim Handeln unter fremdem Namen Anwendung.[3] Eine Bindung des Account-Inhabers an die Erklärung des Handelnden kommt somit in Betracht, wenn Vertretungsmacht bestand. Bei der Annahme die Übergabe sei eine konkludente Bevollmächtigung,[4] fällt es schwer, den Umfang der Vollmacht zu bestimmen. Nur wenn der Dritte die Vollmacht im Außenverhältnis nicht überschreitet, jedoch im Innenverhältnis strengere Vorgaben hat, kann er die Vertretungsmacht so missbrauchen, dass eine Bindung des Vertretenen entsteht.[5] Überschreitet der Dritte eine bestehende Vollmacht im Außenverhältnis kommt eine Bindung des Vertretenen nur mit dessen Zustimmung in Betracht (vgl. § 179 Abs. 1 BGB).[6] In Fällen, in denen die Übergabe nicht als konkludente Bevollmächtigung zu sehen ist oder in denen der Dritte eine bestehende Vollmacht im Außenverhältnis 294

1 Dazu oben Rn. 125.
2 Die willentliche Schaffung ist eine Fallgruppe der Zurechnung von Rechtsscheinen, dazu oben Rn. 249.
3 Oben Rn. 283.
4 In diese Richtung *Spindler*, in: Internet-Auktionen[2], Kap. 5 Rn. 128, dagegen *Herresthal*, K&R 2008, 705; *ders.*, in: *Taeger/Wiebe*, 21, 26.
5 *Faust*, BGB AT[3], § 28 Rn. 23.
6 Siehe auch *M. Wolf/Neuner*[10], § 49 Rn. 100.

überschreitet, stellt sich daher die Frage, ob der Account-Inhaber für den Missbrauch haften muss.

I. Begriff der Weitergabe

295 Entscheidende Vorfrage bei der Haftung für den Missbrauch von Zugangsdaten nach Weitergabe ist, was unter der Weitergabe verstanden wird. Bei engem Verständnis des Begriffs fallen nur Fälle darunter, bei denen der Account-Inhaber mit dem Bewusstsein, dass der Dritte die Zugangsdaten später eigenständig verwenden wird, ihm die Zugangsdaten mitteilt.[7] Bei einem weiten Verständnis der Weitergabe fallen Konstellationen darunter, bei denen der Account-Inhaber dem Dritten die Zugangsdaten nicht wissentlich mitteilt.[8] Unter Weitergabe fällt bei weitem Verständnis auch die Kenntnisnahme des Dritten durch das Lesen einer Notiz der Zugangsdaten[9] oder das Speichern in der Schlüsselbund-Verwaltung[10] des Rechners.[11] Unter die Weitergabe fällt nach keinem dieser Begriffe das Ausspähen der Zugangsdaten durch einen Phishing-Angriff.[12] Zwar gibt der Account-Inhaber die Zugangsdaten beim Phishing auch in ein Formular ein, er glaubt wegen der Täuschung jedoch sie dem Authentisierungsnehmer zur Authentisierung zu übermitteln, nicht einem Dritten zu offenbaren.

296 Bei dieser Untersuchung wird das enge Verständnis der Weitergabe zu Grunde gelegt. Bei der rechtlichen Bewertung macht es einen Unterschied, ob der Account-Inhaber dem Dritten im vollen Bewusstsein, dass dieser anschließend den Account verwenden kann und dies auch tun wird, die Zugangsdaten mitgeteilt hat, oder ob der Dritte diese durch Nachlässigkeiten des Account-Inhabers erfährt. So zeigt beispielsweise der Blick auf § 172 Abs. 1 BGB, dass eine solche Unterscheidung für die rechtliche Wertung von Bedeutung ist. Nach dem Wortlaut führt die willentliche Aushändi-

---

7 Für den engen Weitergabebegriff *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 181; *Oechsler*, AcP 208 (2008), 565, 582.

8 Für ein weites Verständnis *Borges*, Elektronischer Identitätsnachweis, S. 136; *ders.*, NJW 2011, 2400, 2403; *Sonnentag*, WM 2012, 1614, 1618; *Verse/Gaschler*, Jura 2009, 213, 215 f.

9 Dazu oben Rn. 132.

10 Dazu oben Rn. 135.

11 *Borges*, NJW 2011, 2400, 2403; *Sonnentag*, WM 2012, 1614, 1618.

12 Dazu Oben Rn. 138.

gung der Vollmachtsurkunde zu einer Zurechnung.[13] Ob § 172 Abs. 1 BGB analog auf den Fall des fahrlässigen Ermöglichens des Abhandenkommens der Vollmachtsurkunde übertragen werden kann, ist umstritten.[14] Unabhängig davon, ob beide Fälle im Ergebnis rechtlich gleich zu behandeln sind, zeigt die Unterscheidung, dass für beide Fälle andere Wertungen eine Rolle spielen. Um diese unterschiedlichen Wertungen berücksichtigen zu können, wird die Weitergabe hier eng verstanden.

II. Lösung über die Duldungsvollmacht

Ein Weg die Haftung des Account-Inhabers für den Missbrauch von Zu- **297**
gangsdaten nach deren Weitergabe zu lösen, besteht in der Anwendung der Grundsätze Rechtsscheinvollmacht in Form der Duldungsvollmacht.[15] Dieser Lösungsweg kann sowohl in Zwei- als auch in Drei-Personen-Konstellationen angewendet werden. Mit der Weitergabe der Zugangsdaten lasse es der Account-Inhaber wissentlich geschehen, dass der Dritte für ihn wie ein Vertreter auftrete und ein Geschäftsgegner nach Treu und Glauben dieses Verhalten als Bevollmächtigung verstehen könne.[16] Der Account-Inhaber hafte daher für den Rechtsschein in Form der Duldungsvollmacht.[17] In den Kategorien der Rechtsscheinhaftung getrennt bedeutet dies: Der Handelnde schafft durch die Verwendung des fremden Accounts einen Rechtsscheintatbestand. Diesen von einem Dritten geschaffenen Rechtsscheintatbestand muss sich der Handelnde zurechnen lassen, weil er ihn vorsätzlich durch die willentliche Weitergabe der Zugangsdaten hervorgerufen hat.[18]

---

13 Unten Rn. 314.

14 Unten Rn. 315.

15 Allgemein zur Duldungsvollmacht oben Rn. 262.

16 *LG Aachen*, Urteil v. 15. 12. 2006, 5 S 184/06 – NJW-RR 2007, 565.

17 *LG Aachen*, Urteil v. 15. 12. 2006, 5 S 184/06 – NJW-RR 2007, 565; *AG Saarbrücken*, Urteil v. 15. 2. 2008, 37 C 1251/06, Rn. 31; *Ellenberger*, in: *Palandt*[73], § 172 BGB Rn. 18; *Frensch*, in: *Prütting/Wegen/Weinreich*[8], § 167 BGB Rn. 41; *Hanau*, Handeln unter fremder Nummer, S. 40; *Klein*, MMR 2011, 450, 451; *Kitz*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.1 Rn. 77; *Mankowski*, CR 2007, 606, 607; *Schramm*, in: MüKo-BGB[6], § 164 Rn. 45a; *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 9. Wohl auch *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 15; *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06 – NJW 2007, 611, 612. Haftung über die Anscheinsvollmacht: *OLG Schleswig*, Beschluss v. 19. 7. 2010, 3 W 47/10 – CR 2011, 52.

18 *Mankowski*, CR 2007, 606, 607.

298 Der Hinweis, dass der Account-Inhaber bereits mit der Weitergabe der Zugangsdaten gegen die AGB des Authentisierungsnehmers wie beispielsweise eine Internet-Auktionsplattform verstoßen hat,[19] kann – sofern der Authentisierungsnehmer im Einzelfall solche AGB einsetzt – nicht direkt zur Begründung der Duldungsvollmacht herangezogen werden. Eine Pflichtverletzung gegenüber dem Authentisierungsnehmer durch den Account-Inhaber wirkt sich nicht auf das Verhältnis zum insoweit unbeteiligten Geschäftsgegner aus.[20] Die AGB des Authentisierungsnehmers können jedoch zur Ausformung des Rechtsscheintatbestandes dienen. Verbieten diese AGB die Weitergabe der Zugangsdaten und halten sich die meisten Nutzer daran, ist dies ein Indiz dafür, dass nach der Verkehrserwartung über den Account abgegebene Willenserklärungen dem Ersteller des Accounts zugerechnet werden.

299 Andere Stimmen kommen ohne[21] oder durch eine abweichende dogmatische Begründung ebenfalls zur Haftung des Account-Inhabers bei Weitergabe der Zugangsdaten. Der Begründung, dass die Zugangsdaten als Legitimationsmerkmale ein dem mehrmaligen Auftreten unter fremdem Namen gleichwürdiges Vertrauen begründen,[22] kann nicht zugestimmt werden. Der Erklärungsempfänger kann nicht erkennen, dass der Dritte handelt, sodass er kein schützenswertes Vertrauen in dessen Vertretungsmacht bilden kann. Die Anwendung der Anscheinsvollmacht[23] erscheint fernliegend. Mangels Begründung kann jedoch nur allgemein auf die Ungeeignetheit der Anscheinsvollmacht eingegangen werden.[24]

---

19 *LG Aachen*, Urteil v. 15. 12. 2006, 5 S 184/06 – NJW-RR 2007, 565; *AG Saarbrücken*, Urteil v. 15. 2. 2008, 37 C 1251/06, Rn. 31.

20 Vgl. hierzu *BGH*, Urteil v. 7. 11. 2001, VIII ZR 13/01 (ricardo.de) – BGHZ 149, 129, 135 f.: bei der Auslegung der Willenserklärung können die AGB des Plattformbetreibers subsidiär herangezogen werden.

21 *OLG München*, Urteil v. 5. 2. 2004, 19 U 5114/03 – NJW 2004, 1328, 1329.

22 So *Hanau*, Handeln unter fremder Nummer, S. 40.

23 Wie ohne weitere Begründung durch das *OLG Schleswig*, Beschluss v. 19. 7. 2010, 3 W 47/10 – CR 2011, 52.

24 Unten Rn. 378.

1. Bildschirmtext (Btx)

Dieser Lösungsweg über die Rechtsscheinvollmacht wurde bereits zum Bildschirmtext (Btx)[25] vertreten.[26] Bei Anwendung dieser Ansicht haftet der Account-Inhaber bei der Weitergabe der Zugangsdaten dem Geschäftspartner auf das positive Interesse. Diese Ansicht begründen manche Gerichte mit der Anwendung der Anscheinsvollmacht,[27] wobei die Argumente jedoch die Anwendung der allgemeinen Rechtsscheingrundsätze näher legen.[28] Stimmen der Literatur teilen die Meinung, dass der Anschlussinhaber nach den Grundsätzen der Anscheinsvollmacht hafte.[29] *Redeker* vertritt die restriktive Auffassung, dass nur im kaufmännischen Verkehr für die Weitergabe der Zugangsdaten gehaftet werde.[30] Im privaten Bereich überwiege der Schutz der Familie (Art. 6 Abs. 1 GG), sodass eine Haftung ausscheide.[31] Obwohl der Bildschirmtext-Anschluss auf eine Person registriert ist und zum Abschluss von Rechtsgeschäften dient, erfüllt er auch ein allgemeines Informationsbedürfnis, sodass bei privaten Haushalten wegen des Teilens des Anschlusses kein Rechtsscheintatbestand bezüglich des Handeln des Anschlussinhabers bestehe.[32] 300

Jedenfalls außerhalb des Btx kann diese Einschränkung nicht aufrecht erhalten werden.[33] Passwortgeschützte Accounts mit Identifikationsfunktion, wie z.B. der eBay-Account,[34] können individuell einer Person zugeordnet werden. Für die Befriedigung des Informationsbedürfnis der Familienmitglieder ist der Internetzugang, nicht jedoch die Weitergabe der Zugangsda- 301

---

25 Zur technischen Funktionsweise von Btx unten Rn. 498.

26 *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552; *LG Koblenz*, Urteil v. 17. 9. 1990, 3 S 78/90 – NJW 1991, 1360; *LG Ravensburg*, Urteil v. 13. 6. 1991, 2 S 6/91 – CR 1992, 472, 473; *Lachmann*, NJW 1984, 405, 408; *Redeker*, NJW 1984, 2390, 2394; **a.A.**: *Borsum/Hoffmeister*, NJW 1985, 1205, 1206 nur mittels eines sicheren Benutzeridentifikationssystems werde ein Rechtsschein hervorgerufen.

27 *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552; *LG Ravensburg*, Urteil v. 13. 6. 1991, 2 S 6/91 – CR 1992, 472, 473.

28 Unten Rn. 302.

29 *Lachmann*, NJW 1984, 405, 408. Dogmatisch Begründung unklar bei *Redeker*, NJW 1984, 2390, 2393.

30 Ebd., 2394.

31 Ebd., 2394.

32 Ausführlich dazu unten Rn. 508.

33 *Rieder*, S. 198. Gegen diese Ansicht im Anwendungsbereich des Btx: *Paefgen*, CR 1993, 559, 562; *Kuhn*, S. 221.

34 Dazu oben Rn. 64.

ten zu den Accounts erforderlich. Einschränkungen bei der Haftung für den Missbrauch von Zugangsdaten im familiären Bereich ergeben sich daher nicht aus Art. 6 Abs. 1 GG.

2. Kritik

302 Die Anwendung der Duldungsvollmacht stellt keine überzeugende dogmatische Herleitung der Haftung für den Missbrauch von Zugangsdaten nach deren Weitergabe dar. Der Geschäftsgegner kann nicht erkennen, dass ein Dritter gehandelt hat.[35] Er kann daher nicht darauf vertrauen, dass dieser für ihn nicht erkennbar handelnde Dritte Vertretungsmacht für den Account-Inhaber hatte.[36] Für den Rechtsscheintatbestand ist der Schein einer Vertretungsmacht daher kein geeigneter Anknüpfungspunkt. Vielmehr muss sich der Rechtsscheintatbestand darauf beziehen, ob der Erklärungsempfänger schützenswert darauf vertrauen konnte, dass der Account-Inhaber gehandelt hat.[37] Bei der Duldungsvollmacht kann zwar im Gegensatz zur Anscheinsvollmacht[38] ein erstmaliges Auftreten die Haftung begründen,[39] dies kann jedoch mangels Erkennbarkeit für den Geschäftsgegner keine Haftung begründen.[40] Schon früh erkannte das *LG Ravensburg* dies. Es bezeichnet die Haftung zwar als eine Haftung kraft Anscheinsvollmacht, es verwendet jedoch in der Begründung allgemeine Rechtsscheingrundsätze.[41]

III. Lösung über die Übertragung des Rechtsgedankens des § 172 Abs. 1 BGB

303 In Teilen der Literatur hat sich gegen die Anwendung der Duldungsvollmacht eine Ansicht gebildet, die das Ergebnis auf einer dogmatisch überzeugenderen Weise herzuleiten versucht. Die Rechtsscheinhaftung für den Missbrauch der Zugangsdaten bei deren Weitergabe lasse sich aus dem

35 *Wiebe*, Elektronische Willenserklärung, S. 426.
36 *Dörner*, AcP 202 (2002), 363, 389 f.
37 Unten Rn. 378.
38 Oben Rn. 268.
39 Oben Rn. 263.
40 *Herresthal*, K&R 2008, 705, 707; *ders.*, in: *Taeger/Wiebe*, 21, 31.
41 *LG Ravensburg*, Urteil v. 13. 6. 1991, 2 S 6/91 – CR 1992, 472, 473.

Rechtsgedanken des § 172 Abs. 1 BGB begründen.[42] Zur Veranschaulichung der Meinung soll zunächst der ursprüngliche Anwendungsbereich des § 172 Abs. 1 BGB sowie seine schrittweise Erweiterung auf die Blanketterklärungen dargestellt werden. Im Anschluss werden diese Grundsätze auf die Haftung für den Missbrauch von Zugangsdaten im Internet angewendet. Die Lösung über eine analoge Anwendung des § 172 Abs. 1 BGB kann sowohl in Zwei- als auch in Drei-Personen-Konstellationen angewendet werden.

1. Ursprünglicher Anwendungsbereich des § 172 Abs. 1 BGB

Nach § 172 Abs. 1 BGB ist derjenige, der einem Dritten eine Vollmachtsurkunde vorlegt, diesem gegenüber zur Vertretung des Ausstellers der Urkunde befugt. Es handelt sich dabei um eine gesetzlich kodifizierte Rechtsscheinhaftung.[43] 304

a) Bedeutung des § 172 Abs. 1 BGB

Zweck des § 172 Abs. 1 BGB ist es, zusammen mit § 171 Abs. 1 BGB die nach außen getragene Innenvollmacht einer Außenvollmacht gleichzusetzen.[44] Der zufällig gewählte Akt der Vollmachtskundgabe, ob sie gegenüber dem Vertreter oder dem Dritten erfolgt, soll keine Unterschiede in den Rechtsfolgen hervorrufen. Die Außenvollmacht bleibt bestehen, bis der Geschäftsherr sie gegenüber dem Dritten widerruft (§ 170 BGB). Die Rechtsscheintatbestände der §§ 171 Abs. 1, 172 Abs. 1 BGB, die durch den *actus contrarius* zerstört werden können (§§ 171 Abs. 2, 172 Abs. 2 BGB) stellen diesen Gleichlauf sicher. 305

---

42 Insbesondere *Oechsler*, AcP 208 (2008), 565 sowie auch *Faust*, BGB AT[3], § 26 Rn. 41; *Frensch*, in: *Prütting/Wegen/Weinreich*[8], § 172 BGB Rn. 8; *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 177; *Kuhn*, S. 217; *Rieder*, S. 158; *Reese*, S. 125; *Schinkels*, LMK 2011, 320461, 2 b bb; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 8; *Schramm*, in: MüKo-BGB[6], § 172 Rn. 18; *Spiegelhalder*, S. 160; *Sonnentag*, WM 2012, 1614, 1617; *Stöber*, EWiR 2011, 521. Zur Botenkonstellation: *Leible/Sosnitza*, CR 2003, 344, 347.

43 *Canaris*, Vertrauenshaftung, S. 134.

44 Motive, S. 237; *Mugdan*, S. 484; *Kindl*, S. 12 f.

306 Diese Gleichbehandlung von Außen- und Innenvollmacht überzeugt dort, wo frei zwischen den beiden Kundgabearten gewählt werden kann. Bei den „typischen Innenvollmachten“[45], in denen eine Erteilung als Außenvollmacht theoretisch oder praktisch nicht möglich ist, endet die systematische Parallele zur Außenvollmacht. Im Massenverkehr kann es daher zu unterschiedlichen Wertungen kommen.[46]

307 Zwei Grundsätze lassen sich aus den Regelungen der §§ 170 ff. BGB herauskristallisieren. Zum einen haben schriftliche Willenserklärungen wie Urkunden keinen stärkeren Vertrauenstatbestand als mündliche Erklärungen.[47] Dies wird dadurch zum Ausdruck gebracht, dass das Vertrauen in eine Vollmachtsurkunde (§ 172 Abs. 1 BGB) genauso geschützt ist, wie die mündliche Erklärung über eine bestehende Vollmacht (§ 171 Abs. 1 BGB). Zweitens handelt es sich bei den §§ 170 ff. BGB um eine Haftung für die wissentliche Schaffung eines Rechtsscheintatbestandes.[48]

b) Auslegung des § 172 Abs. 1 BGB

308 Als gesetzlich kodifizierte Rechtsscheinhaftung soll sich die Auslegung des § 172 Abs. 1 BGB anhand der Voraussetzungen der allgemeinen Rechtsscheinhaftung[49] orientieren. Die allgemeinen Voraussetzungen sind der Rechtsscheintatbestand, dessen Zurechnung, die kausale Disposition des Vertrauenden sowie dessen Schutzwürdigkeit.

aa) Rechtsscheintatbestand

309 Die Vollmachtsurkunde muss zunächst die Schriftform des § 126 Abs. 1 BGB erfüllen.[50] Sie muss daher eigenhändig mit Namensunterschrift unter-

---

45 Dieser Begriff umfasst Vollmachten, die zur Vornahme von Rechtsgeschäften mit einem unbegrenzten Personenkreis bevollmächtigen, wie die Generalvollmacht und die Prokura. Der Begriff wurde geprägt durch *Canaris*, Vertrauenshaftung, S. 33.

46 *Oechsler*, AcP 208 (2008), 565, 575.

47 *Canaris*, JZ 1976, 132.

48 *Rieder*, S. 111.

49 Oben Rn. 226.

50 *Leptien*, in: *Soergel*[13], § 172 BGB Rn. 2; *Maier-Reimer*, in: *Erman*[13], § 172 BGB Rn. 4; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 1; *Schramm*, in: MüKo-BGB[6], § 172 Rn. 2.

schrieben sein oder mittels notariell beglaubigten Handzeichens unterzeichnet werden. Diese Voraussetzung deutet der Wortlaut des § 172 Abs. 1 BGB mit der Verwendung des Begriffes „Urkunde" an. Systematisch ist daher die Gleichsetzung von Urkunde und der schriftlichen Form nach § 126 Abs. 1 BGB naheliegend. Teleologisch betrachtet stellt dies die Perpetuierung durch die Verkörperung des Willens des Geschäftsherren dar, auf das der Geschäftsgegner sein Vertrauen stützen kann.[51] Die erforderliche Schriftform erfüllt zwei wichtige Komponenten bei der Etablierung des Rechtsscheintatbestandes. Zum einen erfüllt die Schriftform die Warnfunktion, dem Unterschreibenden die Ernsthaftigkeit der Unterschrift vor Augen zu führen.[52] Der Vertrauende kann somit schützenswert von der Vollmachtsurkunde auf die Ernsthaftigkeit des Abschlusses von Rechtsgeschäften auf Seiten des Geschäftsherren vertrauen. Zum anderen hat die Schriftform darüber hinaus eine entscheidende Funktion bei der Überprüfung der Echtheit. Die Unterschrift als Teil der Handschrift einer Person ist ein für jede Person individuelles Sein-Merkmal.[53] Die Unterschrift kann zwar leicht nachgemacht werden. Fälschungen der Unterschrift können jedoch im Nachhinein aufgedeckt werden, sodass nur die Person selbst eine Vollmachtsurkunde mit der eigenhändigen Unterschrift herstellen kann. Das Schriftformerfordernis sorgt neben der Warnfunktion auch dafür, dass Vollmachtsurkunden nur schwer gefälscht werden können.

Ferner ist erforderlich, dass der Vertreter die Urschrift oder eine notarielle Ausfertigung (§ 47 BeurkG) der Vollmachtsurkunde vorlegt.[54] Eine Fotokopie oder eine beglaubigte Abschrift reicht somit nach überwiegender Meinung nicht aus. Nach anderer Ansicht soll das Vertrauen in den mittelbaren Scheintatbestand der Kopie ausreichen, jedoch nur solange der Vertreter noch im Besitz des Originals ist.[55] Die Voraussetzung, dass das Original oder eine notarielle Ausfertigung vorgelegt werden muss, entspricht schon dem natürlichen Verständnis der grammatikalischen Formulierung des § 172 Abs. 1 BGB. Erforderlich ist demnach, dass „eine Vollmachts- **310**

---

51 *Schramm*, in: MüKo-BGB[6], § 172 Rn. 2.

52 Dazu etwa *Faust*, BGB AT[3], § 8 Rn. 1.

53 Oben Rn. 116.

54 *RG*, Urteil v. 25. 4. 1934, V 32/34 – JW 1934, 2394; *BGH*, Urteil v. 15. 10. 1987, III ZR 235/86 – BGHZ 102, 60, 63; *Faust*, BGB AT[3], § 26 Rn. 28; *H. Köhler*, BGB AT[37], § 11 Rn. 40; *Leptien*, in: *Soergel*[13], § 172 BGB Rn. 4; *Maier-Reimer*, in: *Erman*[13], § 172 BGB Rn. 6; *Oechsler*, AcP 208 (2008), 565, 574; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 4; *Schramm*, in: MüKo-BGB[6], § 172 Rn. 8.

55 *Canaris*, Vertrauenshaftung, S. 509.

urkunde“ ausgehändigt wird und „*sie*“ dem Dritten vorgelegt wird. Systematisch lässt sich diese Auslegung dadurch begründen, dass für den Vertretenen die Möglichkeit bestehen muss durch Rücknahme der Vollmachtsurkunde den Rechtsschein zu zerstören (vgl. § 172 Abs. 2 BGB). Würden Kopien oder beglaubigte Abschriften für den Rechtsschein genügen, könnte der Vertreter diese Möglichkeit der Zerstörung des Rechtsscheins durch unzählige Reproduktionen der Urschrift unterlaufen. Denn diese lassen keinen Rückschluss über den Verbleib des Originals sowie über den Fortbestand der Vollmacht zu.[56] Ferner stellt diese Voraussetzung sicher, dass der Vertretene die Vollmacht wirklich bereits erteilt hat und es ihm nicht kraft Zurückhaltens des Originals an einem Erklärungswillen fehlt.[57] Teleologisch betrachtet dient diese Voraussetzung der Etablierung eines starken Rechtsscheintatbestandes. Eine Urschrift oder eine notarielle Ausfertigung erwecken mehr Vertrauen als eine Kopie oder eine beglaubigte Abschrift, weil sie physisch einmalig sind. Der Besitz einer physisch einmaligen Sache ist ein geeigneter Rechtsscheinträger, wie systematisch § 1006 Abs. 1 S. 1 BGB zeigt. Der Besitz der physisch einmaligen Vollmachtsurkunde ist ein zentraler Aspekt des Rechtsscheintatbestandes des § 172 Abs. 1 BGB

311 Darüber hinaus muss der Vertreter sowie der Umfang der Vertretungsmacht auf der Urkunde benannt sein.[58] Dieses Erfordernis wird behauptet, ohne es näher zu begründen. Aus dem Wortlaut des § 172 Abs. 1 BGB ergibt sich diese Einschränkung nicht. Diese Voraussetzung folgt jedoch aus dem Sinn und Zweck des § 172 Abs. 1 BGB. Als gesetzlich kodifizierter Rechtsscheintatbestand muss auch im Fall des § 172 Abs. 1 BGB ein schützenswertes Vertrauen auf Seiten des Geschäftsgegner vorhanden sein. Dieses kann nur bestehen, wenn die Vollmacht nicht nur schriftlich verfasst, sondern auch durch Angabe des Umfangs hinreichend bestimmt ist. Diese Voraussetzungen schränken die vielfältigen Missbrauchsmöglichkeiten einer Vollmachtsurkunde ein. Die Vollmachtsurkunde kann der Vertreter beliebig oft wieder verwenden, um den Geschäftsherrn zu verpflichten. Er kann gegenüber einer Vielzahl von Personen zahlreiche Rechtsgeschäfte im Namen des Geschäftsherren abschließen. Durch das Erfordernis des Umfangs werden seine Möglichkeiten eingeschränkt. Erteilt der Geschäfts-

---

56 *Rieder*, S. 112.

57 *Oechsler*, AcP 208 (2008), 565, 574.

58 *RG*, Urteil v. 14. 6. 1929, VII 561/28 – RGZ 124, 383, 363; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 1; *Frensch*, in: *Prütting/Wegen/Weinreich*[8], § 172 BGB Rn. 2; *Valenthin*, in: *Bamberger/H. Roth*[3], § 172 BGB Rn. 4.

herr eine sehr umfangreiche Vollmacht, erfüllt das Erfordernis, den Umfang zu bestimmen, wenigstens eine Warnfunktion. Dieses Erfordernis zeigt, dass für den Rechtsscheintatbestand eine Beschränkung der Missbrauchsmöglichkeit oder wenigstens eine Warnung vor möglichem, umfangreichem Missbrauch erforderlich ist.

Die Urkunde muss zudem echt sein,[59] also vom erkennbaren Aussteller stammen. Diese Einschränkung ist im Wortlaut des § 172 Abs. 1 BGB angedeutet. Er fordert die Aushändigung der Vollmachtsurkunde durch den Vertretenen. Es sind zwar Fälle denkbar, in denen der Vollmachtgeber die Urkunde nicht selbst ausgestellt hat. Die Tatsache, dass sie von ihm stammen muss, soll jedoch die Echtheit der Urkunde sicherstellen. Dieses Erfordernis erfüllt die allgemeine Voraussetzung eines Rechtsscheintatbestandes, dass er sich auf das Verhalten des In-Haftung-Genommenen beziehen muss.[60] Fehlt es an einer Anknüpfung an das Verhalten des Geschäftsherren, kann seine Haftung nicht begründet werden. **312**

Die Betrachtung der Ausformung des Rechtsscheintatbestandes des § 172 Abs. 1 BGB zeigt, dass er aus mehreren Komponenten besteht. Die entscheidende Komponente ist, dass der Rechtsschein von dem Besitz der physisch einmaligen Vollmachtsurkunde als Rechtsscheinträger ausgeht. Die Vollmachtsurkunde sorgt durch das Schriftformerfordernis für eine Warnfunktion und eine hohe Fälschungssicherheit. Durch das Erfordernis, dass der Umfang benannt werden muss, werden Missbrauchsmöglichkeiten eingeschränkt oder wenigstens vor ihnen gewarnt. **313**

bb) Zurechenbarkeit

Als Aushändigung wird nur die willentliche Übergabe zum Zwecke des Gebrauchmachens verstanden.[61] Diese Auslegung ergibt sich unmittelbar aus dem natürlichen Wortsinn des „Aushändigens“, das die von einem Willensentschluss getragene Besitzübertragung beinhaltet. Dass die Überga- **314**

---

59 *RG*, Urteil v. 23. 5. 1917, V 29/17 – RGZ 90, 273, 279; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 1; *Schramm*, in: MüKo-BGB[6], § 172 Rn. 3.

60 Oben Rn. 230.

61 *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13; *OLG Karlsruhe*, Urteil v. 13. 6. 2006, 1 U 22/05 – ZIP 2005, 1633, 1634; *Canaris*, Vertrauenshaftung, S. 39; *Faust*, BGB AT[3], § 26 Rn. 30; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 2; *Schramm*, in: MüKo-BGB[6], § 172 Rn. 4.

be zum Zwecke des Gebrauchmachens erfolgen muss, zeigt systematisch die Voraussetzung, dass der Vertreter die Vollmachtsurkunde vorlegen muss (§ 172 Abs. 1 a.E. BGB). Eine freiwillige Aushändigung ist systematisch betrachtet das Gegenteil einer abhandengekommenen Vollmachtsurkunde (vgl. § 935 Abs. 1 BGB), sodass eine gestohlene, verloren gegangene oder sonst abhandengekommene Vollmachtsurkunde dem Aussteller nicht zurechenbar ist.[62]

315 Das schuldhafte Ermöglichen des Abhandenkommens der Vollmachtsurkunde reicht somit nach § 172 Abs. 1 BGB nicht aus.[63] Es ist jedoch zu erwägen, § 172 Abs. 1 BGB analog bei abhandengekommenen Vollmachtsurkunden anzuwenden.[64] Dazu müssten die Voraussetzungen einer Analogie vorliegen, nämlich eine planwidrige Regelungslücke und eine vergleichbare Interessenlage.[65] Gegen das Vorliegen einer planwidrigen Regelungslücke spricht zunächst, dass in §§ 170 ff. BGB nur Rechtsscheintatbestände, die eine willentliche Schaffung des Rechtsscheins verlangen,[66] geregelt sind. Die Gesetzessystematik anderer Rechtsscheintatbestände zeigt ebenfalls, dass nur die willentliche Schaffung des Rechtsscheintatbestandes die Haftung begründet. Nach § 935 Abs. 1 BGB ist ein gutgläubiger Erwerb nur möglich, wenn der Eigentümer die Sache willentlich aus der Hand gegeben hat. Kommt die Sache abhanden, selbst aufgrund leichter Fahrlässigkeit des Eigentümers, scheidet der gutgläubige Erwerb aus. Zwar lässt die Vollmachtsurkunde ihren Aussteller erkennen, sodass ihr eine Identifikationsfunktion zukommt.[67] Dies beschreibt jedoch nur eine sachlogische Notwendigkeit bei Stellvertretungskonstellationen und dementsprechende Aus-

---

62 *Canaris*, Vertrauenshaftung, S. 38 f.; *ders.*, JZ 1976, 132, 133; *Oechsler*, AcP 208 (2008), 565, 577 sowie ohne Bezug zu § 935 Abs. 1 BGB *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13; *Frensch*, in: *Prütting/Wegen/Weinreich*[8], § 172 BGB Rn. 3; *Jauernig*, in: *Jauernig*[15], §§ 170-172 BGB Rn. 8; *Schramm*, in: MüKo-BGB[6], § 172 Rn. 5.

63 *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13, 14 f.; *Bous*, RPfleger 2006, 357, 360; *Canaris*, Vertrauenshaftung, S. 38; *ders.*, JZ 1976, 132; *Kindl*, S. 17; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 7; *M. Wolf/Neuner*[10], § 50 Rn. 78.

64 So im Ergebnis *Coing*, in: *Staudinger*[11], §§ 171-172 BGB Rn. 6; *Enneccerus/Nipperdey*[15], § 188 I 1c; *Gotthardt*, S. 48; *Hupka*, S. 174; *Isay*, S. 239; *Weinschenk*, LZ 1931, 1310, 1311 sowie jüngst *Spiegelhalder*, S. 151; *Stöber*, JR 2012, 225, 227 f.

65 Unten Rn. 329 ff.

66 *Canaris*, Vertrauenshaftung, S. 32.

67 *Stöber*, JR 2012, 225, 228.

formung des Rechtsscheintatbestandes. Eine erweiterte Zurechnung lässt sich damit nicht begründen.

316 Eine vergleichbare Interessenlage liegt ebenso nicht vor. § 172 Abs. 1 BGB hat mehrere Betroffene. Der Geschäftsgegner hat ein Interesse daran, dass auch fahrlässig abhandengekommene Vollmachtsurkunden die Vollmacht des Vertreters begründen. Der Vertretene hingegen hat ein schützenswertes Interesse, dass die Rechtsscheinhaftung auf ein angemessenes Maß reduziert ist. Der von einer unterschriebenen Urkunde ausgehende Rechtsschein ist daher nicht grenzenlos. Sie muss unter anderem echt sein.[68] Dies kann der Geschäftsgegner genau so überprüfen wie das Abhandenkommen, nämlich durch Rückfrage beim Vertretenen. Bei einem fahrlässigen Abhandenkommen besteht daher nicht die gleiche Interessenlage wie bei einer willentlichen Übergabe.

317 Die Wertungen der wertpapierrechtlichen Vorschriften des § 935 Abs. 2 BGB lässt sich nicht auf § 172 Abs. 1 BGB übertragen.[69] Der Gesetzgeber wollte durch die §§ 170 ff. BGB die Gleichstellung von Außen- und Innenvollmachten erreichen.[70] Im Massenverkehr bei „typischen Innenvollmachten" wie Generalvollmachten besteht dabei zwar ein erhöhtes Vertrauensbedürfnis.[71] Doch auch „typische Innenvollmachten", die für den Massenverkehr perpetuiert wurden, werden nicht wie Geld oder Inhaberpapiere gehandelt. Die dadurch erreichte Beschleunigung und Rechtssicherheit bedarf es bei Vertretergeschäften nicht. Die Wertung des § 935 Abs. 2 BGB kann nicht auf sie übertragen werden.

318 Eine allgemeine Risikoabgrenzung begründet die vergleichbare Interessenlage ebenfalls nicht. Der Geschäftsherr schaffe durch die Urkunde ein objektives Moment, das im Rechtsverkehr einen gewissen Schein hervorruft, sodass er dafür einzustehen habe.[72] Für diesen Rechtsschein habe der Aussteller einzustehen.[73] Diese allgemeinen Risikoabwägungen können jedoch dort nicht überzeugen, wo der Gesetzgeber – wie in § 172 Abs. 1 BGB – eine eindeutige Wertung über die Risikoverteilung getroffen hat. Diese gilt es zu respektieren.

---

68 Oben Rn. 312.
69 A.A. *Spiegelhalder*, S. 151; *Weinschenk*, LZ 1931, 1310, 1311.
70 Oben Rn. 305.
71 *Canaris*, Vertrauenshaftung, S. 33, 39; *ders.*, JZ 1976, 132, 133 f.
72 *Isay*, S. 239.
73 *Coing*, in: *Staudinger*[11], §§ 171-172 BGB Rn. 6.

319 Die vergleichbare Interessenlage lässt sich auch nicht aus einer Übertragung der Wertung des § 370 BGB schließen.[74] Selbst bei der Annahme, die Ermächtigung der Quittung gelte auch für abhandengekommene Quittungen, kann daraus kein systematischer Schluss für die Auslegung des § 172 Abs. 1 BGB gezogen werden. In dessen Wortlaut verhindert das Erfordernis des „Aushändigens" diese Interpretation. Eine analoge Anwendung des § 172 Abs. 1 BGB auf den Fall von abhandengekommenen Vollmachtsurkunden scheidet somit aus.

cc) Disposition im Vertrauen auf den Rechtsschein

320 Das Merkmal des § 172 Abs. 1 BGB, dass die Vollmachtsurkunde dem Dritten vorgelegt wird, setzt zunächst voraus, dass dem Dritten die Urkunde zur sinnlichen Wahrnehmung unmittelbar zugänglich gemacht wird.[75] Lesen muss der Dritte die Urkunde nicht.[76] Systematisch lässt sich dieses Erfordernis mit der Gleichstellung zur Mitteilung einer Innenvollmacht an einen Dritten (§ 171 Abs. 1 BGB) begründen.[77] Teleologisch betrachtet wird durch den Rechtsscheinträger der Urkunde sowie dem Vorlegen die Voraussetzungen des schützenswerten Vertrauens ausgeformt.

dd) Gutgläubigkeit des Dritten

321 Das Erfordernis der Gutgläubigkeit des Dritten ergibt sich aus dem systematischen Zusammenhang mit § 173 BGB. Dem Geschäftsgegner schadet Kenntnis sowie fahrlässige Unkenntnis bezüglich des Erlöschen der Vollmacht.[78] Dies ergibt sich aus dem Wortlaut des § 173 BGB „kennen müssen", das, systematisch betrachtet, die fahrlässige Unkenntnis erfasst (§§ 122 Abs. 2, 276 Abs. 2 BGB). Zwar verweist § 173 BGB nicht auf den

74 *Canaris*, JZ 1976, 132.

75 *RG*, Urteil v. 26. 11. 1903, VI 140/03 – RGZ 56, 63, 66; Urteil v. 10. 12. 1919, V 249/19 – RGZ 97, 273, 275; *BGH*, Urteil v. 15. 10. 1987, III ZR 235/86 – BGHZ 102, 60, 63; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 3; *Leptien*, in: *Soergel*[13], § 172 BGB Rn. 4.

76 A.A.: *Frotz*, S. 301; *Kindl*, S. 19.

77 *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 3.

78 *Schilken*, in: *Staudinger*[2009], § 173 BGB Rn. 2; *Schramm*, in: MüKo-BGB[6], § 173 Rn. 3.

Fall der ursprünglichen Unrichtigkeit der Vollmachtsurkunde. Diese Formulierung des Wortlauts ist als Redaktionsversehen anzusehen, sodass § 173 BGB (analog) auf § 172 Abs. 1 BGB angewendet werden kann.[79]

2. *Anwendung des § 172 Abs. 1 BGB auf den Missbrauch von Zugangsdaten*

Eine direkte oder entsprechende Anwendung des § 172 Abs. 1 BGB auf Fälle des Missbrauchs von Zugangsdaten im Internet ist in einigen Konstellationen möglich. Zunächst kann der Geschäftsherr dem Dritten anstatt eine Vollmachtsurkunde auszustellen, die Vollmacht in elektronischer Form erteilen. Die Voraussetzungen, dass die Vollmachtsurkunde der Schriftform nach § 126 Abs. 1 BGB genügen muss, kann nur die qualifizierte elektronische Signatur erfüllen (§ 126 Abs. 3 BGB i.V.m. § 2 Nr. 3 SigG).[80] Diese Vollmacht in elektronischer Form kann auch dem Bevollmächtigten ausgehändigt werden. Zwar kann das Aushändigen nicht in der körperlichen Form des natürlichen Wortsinnes erfolgen. Gleichwohl kann ein Versenden per E-Mail als ebenbürtig eingestuft werden. Diese E-Mail kann der Bevollmächtigte auch der sinnlichen Wahrnehmung des Dritten unmittelbar zugänglich machen. Problematisch ist jedoch, dass eine elektronische Vollmacht nicht verkörperlicht ist. Die Perpetuierungsfunktion des Schriftformerfordernisses ist erfüllt, nicht jedoch die Anforderung der physischen Einmaligkeit. Dem Geschäftsherren fehlt die systematisch bedeutende Möglichkeit wieder in Besitz der Urkunde zu gelangen (§ 172 Abs. 2 BGB) und dadurch den Rechtsschein zu zerstören. Im Internet gibt es keinen Unterschied zwischen Original und Kopie.[81] Dort sind vielmehr alle Wiedergaben einer Erklärung lediglich Kopien.[82] Ebenso wie bei § 172 Abs. 1 BGB eine Kopie nicht ausreichend für die Rechtsscheinhaftung ist,[83] reicht eine elektronische Vollmachtsurkunde nicht aus. 322

79 *RG*, Urteil v. 19. 3. 1923, V 427/22 – RGZ 108, 125, 127; *BGH*, Urteil v. 8. 11. 1984, III ZR 132/83 – NJW 1984, 730; *Enneccerus/Nipperdey*[15], § 188 I 2; *Faust*, BGB AT[3], § 26 Rn. 30, 27; *Maier-Reimer*, in: *Erman*[13], § 173 BGB Rn. 2; *Schilken*, in: *Staudinger*[2009], § 173 BGB Rn. 7.

80 So auch *Oechsler*, AcP 208 (2008), 565, 570.

81 *Roßnagel*, MMR 2002, 67, 68; *Spiegelhalder*, S. 120.

82 *Spiegelhalder*, S. 120.

83 Ebd., S. 121 sowie oben Rn. 312.

323 Ein weiterer diskutierter, jedoch kaum vorkommender Fall ist, dass die Zugangsdaten auf einer schriftlichen Urkunde übergeben werden.[84] Diese Urkunde müsste dem Geschäftsgegner auch vorgelegt werden. Allein die Verwendung der Zugangsdaten im Authentisierungsvorgang reicht dafür nicht aus. Somit scheidet auch für den unwahrscheinlichen Fall, dass der Account-Inhaber dem Handelnden die Zugangsdaten auf einer schriftlichen Urkunde ausgehändigt hat, die Anwendung des § 172 Abs. 1 BGB aus. Lediglich Vollmachts-Attributzertifikate nach § 8 Abs. 2 SigG haben eine vergleichbare Funktion wie Vollmachtsurkunden, sodass für diese § 172 Abs. 1 BGB analog angewendet werden kann.[85]

3. Analoge Anwendung des § 172 Abs. 1 BGB auf verdeckte Blanketterklärungen

324 Die Auslegung des § 172 Abs. 1 BGB hat dessen enge Voraussetzungen aufgezeigt. Angewendet auf das Internet können nur Vollmachts-Attributzertifikate diese strengen Anforderungen erfüllen. In der Rechtspraxis wurden die Voraussetzungen des § 172 Abs. 1 BGB jedoch schrittweise durch die Anwendung auf offene und verdeckte Blankette aufgelockert.

325 Ein Blankett, auch Blanko genannt, ist eine schriftliche Erklärung, die zwar eine Unterschrift enthält, bei der jedoch bewusst mindestens ein inhaltlicher Punkt unvollständig ausgefüllt ist, damit ein Dritter die offene, auch als blank bezeichnete, Stelle ausfüllen kann. Ein Beispiel für ein Blankett ist ein vom Geschäftsherrn unterschriebener Kaufvertrag, bei dem der Vertreter nach Verhandlungen mit dem Käufer noch den ausgehandelten Kaufpreis einträgt, den der Geschäftsherr im Gegensatz zu allen anderen Teilen des Vertrags offen gelassen hat. Das Ausfüllen des Blanketts wird als „Perifizierung“ bezeichnet.[86] Einhergehend mit dem Ausstellen des Blanketts ergeht regelmäßig die Erteilung einer „Ermächtigung“, das Blankett auszufüllen.[87]

326 Dogmatisch fällt die Einordnung des Blankettausfüllers schwer. Bei einer offenen Blanketterklärung erweckt der Besitz der Blankourkunde den Anschein, dass der Ausfüller eine der Vertretungsmacht ähnliche Ausfül-

84 *Hanau*, Handeln unter fremder Nummer, S. 34; *ders.*, VersR 2005, 1215, 1218.
85 *Rieder*, S. 141 ff. ihm folgend *Reese*, S. 110.
86 Begriff geprägt durch *Canaris*, Vertrauenshaftung, S. 55.
87 *Schramm*, in: MüKo-BGB[6], § 172 Rn. 14.

lungsermächtigung hat. Bei der verdeckten Blanketterklärung hingegen erscheint er dem Erklärungsempfänger als Bote. Im Ergebnis stellt sich die Blanketterklärung als arbeitsteilig erstellte Willenserklärung dar.[88]

327 Bei der abredewidrigen Ausfüllung ergibt sich das gleiche Problem, wie beim Missbrauch von Zugangsdaten im Internet, nämlich ob der Geschäftsherr durch das Handeln des Dritten rechtsgeschäftlich verpflichtet wird. Gesetzlich ist die Frage des abredewidrig ausgefüllten Blankos für Wechsel in Art. 10 WechselG und für Schecks Art. 13 ScheckG geklärt.[89] In älterer Literatur wird deren analoge Anwendung diskutiert.[90] Schecks und Wechsel bedürfen jedoch wie alle Wertpapiere einer erhöhten Umlauffähigkeit.[91] Wertpapierrechtliche Vorschriften bieten wegen dieser fundamental unterschiedlichen Interessenlage keine Grundlage für eine Analogie zu Blanketterklärungen im Bürgerlichen Recht.[92]

328 Zu erwägen ist daher, ob die abredewidrige Blankettvervollständigung über eine analoge Anwendung des § 172 Abs. 1 BGB erfolgen kann. Dies wird häufig über zwei Schritte gelöst. Dabei wird nicht nur die Analogie in mehreren Schritten begründet, sondern die tatbestandlichen Voraussetzungen werden auch schrittweise aufgeweicht.

a) Exkurs: Voraussetzungen einer analogen Anwendung

329 Bei der analogen Anwendung einer Norm auf einen anderen Fall im Rahmen der Rechtsfortbildung stellt sich die Frage, unter welchen Voraussetzungen dies möglich ist. Dazu muss zunächst eine Unvollständigkeit des Gesetzes oder der Rechtsordnung vorliegen.[93] Ob eine Unvollständigkeit im Gesetz eine Lücke darstellt, ist bei Gesetzen am Plan des historischen Gesetzgebers zu beurteilen.[94] Stellt sich heraus, dass diese Unvollständig-

88 Zum Streit zwischen Boten-, Ermächtigungs- und Vertretertheorie vgl. *Binder*, AcP 207 (2007), 155, 160 ff.; *Kindl*, S. 124 ff.; *Gerd Müller*, AcP 181 (1981), 515, 518 ff.

89 *Bork*[3], Rn. 1650.

90 *K. Feldmann*, S. 45 ff.; *P. Fischer*, S. 207 ff.

91 Dieses Bedürfnis kommt auch in § 935 Abs. 2 BGB zum Ausdruck.

92 *Canaris*, Vertrauenshaftung, S. 62; *G. Fischer*, S. 64 f.; *Kindl*, S. 129 Fn. 45; *Gerd Müller*, AcP 181 (1981), 515, 145 ff.; *Wurm*, JA 1986, 577, 581.

93 *Canaris*, Lücken im Gesetz[2], S. 25.

94 *Pawlowski*, Methodenlehre[3], Rn. 463.

keit mit dem Plan des Gesetzgebers nicht vereinbar ist, handelt es sich um eine Lücke.[95]

330 Es sind verschiedene Arten von Lücken zu unterscheiden. Bei der Gesetzeslücke,[96] auch Normlücke[97] oder Formulierungslücke[98] genannt, ist die Regelung einer Norm in sich oder im Zusammenhang mit den Gesetz, in dem sie geregelt ist, lückenhaft. Eine Gesetzeslücke liegt nur vor, wenn nach dem historischen Konzept des Gesetzgebers eine Regelung des Falls den anderen geregelten Fällen entspricht, aber nicht vorgesehen wurde.[99]

331 Die zweite Form der Lücke ist die Regelungslücke,[100] auch Wertungsmangel genannt.[101] Regelungslücken liegen vor, wenn ein Gesetz an sich abschließend ist, ein anderer Teil der Rechtsordnung dadurch jedoch eine Unvollständigkeit aufweist.[102] Dabei ist zu unterscheiden zwischen anfänglichen, bei denen der Gesetzgeber schon bei Erlass von einer Lücke ausgeht, und nachträglichen Regelungslücken, die durch Änderungen anderer Gesetze oder technologischen Fortschritt entstehen.[103] Die erste Voraussetzung ist somit eine planwidrige Regelungslücke.

332 Entscheidende Voraussetzung für die Anerkennung einer Analogie nach der Interessenjurisprudenz ist, dass das Recht ansonsten widersprüchlich wäre und dem Grundsatz der Gleichbehandlung nicht gerecht würde.[104] Der Gleichbehandlungsgrundsatz ist dabei nicht nur eine Voraussetzung für die Analogiebildung sondern auch ein Instrument zur Lückenfindung.[105] Denn häufig steht am Anfang der Überlegung eines Analogieschlusses, dass eine Regelung für einen ähnlich gelagerten Fall vorhanden ist, dessen Wertung übertragen werden soll. Entscheidend für die Gleichheit ist die Überein-

---

95 *Larenz/Canaris*[3], S. 192.
96 Ebd., S. 193.
97 *Canaris*, Lücken im Gesetz[2], S. 59; *Pawlowski*, Methodenlehre[3], Rn. 464.
98 *Zippelius*[11], S. 52.
99 *Larenz/Canaris*[3], S. 196.
100 *Canaris*, Vertrauenshaftung, S. 60; *Larenz/Canaris*[3], S. 193; *Pawlowski*, Methodenlehre[3], Rn. 467.
101 *Zippelius*[11], S. 52.
102 *Larenz/Canaris*[3], S. 196.
103 *Canaris*, Lücken im Gesetz[2], S. 135 f.; *Larenz/Canaris*[3], S. 200; *Pawlowski*, Methodenlehre[3], Rn. 470.
104 *Larenz/Canaris*[3], S. 195 f.; *Pawlowski*, Methodenlehre[3], Rn. 475.
105 *Canaris*, Lücken im Gesetz[2], S. 57; *Zippelius*[11], S. 53.

stimmung der Interessen bezüglich des Telos der Regelung.[106] Die zweite Voraussetzungen einer Analogie ist somit die vergleichbare Interessenlage.

Der Analogie verwandt ist das *argumentum a maiore ad minus*, der Erst- 333
Recht-Schluss.[107] Bei der Begründung einer Analogie ist stets auch die Möglichkeit eines *argumentum e contrario*, ein Umkehrschluss, in Betracht zu ziehen.[108] Aus der Tatsache, dass der Gesetzgeber eine Sache geregelt hat, kann bei entsprechendem gesetzgeberischen Willen geschlossen werden, dass er den nicht geregelten Fall nicht unter die Regelung fassen wollte.

b) Erster Schritt: offene Blanketterklärungen

Der erste Schritt ist die analoge Anwendung des § 172 Abs. 1 BGB auf 334
offene Blanketterklärungen. Bei einem offenen Blankett füllt der Ausfüllende dieses im Beisein des Dritten aus. Für die Analogie bedarf es einer planwidrigen Regelungslücke sowie einer vergleichbaren Interessenlage.[109] Der Fall der Blanketterklärung sowie deren abredewidrige Ausfüllung ist gesetzlich nicht geregelt. Somit liegt eine planwidrige Lücke in Form einer nachträglichen Regelungslücke[110] mangels gesetzgeberischer Regelung vor.

Ferner muss die Interessenlage vergleichbar sein. Die zentralen Merkma- 335
le des Rechtsscheintatbestandes des § 172 Abs. 1 BGB erfüllt das offene Blankett. Das Blankett ist wie die Vollmachtsurkunde ein physisch einmaliges Objekt, dessen Besitz ein starker Rechtsscheinträger ist.[111] Ferner ist durch das zu übertragende Schriftformerfordernis nicht nur die Warnfunktion, sondern durch die Unterschrift als Sein-Merkmal auch eine gewisse Fälschungssicherheit[112] erreicht.

Das offene Blankett unterscheidet sich jedoch von der Vollmachtsurkun- 336
de dadurch, dass der Dritte nicht als Vertreter genannt wird und somit der Umfang seiner Vollmacht nicht benannt ist.[113] Aus Sicht des Dritten ist

106 *Larenz/Canaris*[3], S. 202 f.
107 Ebd., S. 208.
108 *Canaris*, Lücken im Gesetz[2], S. 44; *Larenz/Canaris*[3], S. 209.
109 Oben Rn. 329 ff.
110 Oben Rn. 331.
111 Vgl. *Kindl*, S. 129; *Gerd Müller*, AcP 181 (1981), 515, 524.
112 Oben Rn. 309.
113 Dazu oben Rn. 311.

die offene Stelle im Blankett jedoch ein Indiz dafür, dass der Ausfüller eine gewisse Ausfüllungsermächtigung von dem Urkundenaussteller erhalten hat.[114] Die Anforderungen an den Rechtsscheintatbestand werden dadurch leicht abgeschwächt.[115] Eine Rechtsscheinhaftung trete beim offenen Blankett nur ein, wenn das Ausfüllen im Rahmen des Üblichen erfolgt.[116] Demgegenüber sind jedoch die Missbrauchsmöglichkeiten erheblich eingeschränkt. Da es sich beim Blankett um ein physisch einmaliges Objekt handelt, kann es nur einmal ausgefüllt werden. Im Gegensatz zur Vollmachtsurkunde kann der Dritte das offene Blankett nur für ein Rechtsgeschäft verwenden. Eine Benennung des Umfangs der Ausfüllungsermächtigung ist somit weniger entscheidend, weil der Geschäftsherr durch das Blankett bereits einen Rahmen vorgegeben hat. Diese Interessenlage ist zwar nicht identisch, die Gemeinsamkeiten sind jedoch so groß, dass sie vergleichbar sind.[117] § 172 Abs. 1 BGB kann daher analog auf offene Blanketterklärungen angewendet werden.

c) Zweiter Schritt: verdeckte Blanketterklärungen

337 Bei einer verdeckten Blanketterklärung füllt der Ausfüllende das Blankett aus, bevor er es dem Dritten übergibt. Aus dessen Sicht liegt daher eine Erklärung des Unterschreibenden vor, die der scheinbare Bote – der eigentlich Ausfüllender ist – übergibt. Die analoge Anwendung des § 172 Abs. 1 BGB wird unterschiedlich begründet.[118] Zum einen wird die analoge Anwendung des § 172 Abs. 1 BGB auf offene Blanketterklärungen analog auf die verdeckte Blanketterklärung angewandt. Bei dem verdeckten Blankett dürfe der Dritte nicht schlechter stehen als beim offenen.[119] Es soll nicht vom Zufall abhängen, ob das Blankett offen oder verdeckt ausgefüllt wor-

114 *Oechsler*, AcP 208 (2008), 565, 569; *Canaris*, Vertrauenshaftung, S. 59.
115 *Gerd Müller*, AcP 181 (1981), 515, 524.
116 *Canaris*, Vertrauenshaftung, S. 59.
117 *Oechsler*, AcP 208 (2008), 565, 569; *Wurm*, JA 1986, 577, 578.
118 *Hanau*, Handeln unter fremder Nummer, S. 34 wendet § 172 Abs. 1 BGB direkt an, geht dabei jedoch fälschlicherweise davon aus, dass „§ 172 BGB von einer Blanketturkunde [spricht]".
119 *Canaris*, Vertrauenshaftung, S. 65; *Kindl*, S. 132; *Oechsler*, AcP 208 (2008), 565, 569; *Wurm*, JA 1986, 577, 579. Einschränkend *Gerd Müller*, AcP 181 (1981), 515, 526: der Geschäftspartner dürfe jedoch nicht besser dastehen als beim offenen Blankett.

den ist. Dagegen spreche, dass die offene Blanketterklärung ein fiktiver Fall sei, der keine Rückschlüsse für den praxisrelevanten Fall der verdeckten Blanketterklärung zulasse.[120] Methodisch lässt sich jedoch auch der Erst-Recht-Schluss zu einem fiktiven Fall begründen.[121] Ferner kommen Fälle offener Blanketterklärungen in der Praxis durchaus vor.[122]

Zum anderen wird die Erfassung der verdeckten Blanketterklärungen mit **338** einer analogen Anwendung des § 172 Abs. 2 BGB begründet, ohne auf die offenen Blankette einzugehen.[123] Die Wahl des zweiten Absatzes von § 172 BGB scheint jedoch nicht mit einer abweichenden Wertung verbunden zu sein. Bei beiden Absätzen des § 172 BGB handelt es sich um zwei Seiten einer Medaille. Nach § 172 Abs. 1 BGB haftet der Aussteller der Urkunde für das Ausstellen und Aushändigen. Nach § 172 Abs. 2 BGB haftet er jedoch nur so lange, wie die Urkunde im Umlauf ist.

Vereinzelt wird die Haftung für das abredewidrig ausgefüllte Blankett aus **339** einer analogen Anwendung des § 172 Abs. 1 BGB abgelehnt.[124] Der Geschäftsherr erkenne nicht, dass es sich um ein Blankett handele, sodass er kein Vertrauen in eine bestehende Vertretungsmacht wie bei der Vollmachtsurkunde entwickeln könne.[125]

Unabhängig von dem gewählten dogmatischen Weg soll nachfolgend un- **340** tersucht werden, ob ein verdecktes Blankett entsprechend § 172 Abs. 1 BGB zu behandeln ist. Eine planwidrige Regelungslücke liegt ebenso wie beim offenen Blankett[126] in Form einer nachträglichen Regelungslücke[127] vor. Es stellt sich daher die Frage, ob die Interessenlage vergleichbar ist. Gemeinsam mit der Vollmachtsurkunde hat das verdeckte Blankett, dass von dem Besitz des Blanketts als physisch einmaliges Objekt ein starker Rechtsschein ausgeht. Ferner ist ebenso wie bei der Vollmachtsurkunde durch das zu übertragende Schriftformerfordernis nicht nur eine Warnfunktion erfüllt, sondern die Fälschung von Blanketts wird erheblich erschwert.[128] Im

120 *Reinicke/Tiedtke*, JZ 1984, 550, 552.
121 *Kindl*, S. 132.
122 Vgl. dazu die Sachverhalte von *BGH*, Urteil v. 12. 1. 1984, IX ZR 83/82 – NJW 1984, 798; Urteil v. 29. 2. 1996, IX ZR 153/95 – BGHZ 132, 119.
123 *BGH*, Urteil v. 11. 7. 1963, VII ZR 120/62 – BGHZ 40, 65, 68; Urteil v. 25. 11. 1963, II ZR 54/61 – BGHZ 40, 297, 304 f., zustimmend *Flume*[4], § 23 2 c).
124 *G. Fischer*, S. 70; *Reinicke/Tiedtke*, JZ 1984, 550, 552.
125 *Reinicke/Tiedtke*, JZ 1984, 550, 552.
126 Oben Rn. 334.
127 Oben Rn. 331.
128 Vgl. oben Rn. 309.

Gegensatz zur Vollmachtsurkunde offenbart das verdeckte Blankett weder die Vertretungssituation noch den Umfang einer Ausfüllungsermächtigung. Daher muss das verdeckte Blankett als Urkunde bereits im Kern vor der Aushändigung geschaffen sein.[129] Ein Vertragsformular[130] oder eine „Oberschrift“[131] reicht dafür nicht aus. Nur eine unterschriebene, teilweise inhaltlich offen gelassene Willenserklärung begründet den Rechtsschein. Somit ist zwar der Umfang der Ausfüllungsermächtigung für den Empfänger nicht erkennbar, das hinter dem Erfordernis stehende Prinzip ist jedoch erfüllt. Die Missbrauchsmöglichkeiten sind beim verdeckten Blankett jedoch durch zwei Aspekte beschränkt. Da das Blankett bereits im Kern geschaffen sein muss, ist der Umfang, in dem der Missbrauch erfolgen kann, nicht genau so präzise aber ähnlich wirksam beschränkt, wie bei einer Vollmachtsurkunde. Hinzu kommt, dass das physisch einmalige Blankett im Original nur einmal ausgefüllt werden kann. Ein vielfacher Missbrauch wie bei der Vollmachtsurkunde ist somit nicht möglich. § 172 Abs. 1 BGB kann somit analog auf verdecke Blanketturkunden angewendet werden.

341 Bei der Schutzwürdigkeit des Vertrauenden ist es erforderlich, dass der Geschäftsgegner nicht erkennt, dass es sich um eine Blanketturkunde handelt. Füllt er die Urkunde selbst aus, tritt wegen seiner Bösgläubigkeit keine Rechtsscheinhaftung ein.[132] Entgegen der vom *RG*[133] sowie Teilen der Literatur[134] vertretenen Meinung kommt eine Anfechtung der ausgefüllten Blanketterklärung wegen des abredewidrigen Ausfüllens nicht in Betracht.[135] Das Aushändigen des Blanketts an den Ausfüller erfolgt lediglich

129 *Gerd Müller*, AcP 181 (1981), 515, 528.

130 *BGH*, Urteil v. 10. 3. 1976, VIII ZR 210/74 – WM 1976, 507, 508.

131 *BGH*, Urteil v. 20. 11. 1990, XI ZR 107/89 – BGHZ 113, 48, 53 f. Bei einer „Oberschrift“ ist im Gegensatz zur Unterschrift das Dokument oben signiert. Die „Oberschrift“ kann nicht wie eine untenstehende Signatur die Abschlussfunktion erfüllen.

132 *BGH*, Urteil v. 12. 1. 1984, IX ZR 83/82 – NJW 1984, 798, 799; Urteil v. 29. 2. 1996, IX ZR 153/95 – BGHZ 132, 119, 128; **a.A.** *Reinicke/Tiedtke*, JZ 1984, 550, 552: Rechtsscheinhaftung höhenmäßig begrenzt auf die abredegemäße Summe.

133 *RG*, Urteil v. 25. 9. 1922, VI 78/22 – RGZ 105, 183, 185.

134 *Enneccerus/Nipperdey*[15], § 167 II 1; *Enneccerus/H. Lehmann*[15], § 191 II 3; *Gerd Müller*, AcP 181 (1981), 515, 541; *Pawlowski*, JZ 1997, 309, 312; *Reinicke/Tiedtke*, JZ 1984, 550, 552; *Siegel*, Blanketterklärung, S. 45 ff.; *ders.*, AcP 111 (1914), 1, 95; *v. Tuhr*, S. 415, 571 f.

135 *Armbrüster*, in: MüKo-BGB[6], § 119 Rn. 55; *Canaris*, Vertrauenshaftung, S. 60; *Leipold*, BGB I: Einführung und Allgemeiner Teil[7], § 23 Rn. 30; *Medicus*[10], Rn. 913; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 8; *Schramm*, in: MüKo-BGB[6], § 172

mit dem Motiv, dass dieses abredegemäß ausgefüllt wird.[136] Motivirrtümer stellen jedoch keinen Anfechtungsgrund dar.[137] Ferner sprechen ein systematischer Gegenschluss zu § 172 Abs. 2 BGB (analog) sowie der Zweck des Verkehrsschutzes durch Rechtsscheinhaftung gegen die Möglichkeit zur Anfechtung.

d) Kein dritter Schritt: Der Kreditkartenmissbrauch

Oechsler behauptet, dass beim Kreditkartenmissbrauch die Voraussetzungen des § 172 Abs. 1 BGB noch weiter aufgelockert werden: Bereits der Besitz der Kreditkarte oder sogar nur die darauf enthaltenen Informationen würden zur Rechtsscheinhaftung ausreichen.[138] Zwar ist im Telefon- oder Mail-Order-Verfahren noch nicht einmal der Besitz der Kreditkarte erforderlich, sondern lediglich das Wissen der Informationen auf der Karte reicht dabei zur Legitimation aus.[139] Dies betrifft jedoch eine vom Missbrauch von Zugangsdaten im Internet grundsätzlich verschiedene Konstellation. Beim Mail-Order-Verfahren benutzt der Dritte die Informationen auf der Kreditkarte des Inhabers, um bei einem Vertragsunternehmer eine Zahlung, die das Acquiring-Unternehmen[140] garantiert, auszulösen. Vergleichbar mit der Frage der Haftung des Missbrauchs von Zugangsdaten im Internet, wäre die Frage, ob der Karteninhaber dem Acquiring-Unternehmen für den Missbrauch nach Rechtsscheingrundsätzen haftet. Der Karteninhaber haftet jedoch nicht.[141] Es fehlt an einem mit der Vollmachtsurkunde in sei- 342

Rn. 17. Implizit auch: *BGH*, Urteil v. 11. 7. 1963, VII ZR 120/62 – BGHZ 40, 65, 68; Urteil v. 25. 11. 1963, II ZR 54/61 – BGHZ 40, 297, 304.

136 So auch *Canaris*, Vertrauenshaftung, S. 60, 66.

137 *Bork*[3], Rn. 830 m.w.N.

138 *Oechsler*, AcP 208 (2008), 565, 570.

139 *BGH*, Urteil v. 16. 4. 2002, XI ZR 375/00 – BGHZ 150, 286, 297 ff.; Urteil v. 13. 1. 2004, XI ZR 479/02 – BGHZ 157, 256, 263. Kritisch dazu *Meder*, WM 2002, 1993, 1995 f.

140 Bei Kreditkarten gibt es regelmäßig vier Beteiligte: den Kreditkarteninhaber, den Emittenten der Kreditkarte, das Acquiring-Unternehmen sowie die Vertragshändler. Früher waren Emittent und Acquiring-Unternehmen häufig eine Person, die als Kreditkartenunternehmen bezeichnet wurde. Dazu *Jungmann*, in: *Langenbucher/Bliesener/Spindler*, Kap. 6 Rn. 2 ff.; *Martinek*, in: *Schimansky/Bunte/Lwowski*[4], § 67 Rn. 2.

141 *Langenbucher*, S. 261; zustimmend *BGH*, Urteil v. 16. 4. 2002, XI ZR 375/00 – BGHZ 150, 286, 292.

ner physischen Einmaligkeit vergleichbaren Rechtsscheinträger, der einen Rechtsscheintatbestand begründen kann.[142]

343 Beim Mail-Order-Verfahren besteht eine Haftung zwischen anderen Beteiligten. Das Acquiring-Unternehmen haftet dem Vertragspartner unter den in den AGB vereinbarten Voraussetzungen. Durch die vertraglichen Vereinbarungen zwischen dem Acquiring-Unternehmen und dem Vertragspartner entsteht ein abstraktes Schuldversprechen (§ 780 BGB) in den festgelegten Fällen.[143] Ob sich die Haftung aus allgemeinen Risikoerwägungen[144] oder aus einer analogen Anwendung des § 172 Abs. 1 BGB[145] ergibt, kann hier dahinstehen. Die für den Missbrauch der Zugangsdaten entscheidende Perspektive ist die des Kreditkarteninhabers. Er haftet dem Acquiring-Unternehmen bei missbräuchlicher Verwendung im Telefon- und Mail-Order-Verfahren nicht nach Rechtsscheingrundsätzen. Die Haftung des Acquiring-Unternehmens beim Missbrauch der Kreditkarte stellt somit keinen dritten Schritt der Aufweichung der Voraussetzungen des § 172 Abs. 1 BGB dar, die zur Begründung der Haftung des Account-Inhabers beim Missbrauch der Zugangsdaten relevant wäre.

e) Analoge Anwendung des § 172 Abs. 1 BGB auf den Missbrauch von Zugangsdaten im Internet

344 Es stellt sich somit die Frage, ob der Missbrauch von Zugangsdaten im Internet über eine analoge Anwendung des § 172 Abs. 1 BGB gelöst werden kann. Da die hier untersuchte Lösung nur den Fall der rein wissensbasierten Authentisierung zu lösen versucht, beschränken sich die nachfolgenden Ausführungen auf diese Authentisierungsmethode. Dabei wird nachfolgend untersucht, ob die Voraussetzungen für eine analoge Anwendung des § 172 Abs. 1 BGB auf den Fall des Missbrauchs von Zugangsdaten im Internet erfüllt sind. Von einem dogmatischen Weg über die analoge Anwendung der analogen Anwendung des § 172 Abs. 1 BGB auf die verdeckten Blanketterklärung[146] ist Abstand zu nehmen. Weil bei der analogen Anwendung der verdeckten Blanketterklärung auf die Haftung für den Missbrauch von

142 In diese Richtung auch *Langenbucher*, S. 261.
143 *BGH*, Urteil v. 16. 4. 2002, XI ZR 375/00 – BGHZ 150, 286, 294.
144 Ebd., 297.
145 *Martinek*, in: *Schimansky/Bunte/Lwowski*[4], § 67 Rn. 40.
146 Wie ihn *Oechsler*, AcP 208 (2008), 565, 578 ff. beschreitet.

Zugangsdaten im Internet die Gefahr besteht, dass der Anwendungsfall sich zu weit von der ursprünglichen Norm entfernt, werden die Voraussetzungen der analogen Anwendung von § 172 Abs. 1 BGB, nämlich die planwidrige Regelungslücke und die vergleichbare Interessenlage,[147] geprüft. Dabei werden jedoch die Wertungen der analogen Übertragung auf das offene und verdeckte Blankett, welche Tatbestandsmerkmale verzichtbar sind, berücksichtigt. Eine planwidrige Unvollständigkeit des Gesetzes liegt in Form einer nachträglichen Regelungslücke[148] vor. Ob eine vergleichbare Interessenlage vorhanden ist, soll für den Rechtsscheintatbestand sowie für die Zurechnung untersucht werden.

aa) Rechtsscheintatbestand

Neben der planwidrigen Regelungslücke müsste eine vergleichbare Interessenlage vorliegen. Häufig wird pauschal behauptet, mit den Zugangsdaten gebe der Account-Inhaber ein Legitimationsmittel aus der Hand, das im Rechtsschein der Vollmachtsurkunde vergleichbar sei.[149] Bei dieser Behauptung trifft zwar zu, dass die Zugangsdaten den Handelnden gegenüber dem Authentisierungsnehmer legitimieren, ähnlich wie eine Vollmachtsurkunde den Vertreter legitimiert. Diese Legitimationsfunktion sagt jedoch nichts über die Stärke des Rechtsscheins aus. 345

Zunächst ist für eine vergleichbare Interessenlage entscheidend, ob von beiden Konstellationen ein ähnlich starker Rechtsschein ausgeht. Bei der Vollmachtsurkunde geht dieser Schein von dem Besitz eines physisch einmaligen Objekts aus.[150] Bei einer rein wissensbasierten Authentisierung kommt jedoch eine Besitz-Komponente nicht zum Einsatz. Dabei wird nur das Wissen um ein Geheimnis abgefragt, das unendlich teilbar ist und somit die gegenteilige Eigenschaft zur physischen Einmaligkeit besitzt. Selbst eine potentiell zu erwartende Geheimhaltung des Geheimnisses verstärkt den vom Wissen um das Geheimnis ausgehenden Rechtsschein nicht in einem vergleichbaren Maße. Wegen der unendlichen Teilbarkeit des Wissens und der fehlenden Möglichkeit des Account-Inhabers die Teilung des Wissens sowie das erstmalige In-Erfahrung-Bringen durch einen Dritten zu bemer- 346

147 Oben Rn. 329.
148 Dazu oben Rn. 331.
149 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 177; *Sonnentag*, WM 2012, 1614, 1617.
150 Oben Rn. 310.

ken, kann er das Wissen im Gegensatz zu dem Besitz an einer physisch einmaligen Sache schlechter bis gar nicht kontrollieren. Der Rechtsscheinträger des Besitzes, der entscheidender Bestandteil des Rechtsscheintatbestandes des § 172 Abs. 1 BGB ist, liegt somit beim Missbrauch von Zugangsdaten im Internet nicht vor.

347 Eine zweite entscheidende Komponente des Rechtsscheintatbestandes des § 172 Abs. 1 BGB liegt ebenfalls nicht vor: das Schriftformerfordernis.[151] Beide Funktionen, die die Schriftform bei der Vollmachtsurkunde erfüllen soll, sind beim Missbrauch von Zugangsdaten im Internet nicht gegeben. Zum einen ist eine Warnfunktion bei Accounts im Internet nicht gegeben. Sie zu erstellen, eröffnet zunächst nur die Möglichkeit zur Kontaktaufnahme.[152] Die Weitergabe der Zugangsdaten hat ebenfalls nicht eine mit einer Vollmachtsurkunde vergleichbare Warnfunktion. Denn die Unterschrift unter ein konkretes, den Unterzeichner verpflichtendes Dokument warnt ihn deutlicher vor den Konsequenzen als das einfache Mitteilen von Wissen über die Zugangsdaten. Ferner muss bei der Weitergabe kein Bezug zu einem Rechtsgeschäft bestehen. Der Account-Inhaber kann den Dritten bitten den Account auf neue Nachrichten zu überprüfen oder ihm die Zugangsdaten überlassen, damit er spezielle Funktionen des Accounts verwenden kann. Die erste Funktion des Schriftformerfordernisses erfüllen Zugangsdaten im Internet somit nicht.

348 Die zweite Funktion des Schriftformerfordernisses besteht darin, Fälschungen zu erschweren.[153] Manche Stimmen der Literatur behaupten, dass bei Accounts im Internet, die eine rein wissensbasierte Authentisierung verwenden, das Fälschungsrisiko erheblich geringer sei als bei Vollmachtsurkunden, weil das Ausspähen des Passworts viel schwieriger sei.[154] Aus zwei Gründen kann dem nicht zugestimmt werden. Zum einen kann eine Unterschrift zwar recht leicht nachgemacht werden. Die Handschrift ist jedoch ein bei jeder Person unterschiedliches Sein-Merkmal,[155] sodass es sehr schwer ist, diese nachzumachen, ohne dass die Fälschung aufgedeckt werden kann. Zugangsdaten hingegen sind ein Geheimnis, sodass ein Dritter sie mittels vielfältiger Möglichkeiten[156] in Erfahrung bringen kann. Kennt

151 Oben Rn. 309.
152 Unten Rn. 437.
153 Oben Rn. 309.
154 *Faust*, JuS 2011, 1027, 1028 f.; *Sonnentag*, WM 2012, 1614, 1617.
155 Oben Rn. 116.
156 Oben Rn. 124 ff.

der Angreifer die Zugangsdaten, kann er sie einsetzen, wie der Account-Inhaber. Für einen Dritten ist dann im Gegensatz zur Unterschrift nicht überprüfbar, dass ein Dritter gehandelt hat. Bei gefälschten Unterschriften gibt es keine Rechtsscheinhaftung, sodass diese auch nicht auf Zugangsdaten im Internet übertragen werden kann.[157] Gegen die Behauptung, das Fälschungsrisiko bei Accounts ohne Überprüfung der Identität sei geringer als bei Vollmachtsurkunden, spricht, dass diese Accounts durch einen Dritten erstellt werden können.[158] Die Echtheit eines Accounts lässt sich im Nachhinein im Gegensatz zur Unterschrift nicht überprüfen.[159] Insofern muss ein Angreifer noch nicht einmal Zugangsdaten vom Account-Inhaber ausspähen. Die zweite Funktion des Schriftformerfordernisses, eine Fälschung zu erschweren, ist ebenfalls nicht erfüllt. Ferner ist durch die fehlende Unterschrift die Rückkopplung an den Geschäftsherren abgeschwächt. Der Geschäftsherr hat bei dem Blankett durch seine Unterschrift teilweise eine Erklärung geschaffen.[160] Mit der Erstellung seines Accounts hat der Account-Inhaber im Vergleich dazu jedoch nur die Möglichkeit geschaffenen, neue Erklärungen zu abzugeben. Im Vergleich zum Blankett stellt sich dies nur als Unterschriftsmöglichkeit dar.[161] Der Account-Inhaber gibt durch das Erstellen des Accounts noch keinen Inhalt für ein oder mehrere über den Account abschließbare Rechtsgeschäfte vor. Beim Missbrauch von Zugangsdaten im Internet von Accounts, die eine rein wissensbasierte Authentisierungsmethode einsetzen, sind die zentralen Aspekte der Stärke des Rechtsscheintatbestandes des § 172 Abs. 1 BGB nicht gegeben.

Selbst die Voraussetzung, dass der Umfang der Vollmacht benannt ist, **349**
wodurch Missbrauchsmöglichkeiten eingeschränkt werden, ist beim Missbrauch von Zugangsdaten im Internet nicht in vergleichbarer Weise vorhanden. Bei der Vollmachtsurkunde wird durch die Angabe des Umfangs sichergestellt, dass einem möglichen Missbrauch durch Vertreter Grenzen gesetzt sind.[162] Bei der Vollmachtsurkunde ist ein Missbrauch somit jedoch nur im begrenzten Umfang möglich. Die offene und verdeckte Blanketterklärung zeigen, dass dieses Erfordernis auch in vergleichbarer Weise durch eine andere Gestaltung erfolgen kann. Beim offenen und verdeckten

157 *J. Münch*, NJW-CoR 4/1989, 7, 9.
158 Oben Rn. 210.
159 Unten Rn. 603.
160 *Wiebe*, Elektronische Willenserklärung, S. 434.
161 Ebd., S. 434.
162 Oben Rn. 311.

Blankett ist zwar der Umfang der Ausfüllungsmacht in der Urkunde nicht benannt, sodass ein Missbrauch in größerem Umfang möglich ist. Weil ein Blankett im Original jedoch nur einmal ausgefüllt werden kann, ist der Missbrauch nur einmalig möglich. Eine im Umfang beschränkte, mehrfach nutzbare Missbrauchsmöglichkeit ist dabei mit einer einmaligen, umfänglicheren Möglichkeit vergleichbar. Bei den Zugangsdaten im Internet ist noch nicht einmal diese in unterschiedlichen Ausprägungen mögliche Voraussetzung der Beschränkung des Missbrauchs erfüllt. Hat ein Dritter die Zugangsdaten zu einem Account im Internet, kann er die gleichen Handlungen vornehmen, wie der Account-Inhaber. Beim Blankett ist durch die Anforderung, dass die Urkunde im Kern geschaffen sein muss, ein konkretes Rechtsgeschäft im noch zu bestimmenden Umfang vorgegeben. Ein Dritter kann mit dem Account des Inhabers jedoch eine Vielzahl von Rechtsgeschäften im gleichen Umfang, wie es der Account-Inhaber könnte, vornehmen. Die Voraussetzung, dass Missbrauchsmöglichkeiten durch den Rechtsscheintatbestand eingeschränkt werden, ist somit ebenfalls nicht gegeben.

350 Bei der Vollmachtsurkunde sowie beim Blankett liegt ein eigenes Handeln des Geschäftsherren vor, das rechtsgeschäftlichen Charakter hat. Ohne diesen rechtsgeschäftlichen Charakter geht von der Urkunde kein ausreichender Rechtsschein aus.[163] Sowohl bei Vollmachtsurkunden als auch bei Blanketten gibt der Aussteller zumindest eine grobe Richtung des Rechtsgeschäfts vor. Bei der Vollmachtsurkunde schafft er eine vollständige eigene Willenserklärung mit rechtsgeschäftlichem Charakter. Bei der Blanketturkunde erstellt er zumindest einen Teil davon. Bei der Weitergabe von Zugangsdaten im Internet fehlt dieser rechtsgeschäftliche Charakter des Handelns des Account-Inhabers. Er gibt weder eine Richtung für ein mögliches Rechtsgeschäft vor, noch tritt sein Verhalten nach außen, sodass der Rechtsverkehr ein schützenswertes Vertrauen aufgrund seiner Handlung entwickeln könnte.

351 Die zentralen und nebensächlichen Anforderungen an die Stärke des Rechtsscheintatbestandes des § 172 Abs. 1 BGB sind somit beim Missbrauch von Zugangsdaten im Internet von Accounts, die eine rein wissensbasierte Authentisierung einsetzen, nicht gegeben. Nachfolgend sollen noch einige Argumente, die für eine Anerkennung eines Rechtsscheintatbestandes vorgebracht werden, relativiert oder widerlegt werden. Zunächst wird für den Rechtsscheintatbestand angeführt, dass die Missbrauchsmöglich-

163 *Canaris*, Vertrauenshaftung, S. 61, 443.

keiten der Anerkennung nicht schaden.[164] Eine Rechtsscheinhaftung für abredewidrig ausgefüllte Blanketterklärungen wäre nicht begründbar, weil bei einer teilweise offen gelassenen Willenserklärung die Missbrauchsmöglichkeiten hoch sind.[165] Ganz im Gegenteil wird die Haftung gerade mit der Gefährlichkeit der Blanketterklärung und deren Anfälligkeit für Missbrauchsmöglichkeit begründet.[166] Die Missbrauchsmöglichkeiten sprechen somit zwar nicht grundsätzlich gegen die Anerkennung einer Haftung, sagen jedoch nichts zur Vergleichbarkeit der Stärke des Rechtsscheintatbestandes aus.

Bei der Vollmachtsurkunde wird die Vertretungskonstellation ebenso wie **352**
beim Ausfüllen des offenen Blanketts vor den Augen des Geschäftsgegners deutlich. Zugangsdaten im Internet erfüllen zugleich Identifikations- und Legitimationsfunktion.[167] Bei ihrem Missbrauch kann der Erklärungsempfänger nicht erkennen, dass ein Dritter gehandelt hat. Insofern kann er kein schützenswertes Vertrauen in eine möglicherweise vorhandene Vollmacht des Dritten entwickeln, wie er es bei Vollmachtsurkunde und offenem Blankett kann. Die analoge Anwendung auf die verdeckte Blanketterklärung zeigt jedoch, dass auf die Erkennbarkeit der Drei-Personen-Konstellation verzichtet werden kann.[168]

Einzelne Stimmen der Literatur erwägen, dass der Geschäftsgegner **353**
schutzwürdiger sei, weil er das Handeln des Dritten nicht erkennen könne.[169] Zwar kann der Erklärungsempfänger der Erklärung nicht ansehen, ob der Account-Inhaber oder ein Dritter sie abgegeben hat. Dies ist jedoch nur eine Zustandsbeschreibung der Kommunikationsmodalitäten. Eine Schutzwürdigkeit begründet dies nicht. Der Erklärungsempfänger möchte ebenso wie der Account-Inhaber von den Vorteilen der schnellen Kommunikation profitieren, sodass er die Nachteile gleichfalls mit in Kauf nimmt. Ob er deswegen schutzwürdig ist, kann sich nicht aus der Zustandsbeschreibung, sondern nur aus einer angemessenen Risikoverteilung ergeben. Die entscheidende Frage ist, mit welcher Sicherheit sich der Erklärungsempfän-

---

164 *Oechsler*, AcP 208 (2008), 565, 579 sowie implizit auch *Bork*[3], Rn. 1411.

165 *Oechsler*, AcP 208 (2008), 565, 579.

166 *BGH*, Urteil v. 25. 11. 1963, II ZR 54/61 – BGHZ 40, 297, 305: „dass es allein darauf ankommt, wie der redliche Dritte, der den Blankettmißbrauch nicht kannte, die Erklärung [. . .] auffassen durfte".

167 Oben Rn. 120.

168 Vgl. oben Rn. 337.

169 *Faust*, BGB AT[3], § 26 Rn. 41; *ders.*, JuS 2011, 1027, 1028.

ger aufgrund der objektiv erkennbaren Tatsachen auf das Vorliegen einer Legitimation verlassen kann, also die Stärke des Rechtsscheintatbestandes.

354 Die angemessene Risikoverteilung solle jedoch eine analoge Anwendung des § 172 Abs. 1 BGB rechtfertigen.[170] Beide Seiten wählen das Medium inklusive der dazugehörigen Risiken. Verbraucher werden gesetzlich häufig von Risiken befreit. Von der Zurechnung einer Willenserklärung zum Kauf beim Fernabsatz kann sich ein Verbraucher, der bei einem Unternehmen kauft, ohnehin nach § 312d Abs. 1 S. 1 BGB lösen. Im Verkehr zwischen zwei Kaufleuten oder zwei Nicht-Kaufleuten untereinander hingegen sei eine einseitige Risikoauferlegung unangemessen.[171] Ohne Anerkennung einer Rechtsscheinhaftung wären Schutzbehauptungen Tür und Tor geöffnet.[172] Diese Situation des „Widerrufsrecht kraft Beweislast“ solle verhindert werden.[173] Dies begründet jedoch weder, warum Schutzbehauptungen zu verhindern sind, noch ob die Risikoverteilung anschließend angemessen ist.[174]

355 Zusammenfassend lässt sich festhalten, dass die Umstände, die den Rechtsschein bei Vollmachtsurkunden sowie Blanketten begründen, beim Missbrauch von Zugangsdaten im Internet bei einer rein wissensbasierten Authentisierung nicht vorhanden sind. Ein Rechtsscheintatbestand, der so stark ist, dass er eine analoge Anwendung des § 172 Abs. 1 BGB rechtfertigt, besteht somit insoweit nicht. Bei der noch zu untersuchenden Zwei-Faktor-Authentisierung kann sich ein abweichendes Ergebnis ergeben.[175]

bb) Zurechenbarkeit

356 Es stellt sich die Frage, ob hinsichtlich der Zurechenbarkeit zwischen der Vollmachtsurkunde und den Zugangsdaten im Internet eine vergleichbare Interessenlage besteht. Dazu sollen die beiden Komponenten der Zurechenbarkeit beleuchtet werden. Der Rechtsschein muss dem Account-Inhaber durch dessen Handeln subjektiv zurechenbar sein und er muss objektiv die Möglichkeit haben, den Rechtsschein zu verhindern.

---

170 *Oechsler*, AcP 208 (2008), 565, 579.
171 Ebd., 579.
172 Ebd., 579.
173 *Mankowski*, CR 2003, 44; *ders.*, MMR 2004, 181.
174 Dazu ausführlich unten Rn. 625 ff.
175 Siehe unten Rn. 578 ff.

Bei der subjektiven Zurechnung lässt sich die vergleichbare Interessenlage mit dem Missbrauch von Zugangsdaten im Internet begründen. Bei der Vollmachtsurkunde sowie den Blanketten muss der Geschäftsherr dem Dritten die Urkunde aushändigen. Dies entspricht der Weitergabe der Zugangsdaten durch den Account-Inhaber. Nach dem Risikoprinzip[176] stammt die willentliche Schaffung eines Rechtsscheintatbestandes aus der Sphäre des Geschäftsherren, sodass diese zurechenbar ist. Nach dem Verschuldensprinzip[177] stellt dies eine vorsätzliche Schaffung des Rechtsscheintatbestandes dar, die zurechenbar ist. 357

Vereinzelt wird einschränkend vertreten, dass die Zurechenbarkeit nur begründet ist, wenn der Account-Inhaber wenigstens Eventualvorsatz bezüglich des späteren Missbrauchs durch den Handelnden hatte.[178] Begründet wird diese Einschränkung mit dem Erfordernis des wissentlichen Schaffens eines Rechtsscheintatbestandes, wie es in §§ 170 ff. BGB gefordert wird. Der Geschäftsherr verursache den „Rechtsscheintatbestand (abredewidrig ausgefülltes Blankett) nicht in positiver Kenntnis."[179] Diese Begründung verfehlt die relevanten Aspekte der Zurechnung des Rechtsscheins. Die gesetzlichen Rechtsscheintatbestände zeigen, dass nur der Rechtsschein willentlich gesetzt werden muss, nicht jedoch die eventuell resultierende Haftung vom Vorsatz umfasst sein muss. Nach § 172 Abs. 1 BGB ist ein willentliches Aushändigen erforderlich. Der spätere Missbrauch der Vertretungsmacht ist kein Erfordernis des § 172 Abs. 1 BGB. Der systematische Blick auf den gutgläubigen Erwerb von beweglichen Sachen (§§ 932 ff. BGB) bestätigt dies. Der Rechtsschein des Besitzes (§ 1006 Abs. 1 BGB) ist zurechenbar, wenn der Eigentümer den Besitz der Sache einem anderen verschafft hat (vgl. § 935 Abs. 1 BGB). Ein voluntatives Element, dass der Eigentümer schon bei der Übertragung des unmittelbaren Besitzes mit einer späteren Veräußerung durch den neuen Besitzer rechnet, ist hingegen nicht erforderlich. Das einzig relevante Moment bei der Zurechnung des Rechtsscheins beim Missbrauch nach Weitergabe der Zugangsdaten ist daher, dass der Account-Inhaber dem Handelnden ermöglicht, sich als Account-Inhaber zu gerieren. Die Einschränkung, dass der Account-Inhaber Eventualvorsatz 358

176 Dazu oben Rn. 243.

177 Dazu oben Rn. 237.

178 *Schnell*, S. 267. Für das abredewidrig ausgefüllte Blankett: *Gerd Müller*, AcP 181 (1981), 515, 534.

179 *Gerd Müller*, AcP 181 (1981), 515, 534. *Schnell*, S. 267 begründet die Einschränkung nicht.

bezüglich eines späteren Missbrauchs haben muss, kann daher nur gerechtfertigt werden, wenn neben dem willentlichen Schaffen des Rechtsscheintatbestandes nach dem Verschuldensprinzip[180] auch die fahrlässige Schaffung des Rechtsscheintatbestandes ausreicht.

359 Ferner lässt sich ein Argument, das zur Begründung der Anscheinsvollmacht verwendet wird, fruchtbar machen. Bei der Anscheinsvollmacht ist der Rechtsschein zurechenbar, wenn jemandem eine Stellung eingeräumt wird, die typischerweise mit einer Vertretungsmacht verbunden ist.[181] Die Überlassung der Zugangsdaten ist typischerweise mit einer Vertretungsmacht verbunden. Eine Handlung über den Account könnte daher den Rechtsschein erwecken, der Account-Inhaber habe sich rechtsgeschäftlich verpflichtet.

360 Die willentliche Mitteilung der Zugangsdaten kann daher die subjektive Komponente der Zurechnung begründen. Dabei ist jedoch fraglich, was unter einer willentlichen Weitergabe zu verstehen ist. Eine explizite Mitteilung der Zugangsdaten ist jedenfalls erfasst. Problematisch ist hingegen, was unter der Weitergabe noch zu verstehen ist. Bei einem weiten Verständnis des Begriffs der Weitergabe[182] fällt auch die Kenntnisnahme des Dritten durch das Lesen einer Notiz der Zugangsdaten[183] oder das Speichern in der Schlüsselbund-Verwaltung[184] darunter. Bei dem hier zugrunde gelegtem engen Verständnis der Weitergabe[185] fällt nur die Weitergabe des Account-Inhabers an einen Dritten im Bewusstsein, dass dieser die Zugangsdaten später eigenständig nutzen wird, darunter. Offenbart der Account-Inhaber einem Angreifer im Rahmen eines Phishing-Angriffs[186] durch Täuschung die Zugangsdaten, liegt keine Weitergabe vor.

361 Eine vergleichbare Interessenlage zu § 172 Abs. 1 BGB besteht beim Missbrauch von Zugangsdaten im Internet dann, wenn der Account-Inhaber die Zugangsdaten weitergibt. Daraus lässt sich schließen, dass ein etwaiger Rechtsscheintatbestand bei Weitergabe zurechenbar ist. Davon getrennt ist die Frage, ob auch ohne Weitergabe der Zugangsdaten, ein Rechtsscheintat-

---

180 Dazu oben Rn. 237 ff.

181 *Schramm*, in: MüKo-BGB[6], § 167 Rn. 62.

182 So *Borges*, Elektronischer Identitätsnachweis, S. 136; *ders.*, NJW 2011, 2400, 2403; *Sonnentag*, WM 2012, 1614, 1618; *Verse/Gaschler*, Jura 2009, 213, 215 f.

183 Dazu oben Rn. 132.

184 Dazu oben Rn. 135.

185 Oben Rn. 295.

186 Oben Rn. 138 ff.

bestand zurechenbar ist.[187] Die analoge Anwendung des § 172 Abs. 1 BGB auf das fahrlässige Abhandenkommen der Urkunde kann dafür eine maßgebliche Wertung geben. Die Frage, ob ohne Weitergabe der Zugangsdaten eine Zurechnung in Betracht kommt, kann in die gleiche Richtung entschieden werden, ob das fahrlässige Ermöglichen des Abhandenkommens der Vollmachtsurkunde ausreicht.[188] Bei der objektiven Komponente der Zurechnung besteht somit eine vergleichbare Interessenlage.

Fraglich ist, ob auch bei der objektiven Komponente eine vergleichbare Interessenlage besteht. Objektiv muss derjenige, der den Rechtsschein geschaffen hat, die Möglichkeit haben diesen zu verhindern oder zu zerstören.[189] Bei der Vollmachtsurkunde ist die objektive Zurechnung in § 172 Abs. 2 BGB geregelt. Der Rechtsschein der Vollmachtsurkunde besteht solange, bis diese zurückgegeben ist oder für kraftlos erklärt wird. Der Geschäftsherr hat somit zum einen die Möglichkeit den Rechtsscheinträger, den Besitz an der Urkunde, wieder an sich zu nehmen. Zum anderen kann er, wenn dies scheitern sollte, die Urkunde für kraftlos erklären, sodass er in jedem Fall eine Möglichkeit hat, den Rechtsscheintatbestand zu zerstören. **362**

Diese Möglichkeiten hat der Account-Inhaber bei den Zugangsdaten nicht in gleichem Maße. Bei einer rein wissensbasierten Authentisierung erfolgt bei einer Weitergabe die Duplizierung des Wissens um die Zugangsdaten. Das Wissen um die Zugangsdaten ist nicht wie die Erklärung bei der Vollmachts- oder Blanketturkunde in einer Besitz-Komponente perpetuiert.[190] Das Wissen um die Zugangsdaten kann sich der Account-Inhaber nicht zurückholen. Es ist jedoch zu erwägen, ob die Möglichkeit, das Kennwort zu ändern, eine vergleichbare Methode ist, den Rechtsschein zu zerstören. Solange der Dritte, der das Passwort kennt, dieses nicht ändert, kann der Account-Inhaber den Zugang des Dritten zum Account unterbinden. Dazu hat der Account-Inhaber aber erst Anlass, wenn er von dem ersten Missbrauch erfährt. Ändert der Dritte das Kennwort und womöglich auch die E-Mail-Adresse, über die ein vergessenes Kennwort geändert werden kann, so hat der Account-Inhaber nur schwer die Möglichkeit den Rechtsschein zu unterbinden.[191] Dies stellt einen großen Unterschied zur Interessenlage bei der Vollmachtsurkunde dar. Der Geschäftsherr kann, falls **363**

187 Dazu unten Rn. 671 ff.
188 Dazu oben Rn. 315.
189 Oben Rn. 246.
190 Zur Bedeutung der Perpetuierungsfunktion *Oechsler*, AcP 208 (2008), 565, 577.
191 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 177.

er den Besitz der Vollmachtsurkunde vom Vertreter nicht zurückerlangen kann, den Rechtsschein durch Kraftloserklärung verhindern. Eine vergleichbare Interessenlage zwischen § 172 Abs. 1 BGB und dem Missbrauch von Zugangsdaten im Internet besteht somit bezüglich der objektiven Zurechnungskomponente nicht.

f) Zwischenergebnis

364 Eine analoge Anwendung des § 172 Abs. 1 BGB auf den Missbrauch von Zugangsdaten im Internet kommt somit bezüglich Accounts, die auf eine rein wissensbasierte Authentisierung setzen, nicht in Betracht.

4. Zwischenergebnis

365 Die Haftung für den Missbrauch von Zugangsdaten im Internet kann nach deren Weitergabe daher nicht überzeugend durch eine analoge Anwendung des § 172 Abs. 1 BGB begründet werden, da deren Voraussetzungen nicht vorliegen. Eine vergleichbare Interessenlage bezüglich des Rechtsscheintatbestandes besteht nicht. Zwar zeigt die analoge Anwendung auf verdeckte Blanketterklärungen, dass auf die Erkennbarkeit des Handelnden verzichtet werden kann.[192] Die wesentlichen Elemente des Rechtsscheins der Vollmachtsurkunde sind jedoch bei Zugangsdaten im Internet nicht gegeben.[193] Werden lediglich die Wertungen der Zurechenbarkeit übertragen, entsteht dadurch eine Rechtsscheinhaftung ohne Rechtsscheintatbestand.[194] Bei der Zurechenbarkeit besteht zwar im Hinblick auf das Handeln des Account-Inhabers eine vergleichbare Interessenlage.[195] Mangels vergleichbarer Möglichkeiten den Rechtsschein zu zerstören, ist nicht einmal bezüglich der Zurechenbarkeit eine vergleichbare Interessenlage vorhanden.[196]

192 Oben Rn. 352.
193 Oben Rn. 345 ff.
194 Dies wird ebenfalls der Lösung über die Anscheinsvollmacht vorgeworfen, unten Rn. 380.
195 Oben Rn. 357.
196 Oben Rn. 362.

IV. Zwischenergebnis

366 Die Haftung für Missbrauch von Zugangsdaten im Internet kann weder durch die Duldungsvollmacht noch durch analoge Anwendung des § 172 Abs. 1 BGB überzeugend gelöst werden. Die Duldungsvollmacht passt strukturell nicht auf die Konstellation der Zugangsdaten im Internet, weil das Handeln des Dritten nicht erkennbar wird.[197] Die analoge Anwendung des § 172 Abs. 1 BGB scheitert an einer Vergleichbarkeit der Stärke der Rechtsscheintatbestände.[198]

367 Bei Weitergabe der Zugangsdaten besteht eine im Ergebnis bisher unbestrittene Meinung, dass der Account-Inhaber auch bei einer rein wissensbasierten Authentisierungsmethode für den Missbrauch der Zugangsdaten hafte. Diese Meinung steht – wie noch zu zeigen sein wird – im Widerspruch zu den Ansichten bei Konstellationen ohne Weitergabe der Zugangsdaten.[199] Im Laufe der weiteren Untersuchung wird gezeigt, dass man die Haftung für den Missbrauch von Zugangsdaten sowohl mit und ohne deren Weitergabe überzeugend über die allgemeine Rechtsscheinhaftung lösen kann.[200]

368 Der Geschäftsgegner des Account-Inhabers ist selbst, wenn eine Rechtsscheinhaftung scheitert, nicht schutzlos gestellt. Insbesondere in Zwei-Personen-Konstellationen, in denen eine vertragliche Vereinbarung zwischen dem Geschäftsgegner und dem Account-Inhaber besteht, dürften vertragliche Ansprüche regelmäßig einschlägig sein.[201]

197 Oben Rn. 302.
198 Oben Rn. 344 ff.
199 Dazu ausführlich unten Rn. 667.
200 Unten Rn. 489 ff.
201 Zur Lösung über die vertraglichen Beziehungen unten Rn. 397.

§ 6 Haftung des Account-Inhabers ohne bewusste Weitergabe der Zugangsdaten

Im Gegensatz zur Weitergabe der Zugangsdaten hat der Handelnde bei Konstellationen ohne deren Weitergabe die Zugangsdaten nicht vom Account-Inhaber erhalten. Die Weitergabe wird hier eng verstanden als bewusste Mitteilung der Zugangsdaten an einen Dritten im Bewusstsein, dass dieser die Zugangsdaten eigenständig verwenden wird.[1] Der Handelnde hat die Zugangsdaten vielmehr auf einem der zahlreichen Wege zum Erlangen der Zugangsdaten[2] bekommen. Häufig bemerkt der Account-Inhaber den Missbrauch der Zugangsdaten erst, wenn er von einem Geschäftsgegner in Anspruch genommen wird. Dabei kommt es häufig zum Streit, ob der Account-Inhaber durch die Handlung des Dritten wirksam verpflichtet wurde. Nachfolgend werden die unterschiedlichen Lösungen untersucht, nach denen sich die Haftung des Account-Inhabers in diesen Konstellationen richten kann. Dabei werden zunächst verschiedene in Literatur und Rechtsprechung vertretene Lösungsansätze untersucht und bewertet, um zum Schluss einen überzeugenden Lösungsweg aufzuzeigen. 369

I. Lösung über die Anscheinsvollmacht

Bei der Haftung bei Weitergabe der Zugangsdaten wird teilweise eine Lösung über die Duldungsvollmacht vertreten.[3] Diese Lösung führt bei der Haftung ohne Weitergabe der Zugangsdaten konsequenterweise zu einer Anwendung der Anscheinsvollmacht. Eine Lösung über die Anscheinsvollmacht bietet eine Antwort auf die Frage der Haftung des Account-Inhabers bei Missbrauch seiner Zugangsdaten sowohl in Zwei- als auch in Drei-Personen-Konstellationen. Bei der Anwendung kommen die Vertreter des Lösungswegs über die Anscheinsvollmacht jedoch zu unterschiedlichen Ergebnissen. Einige bejahen eine Rechtsscheinhaftung bei einer rein 370

1 Oben Rn. 295.
2 Oben Rn. 124 ff.
3 Oben Rn. 297.

wissensbasierten Authentisierung.[4] Die überwiegende Rechtsprechung[5] sowie zahlreiche Stimmen in der Literatur[6] lehnen in dieser Konstellation im Ergebnis die Rechtsscheinhaftung ab. Nachfolgend sollen für den Rechtsscheintatbestand und dessen Zurechnung die Herleitungswege, über die diese Ergebnisse zustande kommen, aufgezeigt und bewertet werden.

1. Rechtsscheintatbestand

371 Zum Rechtsscheintatbestand lassen sich Überlegungen zu verschiedenen Aspekten finden. Neben dem Sicherheitsstandard im Internet spielen Erwägungen zur angemessenen Verteilung des Risikos sowie zu der allgemeinen Voraussetzung des wiederholten und häufigen Auftretens des Vertreters eine Rolle.

a) Sicherheitsstandard im Internet

372 Das häufigste Argument zur Verneinung des Rechtsscheintatbestandes ist der pauschale Verweis darauf, dass der kontemporäre Sicherheitsstandard im Internet keine Gewähr dafür biete, dass der Account-Inhaber handelt.[7]

---

4 *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518; *Wenn*, CR 2006, 137, 138; *Härting/Strubel*, BB 2011, 2188, 2189; *Härting*[4], Rn. 562 ff.

5 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346; *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813; *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06 – NJW 2007, 611; *OLG Bremen*, Beschluss v. 21. 6. 2012, 3 U 1/12 – MMR 2012, 593, 594; *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255; Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179; *LG Gießen*, Beschluss v. 6. 3. 2013, 1 S 337/12 (nicht veröffentlicht); *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05; *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002, 127.

6 *Hanau*, Handeln unter fremder Nummer, S. 52, 213 f.; *Holzbach/Süßenberger*, in: *Moritz/Dreier*[2], C Rn. 127; *Klees/Keisenberg*, MDR 2011, 1214, 1217; *Klein*, MMR 2011, 450, 450; *Kitz*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.1 Rn. 78; *Lilja*, NJ 2011, 427; *T. Stadler*, jurisPR-ITR 14/2011, Anm. 2; *Schramm*, in: MüKo-BGB[6], § 164 Rn. 45a.

7 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18; *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676, 1677; *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 181; *LG Gießen*, Beschluss v. 6. 3. 2013, 1 S 337/12 (nicht veröffentlicht); *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002,

Dieser biete wegen der vielfältigen Möglichkeiten des Ausspähens von Zugangsdaten[8] keine hinreichende Sicherheit dafür, dass unter einem registrierten Mitgliedsnamen ausschließlich der tatsächliche Inhaber auftritt. Das *LG Bonn* präzisiert diese Aussage, in dem es auf den „Stand der Verschlüsselungsmöglichkeiten" abstellt.[9] Missbrauchsmöglichkeiten stellen jedoch die grundsätzliche Eignung als Rechtsscheintatbestand nicht in Frage.[10] Vielmehr ist zu untersuchen, zu welchem Grad die verwendeten Authentisierungsmethoden sicherstellen, dass der Account-Inhaber selbst gehandelt hat.[11]

Gegen das Vorliegen eines Rechtsscheintatbestandes spreche darüber hin- 373
aus, dass die kennwortgeschützte Erklärung als solche kein einheitlicher Sicherheitsstandard sei.[12] Was ein Passwort ist, sei nicht festgelegt. Jeder könne auf seiner Internetseite Nutzer zur Eingabe von Passwörtern auffordern und deren Eingabe später verlangen.[13] Dabei existieren für Seiten keine rechtlich verbindlichen Vorgaben für Sicherheitsstandards.[14] Der Authentisierungsnehmer kann jede noch so unsichere Buchstaben- und Ziffernkombination zulassen. Er kann selbst entscheiden, wie sicher er die abverlangten Passwörter technisch vor dem Angriff von außenstehenden Dritten sichert und ab welcher Länge und Kombination von Buchstaben und Ziffern er ein Passwort akzeptiert. GMX, der Authentisierungsnehmer im vom *LG Bonn* zu entscheidenden Fall, habe in seinen AGB darauf hingewiesen, dass er den Schutz der übertragenen Daten nicht gewährleisten könne.[15] In diesem Fall hatte der Account-Inhaber sein Geburtsdatum in einer vierstelligen Zahlenkombination als Passwort gewählt, was der Authentisierungsnehmer zugelassen hat.[16] Den Account-Inhaber treffen ebenfalls keine verbindlichen Vorgaben, wie sicher er das Passwort zu verwahren hat. Er kann das Passwort z.B. in dem Schlüsselbund seines Browsers oder Betriebssys-

---

127, 256; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 17; *Hanau*, Handeln unter fremder Nummer, S. 214.

8 Oben Rn. 124 ff.

9 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257.

10 Unten Rn. 530.

11 Dazu unten Rn. 534.

12 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.

13 Ebd., 256 f.

14 *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002, 127, 128.

15 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257.

16 Ebd., 257.

tems speichern oder es auf einem Zettel neben seinem Computer notieren.[17] Die wissensbasierte Authentifizierung mittels eines Passworts sei daher unsicher.[18] Dies führe dazu, dass nicht davon ausgegangen werden könne, dass der Ersteller des Accounts auch derjenige ist, der ihn später nutzt.

b) Handeln eines Dritten von gewisser Dauer und Häufigkeit

374 Durch die Anwendung der Anscheinsvollmacht muss das Verhalten des Vertreters von einer gewissen Dauer und Häufigkeit sein, um einen Rechtsschein begründen zu können.[19] Beim erstmaligen Missbrauch fehlt ein solches Handeln von gewisser Dauer und Häufigkeit. Regelmäßig scheitert demnach die Rechtsscheinhaftung für den Missbrauch von Zugangsdaten ohne deren Weitergabe.

375 Soll der Rechtsscheintatbestand bejaht werden, muss die Voraussetzung des Handelns von gewisser Dauer und Häufigkeit überwunden werden. Zum einen könnte diese Voraussetzung einfach ignoriert werden.[20] Dann haftet der Account-Inhaber, „wenn er das Verhalten des unter seinem Namen Handelnden entweder kannte und trotz Verhinderungsmöglichkeiten duldete oder wenn er es hätte erkennen müssen und verhindern können und der Dritte nach Treu und Glauben davon ausgehen durfte, dass der Namensträger selbst oder eine von ihm bestimmte Person handele.“[21] Diese Voraussetzung übernimmt das *AG Bremen* wortgleich aus einer Entscheidung zum Bildschirmtext,[22] bei der ebenfalls behauptet wurde, dass ein im Haushalt lebender Familienangehöriger den Account missbrauchte. Durch diese übernommenen Anforderungen wird die in diesen Fällen problematische Voraussetzung des häufigen und wiederholten Handelns des Vertreters bei der Anscheinsvollmacht umgangen.[23]

376 Zum anderen kann das Erfordernis des wiederholten Handelns explizit abgelehnt werden. Schon früh erkannten Teile von Rechtsprechung und Li-

17 Dazu oben Rn. 132 ff.
18 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257.
19 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18. Allgemein zum Erfordernis des Handeln von gewisser Häufigkeit und Dauer, oben Rn. 268.
20 So *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 519.
21 Ebd., 519.
22 *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 1401.
23 Zu dieser Voraussetzung oben Rn. 268.

teratur, dass das Erfordernis des Handelns von Dauer und Häufigkeit auf den Missbrauch von Zugangsdaten nicht passt.[24] Wegen der Eigenart des Bildschirmtextes komme es nicht auf ein Handeln von Dauer und Häufigkeit an.[25] Ohne dies explizit auszusprechen, wenden sich auch neuere Gerichtsurteile gegen das Erfordernis des Handelns von Häufigkeit und Dauer. Mit dem Verweis auf die einschlägige Bildschirmtext-Ansicht wird dieses Merkmal fallengelassen, ohne die Definition des *BGH* von der Anscheinsvollmacht ausdrücklich in Frage zu stellen.[26] Dogmatisch lasse sich die Nichtanwendung dieses Merkmales damit begründen, dass es nur „in der Regel" vorliegen müsse.[27] Der behauptete starke Rechtsschein der Legitimation durch eine rein wissensbasierte Authentisierung mache das Erfordernis des Handelns von gewisser Häufigkeit und Dauer überflüssig.[28]

Gegen die Voraussetzung des wiederholten und häufigen Handelns des **377**
Dritten spreche ferner, dass die Unterscheidung zwischen erstem und wiederholtem Missbrauchsfall willkürlich sei.[29] Willkürlich bedeutet nicht nach einem System erfolgend, sondern wie es sich zufällig ergibt.[30] Aus Sicht des Account-Inhabers kann diese Behauptung nicht nachvollzogen werden. Nach dem ersten Missbrauch, der ihm bekannt wird, hat der Account-Inhaber die Möglichkeit und einen Anlass einen weiteren Missbrauch zu verhindern. Aus der Sicht des Erklärungsempfänger hingegen macht die Häufigkeit des Missbrauchs keinen Unterschied. Er kann nicht erkennen, ob der Dritte die Zugangsdaten zum ersten Mal oder wiederholt missbraucht. Dies spricht jedoch nicht gegen die Voraussetzung des wiederholten Handelns des Dritten bei der Anwendung der Anscheinsvollmacht, sondern zeigt auf, dass diese strukturell ungeeignet ist, den Missbrauch von Zugangsdaten im Internet überzeugend zu lösen.

Das Erfordernis des Handeln eines Dritten von gewisser Häufigkeit und **378**
Dauer verdeutlicht sichtbar, dass der Missbrauch von Zugangsdaten im In-

---

24 Zum Bildschirmtext: *LG Ravensburg*, Urteil v. 13. 6. 1991, 2 S 6/91 – CR 1992, 472, 473; *Lachmann*, NJW 1984, 405, 408.

25 *LG Ravensburg*, Urteil v. 13. 6. 1991, 2 S 6/91 – CR 1992, 472, 473.

26 So macht es *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257.

27 *Verse/Gaschler*, Jura 2009, 213, 216 unter Verweis auf *BGH*, Urteil v. 9. 6. 1986, II ZR 193/85 – NJW-RR 1986, 1169; Urteil v. 5. 3. 1998, III ZR 183/96 – NJW 1998, 1854, 1855; Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 17.

28 *Hanau*, VersR 2005, 1215, 1217.

29 So *Härting*[4], Rn. 572.

30 Duden[3], willkürlich.

ternet ohne deren Weitergabe nicht überzeugend über die Anscheinsvollmacht gelöst werden kann.[31] Gegen die Anwendung der Anscheinsvollmacht spricht zunächst, dass das Handeln des Dritten nicht ersichtlich wird. Bei der Anscheinsvollmacht bezieht sich der Rechtsschein darauf, dass ein Dritter mehrfach als Vertreter des Geschäftsherren aufgetreten ist und der Geschäftsherr diese Geschäfte erfüllt hat.[32] Schon *qua definitionem* kann der Geschäftsgegner das Handeln des Dritten beim Handeln *unter* fremdem Namen nicht erkennen.[33] Er kann daher kein Vertrauen in eine eventuell bestehende Vollmacht des handelnden Dritten haben, denn für ihn erscheint es, als handele der Account-Inhaber. Den Parteien mangelt es an einem persönlichen Kontakt, der das Handeln des Dritten erkennbar macht. Der Rechtsscheintatbestand, der beim Vertretenen Vertrauen wecken soll, kann sich nur auf Umstände beziehen, die er wahrnehmen kann. Strukturell passt daher die Anscheinsvollmacht nicht auf Fälle des Handelns unter fremdem Namen. Ihre Anwendung ist daher sinnlos.[34] Diese mangelnde Drittbezogenheit hat der *BGH* an anderer Stelle erkannt,[35] jedoch nicht die nötigen Konsequenzen daraus gezogen.

379 Unmittelbar aus der mangelnden Erkennbarkeit des Handelns des Dritten folgt die zweite Schwachstelle der Anscheinsvollmacht. Das Erfordernis, das Handeln des Dritten müsse von gewisser Dauer und Häufigkeit sein, überzeugt nicht. Der Geschäftsgegner kann nicht erkennen, dass der Dritte gehandelt hat. Die Tatsache, ob der Dritte erstmalig oder bereits mehrfach gehandelt hat, kann daher mangels Erkennbarkeit kein Vertrauen des Geschäftsgegners wecken.[36] Bei Anwendung der Anscheinsvollmacht ist es jedoch konsequent, ein mehrmaliges Auftreten zu fordern.[37] Das zeigt wie-

---

31 *Borges*, NJW 2011, 2400; *Faust*, JuS 2011, 1027; *Linardatos*, Jura 2012, 53, 55; *Oechsler*, MMR 2011, 631, 633; *Schinkels*, LMK 2011, 320461, 2 baa; *Stöber*, EWiR 2011, 521; *Dennis Werner*, K&R 2011, 499, 500.

32 Oben Rn. 268.

33 *Faust*, JuS 2011, 1027, 1028; *Herresthal*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 28; *ders.*, JZ 2011, 1171, 1171. Zum Bildschirmtext schon *Redeker*, NJW 1984, 2390, 2393; *Probandt*, UFITA 98 (1984), 9, 17. Zur Duldungsvollmacht *Kuhn*, S. 208.

34 *Faust*, BGB AT[3], § 26 Rn. 41.

35 *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 17 f.; Urteil v. 14. 3. 2000, XI ZR 55/99, Rn. 12. Darauf weisen hin *Linardatos*, Jura 2012, 53, Fn. 10; *Herresthal*, JZ 2011, 1171, 1173.

36 *Herresthal*, K&R 2008, 705, 707; *ders.*, in: *Taeger/Wiebe*, 21, 31; *ders.*, JZ 2011, 1171, 1173; *Schinkels*, LMK 2011, 320461, 2 bbb; *Faust*, JuS 2011, 1027, 1028.

37 *Rieder*, S. 196.

derum, dass die Anscheinsvollmacht strukturell nicht geeignet ist, die Fälle des Missbrauchs von Zugangsdaten im Internet überzeugend zu lösen.

Der Lösungsweg über die Anscheinsvollmacht statuiert somit eine Rechtsscheinhaftung für eine Zurechenbarkeit, ohne dass ein Rechtsschein besteht.[38] Bei einem Handeln des Dritten von gewisser Dauer und Häufigkeit solle der Account-Inhaber haften.[39] Obwohl der Geschäftsgegner nicht erkennen kann, also kein Rechtsscheintatbestand dahingehend besteht, dass der Dritte gehandelt hat, soll bei einem wiederholten Handeln nach Rechtsscheingrundsätzen gehaftet werden.[40] Das Handeln des Dritten von gewisser Dauer und Häufigkeit kann mangels Erkennbarkeit nicht für den Rechtsscheintatbestand relevant sein. Der relevante Anknüpfungspunkt für das Vertrauen des Geschäftsgegners kann nur sein, ob die Absendung der Erklärung über den Account einen so starken Rechtsschein setzt, dass der Geschäftsgegner darauf vertrauen darf, dass diese vom Account-Inhaber stammt. Die Haftung für den Missbrauch von Zugangsdaten im Internet kann somit nicht überzeugend über die Anscheinsvollmacht gelöst werden. **380**

c) Identifikationsfunktion

Gegen das Vorliegen eines Rechtsscheintatbestandes spreche, dass nicht davon ausgegangen werden kann, dass derjenige, der als Namensträger im Account bezeichnet ist, auch der Account-Inhaber ist.[41] Der Authentisierungsnehmer muss überprüfen, ob die Person, die den Account erstellt, auch diejenige ist, die namentlich im Account als Inhaber benannt wird. Der Rechtsschein scheitere auch, wenn diese Identitätsbehauptung nicht ausreichend zuverlässig überprüft wird, also die Identifikationsfunktion des Accounts nicht ausreichend zuverlässig ist.[42] **381**

38 *Schinkels*, LMK 2011, 320461, 2 b aa; *Sonnentag*, WM 2012, 1614, 1615.

39 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 16.

40 So auch *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 17.

41 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257.

42 Ebd., 257. Zur Identifikationsfunktion von Accounts im Internet, unten Rn. 595.

d) Risikoverteilung

382 Bei der angemessenen Verteilung des Risikos zeigen sich die Grundlagen für die unterschiedlichen Ergebnisse der Vertreter dieser Meinung. Eine allgemeine Risikoabwägung spreche gegen die Bejahung eines Rechtsscheintatbestandes.[43] Die gesetzliche Wertung der Risikoverteilung (vgl. §§ 164, 177, 179 BGB ggfs. analog) weise das Risiko einer fehlenden Vertretungsmacht dem Geschäftspartner zu.[44] Eine Durchbrechung dieses Grundsatzes komme nicht bereits in Betracht, wenn der vermeintlich Vertretene fahrlässig verkannt und nicht verhindert hat, dass der Dritte eine Erklärung über seinen Account abgegeben konnte.

383 Dadurch berge diese Ansicht ein erhebliches Missbrauchspotential in Form von Schutzbehauptungen.[45] Der Teilnehmer einer Internetauktion könne sich aus Reue auf den Missbrauch der Zugangsdaten berufen und somit die Verbindlichkeit seiner Willenserklärung aufheben. Dagegen wird jedoch eingewandt, dass der Markt diesem Missbrauchspotential mit vertrauensbildenden Maßnahmen begegnen kann.[46] Das Bewertungssystem von zahlreichen Internet-Auktionsplattformen wie eBay sorge dafür, dass Nutzer, die sich häufiger von Verträgen durch Schutzbehauptungen lösen, als vertrauensunwürdig erscheinen. Dieses Gegenargument vermag nicht zu überzeugen. Käufer können auf dem Internetauktionshaus eBay vom Verkäufer nur positiv bewertet werden.[47] Verkäufer haben daher keine Möglichkeit Käufer, die sich mit Schutzbehauptungen von den Verträgen lösen, als solche zu bewerten und andere dadurch davor zu schützen.[48] Andererseits lässt sich einwenden, dass der Verkäufer sich den Käufer ohnehin nicht aussuchen kann.[49] Nur den Käufern steht die Möglichkeit offen, sich den

43 Ausführlich dazu unten Rn. 625.

44 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 20.

45 *Mankowski*, CR 2011, 458; *Härting/Strubel*, BB 2011, 2188, 2189; *Herresthal*, JZ 2011, 1171, 1174; *Stöber*, EWiR 2011, 521; *Dennis Werner*, K&R 2011, 499.

46 *Klein*, MMR 2011, 450, 451.

47 *eBay*, So funktioniert das Bewertungssystem.

48 In zahlreichen Entscheidungen ging es jedoch um Käufer, die sich nicht an den Vertrag gebunden fühlen: *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06 – NJW 2007, 611; *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179.

49 eBay ermöglicht lediglich den Ausschluss von Käufern anhand einiger Formalkriterien, *eBay*, Von Käufern zu erfüllende Bedingungen auswählen.

Verkäufer auszusuchen und bei Zweifeln an seiner späteren Vertragstreue von einem Gebot abzusehen.

Andererseits wird eine mögliche Haftung mit Billigkeitserwägungen be- 384
gründet.[50] Der Teilnehmer einer Internetauktion – egal ob Anbieter oder Bieter – dürfe nicht nur einseitig von dem Vorteil, einen großen Interessenkreis mit der Internetauktion anzusprechen, profitieren. Im Gegenzug müsse er auch die Nachteile dieses Geschäftskanals tragen. Er habe daher die bekannten Sicherheitsrisiken des Internets zu tragen. Dagegen ist jedoch einzuwenden, dass jemand, der dieses Risiko minimieren möchte, darauf achten könne, dass nur sichere Authentisierungsmethoden verwendet würden. Das TAN-Verfahren beim Online-Banking biete z.B. durch die dreifache Absicherung einen höheren Schutz als eine wissensbasierte Authentisierung mit Nutzername und Passwort.[51]

Ferner wird für die Rechtsscheinhaftung teleologisch mit der pauschalen 385
Behauptung argumentiert, dass ohne eine Rechtsscheinhaftung auf das positive Interesse mangels Vertrauens des Geschäftsverkehrs in die Identität der übrigen Benutzer der Handel auf Internetplattformen wie eBay gefährdet wäre.[52] Dass diese Behauptung nicht stimmt, lässt sich sogar anhand der Lebenswirklichkeit bestätigen. Die zahlreichen Entscheidungen, die eine Rechtsscheinhaftung ablehnen, sowie deren höchstrichterliche Bestätigung,[53] haben zu keinem spürbaren Rückgang der Aktivitäten auf eBay geführt. Ferner hat der Rechtsverkehr Methoden entwickelt, die im Vorfeld und im Nachhinein das Vertrauen in die ordnungsgemäße Abwicklung des Geschäftes stärken. Eine dieser Methoden stellt das Bewertungssystem der Internetauktionshäuser dar.[54] Die Mitglieder können selbst auswählen, ob sie nur mit Anbietern mit zahlreichen positiven Bewertungen Geschäfte schließen oder ob sie das Risiko eingehen, einem (noch) nicht positiv bewerteten Nutzer zu vertrauen. Eine weitere, weit verbreitete Möglichkeit der Vertrauensbildung vor Vertragsschluss stellt die Angabe der Kontaktdaten dar.[55] Dies ermöglicht dem Interessenten auf schnellem Wege etwaige

50 *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 18.
51 *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002, 127, 128.
52 *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 519.
53 Dazu oben Rn. 370.
54 Dazu oben Rn. 66.
55 E-Mail-Adresse sowie Mobilfunk- oder Telefonnummer werden häufig zur Kontaktaufnahme angegeben, z.B. bei *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 10.

Zweifel bezüglich des Angebots oder des Anbieters zu klären. Nach Vertragsschluss existieren ferner für Verkäufer und Käufer Schutzmöglichkeiten. Regelmäßig vereinbaren die Parteien bei Internetauktionen die Vorleistung des Käufers, sodass der Verkäufer nicht das Risiko eingeht, die Ware zu verschicken, ohne den Kaufpreis zu erhalten. Es besteht jedoch auch die Möglichkeit, sich die Gegenleistung durch Diensteanbieter garantieren zu lassen.[56]

386 Die Risikoverteilung sei teleologisch bei der Rechtsscheinhaftung ebenfalls zu berücksichtigen. Dabei sei der Missbrauch der Zugangsdaten im Internet mit dem Fall der missbräuchlichen Verwendung der Kreditkartendaten im Telefon- und Mail-Order-Verfahren zu vergleichen.[57] Diese Risikoverteilung sei auch für den Missbrauch von Zugangsdaten im Internet anzuwenden. Der Account-Inhaber müsse wegen der Einrichtung des Accounts dessen Risiko ebenso wenig tragen wie der Besitzer einer Kreditkarte deren Missbrauch im Telefon- und Mail-Order-Verfahren.[58] Beim Telefon- und Mail-Order-Verfahren trägt der Inhaber der Kreditkarte nicht das Risiko der missbräuchlichen Verwendung der Kreditkarte.[59] Lediglich das Acquiring-Unternehmer hat dem Vertragshändler unter den vertraglich vereinbarten Bedinungen bei deren Vorliegen die Zahlung zu garantieren.[60]

387 Des Weiteren wird teleologisch mit den Risikosphären argumentiert. Dem Account-Inhaber sei die Sicherung seines Accounts möglich und zumutbar, wohingegen der Geschäftsgegner kaum die Möglichkeit habe, die Echtheit der Erklärung zu überprüfen.[61] Zwar haben die Account-Inhaber regelmäßig die Möglichkeit die Zugangsdaten so gut zu sichern, dass auch zahlreiche Wege an diese zu gelangen[62] nicht funktionieren. Dies setzt zum einen jedoch ein hohes Maß an technischem Sachverstand voraus, denn neuere Missbrauchswege sind nur für das geschulte Auge erkennbar. An der Zumutbarkeit der Sicherung kann daher gezweifelt werden. Hat ein Dritter jedoch Kenntnis der Zugangsdaten erlangt, kann der Account-

56 Unten Rn. 664 sowie *Jehle*, S. 346; *Meder/Grabe*, BKR 2005, 467, 476.

57 *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 813 f.; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 17; *Oechsler*, AcP 208 (2008), 565, 570; *Wenn*, CR 2006, 137, 138.

58 *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 813 f.; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 17.

59 Oben Rn. 342.

60 Oben Rn. 342.

61 *Härting*[4], Rn. 570.

62 Dazu oben Rn. 124 ff.

Inhaber dies regelmäßig erst nach einem Missbrauch feststellen. Darüber hinaus gibt es Wege an die Zugangsdaten zu gelangen, die der Account-Inhaber nicht beeinflussen kann.[63] Der Account-Inhaber kann daher nicht in jedem Fall ohne Weiteres vermeiden, dass die Zugangsdaten missbraucht werden. Ebenso stimmt es zwar, dass der Geschäftsgegner der elektronischen Willenserklärung deren Echtheit nicht ansehen kann. Auf der anderen Seite kann er auf einem anderen Kommunikationsweg die Echtheit beim Account-Inhaber erfragen. Bei Zweifeln hat er daher Möglichkeiten sich von der Echtheit der Erklärung zu überzeugen.[64]

e) Keine Zurechnung nach deliktischen Grundsätzen

Manche Stimmen in der Literatur befürworten eine Übertragung der deliktischen Lösung der Haftung für den Missbrauch von Zugangsdaten auf den rechtsgeschäftlichen Bereich.[65] In der „Halzband"-Entscheidung[66] hat der *BGH* postuliert, dass im Immaterialgüter- und Wettbewerbsrecht die unzureichende Sicherung der Zugangsdaten zu einem eBay-Account einen eigenen Zurechnungsgrund für das Verhalten des Dritten zum Account-Inhaber darstelle.[67] Durch eine Anwendung dieser Lösung im rechtsgeschäftlichen Bereich werde die missliche Lage des „Widerrufsrecht kraft Beweislastverteilung"[68] verhindert.[69] Bei einer Übertragung des deliktischen Haftungsmodells müsste der Account-Inhaber bei Missbrauch seiner Zugangsdaten auf das positive Interesse des Geschäftsgegners haften. **388**

Durch die Übertragung kann ein Gleichlauf zwischen deliktischer und vertraglicher Haftung erreicht werden.[70] Ob dies ein anzustrebendes Ziel darstellt, ist jedoch zu bezweifeln. Im Deliktsrecht werden absolute Rechte geschützt.[71] Diese Wertungen lassen sich nicht auf den Fall der Rechtsscheinhaftung übertragen, weil dort eine Interessenabwägung zwischen den **389**

63 Dazu oben Rn. 215.
64 Unten Rn. 657.
65 So *Härting/Strubel*, BB 2011, 2188, 2189; *Hecht*, K&R 2009, 462; *Rössel*, CR 2009, 453, 455.
66 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134.
67 Unten Rn. 726.
68 *Mankowski*, CR 2003, 44; *ders.*, MMR 2004, 181.
69 *Rössel*, CR 2009, 453, 454 f.
70 *Härting/Strubel*, BB 2011, 2188, 2189.
71 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 19.

nicht absolut geschützten Rechten des vermeintlichen Erklärenden und des Erklärungsempfängers stattfinden kann.[72] Auch in die andere Richtung lassen sich die Lösungen daher nicht übertragen.[73]

390 Ferner spricht gegen die Übertragung der deliktischen Haftung die unten herausgearbeitete Kritik, die gegen die Haftungskonstruktion des *BGH* eingewendet werden kann. Zum einen handelt es sich um einen Lösungsweg, der dogmatisch weder begründet noch überzeugend begründbar ist.[74] Zum anderen ist daran zu zweifeln, dass es einer so weitreichenden und belastenden Haftung bedarf.[75] Diese verfehlte deliktische Haftungskonstruktion sollte daher nicht auf die rechtsgeschäftliche Haftung übertragen werden.

f) Zwischenergebnis

391 Die überwiegenden Vertreter des Lösungswegs über die Anscheinsvollmacht sind somit der Ansicht, bei der Abgabe einer kennwortgeschützten Erklärung bestehe kein Rechtsscheintatbestand dafür, dass der Account-Inhaber diese Erklärung abgegeben habe. Dies widerspricht der Ansicht, dass bei der Weitergabe der Zugangsdaten über die Rechtsscheinhaftung gehaftet wird.[76] Bei beiden Konstellationen ist der durch den Erklärungsempfänger wahrnehmbare Rechtsscheintatbestand der Gleiche: er erhält eine Erklärung, die den Account-Inhaber als Absender ausweist. Die nicht wahrnehmbare Zurechnung kann auf dieser Ebene keinen Unterschied ausmachen, wohl aber auf der Ebene der Zurechnung. Die scheinbar gleichen Lösungsansätze über die Duldungs-[77] und über die Anscheinsvollmacht widersprechen sich somit in ihren Ergebnissen.

2. Zurechenbarkeit

392 Nicht nur bei dem Rechtsscheintatbestand, sondern auch bei der Zurechnung des etwaigen Rechtsscheintatbestandes lassen sich unterschiedliche

---

72 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 19; *LG Gießen*, Beschluss v. 6. 3. 2013, 1 S 337/12 (nicht veröffentlicht).
73 *LG Köln*, Urteil v. 18. 10. 2006, 28 O 364/06 – MMR 2007, 337, 338.
74 Unten Rn. 731.
75 Siehe unten Rn. 758.
76 Dazu oben Rn. 297.
77 Oben Rn. 297.

Meinungen bei dem Lösungsweg über die Anscheinsvollmacht finden. Einige Vertreter der Lösung über die Anscheinsvollmacht möchten die Zurechnung auf die Weitergabe[78] beschränken. Die Speicherung des Passworts auf einer Diskette, die sich in räumlicher Nähe zum Computer befindet, reiche demnach für eine Zurechnung nicht aus.[79] Diejenigen, die eine Haftung bejahen, lassen für die Zurechnung nicht nur die Weitergabe der Zugangsdaten an den Dritten, sondern auch das fahrlässige Ermöglichen der Kenntniserlangung durch den Dritten ausreichen.[80] Unter dem fahrlässigem Ermöglichen fällt z.B. das Speichern der Zugangsdaten in der Schlüsselbund-Verwaltung des Browsers oder des Betriebssystems.[81] Entsprechend der Abgrenzung nach Risikosphären soll die fahrlässige Versäumung der Verhinderung von Missbrauch zur Zurechnung führen.[82] Nur wenn der Account-Inhaber angemessene Maßnahmen zur Vermeidung des Missbrauchs unternommen hat, sowie nicht fahrlässig mit seinen Zugangsdaten umgegangen ist, sei eine Zurechnung ausgeschlossen.[83] Eine Zurechnung solle jedoch bei „Computerspionage" ausscheiden.[84] Der Behauptung, dass die Computerspionage jeder Lebenserfahrung widerspreche,[85] ist jedoch zu widerlegen. Es existieren zahlreiche Möglichkeiten, wie die Zugangsdaten für Accounts ausgespäht und missbraucht werden können.[86] Diese Behauptung des *AG Bremen* verwundert insbesondere deswegen, weil es eine Entscheidung zitiert, die den Anscheinsbeweis wegen der Missbrauchsmöglichkeiten im Internet ablehnt.[87]

Ferner wird vertreten, dass die Zurechenbarkeit eines etwaigen Rechts- **393**
scheins wegen der fehlenden Möglichkeiten dessen Zerstörung ausscheide. Grundsätzlich muss derjenige, der den Rechtsschein geschaffen hat, auch die Möglichkeit haben, den Rechtsschein zu zerstören, und dadurch seine Haftung zu verhindern.[88] Diese Möglichkeit fehle beim Missbrauch von Zu-

78 Oben Rn. 295.
79 *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 181.
80 *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 519.
81 Dazu oben Rn. 135.
82 *Härting*[4], Rn. 570.
83 *Wenn*, CR 2006, 137, 138.
84 *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 519.
85 Ebd., 519.
86 Oben Rn. 124 ff.
87 *OLG Naumburg*, Urteil v. 2. 3. 2004, 9 U 145/03 – OLG-NL 2005, 51.
88 Oben Rn. 246.

gangsdaten im Internet ohne deren Weitergabe.[89] Der Account-Inhaber habe nicht die Möglichkeit, die missbräuchliche Verwendung seiner Zugangsdaten vorherzusehen oder zu erkennen. Daher fehle ihm die Möglichkeit, den Missbrauch zu verhindern. Eine Zurechnung könne sich erst dann ergeben, wenn der Account-Inhaber den Missbrauch bemerkt und diesen trotzdem nicht verhindert.[90] Wegen der fehlenden Möglichkeit den Missbrauch frühzeitig zu erkennen, betrifft dies nur Fälle, in denen aus einem bekannt gewordenen Missbrauch keine Maßnahmen getroffen wurden, zukünftigen Missbrauch zu verhindern.

3. Zwischenergebnis

394 Die Anscheinsvollmacht ist strukturell nicht geeignet, Fälle des Missbrauchs von Zugangsdaten im Internet ohne deren Weitergabe in den Griff zu bekommen. Weil das Handeln des Dritten nicht ersichtlich wird, kann auch ein mehrfaches Auftreten des Dritten kein schützenswertes Vertrauen beim Geschäftsgegner wecken.[91] Die Anwendung der Anscheinsvollmacht statuiert somit eine Rechtsscheinhaftung ohne Rechtsschein.[92] Darüber hinaus lässt sich ein überzeugendes Gesamtkonzept nicht begründen, weil die Verneinung des Rechtsscheintatbestandes bei Anwendung der Anscheinsvollmacht im Widerspruch zur unwidersprochenen Lösung über die Duldungsvollmacht bei Weitergabe steht.[93]

395 Das *LG Frankfurt*[94] zeigt jedoch, dass für die Anscheinsvollmacht auch im digitalen Bereich ein Anwendungsbereich bleibt, sofern die Parteien nicht ausschließlich über das Internet kommunizieren. Es hatte einen Fall zu entscheiden, bei dem der minderjährige Sohn der GmbH-Geschäftsführerin unter der Kundennummer der GmbH sowie unter Verwendung einer E-Mail-Adresse mit der Domain der GmbH Mobiltelefone bestellt hatte. Zum einen hatte der Sohn bereits mehrfach Mobiltelefone über diese Kundennummer bestellt, wobei die Kaufverträge beanstandungslos erfüllt wurden. Ferner

89 *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814; *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06 – NJW 2007, 611, 612; *OLG Bremen*, Beschluss v. 21. 6. 2012, 3 U 1/12 – MMR 2012, 593, 594.

90 Vgl. *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814.

91 Oben Rn. 378.

92 Oben Rn. 380.

93 Oben Rn. 391.

94 *LG Frankfurt*, Urteil v. 15. 12. 2004, 3-13 O 28/04 (nicht veröffentlicht).

hatte der Verkäufer bei der Bestellung Rücksprache mit der Geschäftsführerin gehalten, um die Einzelheiten bezüglich des Transports zu klären. Somit lagen sowohl die Voraussetzungen der Duldungs- als auch der Anscheinsvollmacht vor.[95] In Fällen ohne persönlichen Kontakt, wo das Handeln des Dritten nicht ersichtlich wird, kann die Anscheinsvollmacht hingegen nicht sinnvoll angewendet werden.

II. Lösung über vorhandene vertragliche Beziehungen

Für eine Lösung des Problems der Haftung für den Missbrauch von Zugangsdaten im Internet ist es möglich, bestehende vertragliche Beziehungen zwischen dem Authentisierungsnehmer und dem Account-Inhaber als Grundlage zu nehmen. Diese Lösung hat je nach Konstellation einen unterschiedlichen Ansatzpunkt. Bei Zwei-Personen-Verhältnissen, in denen der Geschäftsgegner zugleich der Authentisierungsnehmer ist, mit dem der Account-Inhaber eine vertragliche Beziehung unterhält, können sich aus diesem Vertrag Ansprüche ergeben. In Drei-Personen-Verhältnissen, in denen der Geschäftsgegner unabhängig vom Authentisierungsnehmer ist, können gleichwohl die vertraglichen Beziehungen zwischen Account-Inhaber und Authentisierungsnehmer Grundlage von Ansprüchen sein. Über die Figur des Schuldverhältnisses mit Schutzwirkungen zu Gunsten Dritter kann der Geschäftsgegner Ansprüche gegen den Account-Inhaber herleiten werden, sofern die Voraussetzungen dafür vorliegen. **396**

1. In Zwei-Personen-Konstellationen: Vertrag als Grundlage

In Zwei-Personen-Konstellationen können sich Ansprüche des Authentisierungsnehmers aus seinem Vertrag mit dem Account-Inhaber ergeben.[96] Diese Lösung hat zunächst zwei offensichtliche Einschränkungen. Zum einen ist sie auf diese Zwei-Personen-Konstellationen beschränkt. Zum anderen ist sie nur anwendbar, wenn zwischen dem Geschäftsgegner und dem Account-Inhaber bereits eine vertragliche Beziehung besteht, was in vielen Fällen nicht der Fall ist. **397**

---

95 *LG Frankfurt*, Urteil v. 15. 12. 2004, 3-13 O 28/04 (nicht veröffentlicht).

96 Dazu auch *Borges/Schwenk/Stuckenberg/Wegener*, S. 278 f.

398 Hat sich jedoch der Account-Inhaber beim Authentisierungsnehmer, beispielsweise einem Online-Versandhändler, registriert, entsteht zwischen ihnen durch die Registrierung ein Rahmenvertrag.[97] Im Rahmen dieser vertraglichen Beziehung treffen die Parteien die gegenseitige Pflicht auf die Rechtsgüter des anderen Rücksicht zu nehmen (§ 241 Abs. 2 BGB). Diese Pflicht kann sich dahin gehend konkretisieren, dass der Account-Inhaber seine Zugangsdaten sichern muss, um den Authentisierungsnehmer vor Schäden durch eine mögliche Identitätsverwirrung nach unbefugtem Einsatz der Zugangsdaten zu bewahren. Der entscheidende Punkt bei dieser Frage ist, welche Sorgfaltspflichten der Account-Inhaber dabei zu beachten hat. Ein Versuch der Konkretisierung der Sorgfaltspflichten von Account-Inhaber wird an späterer Stelle noch erfolgen.[98]

399 Der Authentisierungsnehmer kann jedoch auch durch seine AGB vorgeben, welche Sorgfaltspflichten der Account-Inhaber zu erfüllen hat. Viele Authentisierungsnehmer nehmen diese Möglichkeit wahr, durch die in den Rahmenvertrag einbezogenen AGB Regelungen für den Missbrauch von Zugangsdaten zu treffen. Als Beispiel werden Regelungen der AGB des größten in Deutschland operierenden Versandhändlers Amazon betrachtet. Viele Versandhändler und Online-Plattformen verwenden ähnliche Regelungen. Amazon hat folgende Klausel bezüglich der Haftung für den Missbrauch von Zugangsdaten in den AGB:[99]

> 7 Ihr Konto
>
> Wenn Sie einen Amazon Service nutzen, sind Sie für die Sicherstellung der Vertraulichkeit Ihres Kontos und Passworts und für die Beschränkung des Zugangs zu Ihrem Computer verantwortlich und soweit unter anwendbarem Recht zulässig erklären Sie sich damit einverstanden für alle Aktivitäten verantwortlich zu sein, die über Ihr Konto oder Passwort vorgenommen werden. Sie sollten alle erforderlichen Schritte unternehmen, um sicherzustellen, dass Ihr Passwort geheim gehalten und sicher aufbewahrt wird und Sie sollten uns unverzüglich informieren, wenn Sie Anlass zur Sorge haben, dass ein Dritter Kenntnis von Ihrem Passwort erlangt hat oder das Passwort unautorisiert genutzt wird oder dies wahrscheinlich ist.

400 Die Betrachtung dieses Beispiels zeigt die Probleme der Lösung über vertragliche Vereinbarungen. Zunächst besteht wie bei der Verpflichtung der

---

97 *Hossenfelder*, Pflichten von Internetnutzern, S. 239; *Leupold/Glossner*, in: Handbuch IT-Recht[2], § 2 Rn. 358.

98 Unten Rn. 687; siehe dazu auch *Hossenfelder*, Pflichten von Internetnutzern, S. 237 ff.

99 *Amazon*, § 7.

Rücksichtnahme nach § 241 Abs. 2 BGB das Problem der Konkretisierung der Pflicht. Die AGB spezifizieren jedoch nicht, was die „erforderlichen Schritte“[100] zur Sicherung sind. Der Account-Inhaber kann den AGB daher keine konkreten Handlungspflichten entnehmen. Man könnte als erforderlichen Schritt zur Sicherstellung ansehen, dass der Account-Inhaber die Zugangsdaten nicht auf einem Zettel notiert.[101] Im Recht des Zahlungsverkehrs ist jedoch anerkannt, dass eine AGB-Klausel, nach der der Bankkunde die Zugangsdaten sich nicht notieren darf, keine Wirkung entfaltet.[102] Insofern erscheint fraglich, ob eine solche Klausel der Inhaltskontrolle nach §§ 307 ff. BGB Stand hält.

Ferner führt die Übernahme der Haftung „soweit unter anwendbarem Recht zulässig“[103] zu Problemen. Problematisch erscheint zunächst, dass eine Haftung bis zur Grenze des rechtlich Möglichen statuiert werden soll. Dadurch wird das Risiko der Verwendung einer unwirksamen Klausel vom Verwender der AGB auf den Geschäftsgegner verlagert. Dies könnte gegen das Bestimmtheitsgebot des § 307 Abs. 1 S. 2 BGB verstoßen.[104] Selbst bei einer Wirksamkeit der Klausel stellt sich die Frage nach der rechtlich zulässigen Haftung. Dazu ist entscheidend, in wie weit der Account-Inhaber ohne diese vertragliche Vereinbarung haftet. 401

Das reine Abstellen auf die vertraglichen Beziehungen löst das Problem der Haftung für den Missbrauch von Zugangsdaten im Internet nicht ausreichend. Zum einen bedarf es eines Rückgriffs auf die außervertragliche Ausformung der Haftung des Account-Inhabers sowie der Konkretisierung der Sorgfaltspflichten des Account-Inhabers in Bezug auf die Sicherung der Zugangsdaten, sofern diese nicht detailliert vertraglich gelöst sind. Zum anderen hat dieser Lösungsweg die entscheidenden Schwächen, dass er nur in Zwei-Personen-Verhältnissen anwendbar ist und häufig keine vertraglichen Beziehungen vorliegen. Sofern jedoch vertragliche Beziehungen zwischen dem Authentisierungsnehmer und dem Account-Inhaber vorliegen, die konkrete Pflichten zur Sicherung der Zugangsdaten statuieren, sind Fälle des Missbrauchs von Zugangsdaten im Internet darüber zu lösen. 402

100 *Amazon*, § 7.
101 Dazu oben Rn. 132.
102 Unten Rn. 562.
103 *Amazon*, § 7.
104 Zu den Einzelheiten des Bestimmtheitsgebotes *Wurmnest*, in: MüKo-BGB^{6}, § 307 Rn. 59.

2. In Drei-Personen-Konstellationen: Schuldverhältnis mit Schutzwirkungen zu Gunsten Dritter

403 Sofern kein Vertrag zwischen dem Geschäftsgegner und dem Account-Inhaber besteht, kann jedoch dessen Vertrag mit dem Authentisierungsnehmer zur Lösung des Missbrauchs von Zugangsdaten im Internet herangezogen werden. Dieser Lösungsweg setzt auf die Figur des Schuldverhältnisses mit Schutzwirkungen zu Gunsten Dritter.[105] Dabei muss beachtet werden, dass dieser Lösungsweg nur in einem Drei-Personen-Verhältnis, wie es bei Internet-Auktionsplattformen, der De-Mail oder der qualifizierten elektronischen Signatur vorliegt, angewandt werden kann. In Zwei-Personen-Verhältnissen besteht der Vertrag, der bei diesem Lösungsweg Schutzwirkungen entfalten soll, zwischen dem Account-Inhaber und dem Geschäftsgegner, sodass dieser zur Lösung der Haftungsfrage heranzuziehen ist.[106]

404 Das Schuldverhältnis mit Schutzwirkungen zu Gunsten Dritter wird teilweise als Vertrag mit Schutzwirkungen zu Gunsten Dritter bezeichnet. Diese Bezeichnung ist ungenau, weil auch die *culpa in contrahendo* Schutzwirkungen entfalten kann.[107] Bei ihr besteht jedoch nur ein vorvertragliches Schuldverhältnis und kein Vertrag. Unabhängig davon, ob die dogmatische Grundlage des Schuldverhältnisses mit Schutzwirkungen zu Gunsten Dritter in einer Analogie zu § 328 BGB, in einer ergänzenden Vertragsauslegung (§§ 133, 157 BGB) oder in einer Verankerung in § 311 Abs. 3 S. 1 BGB gesehen wird,[108] besteht über die Voraussetzungen Einigkeit. Die vier Voraussetzungen für einen Anspruch aus einem Schuldverhältnis mit Schutzwirkungen zu Gunsten Dritter sind die Leistungsnähe des Dritten, das schutzwürdige Interesse des Gläubigers, die Erkennbarkeit für den Schuldner sowie die Schutzbedürftigkeit des Dritten.[109] Folgend wird zunächst untersucht, welches Schuldverhältnis Schutzwirkungen entfalten könnte und anschließend werden die vier Voraussetzungen der Schutzwirkung zu Gunsten Dritter auf den Missbrauch von Zugangsdaten im Internet angewandt.

---

105 Für diesen Lösungsweg *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 178; *R. Koch*, CR 2005, 502, 507; *Mankowski*, CR 2011, 458.

106 Oben Rn. 397.

107 *BGH*, Urteil v. 28. 1. 1976, VIII ZR 246/74 (Salatblatt) – BGHZ 66, 51, 56 f.

108 Dazu *Looschelders*, Schuldrecht AT[11], Rn. 200 m.w.N.

109 *BGH*, Urteil v. 6. 5. 2008, XI ZR 56/07 – BGHZ 176, 281, Rn. 27.

a) Bestehendes Vertragsverhältnis des Account-Inhabers zu einem Diensteanbieter

Die Pflicht, die Zugangsdaten geheim zu halten, wird regelmäßig in AGB aufgenommen.[110] Folgend werden die AGB von eBay als Beispiel betrachtet. eBay bietet sich insofern gut als Beispiel an, als eBay die Internet-Auktionsplattform mit dem größten Marktanteil ist und weil zahlreiche Rechtsprechungsfälle durch Auktionen bei eBay ausgelöst wurden. Die Regelung in den eBay-AGB statuieren für die Mitglieder eine Geheimhaltungspflicht des Passworts sowie eine Haftung für den Missbrauch von diesen Zugangsdaten:[111] 405

> § 2 Anmeldung und Mitgliedskonto
>
> [...]
>
> 7. Mitglieder müssen ihr Passwort geheim halten und den Zugang zu ihrem Mitgliedskonto sorgfältig sichern. Mitglieder sind verpflichtet, eBay umgehend zu informieren, wenn es Anhaltspunkte dafür gibt, dass ein Mitgliedskonto von Dritten missbraucht wurde.
>
> [...]
>
> 9. Mitglieder haften grundsätzlich für sämtliche Aktivitäten, die unter Verwendung ihres Mitgliedskontos vorgenommen werden. Hat das Mitglied den Missbrauch seines Mitgliedskontos nicht zu vertreten, weil eine Verletzung der bestehenden Sorgfaltspflichten nicht vorliegt, so haftet das Mitglied nicht.

Diese AGB müssen von jedem eBay-Mitglied bei der Registrierung akzeptiert werden.[112] In dieser Form würde § 2 Nr. 9 der eBay-AGB einer Inhaltskontrolle nach § 307 Abs. 1 S. 1 BGB wegen der erheblichen Abweichungen zu einer etwaigen Rechtsscheinhaftung nicht standhalten.[113] Es ist jedoch eine Veränderung der Klausel denkbar, die einer höchstrichterlichen Inhaltskontrolle standhalten könnte.[114] Unabhängig von § 2 Nr. 9 der eBay- 406

110 Siehe die Empfehlung von *Ernst*, in: IT-Verträge, Kap. 3.13 Rn. 22, § 3 Abs. 2.
111 *eBay*, AGB.
112 *R. Koch*, CR 2005, 502.
113 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 21; *Lilja*, NJ 2011, 427, 428.
114 *Mankowski*, CR 2011, 458, 459.

AGB kann § 2 Nr. 7 der eBay-AGB, wenn diese Regelung im Verhältnis des Account-Inhabers zum Geschäftsgegner Anwendung findet, eine Schadenersatzhaftung für die Verletzung dieser Pflicht begründen. Es stellt sich daher die Frage, ob die Regelung des § 2 Nr. 7 der eBay-AGB in diesem Verhältnis gilt.

407 Die Erwägung, dass die AGB der Internet-Auktionsplattform direkt zwischen ihren Mitgliedern gelten,[115] liegt fern. Die AGB gelten unmittelbar nur zwischen dem Account-Inhaber und der Internet-Auktionsplattform.[116] Das ergibt sich aus der Relativität der Schuldverhältnisse.[117] Insbesondere bei der De-Mail und der qualifizierten elektronischen Signatur, wo nicht unbedingt alle Teilnehmer ein Schuldverhältnis mit demselben Anbieter eingehen, liegt eine direkte Geltung fern.

408 Die Überlegung, dass der Nutzer, der sich auf einer Internet-Auktionsplattform registriert, über die Geltung der AGB als Marktordnung einen Rahmenvertrag mit allen gegenwärtigen und zukünftigen Nutzern der Plattform schließt,[118] vermag nicht zu überzeugen.[119] Diese Vereinbarung müsste sich zunächst aus der objektiven Auslegung der AGB nach §§ 133, 157 BGB ergeben, woran es regelmäßig scheitern wird. Wäre eine solche Klausel in den AGB vorhanden, ist sie als überraschend nach § 305c Abs. 1 BGB einzuordnen und damit für unwirksam zu halten.[120] Ebenso würden belastende Regelungen einen unzulässigen Vertrag zu Lasten Dritter darstellen.[121]

409 Ebenso wird erwogen, dass das Nutzungsverhältnis zur Internet-Auktionsplattform ein Vertrag zu Gunsten Dritter sei und damit unmittelbar wirke.[122] Dies ergebe sich aus der Notwendigkeit der Etablierung einer Markt-

---

115 *LG Berlin*, Urteil v. 20. 12. 2000, 26 O 397/00 – CR 2001, 412, 413; *AG Erlangen*, Urteil v. 26. 5. 2004, 1 C 457/04 – NJW 2004, 3720, 3721.

116 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 21; *Borges*, in: Internet-Auktion, 214, 216; *Striepling*, S. 137 ff.

117 *Glatt*, S. 58; *J. Meyer*, in: Internet-Auktion, 26, 33. Allgemein dazu statt vieler *Olzen*, in: *Staudinger*[2009], § 241 BGB Rn. 293.

118 *Burgard*, WM 2001, 2102, 2106 f.; *Spindler*, ZIP 2001, 809, 812; *Sester*, CR 2001, 98, 107.

119 *Borges*, NJW 2005, 3313, 3315; *ders.*, in: Internet-Auktion, 214, 217; *Deutsch*, MMR 2004, 586, 587 f.; *R. Koch*, CR 2005, 502, 504.

120 *Deutsch*, MMR 2004, 586, 587.

121 Vgl. *Wiebe/Neubauer*, in: *Hoeren/Sieber/Holznagel*, Kap. 15 Rn. 28.

122 *Wiebe*, in: Internet-Auktionen[2], Kap. 4 Rn. 134; *ders.*, MMR 2000, 323, 325; *ders.*, CR 2002, 216, 217; *Ernst*, CR 2001, 121, 122; *ders.*, in: IT-Verträge, Kap. 3.13 Rn. 5; *R. Koch*, CR 2005, 502, 507.

ordnung, der alle Teilnehmer bei Registrierung zustimmen.[123] Dagegen ist jedoch einzuwenden, dass der Dritte nicht nur durch die Haftung der anderen begünstigt, sondern auch durch die eigene Einstandspflicht belastet wird. Damit wäre dieser Vertrag als Vertrag zu Lasten Dritter unwirksam.[124] Das Nutzungsverhältnis zur Internet-Auktionsplattform stellt daher keinen Vertrag mit Schutzwirkung zu Gunsten Dritter dar.[125]

b) Leistungsnähe des Dritten

Der Dritte muss bestimmungsgemäß mit der Leistung des Schuldners in Be- **410**
rührung kommen und deshalb den damit verbundenen Risiken in gleichem Maße wie der Gläubiger ausgesetzt sein.[126] Die Leistung muss nicht in der Hauptleistungspflicht, sondern kann auch in einer Nebenpflicht, insbesondere einer Schutzpflicht, bestehen.[127]

Die Geheimhaltungspflicht solle primär dem Schutz Dritter dienen,[128] **411**
wodurch sich die Leistungsnähe des Dritten begründen ließe. Daran ist zu zweifeln. Die Internet-Auktionsplattform ist ebenfalls an der Geheimhaltung der Zugangsdaten und der damit einhergehenden Sicherheit des Authentifizierungsvorgangs interessiert. Der Plattformbetreiber verlangt die Entlohnung seiner Dienste, wofür er ebenso wie ein potentieller Geschäftsgegner sichergestellt haben möchte, dass der Account-Inhaber handelt.

Ferner ist fraglich, ob Geschäftsgegner bestimmungsgemäß in gleicher **412**
Weise wie die Internet-Auktionsplattform mit der Leistung in Berührung kommt. Zwar haben beide im Ergebnis das gleiche Interesse daran, dass der Account-Inhaber handelt, sodass wirksame Verträge geschlossen werden.[129] Bei genauer Betrachtung dient die Schutzpflicht der Geheimhaltung

123 *Wiebe*, in: Internet-Auktionen[2], Kap. 4 Rn. 128.
124 *Grapentin*, GRUR 2001, 713, 714.
125 *OLG Hamm*, Urteil v. 14. 12. 2000, 2 U 58/00 – MMR 2001, 105; *Borges*, in: Internet-Auktion, 214, 217; *ders.*, NJW 2005, 3313, 3315; *Burgard*, WM 2001, 2102, 2105; *J. Meyer*, in: Internet-Auktion, 26, 35 f.; *Grapentin*, GRUR 2001, 713, 714.
126 *BGH*, Urteil v. 2. 7. 1996, X ZR 104/94 (Nitrierofen) – BGHZ 133, 168, 173; Urteil v. 26. 6. 2001, X ZR 231/99 – NJW 2001, 3115, 3116.
127 *BGH*, Urteil v. 26. 6. 2001, X ZR 231/99 – NJW 2001, 3115, 3116; *Gottwald*, in: MüKo-BGB[6], § 328 Rn. 174. Anders noch *BGH*, Urteil v. 2. 7. 1996, X ZR 104/94 (Nitrierofen) – BGHZ 133, 168, 173.
128 So *J. Meyer*, in: Internet-Auktion, 26, 37.
129 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 119.

der Zugangsdaten nur dazu, den Authentifizierungsvorgang so sicher zu gestalten, dass das Missbrauchsrisiko minimiert wird. Der Authentifizierungsvorgang findet jedoch nur zwischen dem Account-Inhaber und dem Diensteanbieter als Authentisierungsnehmer statt. Der Geschäftsgegner bekommt von der Internet-Auktionsplattform durch Mitteilung einer elektronischen Willenserklärung lediglich das Ergebnis des Authentisierungsvorgangs als Autorisierung mitgeteilt. Da sich der Account-Inhaber nicht gegenüber dem Geschäftsgegner authentisiert, kann an der Leistungsnähe gezweifelt werden. Bei anerkannten Fallgruppen wie Wertgutachten oder Körperschäden erreicht die Leistung, die der Schuldner erbringen muss, hingegen direkt und in unveränderter Weise den Dritten.[130] Der Dritte kommt somit bestimmungsgemäß nicht in gleicherweise wie der Gläubiger in Berührung mit der Leistung. Die erste Voraussetzung des Schuldverhältnisses mit Schutzwirkungen zu Gunsten Dritter ist somit nicht gegeben.

c) Schutzwürdige Interessen des Gläubigers

413 Die auch als Gläubigernähe bezeichnete zweite Voraussetzung ist, dass der Gläubiger ein schutzwürdiges Interesse an der Einbeziehung des Dritten in die Schutzwirkung des Vertrags hat.[131] Die frühere geforderte Voraussetzung, dass der Gläubiger für „Wohl und Wehe" des Dritten einzustehen habe,[132] ist demnach nicht mehr erforderlich.

414 Die Internet-Auktionsplattform hat durchaus ein Interesse daran, die anderen Nutzer in den Schutzbereich des Vertrags mit dem Account-Inhaber einzubeziehen.[133] Das Interesse besteht darin, dass ein störungs- und manipulationsfreier Handelsablauf gewährleistet werden kann, wodurch auch die Vermögensinteressen der Nutzer geschützt werden.[134] Ferner wird teleologisch erwogen, dass auch die Nutzer ein Interesse daran hätten, dass alle anderen Nutzer mit eingebunden werden, weil der geschützte und der begünstigte Personenkreis identisch sind.[135] Diese Reziprozität ist jedoch

130 Zu den Fallgruppen *Westermann*, in: *Erman*[13], § 328 BGB Rn. 20a, 29.
131 *Gottwald*, in: MüKo-BGB[6], § 328 Rn. 179; *Looschelders*, Schuldrecht AT[11], Rn. 206.
132 *BGH*, Urteil v. 26. 11. 1968, VI ZR 212/66 (Hühnerpest) – BGHZ 51, 91, 96.
133 *Borges*, in: Internet-Auktion, 214, 217; *ders.*, NJW 2005, 3313, 3315.
134 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 119.
135 Ebd., Rn. 119.

nicht ausreichend, um ein schützenswertes Interesse des Gläubigers zu begründen.[136] Das Argument mit der Reziprozität lässt sich nicht für oder gegen die Haftung einwenden. Es handelt sich viel mehr um eine Wertungsfrage.[137] Kern der Argumentation ist, dass ein Nutzer der in einem Fall haften muss, davon profitiert, dass er im anderen Fall den Geschäftsgegner in Haftung nehmen kann. Würde die Haftung dem Grunde nach bestehen, hätte er einmal den Vor- und einmal den Nachteil. Bei der Betrachtung eines Nutzers, der einmal haftet und einmal einen Dritten in Haftung nimmt, hat nur dann einen wirtschaftlichen Vorteil von der Haftung, wenn zufällig die Haftsumme bei der Inanspruchnahme des Dritten höher ist als der Betrag, für den er haften musste. Genauso würde es sich verhalten, wenn die Haftung dem Grunde nach nicht bestehen würde. Wenn er nicht haftbar gemacht werden kann, hat er den Vorteil aus der rechtlichen Wertung. Wenn er seinen Geschäftsgegner nicht in die Haftung nehmen kann, hat er den Nachteil. Die Reziprozität der Regelungen in den AGB ist daher nur eine Zustandsbeschreibung. Mit ihr lässt sich weder für noch gegen eine Haftung argumentieren.

Die Gläubigernähe scheitert jedoch daran, dass alle Nutzer der Internet- 415
Auktionsplattform gleichrangig sind.[138] Jeden Nutzer trifft die Pflicht die Zugangsdaten geheim zu halten. Ebenso hat jeder Nutzer ein Interesse daran, dass alle anderen Nutzer sorgsam mit ihren Zugangsdaten umgehen. Bei dieser Gleichrangigkeit, die auch bei Mieter- und Arbeitnehmerpflichten gegenüber anderen Mietern und Arbeitnehmern besteht, wird die Schutzwirkung verneint.[139] Die Gläubigernähe kann somit nur annehmen, wer entgegen dieser herrschenden Meinung vertritt, dass eine Gleichrangigkeit ausreicht.[140]

---

136 *Borges*, in: Internet-Auktion, 214, 217; *ders.*, NJW 2005, 3313, 3315.

137 Vgl. *Coase*, The Journal of Law & Economics 3 (1960), 1, 2; *Schäfer/C. Ott*[5], S. 248.

138 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 42; *Sonnentag*, WM 2012, 1614, 1619.

139 Für Mieter: *BGH*, Urteil v. 16. 10. 1963, VIII ZR 28/62 – NJW 1964, 33, 34 f.; *Gottwald*, in: MüKo-BGB[6], § 328 Rn. 228. Für Arbeitnehmer: *Jagmann*, in: *Staudinger*[2009], § 328 BGB Rn. 99. Vgl. auch *BGH*, Urteil v. 2. 7. 1996, X ZR 104/94 (Nitrierofen) – BGHZ 133, 168, 173 f.

140 So *Riesenhuber*, Nebenparteien, S. 174 ff., 178 ff.; *ders.*, JZ 1999, 711, 715.

d) Erkennbarkeit für den Schuldner

416 Bei der dritten Voraussetzung, der Erkennbarkeit für den Schuldner, kommt es darauf an, dass die beiden ersten Voraussetzungen für diesen erkennbar sind.[141] Dafür ist es erforderlich, dass das Risiko übersehbar, kalkulierbar und unter Umständen versicherbar ist.[142]

417 Diese Voraussetzung solle bereits gegeben sein, weil der Nutzer bei der Registrierung durch das Lesen der AGB-Klauseln diesen eindeutig den Drittschutz entnehmen könne.[143] Selbst wenn einer Regelung wie § 2 Nr. 7 der eBay-AGB ein Drittschutz zu entnehmen ist, kann allein damit noch nicht begründet werden, dass das Risiko übersehbar und kalkulierbar ist.

418 Man könnte zunächst meinen, dass für die Erkennbarkeit erforderlich sei, dass der Dritte oder die Dritten namentlich bekannt sind. Dies ist hingegen nicht der Fall.[144] Es reicht jedoch aus, dass der Personenkreis bestimmbar ist. Das ist schon gegeben, wenn eindeutig hervorgeht, dass nur eine kleine Personengruppe mit der Leistung in Berührung kommen wird, wie z.B. der potentielle Käufer eines Grundstückes bezüglich der Leistung des Gutachters.[145] Es lässt sich zwar bestimmen, welche Nutzer zu einem gewissen Zeitpunkt bei einem Authentisierungsnehmer wie eBay registriert sind. Die Nutzergruppe ist daher bestimmbar. Für den sich Registrierenden ist diese Nutzergruppe jedoch nicht erkennbar. Nach eigenen Angaben hat eBay über 112 Millionen aktive Nutzer.[146] Damit ist der Personenkreis der eBay-Nutzer größer als die Einwohnerzahl Deutschlands. Die Anzahl der Nutzer kann steigen oder sinken, ohne dass der Account-Inhaber dies erkennen kann. Die an sich bestimmbare Gruppe der eBay-Nutzer ist für den Account-Inhaber daher nicht überschaubar. Er kann daher nicht erkennen, zu welchen Gunsten seine vertragliche Beziehung mit den Authentisierungsnehmer Wirkungen entfalten soll.

---

141 *Looschelders*, Schuldrecht AT[11], Rn. 208.

142 *BGH*, Urteil v. 2. 7. 1996, X ZR 104/94 (Nitrierofen) – BGHZ 133, 168, 137; Urteil v. 7. 5. 2009, III ZR 277/08 – BGHZ 181, 12, Rn. 17; *Gottwald*, in: MüKo-BGB[6], § 328 Rn. 184.

143 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 119.

144 *Mankowski*, CR 2011, 458, 459; *Ernst*, in: IT-Verträge, Kap. 3.13 Rn. 5.

145 *BGH*, Urteil v. 10. 11. 1994, III ZR 50/94 – BGHZ 127, 378, 386.

146 *eBay*, Das Unternehmen.

Darüber hinaus kann der Account-Inhaber das Risiko, das er eingeht, nicht kalkulieren.[147] Weder die Höhe noch die genaue Anzahl der potentiell geschädigten Nutzer sei vorhersehbar.[148] Ferner spricht gegen die Kalkulierbarkeit des Risikos, dass insofern die Möglichkeiten zum Ausspähen der Zugangsdaten eine erhebliche Rolle spielen. Immer neue technische Entwicklungen schaffen immer mehr Wege an die Zugangsdaten zu gelangen. Der Account-Inhaber kann diese Entwicklung nicht vorhersehen und sie daher nicht angemessen bei der Kalkulation des Risikos berücksichtigen. 419

Mit der Annahme eines Schuldverhältnisses mit Schutzwirkungen zu Gunsten Dritter würde teleologisch betrachtet die Haftung zu weit ausufern.[149] Das Schuldverhältnis mit Schutzwirkungen zu Gunsten Dritter wurde geschaffen, um die Schwächen des Deliktsrechts gegenüber Menschen, die Vertragspartnern nahe stehen, auszugleichen.[150] Nur in eng begrenzten Fällen ist die Anwendung des Schuldverhältnisses mit Schutzwirkungen zu Gunsten Dritter zulässig.[151] Eine Haftung gegenüber einer unüberschaubaren Anzahl an Nutzern, beispielsweise alle Personen mit einer E-Mail-Adresse oder einem eBay-Account, lässt sich mit diesem Grundgedanken nicht vereinbaren. 420

e) Schutzbedürftigkeit des Dritten

Die vierte Voraussetzung, auch als Subsidiarität des Schuldverhältnisses mit Schutzwirkungen zu Gunsten Dritter bezeichnet, ist die Schutzbedürftigkeit des Dritten. Der Dritte ist nicht schutzbedürftig, wenn er einen eigenen gleichwertigen Anspruch gegen den Schuldner hat.[152] 421

Ein eigener vertraglicher Anspruch gegen den Account-Inhaber hat der Geschäftsgegner nur, wenn dieser auf das Erfüllungsinteresse haftet. Muss der Account-Inhaber nach Rechtsscheingrundsätzen einstehen, kommt eine Lösung über den Vertrag mit Schutzwirkungen zu Gunsten Dritter nicht 422

147 *Borges*, in: Internet-Auktion, 214, 217; *ders.*, NJW 2005, 3313, 3315; *J. Meyer*, in: Internet-Auktion, 26, 37 f.

148 *Borges*, in: Internet-Auktion, 214, 217.

149 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 21.

150 *Gottwald*, in: MüKo-BGB[6], § 328 Rn. 161.

151 *Herresthal*, in: *Taeger/Wiebe*, 21, 42.

152 *BGH*, Urteil v. 15. 2. 1978, VIII ZR 47/77 – BGHZ 70, 327, 330; *Looschelders*, Schuldrecht AT[11], Rn. 209.

mehr in Betracht. Erst wenn die Rechtsscheinhaftung auf das positive Interesse scheitert, kann dieser Lösungsweg eine Haftung auf das negative Interesse begründen. Der Lösungsweg über das Schuldverhältnis mit Schutzwirkungen zu Gunsten Dritter ist daher eine Ergänzung zu Lösungsansätzen, die dem Geschäftsgegner das positive Interesse gewähren wollen.

f) Umfang der Haftung

423 Bei dem Umfang der Haftung stellt sich zunächst die Frage, ob der Account-Inhaber auf das positive oder negative Interesse des Geschäftsgegners haften muss. Eine Haftung auf das positive Interesse in Form der Erfüllungshaftung kommt nicht in Betracht. Hätte der Account-Inhaber seine Pflicht erfüllt, sorgsam mit den Zugangsdaten umzugehen und diese geheim zu halten, wäre dem Geschäftsgegner keine Willenserklärung zugegangen. Die Haftung beschränkt sich demnach darauf, dass der Geschäftsgegner in einen Zustand versetzt wird, wie wenn er die Willenserklärung nie erhalten hätte. Er bekommt den Schaden, den er durch das Vertrauen in diese Willenserklärung erlitten hat ersetzt, das sog. negative Interesse.

424 Ist der Geschäftsgegner der Käufer einer vermeintlich vom Account-Inhaber angebotenen Sache, erleidet er regelmäßig keinen Schaden. Er hat die Sache nicht bekommen und wenn er dann so gestellt wird, als ob er das Angebot nie gesehen hätte, stünde er ebenso dar. Nur vergebliche Aufwendungen sind ihm zu ersetzen. Darunter fallen Rechtsverfolgungskosten sowie nutzlos gewordene Aufwendungen. Ebenso wie bei § 122 BGB zählen zu den nutzlos gewordenen Aufwendungen die Kosten für die Vertragsdurchführung sowie die Kosten für den Vertragsschluss.[153]

425 Ein Verkäufer erleidet in der Regel einen Schaden, wenn ein vermeintlich vom Account-Inhaber stammendes Höchstgebot nicht von ihm stammt und der Vertrag mit dem Account-Inhaber nicht zustande kommt. Eine Situation, bei der das Höchstgebot des Account-Inhabers nie abgegeben worden ist, würde den Verkäufer so stellen, als käme der Vertrag mit dem Bieter des zweithöchsten Gebotes zustande. Der Bieter des zweithöchsten Gebotes, hätte die Sache zu einem Preis, der einen Bietschritt über dem Angebot des dritthöchsten Bieters liegt, ersteigern können.[154] Im Rahmen seiner Scha-

153 *Singer*, in: *Staudinger*[2012], § 122 BGB Rn. 13.
154 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 122.

denminderungspflicht (§ 254 Abs. 2 S. 1 Var. 2 BGB) muss der Gläubiger versuchen, den Vertragsschluss mit dem zweithöchsten Bieter herbeizuführen. eBay bietet dem Verkäufer eine automatische Möglichkeit, bei Nicht-Zustandekommen des Vertrags mit dem Höchstbieter, dem oder den unterlegenen Bietern die Ware zu dem Preis, den diese geboten hatten, anzubieten.[155]

Gelingt der Verkauf an die unterlegenen Bieter, muss der Verkäufer die Angebotsgebühr, die der Verkäufer zur Präsentation seines Angebotes gezahlt hat, nur wie bei einem störungsfreien Ablauf der Auktion einmalig zahlen. Versucht er eine zweite Auktion, muss der Verkäufer die Angebotsgebühr des zweiten Angebotes tragen, die der ersten Auktion kann er als Schaden ersetzt verlangen. Erzielt er mit der zweiten Auktion einen Verkaufspreis, der über dem Preis, den er bei der ersten Auktion erlangt hätte, liegt, erleidet er insofern keinen Schaden. Liegt der Preis unter demjenigen, den er bei der ersten Auktion erlangt hätte, gehört die Differenz zu seinem negativen Interesse. Diese Differenz kann er als entgangenen Gewinn geltend machen (§ 252 BGB). **426**

g) Zwischenergebnis

Die Haftung für den Missbrauch von Zugangsdaten kann nicht über den Vertrag mit Schutzwirkungen zu Gunsten Dritter gelöst werden.[156] Es fehlt sowohl an der Leistungsnähe des Geschäftsgegners[157] sowie an der Erkennbarkeit für den Account-Inhaber.[158] **427**

III. Lösung über die culpa in contrahendo

Ein weiterer diskutierter Lösungsweg ist die Anwendung der *culpa in contrahendo* (c.i.c.). Demnach hätte der Geschäftsgegner einen Schadensersatz- **428**

155 *eBay*, Angebot an unterlegenen Bieter.

156 So auch *Herresthal*, K&R 2008, 705, 709 f.; *ders.*, in: *Taeger/Wiebe*, 21, 41 f.; *Borges*, NJW 2005, 3313, 3315; *ders.*, in: Internet-Auktion, 214, 217; *Borges/Schwenk/Stuckenberg/Wegener*, S. 280; *Schramm*, in: MüKo-BGB[6], § 164 Rn. 45a; *Klein*, MMR 2011, 450, 451; *Schinkels*, LMK 2011, 320461, 2 c; *Sonnentag*, WM 2012, 1614, 1619.

157 Oben Rn. 410.

158 Oben Rn. 416.

anspruch aus §§ 280 Abs. 1, 311 Abs. 2 Nr. 3, 241 Abs. 2 BGB gegen den Account-Inhaber auf Erstattung seines negativen Interesses.[159] Im Gegensatz zur Lösung über einen Rechtsscheintatbestand bekommt der Geschäftsgegner hier nicht das positive Erfüllungsinteresse, sondern erhält lediglich den Schaden ersetzt, den er durch das Vertrauen auf den Bestand der über den Account abgegebenen Erklärung erlitten hat. Diese Lösung ist somit für den Account-Inhaber weniger belastend, weswegen sie möglicherweise dem Rechtsempfinden der Billigkeit besser entsprechen könnte. Aus rechtsökonomischer Sicht empfiehlt sich in solchen Konstellationen die Haftung auf das negative Interesse.[160]

429 Der Weg über die *culpa in contrahendo* löst das Problem der Haftung für den Missbrauch von Zugangsdaten im Internet inbesondere in Drei-Personen-Konstellationen. Zwei-Personen-Konstellationen, in denen das Problem über die *culpa in contrahendo* gelöst werden kann, sind möglich, kommen aber sehr selten vor. Sobald der Account-Inhaber einen Account mit Zugangsdaten beim Geschäftsgegner hat, bestehen schon vertragliche Vereinbarungen, auf die primär abzustellen ist.[161] Wurde eine Handlung gegenüber dem Geschäftsgegner über einen Account vorgenommen, den der Account-Inhaber bei einem Authentisierungsnehmer, der nicht der Geschäftsgegner ist, hat, besteht eine Drei-Personen-Konstellation. In Zwei-Personen-Konstellationen kann die *culpa in contrahendo* daher nur zur Lösung herangezogen werden, wenn der Account-Inhaber den Account samt Zugangsdaten selbst erstellt hat. Betreibt der Account-Inhaber eines E-Mail-Accounts beispielsweise einen eigenen Mail-Server, hat er einen E-Mail-Account, ohne gleichzeitig einen Vertrag mit einem Authentisierungsnehmer eingegangen zu sein. In diesen seltenen Fällen ist die Anwendung der *culpa in contrahendo* auch in Zwei-Personen-Konstellationen möglich.

1. Allgemein zur culpa in contrahendo *(c.i.c.)*

430 Die *culpa in contrahendo* ist ein aus dem objektiven Recht stammendes gesetzliches Schuldverhältnis, welches aufgrund eines rechtsgeschäftlichen

159 *Oechsler*, MMR 2011, 631, 633; *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 13; *Spindler*, CR 2011, 309, 318; *Sonnentag*, WM 2012, 1614, 1619; *Ultsch*, DZWir 1997, 466, 473; *M. Wolf/Neuner*[10], § 50 Rn. 111.

160 Unten Rn. 655.

161 Siehe oben Rn. 397.

Kontaktes der Parteien entsteht.[162] Die Bezeichnung der *culpa in contrahendo*, Verschulden bei Vertragsverhandlungen,[163] ist zu eng, denn sie deckt nicht alle Fallgruppen des § 311 Abs. 2 BGB ab. Zutreffender ist der Begriff des vorvertraglichen Schuldverhältnisses.[164] Der Gesetzgeber wollte mit der Kodifizierung der *culpa in contrahendo* in § 311 Abs. 2 BGB deren Anwendungsbereich weder einschränken noch ausweiten, sondern nur einen gesetzlichen Anknüpfungspunkt schaffen.[165] Vor der Kodifizierung wurde die *culpa in contrahendo* aus einer Gesamtanalogie zu §§ 122, 179, 366 BGB sowie §§ 307 a.F. BGB hergeleitet.[166] Sie dient dazu, Schutzlücken der deliktischen Haftung wie die Exkulpationsmöglichkeit oder die mangelnde Ersatzfähigkeit reiner Vermögensschäden auszugleichen.[167] Der Kontakt, der zu der Begründung des vorvertraglichen Schuldverhältnisses führt, muss daher intensiver sein, als die Beziehungen zu der Allgemeinheit, die die Jedermann-Pflichten nach §§ 823 ff. BGB auslösen.

Der für die Haftung des Missbrauchs von Zugangsdaten relevante Fall ist **431**
§ 311 Abs. 2 Nr. 3 BGB. Ähnliche geschäftliche Kontakte im Sinne dieser Vorschrift liegen in einem Stadium vor, in dem ein Vertrag zwar noch nicht angebahnt, aber vorbereitet werden soll.[168] Soziale Kontakte reichen für den insoweit eindeutigen Wortlaut von § 311 Abs. 2 Nr. 3 BGB „geschäftliche Kontakte“ nicht aus.[169] Eine einseitige Kontaktaufnahme begründet noch kein vorvertragliches Schuldverhältnis.[170] Die Zusendung einer Werbe-E-Mail reicht daher beispielsweise nicht aus.[171]

Bei einer Stellvertretung wird der Vertretene, wenn Vertretungsmacht be- **432**
steht, regelmäßig Partei des vorvertraglichen Schuldverhältnisses.[172] Aus-

---

162 *S. Lorenz/Riehm*, Rn. 366.
163 *Medicus/S. Lorenz*[20], Rn. 103.
164 Verwendet z.B. von *Brox/Walker*, Schuldrecht AT[37], § 5 Rn. 1.
165 Begr. SMG, BT-Drucks. 14/6040, S. 162.
166 *Larenz*, Schuldrecht[14], Bd. 1, S. 106 ff.
167 *Looschelders*, Schuldrecht AT[11], Rn. 182.
168 Begr. SMG, BT-Drucks. 14/6040, S. 163.
169 *Canaris*, JZ 2001, 499, 520; *Emmerich*, in: MüKo-BGB[6], § 311 Rn. 44.
170 *Löwisch/C. Feldmann*, in: *Staudinger*[2013], § 311 BGB Rn. 104.
171 *Emmerich*, in: MüKo-BGB[6], § 311 Rn. 50; *Gehrlein/Sutschet*, in: *Bamberger/H. Roth*[3], § 311 BGB Rn. 41.
172 *BGH*, Urteil v. 24. 4. 1978, II ZR 172/76 – BGHZ 71, 284, 286; Urteil v. 4. 7. 1983, II ZR 220/82 – BGHZ 88, 67, 68; *A. Stadler*, in: *Jauernig*[15], § 311 BGB Rn. 48.

nahmsweise wird jedoch der Vertreter Vertragspartner, wenn er ein erhebliches Eigeninteresse am angestrebten Vertrag hat.[173]

2. *Subsidiäre Anwendung der* culpa in contrahendo*?*

433 Wann die *culpa in contrahendo* zur Anwendung kommen soll, wird unterschiedlich beurteilt.[174] Einerseits wird die *culpa in contrahendo* subsidiär angewendet. Erst wenn die Rechtsscheinhaftung scheitert, könne über die *culpa in contrahendo* eine Haftung des Account-Inhabers begründet werden.[175] Bereits in Fällen, bei denen eine Vollmachtsurkunde abhandengekommen war und somit die Rechtsscheinhaftung nach § 172 Abs. 1 BGB scheiterte, wurde subsidiär die *culpa in contrahendo* angewandt.[176]

434 Andererseits wird der Lösungsweg über die *culpa in contrahendo* nicht als Ergänzung zur Lösung über die Rechtsscheinhaftung, sondern als Alternative angesehen. Nur die Haftung nach den Grundsätzen der *culpa in contrahendo* sei sachgerecht.[177] Dieses Konzept stammt aus einer Ablehnung der Rechtsscheinhaftung in Form der Anscheinsvollmacht. Zahlreiche Stimmen in der Literatur wollen die Anscheinsvollmacht im bürgerlichen Verkehr nicht anerkennen.[178] Insofern ist es konsequent, beim Missbrauch von Zugangsdaten im Internet auf diese Form der Rechtsscheinhaftung zu verzichten.

435 Unabhängig davon, ob die *culpa in contrahendo* als direkter Lösungsweg oder als Ergänzung einer Rechtsscheinhaftung angewendet wird, müssen deren Voraussetzungen vorliegen.[179] Ob die Voraussetzungen der *culpa in contrahendo* in Konstellationen des Missbrauchs von Zugangsdaten im Internet vorliegen, soll nachfolgend untersucht werden.

---

173 *Valenthin*, in: *Bamberger/H. Roth*[3], § 164 BGB Rn. 40.

174 Offen gelassen von *Ellenberger*, in: *Palandt*[73], § 126a BGB Rn. 12; *Schramm*, in: MüKo-BGB[6], § 164 Rn. 45a; *Singer*, in: *Staudinger*[2012], Vorbem §§ 116 ff. BGB Rn. 57.

175 *Oechsler*, MMR 2011, 631, 633; *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 13; *Ultsch*, DZWir 1997, 466, 473.

176 *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13, 15.

177 *M. Wolf/Neuner*[10], § 50 Rn. 111.

178 *Canaris*, Vertrauenshaftung, S. 49; *ders.*, in: FG 50 Jahre BGH, Bd. 1, 129, 140, 156 ff.; *Flume*[4], § 49 4; *Medicus*[10], Rn. 971; *Pawlowski*, BGB AT[7], Rn. 720; *M. Wolf/Neuner*[10], § 50 Rn. 98; *Schack*[14], Rn. 515.

179 *Pawlowski*, BGB AT[7], Rn. 720.

3. Vorvertragliches Schuldverhältnis

Zunächst müsste daher ein vorvertragliches Schuldverhältnis zwischen dem Account-Inhaber und dem Geschäftsgegner vorliegen. Werden die Zugangsdaten des Account-Inhabers missbraucht, stand er regelmäßig weder in Vertragsverhandlungen (§ 311 Abs. 2 Nr. 1 BGB) mit dem Geschäftsgegner, noch hat sich ein Vertrag zwischen Ihnen angebahnt (§ 311 Abs. 2 Nr. 2 BGB). **436**

Fraglich ist, ob zwischen Ihnen ein ähnlicher geschäftlicher Kontakt im Sinne des § 311 Abs. 2 Nr. 3 BGB bestand. Bei Drei-Personen-Konstellationen hat der Account-Inhaber im Vorfeld des Missbrauchs lediglich den Account mit den Zugangsdaten angelegt. Bei einer E-Mail-Adresse oder elektronischen Signatur schafft er damit lediglich die Möglichkeit mit ihm Kontakt aufzunehmen. Diese Möglichkeit eröffnet er jedermann, der Kenntnis von seiner E-Mail-Adresse erhält. Ein ähnlicher geschäftlicher Kontakt, der einen konkreten Vertrag vorbereitet, ist darin nicht zu sehen.[180] **437**

Bei einer Internet-Auktionsplattform zum Beispiel ist der Teilnehmerkreis im Vergleich zum Einrichten einer E-Mail-Adresse begrenzter und überschaubarer. Groß ist der Teilnehmerkreis dennoch. Mit der Registrierung bei einer Internet-Auktionsplattform schafft der Account-Inhaber zwar die Möglichkeit, dass er Geschäfte mit anderen abschließen kann. Dies dient jedoch nicht zur Vorbereitung eines konkreten Vertragsschlusses mit einer konkreten Partei, in diesem Fall einem möglichen späteren Geschäftsgegner, sondern schafft nur die Möglichkeit zu einer Kontaktaufnahme.[181] Allein diese Möglichkeit mit dem Geschäftsgegner einen Vertrag abschließen zu können, reicht nicht aus.[182] Ein vorvertragliches Schuldverhältnis liegt insoweit nicht vor.[183] **438**

Unter § 311 Abs. 2 Nr. 3 BGB fallen auch Fälle, in denen der eine Teil in einem von dem anderen Teil zu vertretendem Irrtum über die Person des Gläubigers oder des Schuldners ist.[184] Man könnte erwägen, diese Entschei- **439**

---

180 Vgl. *Kuhn*, S. 244.

181 *Herresthal*, K&R 2008, 705, 709; *ders.*, in: *Taeger/Wiebe*, 21, 41.

182 Vgl. *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 21.

183 So auch *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 181; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 23; *Hanau*, Handeln unter fremder Nummer, S. 215.

184 *BGH*, Urteil v. 20. 3. 2001, X ZR 63/99 – NJW 2001, 2716, 2717 f.; *Emmerich*, in: MüKo-BGB[6], § 311 Rn. 50.

dung für den Missbrauch von Zugangsdaten im Internet zu übertragen. Immerhin ist für den Geschäftsgegner nicht erkennbar, wer die elektronische Willenserklärung abgegeben hat. Bei dem hervorgerufenen Irrtum über die Person des Gläubigers oder Schuldners ging es jedoch darum, dass der In-Anspruch-Genommene Kontakt mit dem Anspruchsteller hatte und der Anspruchsteller redlicherweise davon ausgehen durfte, dass der Gesprächspartner auch sein Vertragspartner war. An einem Kontakt zwischen dem Geschäftsgegner und dem Account-Inhaber fehlt es jedoch beim Missbrauch von Zugangsdaten im Internet. Ein vorvertragliches Schuldverhältnis lässt sich daher auf diese Weise nicht begründen.

440 Ein vorvertragliches Schuldverhältnis entsteht lediglich, wenn der Account-Inhaber und der Geschäftsgegner in konkrete Vertragsverhandlungen eintreten.[185] Dafür ist erforderlich, dass der Account-Inhaber bewusst an den Geschäftsgegner herantritt.[186] Konkrete Vertragsverhandlungen entstehen auf einer Internet-Auktionsplattform zum Beispiel dadurch, dass der Interessent dem Verkäufer eine Frage zur Auktion stellt.[187] Missbraucht anschließend ein Dritter den Account des Inhabers um den Gegenstand zu erwerben, bestünde ein vorvertragliches Schuldverhältnis, das die Haftung aus §§ 280 Abs. 1, 311 Abs. 2 Nr. 3, 241 Abs. 2 BGB begründen kann. Dieser Fall, dass der Account-Inhaber vorher mit dem Geschäftsgegner Kontakt aufnimmt und später ein Dritter diesem konkreten Geschäftsgegner gegenüber die Zugangsdaten missbraucht, ist sehr unwahrscheinlich. Bei E-Mails oder elektronisch signierten Willenserklärungen müsste es ebenfalls vorher einen irgendwie gearteten Kontakt zwischen Account-Inhaber und Geschäftsgegner geben. Dieser wird ebenso in vielen Fällen nicht vorliegen, sodass es auch insoweit an einem vorvertraglichem Schuldverhältnis fehlt.[188]

441 Ein Dritter kann das vorvertragliche Schuldverhältnis für den Account-Inhaber nur begründen, wenn dieser Verhandlungsgehilfe ist oder sonst mit Vertretungsmacht handelt.[189] Dies ist beim Missbrauch von Zugangsdaten jedoch gerade nicht der Fall.

442 Regelmäßig wird daher kein vorvertragliches Schuldverhältnis im Sinne des § 311 Abs. 2 BGB, was eine Haftung aus *culpa in contrahendo* begrün-

185 *Oechsler*, MMR 2011, 631, 633.
186 *Peters*, AcP 179 (1979), 214, 235.
187 *Herresthal*, K&R 2008, 705, 709; *ders.*, in: *Taeger/Wiebe*, 21, 41.
188 *Dörner*, AcP 202 (2002), 363, 391.
189 *Kuhn*, S. 244; *Paefgen*, Bildschrimtext, S. 78.

den könnte, vorliegen. Der Befund, dass in dem vorvertraglichen Schuldverhältnis nicht die entscheidende Anwendungshürde der *culpa in contrahendo* liegen solle,[190] verwundert anhand dieser Ergebnisse. Die zweigliedrige Begründung dieses Befundes vermag nicht zu überzeugen.

Zum einen sei die Haftung für abhandengekommene Willenserklärungen 443
eine mit der Haftung für den Missbrauch von Zugangsdaten vergleichbare Situation.[191] Bei abhandengekommenen Willenserklärungen haftet der Erklärende analog zu § 122 BGB auf das negative Interesse des Erklärungsempfängers.[192] Die Haftung auf das negative Interesse auf den Fall des Missbrauchs von Zugangsdaten, insbesondere in Fällen ohne Weitergabe durch den Account-Inhaber, zu übertragen, mag zu einem gerechten Ergebnis führen. Mit diesem Vergleich wird jedoch nicht etwa eine dogmatische Vergleichbarkeit behauptet, sondern lediglich aufgezeigt, dass das negative Interesse Rechtsfolge der Vertrauenshaftung sein kann. Das erklärt jedoch noch nicht, welche Art von Vertrauensschutz gewährt werden soll. Die *culpa in contrahendo* basiert auf dem Grundgedanken des Rechtsgüterschutzes bei gewährtem Vertrauen im Rahmen einer sich anbahnenden Sonderverbindung nach schuldhaften Pflichtverletzungen.[193] § 122 BGB schützt hingegen das Vertrauen des Erklärungsempfängers im Rahmen einer verschuldensunabhängigen Vertrauenshaftung[194] und ist wegen seiner abweichender Voraussetzungen und seinem abweichenden Haftungsgrund kein Unterfall der *culpa in contrahendo*.[195] Anstatt den dogmatischen Weg dabei über die *culpa in contrahendo* zu suchen, liegt es näher, beim Vergleich zu den abhandengekommenen Willenserklärungen den Weg analog zu § 122 BGB zu ergründen.[196]

Zum anderen wird darauf verwiesen, dass der *BGH* die Haftung in ähn- 444
lichen Fällen über die *culpa in contrahendo* löse.[197] In der Entscheidung

190 *Oechsler*, AcP 208 (2008), 565, 582.

191 *Oechsler*, AcP 208 (2008), 565, 582; *ders.*, MMR 2011, 631, 633; *Sonnentag*, WM 2012, 1614, 1619.

192 Unten Rn. 476.

193 *Emmerich*, in: MüKo-BGB[6], § 311 Rn. 40 ff.

194 *Armbrüster*, in: MüKo-BGB[6], § 122 Rn. 1.

195 *Armbrüster*, in: MüKo-BGB[6], § 122 Rn. 13; *Bork*[3], Rn. 932; *Flume*[4], § 21 7; *Singer*, AcP 201 (2001), 93, 96; **a.A.** *Lobinger*, Rechtsgeschäftliche Verpflichtung, S. 207 ff.

196 Dazu unten Rn. 471.

197 *Oechsler*, AcP 208 (2008), 565, 581 f.; *ders.*, MMR 2011, 631, 633 unter Verweis auf *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13, 15; Urteil v.

über die abhandengekommene Willenserklärung in Form einer Vollmachtsurkunde, wendet der *BGH* lediglich die „Grundsätze, wie sie zu der Haftung auf das negative Interesse entwickelt worden sind,“[198] an. Ob damit die *culpa in contrahendo* oder die Haftung analog § 122 BGB gemeint sind, bleibt dabei offen, wobei letzteres anhand der Begründung mit der abhandengekommenen Willenserklärung näher liegt.[199]

445 Selbst wenn die Ausführungen des *BGH* so verstanden werden, dass die *culpa in contrahendo* Anwendung findet, trifft er keine Aussage über deren Voraussetzungen. In der anderen angeführten Entscheidung zeigt der *BGH*, dass er die *culpa in contrahendo* neben § 122 BGB für anwendbar hält.[200] Er lehnt die Haftung aus der *culpa in contrahendo* bereits wegen des im Fall fehlenden Verschuldens ab, ohne auf die weiteren Voraussetzungen einzugehen.[201] Ob ein vorvertragliches Schuldverhältnis durch das Ausfertigen der Willenserklärung entstanden ist, kann daher nicht anhand der *BGH*-Rechtsprechung begründet werden. Teilweise wird vertreten, dass die Fälle von abhandengekommenen Willenserklärungen oder vom fehlendem Erklärungsbewusstsein über die *culpa in contrahendo* zu lösen seien.[202] Einschränkend wird jedoch betont, dass die Voraussetzungen der *culpa in contrahendo* vorliegen müssen.[203] Teilweise wird angenommen, dass das Anfertigen der Willenserklärung bereits einen ähnlichen geschäftlichen Kontakt im Sinne des § 311 Abs. 2 S. Nr. 3 BGB darstellt.[204] Der Kontakt zwischen dem Aussteller der Willenserklärung und dem Erklärungsempfänger ist jedoch noch nicht so intensiv, dass von einem ähnlichen geschäftlichen Kontakt ausgegangen werden kann. Es fehlt daher bei abhandengekommenen Willenserklärungen regelmäßig an den Voraussetzungen der *culpa in contrahendo*.[205]

---

20. 3. 1986, III ZR 236/84 – NJW 1986, 2104, 2106; *BGH*, Urteil v. 4. 3. 2004, III ZR 96/03 (Dialer) – BGHZ 158, 201.

198 *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13, 15.

199 *Canaris*, JZ 1976, 132, 134.

200 *BGH*, Urteil v. 20. 3. 1986, III ZR 236/84 – NJW 1986, 2104, 2106.

201 Ebd., 2106.

202 *OLG Düsseldorf*, Urteil v. 2. 1. 1982, 5 U 150/81 – OLGZ 1982, 240, 245; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 7; *Medicus*[10], Rn. 266, 608; *Larenz/M. Wolf*[9], § 48 Rn. 12; *Bork*[3], Rn. 1527.

203 *OLG Düsseldorf*, Urteil v. 2. 1. 1982, 5 U 150/81 – OLGZ 1982, 240, 245; *Schilken*, in: *Staudinger*[2009], § 172 BGB Rn. 7.

204 *Musielak*, JuS 2004, 1081, 1084; *H. Köhler*, BGB AT[37], § 6 Rn. 12.

205 *Larenz/M. Wolf*[9], § 48 Rn. 12; *Bork*[3], Rn. 1527.

Selbst wenn ein ähnlicher geschäftlicher Kontakt bei der abhandengekommenen Willenserklärung vorläge, lässt sich dies nicht auf den Missbrauch von Zugangsdaten im Internet übertragen. Während bei einer abhandengekommenen Willenserklärung der Geschäftsgegner schon feststeht und dadurch konkretisiert ist, lassen sich mit dem Missbrauch von Zugangsdaten gegenüber einer Vielzahl von potentiellen Geschäftsgegnern Willenserklärungen abgeben. Das Vorliegen eines vorvertraglichen Schuldverhältnisses im Sinne des § 311 Abs. 2 BGB lässt sich mit dem Verweis auf diese Entscheidungen daher nicht begründen. 446

Dagegen wird eingewendet, dass die ursprüngliche, nicht kodifizierte Rechtsfigur der *culpa in contrahendo* einen weiteren Anwendungsbereich als die Kodifizierung in § 311 Abs. 2 BGB hatte.[206] Es entsprach der Intention des Gesetzgebers mit der Kodifizierung der *culpa in contrahendo* deren Anwendungsbereich weder zu beschränken, noch auszuweiten, sowie sie der Rechtsfortbildung zugänglich zu machen.[207] Im Kern ging es jedoch vor der Kodifizierung ebenfalls um die Aufnahme von Vertragsverhandlungen oder eines sie vorbereitenden geschäftlichen Kontakts.[208] Wenn wie in Fällen des Missbrauchs von Zugangsdaten im Internet kein Kontakt zwischen den beiden Parteien besteht oder bestand, kann kein vorvertragliches Schuldverhältnis angenommen werden. 447

Der Verweis[209] auf den Dialer-Fall[210] kann ebenfalls kein vorvertragliches Schuldverhältnis zwischen dem Account-Inhaber und dem Geschäftsgegner beim Missbrauch von Zugangsdaten begründen. In dem Fall hatte der Anspruchsgegner durch die Täuschung einer irreführender Werbung einen Schaden beim Anspruchsinhaber verursacht. Insofern lag ein geschäftlicher Kontakt zwischen den beteiligten Parteien vor.[211] Zur Begründung eines vorvertraglichen Schuldverhältnisses beim Missbrauch von Zugangsdaten im Internet eignet sich dieser Fall daher nicht. Die *culpa in contrahendo* dient dazu bei Inanspruchnahme oder Gewährung eines besonderen Vertrauens die Parteien zu schützen.[212] Die dazu erforderliche Nähe 448

206 *Oechsler*, AcP 208 (2008), 565, 582.
207 Begr. SMG, BT-Drucks. 14/6040, S. 162.
208 *Larenz*, Schuldrecht[14], Bd. 1, S. 109. Bereits früher *Jhering*, JherJB 4 (1861), 1, 2: „werdende Contractsverhältnisse".
209 *Oechsler*, AcP 208 (2008), 565, 581 f.
210 *BGH*, Urteil v. 4. 3. 2004, III ZR 96/03 (Dialer) – BGHZ 158, 201.
211 Ebd., 211 f.
212 *Emmerich*, in: MüKo-BGB[6], § 311 Rn. 41.

besteht beim Missbrauch von Zugangsdaten im Internet nicht, weil die Parteien sich gegenseitig keine erweiterte Einwirkungsmöglichkeit in die eigenen Rechte und Rechtsgüter gewähren.

449 Ein ähnlicher geschäftlicher Kontakt im Sinne des § 311 Abs. 2 Nr. 3 BGB liegt daher beim Missbrauch von Zugangsdaten nicht vor. Er lässt sich auch nicht durch die Übertragung von Wertungen von abhandengekommenen Willenserklärungen oder Vollmachtsurkunden herleiten. Auf das Erfordernis des ähnlichen geschäftlichen Kontaktes kann nicht verzichtet werden, weil ansonsten die Haftung ausufern würde.[213] Die *culpa in contrahendo* passt somit strukturell mit der Ausrichtung auf schuldhafte Pflichtverletzungen bei Bestehen von sich anbahnenden Sonderverbindungen nicht zu der Situation beim Missbrauch von Zugangsdaten im Internet. Die erste Voraussetzung der *culpa in contrahendo* ist somit regelmäßig nicht gegeben.

4. Pflichtverletzung

450 Zweite Voraussetzung einer Haftung aus *culpa in contrahendo* ist die Verletzung einer Nebenpflicht. Grundsätzlich trifft die gesetzliche Regelung der §§ 311 Abs. 2 Nr. 3, 241 Abs. 2 BGB hauptsächlich eine Aussage über das Vorliegen eines vorvertraglichen Schuldverhältnisses. Der Umfang der Nebenpflichten ist in § 241 Abs. 2 BGB mit unbestimmten Rechtsbegriffen geregelt. Die vorvertraglichen Pflichten müssen anhand der Intensität des rechtsgeschäftlichen Kontakts konkretisiert werden.[214] Als Pflichtverletzung bieten sich beim Missbrauch von Zugangsdaten im Internet zwei Anknüpfungspunkte an: das Handeln des Account-Inhabers sowie das Handeln des Dritten.

a) Verhalten des Account-Inhabers

451 Der Account-Inhaber erstellt den Account mit den Zugangsdaten. Im Anschluss kann darüber nachgedacht werden, eine mögliche Pflicht, die Zugangsdaten keinem anderen zugänglich zu machen, als Anknüpfungspunkt für die Pflichtverletzung zu werten. Zum einen wird eine Pflichtverlet-

213 *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, insoweit nicht abgedruckt Rn. 20; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 23.

214 *S. Lorenz/Riehm*, Rn. 372.

zung darin gesehen, wenn der Account-Inhaber die Zugangsdaten fahrlässig preisgibt.[215] Zum anderen stelle auch eine unsorgfältige Aufbewahrung der Zugangsdaten[216] oder die nicht hinreichende Sicherung des Passworts[217] eine Pflichtverletzung dar. Zusammenfassend lässt sich der unsorgfältige Umgang des Account-Inhabers mit den Zugangsdaten daher als diskutierte Pflichtverletzung ansehen.

Zunächst kann bezweifelt werden, dass den Account-Inhaber die Pflicht **452**
zum sorgfältigen Umgang mit seinen Zugangsdaten bezüglich aller seiner Accounts gegenüber dem Geschäftsgegner trifft. Selbst wenn der Account-Inhaber aus Vertrag zum Authentisierungsnehmer verpflichtet ist, die Zugangsdaten geheim zu halten, würde daraus nicht folgen, dass diese Verpflichtung auch gegenüber dem Geschäftsgegner gilt. Vielmehr müsste eine eigenständige Pflicht zur Geheimhaltung der Zugangsdaten aus dem vorvertraglichen Schuldverhältnis mit dem Geschäftsgegner bestehen. Eine mögliche deliktische Pflicht gegenüber jedem zur Sicherung der Zugangsdaten[218] wäre zu übertragen. Teilweise wird wegen der Identifikationsfunktion von Accounts eine Geheimhaltungspflicht begründet, wobei diese Argumentation zirkulär erscheint.[219] Diese Pflicht könnte bejaht werden, wenn ein regelmäßiger Kontakt zwischen dem Account-Inhaber und dem Geschäftsgegner vor dem Missbrauch der Zugangsdaten bestand. Erhält der Geschäftsgegner mehrfach über den Account Mitteilungen vom Account-Inhaber und bestätigt sich die Echtheit dieser Mitteilungen über andere Kommunikationskanäle, könnte der Geschäftsgegner ein schützenswertes Vertrauen (§ 241 Abs. 2 BGB) in die Echtheit künftiger Mitteilungen durch denselben Account entwickeln. Dieses Vertrauen müsste der Account-Inhaber dann durch den sorgfältigen Umgang mit den Zugangsdaten schützen. Selbst bei regelmäßigem Kontakt zwischen dem Account-Inhaber und dem Geschäftsgegner erscheint die Schutzwürdigkeit des Vertrauens wegen der zahlreichen Missbrauchsmöglichkeiten[220] fraglich.

Entsteht ein vorvertragliches Schuldverhältnis erst durch eine Frage des **453**
Account-Inhabers bezüglich einer Auktion des Geschäftsgegners und missbraucht der Dritte die vor Entstehung des vorvertraglichen Schuldverhältnis-

---

215 *M. Wolf/Neuner*[10], § 50 Rn. 111.
216 *Oechsler*, AcP 208 (2008), 565, 581.
217 *Sonnentag*, WM 2012, 1614, 1619.
218 Zu den ungeklärten Konturen dieser deliktischen Pflicht unten Rn. 753.
219 Unten Rn. 558.
220 Dazu oben Rn. 124 ff.

ses erlangten Zugangsdaten, stellt sich die Frage, ob die Pflichtverletzung vor Begründung des Schuldverhältnisses begangen werden kann. Angenommen der Dritte hat die Zugangsdaten erlangt, bevor der Account-Inhaber mit dem Geschäftsgegner in Kontakt getreten ist. Die Pflicht zum sorgfältigen Umgang hätte der Account-Inhaber in diesem Fall verletzt, bevor das vorvertragliche Schuldverhältnis bestand. Problematisch ist daher, ob ein potentieller Schuldner eine Pflicht aus einem Schuldverhältnis verletzen kann, bevor das Schuldverhältnis und damit die Pflicht begründet wurde. Ein Blick auf die Anwendungsfälle der *culpa in contrahendo* soll diese Frage beantworten.

454 Zunächst sollen die Anwendungsfälle der *culpa in contrahendo* bezüglich der Verkehrssicherungspflichten betrachtet werden.[221] In dem „Linoleumrollen"-Fall des *RG* wollte der Handlungsgehilfe des Verkäufers der potentiellen Käuferin aus den Linoleumrollen ein gewisses Muster zeigen.[222] Dazu stellte er zwei Rollen beiseite. Diese beiden Rollen fielen um und trafen die potentielle Käuferin. In diesem Fall verletzte der Verhandlungsgehilfe des Verkäufers die Pflicht zur Verkehrssicherung durch aktives Handeln nach Begründung des vorvertraglichen Schuldverhältnisses.

455 Anders lag der Sachverhalt beim vom *BGH* zu entscheidenden „Salatblatt"-Fall. In dem Fall rutschte die Tochter einer Supermarkt-Kundin auf einem Salatblatt aus.[223] Ein möglicher Anknüpfungspunkt für die Pflichtverletzung ist der Vorwurf, das Salatblatt auf den Boden fallen gelassen zu haben. Angenommen dies geschah, bevor die Kundin und ihre Tochter den Laden betraten, stellt sich die Frage, ob an diese Pflichtverletzung angeknüpft werden kann. Zum einen fällt dies schwer, weil wahrscheinlich weder der Supermarktbetreiber, noch einer seiner Angestellten das Salatblatt haben fallen lassen. Vielmehr ist anzunehmen, dass dies ein Kunde tat.[224] Die Pflichtverletzung, an die angeknüpft wird, ist daher nicht die Handlung des Fallenlassens eines Salatblatts, sondern das Unterlassen der ordnungsgemäßen Sicherung der beherrschten Gefahren im Rahmen einer Verkehrssicherungspflicht. Diese Verkehrssicherungspflicht besteht zwar grundsätzlich jederzeit, also auch bevor die konkrete Kundin mit ihrer Tochter den Supermarkt betreten hat. Im Rahmen des vorvertraglichen Schuldverhältnisses kann ihm jedoch vorgeworfen werden, dass er diese Pflicht auch gegenüber

221 Dazu *Emmerich*, in: MüKo-BGB[6], § 311 Rn. 63 ff.
222 *RG*, Urteil v. 7. 12. 1911, VI 240/11 (Linoleumrollen) – RGZ 78, 239.
223 *BGH*, Urteil v. 28. 1. 1976, VIII ZR 246/74 (Salatblatt) – BGHZ 66, 51.
224 Ebd., 53.

der Kundin ab deren Eintreten in den Supermarkt verletzt hat. Insofern steht hier die Verletzung einer Pflicht nach der Begründung des vorvertraglichen Schuldverhältnisses im Raum. Bei den Fällen der Verkehrssicherungspflicht geht es daher um Pflichtverletzungen, die nach Begründung des vorvertraglichen Schuldverhältnisses begangen wurden.

456 Bei den Fällen der Aufklärungspflichten wird ebenfalls an eine Pflicht angeknüpft, die nach Entstehen des vorvertraglichen Schuldverhältnisses entstanden ist.[225] In einem vom *BGH* zu entscheidenden Fall hatte der Verkäufer eines Hauses zwei Jahre vor dem Verkauf Umbauarbeiten vorgenommen, für die er keine behördliche Genehmigung eingeholt hatte.[226] Der Verkäufer informierte den Käufer nicht über die fehlende behördliche Genehmigung der Räume, wodurch der Streit entstand. Man könnte auf die Idee kommen, dass die Pflicht des Verkäufers nur mit Baugenehmigung zu bauen, als Anknüpfungspunkt für die Pflichtverletzung genommen wird. Dagegen spricht jedoch, dass diese Pflicht vor Entstehen des vorvertraglichen Schuldverhältnisses entstanden ist und sie nicht gegenüber dem späteren Käufer besteht. Die Pflicht, die der Verkäufer dem Käufer gegenüber verletzt hat, ist vielmehr, dass er ihn nicht aufgeklärt hat, dass er ohne Genehmigung gebaut hat.[227] Diese Pflicht hat der Verkäufer nach Entstehen des vorvertraglichen Schuldverhältnisses verletzt. Der Blick auf zwei bedeutende Anwendungsfälle der *culpa in contrahendo* zeigt, dass stets an eine Pflichtverletzung angeknüpft wird, die nach Entstehen des vorvertraglichen Schuldverhältnisses verletzt wird.

457 Dieser Befund wird systematisch durch § 311a Abs. 2 BGB bestätigt. Bei dieser Haftung für die anfängliche Unmöglichkeit kommt es nicht darauf an, dass der Schuldner die Unmöglichkeit herbeigeführt hat.[228] Die Herbeiführung der Unmöglichkeit fand vor dem Vertragsschluss statt. Gegenüber dem Gläubiger besteht zu diesem Zeitpunkt noch nicht die Pflicht, die Unmöglichkeit zu verhindern. Vielmehr statuiert § 311a Abs. 2 BGB eine Garantiehaftung für das Leistungsversprechen beim Vertragsschluss, bei der nach § 311a Abs. 2 S. 2 BGB die mangelnde Kenntnis einen Exkulpa-

---

225 Dazu *Löwisch/C. Feldmann*, in: *Staudinger*[2013], § 311 BGB Rn. 117 ff.

226 *BGH*, Urteil v. 2. 3. 1979, V ZR 157/77 – NJW 1979, 2243.

227 Ebd.

228 Die Herbeiführung der Unmöglichkeit begründet nach einer Ansicht das Vertretenmüssen im Rahmen der Haftung nach §§ 280 Abs. 1, Abs. 3, 283 BGB, *Oetker*, in: MüKo-BGB[6], § 283 Rn. 6 m.w.N.

tionsgrund darstellt.[229] Während des Vertragsschlusses soll der Schuldner sich über seine Leistungsfähigkeit im Bilde sein, weil er durch den Vertragsschluss das Risiko übernimmt, die Leistung nicht erbringen zu können.[230] Systematisch zeigt der von den §§ 280 ff. BGB abweichende Anknüpfungspunkt des § 311a Abs. 2 BGB daher, dass eine Pflicht aus dem Vertrag erst schuldhaft nach oder bei Entstehen des Schuldverhältnisses verletzt werden kann.

458 Der Blick auf die Anwendungsfälle der *culpa in contrahendo* sowie die systematische Betrachtung des § 311a Abs. 2 BGB haben gezeigt, dass eine mögliche Pflicht regelmäßig erst nach Begründen des Schuldverhältnisses verletzt wird. Der unsorgfältige Umgang mit den Zugangsdaten[231] scheidet daher als Anknüpfungspunkt für die Pflichtverletzung regelmäßig aus, da der Account-Inhaber häufig mit den Zugangsdaten vor Begründung des vorvertraglichen Schuldverhältnisses unsorgfältig umgegangen ist. Denn ein Schuldverhältnis kann in den Drei-Personen-Konstellationen der *culpa in contrahendo*, bei denen der Account-Inhaber beim Geschäftsgegner keinen Account besitzt und mit diesem womöglich vor der Anbahnung des Vertrages noch keinen Kontakt hatte, erst kurz vor dem Missbrauch der Zugangsdaten entstehen. Als Pflichtverletzung kommt daher regelmäßig nur in Betracht, dass der Account-Inhaber den Missbrauch der Zugangsdaten nicht verhindert oder den Geschäftsgegner nicht aufgeklärt hat, dass seine Zugangsdaten von Dritten wegen seines unsorgfältigen Umgangs missbraucht werden könnten. Während der Account-Inhaber bei ersterem möglicherweise fahrlässig handelt, handelt er bei letzterem nur in seltenen Fällen schuldhaft.[232]

b) Verhaltenszurechnung als Anknüpfungspunkt?

459 Man könnte erwägen, dass dem Account-Inhaber das Verhalten des handelnden Dritten zugerechnet wird. Für abhandengekommene Vollmachtsurkunden wird vertreten, dass die *culpa in contrahendo* in Betracht kommt, wenn der Aussteller sich das Verhalten des Vertreters nach § 278 BGB zurechnen

229 *Canaris*, in: FS Heldrich, 11, 29 ff.; *Riehm*, in: FS Canaris, Bd. 1, 1079, 1080 f.
230 *Riehm*, in: FS Canaris, Bd. 1, 1079, 1081.
231 *Oechsler*, AcP 208 (2008), 565, 581; *M. Wolf/Neuner*[10], § 50 Rn. 111.
232 Dazu unten Rn. 462.

lassen muss.[233] Ein dazu denkbarer Fall wäre, dass ein Verhandlungsgehilfe des Geschäftsherren eine Vollmachtsurkunde entwendet, um den Vertrag als Vertreter zu schließen.

Eine Übertragung dieses Gedankens auf den Missbrauch von Zugangs- **460**
daten fällt schwer. Ein vorvertragliches Schuldverhältnis kann in diesem Bereich z.B. mit der Stellung einer Frage zu einem Angebot auf einer Internet-Auktionsplattform entstehen. In dieses Geschehen müsste der Dritte eingebunden werden. Stellt der Dritte eine Frage über den Account des Accounts-Inhabers, dann sind zwei Fälle denkbar. Einerseits könnte der Dritte an die Zugangsdaten ohne eine Weitergabe durch den Account-Inhaber gekommen sein. In diesem Fall kann dem Account-Inhaber das Verhalten des Dritten nicht nach § 278 BGB zugerechnet werden. Hat er die Zugangsdaten andererseits vom Account-Inhaber erhalten und mit dessen Einverständnis gehandelt, kann dem Account-Inhaber das Verhalten des Dritten eventuell nach § 278 BGB zugerechnet werden. Missbraucht er später diese Zugangsdaten, kann diese Pflichtverletzung dem Account-Inhaber zugerechnet werden, falls er nicht bereits durch die Erklärung des Dritten gebunden ist.

Der Anspruch kommt nur in Betracht, wenn sich der Vertretene das Ver- **461**
halten des Handelnden nach § 278 BGB zurechnen lassen muss.[234] Das wird regelmäßig scheitern, weil der Account-Inhaber den Handelnden nicht bewusst bevollmächtigt hat.[235] Bei Dauerschuldverhältnissen hingegen, wie dem Vertrag zwischen einem Internetkunden und dem Internet Service Provider (ISP), kommt eine Zurechnung nach § 278 Abs. 1 BGB in Betracht.[236]

5. Verschulden

Da die Zurechnung einer Pflichtverletzung durch den handelnden Dritten re- **462**
gelmäßig ausscheidet, wird hier betrachtet, unter welchen Voraussetzungen der Account-Inhaber eine Verletzung der möglichen Pflichten zu vertreten hat. Zu verschulden hat der Account-Inhaber Vorsatz und Fahrlässigkeit (§ 276 Abs. 1 S. 1 BGB). Fahrlässig handelt, wer die im Verkehr erforder-

---

233 *Larenz/M. Wolf*[9], § 48 Rn. 12; *Schramm*, in: MüKo-BGB[6], § 172 Rn. 5.

234 *Larenz/M. Wolf*[9], § 48 Rn. 12; *Peters*, AcP 179 (1979), 214, 237; *Schramm*, in: MüKo-BGB[6], § 172 Rn. 5.

235 Vgl. *Peters*, AcP 179 (1979), 214, 236.

236 *Hanau*, Handeln unter fremder Nummer, S. 165 f.

liche Sorgfalt außer Acht lässt (§ 276 Abs. 2 BGB). Eine Begrenzung der Haftung auf grobe Fahrlässigkeit kommt nicht in Betracht.[237]

463 Man kann erwägen, den Verschuldensmaßstab großzügig auszulegen,[238] weil viele Nutzer sich im Internet erst noch orientieren. Ein entsprechend großzügiger Verschuldensmaßstab lässt sich in der früheren *BGH*-Judikatur feststellen.[239] Eine Verschärfung sei jedoch mit zunehmender Vertrautheit der Nutzer mit dem Medium Internet zu erwarten.[240] Der *BGH* wendet jedoch auch in neueren Entscheidungen einen vom Durchschnittsnutzer leicht zu erfüllenden Sorgfaltsmaßstab an.[241] Der Sorgfaltspflichtverstoß des Account-Inhabers ist je nach Weg, über den die Zugangsdaten ausgespäht wurden, zu bestimmen.[242]

464 Fraglich ist, unter welchen Umständen der Account-Inhaber die mangelnde Verhinderung eines Missbrauchs zu vertreten hat. Damit diese Pflicht besteht, muss der Account-Inhaber in einem ersten Schritt so unsorgfältig mit den vertraulichen Zugangsdaten umgegangen sein, dass sie einem Dritten zugänglich sind. Regelmäßig wird der Account-Inhaber nicht mitbekommen, dass der Dritte im Besitz der Zugangsdaten ist und die Möglichkeit hat, diese zu missbrauchen. Zwar handelte er häufig fahrlässig in Bezug auf den Umgang mit den Zugangsdaten, dies bedeutet jedoch nicht gleichzeitig, dass er auch bezüglich der Verhinderung des Missbrauchs durch den Dritten fahrlässig gehandelt hat.

465 Relevant für diese Pflichtverletzung ist, ob der Account-Inhaber nach Entstehen des vorvertraglichen Schuldverhältnisses die im Verkehr erforderliche Sorgfalt zur Verhinderung des Missbrauchs beachtet hat. Insofern muss er lediglich auf Indizien reagieren, die darauf hindeuten, dass eine fremde Person seinen Account mit den Zugangsdaten benutzt. Hat er Anhaltspunkte dafür, dass ein Dritter die Zugangsdaten zu seinem Account benutzt, entspricht es der im Verkehr erforderlichen Sorgfalt diese zu ändern, um einen zukünftigen Missbrauch zu verhindern.

---

237 Unten Rn. 674.

238 So *Oechsler*, AcP 208 (2008), 565, 582.

239 *BGH*, Urteil v. 4. 3. 2004, III ZR 96/03 (Dialer) – BGHZ 158, 201, 209 ff.

240 *Oechsler*, AcP 208 (2008), 565, 582.

241 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 34.

242 Dazu unten Rn. 696 ff.

Zeigt das System an, wann der letzte Login vorlag,[243] hat der Account-Inhaber einen Anhaltspunkt die Verwendung des Accounts durch den Dritten festzustellen. Regelmäßig wird jedoch das erste Anzeichen für die Tatsache, dass ein Dritter im Besitz der Zugangsdaten ist, sein, dass dieser die Zugangsdaten missbraucht. Erst nach dem ersten Missbrauchsfall hat der Account-Inhaber daher das Wissen und die Möglichkeit einen zukünftigen Missbrauch zu verhindern. Für den Fall des ersten Missbrauchs hat er die Pflichtverletzung somit regelmäßig nicht zu vertreten. 466

6. Umfang der Haftung

Der Unterschied des Lösungswegs über die *culpa in contrahendo* besteht im Umfang der Haftung. Während eine Lösung über die Anscheinsvollmacht oder die allgemeinen Rechtsscheingrundsätze primär auf eine Haftung auf das positive Interesse abzielen, kommt der Ersatz des Erfüllungsschadens bei der *culpa in contrahendo* nicht in Betracht. Das negative Interesse, das gemäß §§ 280 Abs. 1, 311 Abs. 2 Nr. 3, 241 Abs. 2 BGB ersatzfähig ist, umfasst häufig vergebliche Aufwendungen sowie Rechtsanwaltskosten.[244] Bei einer Internet-Auktionsplattform gehören zum negativen Interesse z.B., dass der Account-Inhaber dem verkaufenden Geschäftsgegner die Angebotsgebühr erstattet, die dieser nunmehr vergeblich aufgewendet hat. Der Verkäufer muss jedoch dafür sorgen, den Schaden zu minimieren (§ 254 Abs. 2 S. 1 Var. 2 BGB), indem er zum Beispiel versucht, dass die Transaktion mit dem zweithöchst Bietenden zustande kommt.[245] 467

Eine Lösung, die nur das negative Interesse des Geschäftsgegners ersetzt, hat den Vorteil, dass der Interessenausgleich zwischen diesem und dem Account-Inhaber ausgewogener ist. Das positive Interesse umfasst die Expektanz des Geschäftsgegners. Er macht den Gewinn mit dem Geschäft, den er sich erhofft hat, oder bekommt diesen ersetzt (§ 252 S. 1 BGB). Das negative Interesse hingegen ersetzt nur die Eingriffe in den status quo. Dem Geschäftsgegner werden diejenigen Einbußen ersetzt, die er durch das Vertrauen auf die Willenserklärung erlitten hat. Dem Geschäftsgegner werden die tatsächlich erlittenen Einbußen ersetzt, wohingegen der Account-Inha- 468

243 Dies taten die Bildschirmtext-Systeme, *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552; *Auerbach*, CR 1988, 18, 19.

244 *Klein*, MMR 2011, 450.

245 *J. Hoffmann*, in: *Leible*/*Sosnitza*, Rn. 122.

ber dem Geschäftsgegner nicht die Expektanz zu ersetzen hat. Die Expektanz als Hoffnung auf einen zukünftigen Gewinn ist weniger schutzbedürftig als die tatsächlichen Einbußen, die der Geschäftsgegner im Vertrauen auf die Erklärung aufgewendet hat. Insofern hat eine Lösung, die das negative Interesse ersetzt, den Vorteil, dass diese Lösung durch die geringe Belastung des Account-Inhabers als gerechter empfunden werden könnte. Darüber hinaus setzt die Haftung auf das negative Interesse rechtsökonomisch betrachtet die richtigen Anreize zur Verhinderung des Missbrauchs.[246]

7. Konkurrenzen

469 Die Haftung auf das negative Interesse kommt nur in Betracht, wenn der Geschäftsgegner ohnehin nicht das positive Interesse erhält. Hat der Dritte durch den Missbrauch der Zugangsdaten den Account-Inhaber rechtsgeschäftlich gebunden, kommt eine Haftung aus *culpa in contrahendo* nicht in Betracht. Die *culpa in contrahendo* kommt daher entweder als alternativer oder als subsidiärer Lösungsweg zu einer Haftung auf das positive Interesse zur Anwendung.[247] Innerhalb der Haftung auf das negative Interesse verdrängen sich die Anspruchsgrundlagen nicht gegenseitig. Die *culpa in contrahendo* kann neben § 122 BGB angewandt werden.[248]

8. Zwischenergebnis

470 Eine Lösung des Problems des Missbrauchs von Zugangsdaten über die *culpa in contrahendo* ist jedoch nicht möglich. Sie scheitert an den Voraussetzungen der *culpa in contrahendo*. In den weit überwiegenden Fällen liegt kein vorvertragliches Schuldverhältnis im Sinne des § 311 Abs. 2 BGB vor.[249] Ebenso fällt es schwer eine Pflichtverletzung des Account-Inhabers im Rahmen eines möglichen vorvertraglichen Schuldverhältnisses auszumachen, die der Account-Inhaber zu vertreten hat.[250] Die Haftung für den

246 Unten Rn. 655.
247 Oben Rn. 433.
248 *BGH*, Urteil v. 20. 3. 1986, III ZR 236/84 – NJW 1986, 2104, 2106; *Ultsch*, DZWir 1997, 466, 469.
249 Oben Rn. 436 ff.
250 Oben Rn. 450 ff.

Missbrauch von Zugangsdaten im Internet kann somit nicht überzeugend über die *culpa in contrahendo* gelöst werden.

IV. Lösung über eine analoge Anwendung des § 122 BGB

Ein weiterer Lösungsweg ist die analoge Anwendung des § 122 BGB.[251] **471**
Zu untersuchen ist, ob die Haftung analog zu § 122 BGB, wie sie für abhandengekommene Willenserklärungen und das fehlende Erklärungsbewusstsein vertreten wird, auf den Missbrauch von Zugangsdaten im Internet anwendbar ist. Dieser Lösungsweg stellt – ebenso wie bei der *culpa in contrahendo*[252] – eine Alternative oder Ergänzung zu einer Haftung über die Anscheinsvollmacht oder die Rechtsscheingrundsätze dar. Ebenso wie die *culpa in contrahendo* belastet diese Lösung mit der Haftung auf das negative Interesse den Account-Inhaber weniger als eine Haftung auf das positive Interesse. Im Unterschied zur *culpa in contrahendo* ist bei einer analogen Anwendung des § 122 BGB das negative Interesse jedoch durch das positive Interesse begrenzt. Eine Lösung analog zu § 122 BGB wird teilweise bei abhandengekommenen Vollmachtsurkunden der Lösung über die *culpa in contrahendo* vorgezogen.[253] Dieser Lösungsweg über die analoge Anwendung des § 122 BGB kann sowohl in Zwei- als auch in Drei-Personen-Konstellationen angewendet werden.

1. Fehlendes Erklärungsbewusstsein

Die wirksame Willenserklärung besteht aus drei objektiven und drei korre- **472**
spondierenden subjektiven Merkmalen.[254] Die objektiven Merkmale sind die Erklärungshandlung, der Rechtsbindungswille sowie die Bezeichnung von Rechtsfolgen. Subjektiv korrespondieren dazu die Merkmale des Handlungswillens, des Erklärungsbewusstseins und des Geschäftswillens. Fehlt

---

251 Vertreten von *Kuhn*, S. 242; *Friedmann*, S. 106 ff.

252 Dazu oben Rn. 433.

253 *Canaris*, JZ 1976, 132, 134; *Neuner*, JuS 2007, 401, 411; *M. Wolf/Neuner*[10], § 50 Rn. 78. Inkonsequenter Weise solle bei den Zugangsdaten im Internet hingegen die *culpa in contrahendo* angewendet werden *dies.*[10], § 50 Rn. 111.

254 Anstatt aller *Faust*, BGB AT[3], § 2 Rn. 7 ff.

das Erklärungsbewusstsein[255] stellt sich die Frage, ob eine Willenserklärung vorliegt und ob der Handelnde für seine Erklärung in irgendeiner Weise haften muss.

473 Der Lehrbuchfall der Trierer Weinversteigerung dient zur Veranschaulichung des Problems.[256] Ein mit den Gepflogenheiten einer Versteigerung unvertrauter Gast hebt die Hand um einen Bekannten zu grüßen. Das Heben der Hand bedeutet jedoch ein höheres Gebot. Der Versteigerer hat ein Interesse daran, dass er die Geste des Gastes als Gebot verstehen darf, während der Gast ein Interesse daran hat, an seine anders gemeinte Handbewegung nicht gebunden zu sein.

474 Bei der ersten Frage, ob das Erklärungsbewusstsein ein konstitutives Merkmal der Willenserklärung ist, bestehen unterschiedliche Auffassungen. Einerseits kann bei subjektiver Betrachtungsweise im fehlenden Erklärungsbewusstsein der mangelnde Ausdruck privatautonomen Verhaltens gesehen werden und damit das Vorliegen einer Willenserklärung verneint werden.[257] Andererseits kann bei objektiver Betrachtungsweise die Selbstverantwortung betont werden, wonach eine Willenserklärung vorliegt, die jedoch analog § 119 Abs. 1 Var. 2 BGB anfechtbar sei.[258] Vermittelnd dazwischen soll nach der Erklärungsfahrlässigkeit[259] eine Willenserklärung vorliegen, wenn der Erklärende „bei Anwendung der im Verkehr erforderlichen Sorgfalt hätte erkennen und vermeiden können, dass die in seinem Verhalten liegende Äußerung [...] als Willenserklärung aufgefasst werden durfte, und wenn der Empfänger sie auch tatsächlich so verstanden hat."[260]

475 Im Ergebnis weniger umstritten ist die Frage, ob der Handelnde dem Erklärungsempfänger haftet. Überwiegend wird angenommen, dass sich die

255 Auch als Erklärungswille oder Partizipationswille bezeichnet, *M. Wolf/Neuner*[10], § 32 Rn. 20.

256 Statt vieler *Medicus*[10], Rn. 605.

257 *Canaris*, Vertrauenshaftung, S. 427 f.; *ders.*, NJW 1984, 2281; *ders.*, in: FG 50 Jahre BGH, Bd. 1, 129, 141; *Hübner*[2], Rn. 677; *Singer*, in: *Staudinger*[2012], § 118 BGB Rn. 5; *ders.*, JZ 1989, 1030, 1034; *M. Wolf/Neuner*[10], § 32 Rn. 22.

258 *Brox*, S. 50 f.; *S. Lorenz*, S. 216 ff.; *Medicus*[10], Rn. 607.

259 *BGH*, Urteil v. 7. 6. 1984, IX ZR 66/83 – BGHZ 91, 324, 330; *Armbrüster*, in: MüKo-BGB[6], § 119 Rn. 97; *Bork*[3], Rn. 596; *Bydlinski*, JZ 1975, 1; *ders.*, Privatautonomie, S. 155 ff.; *Kindl*, S. 25 ff.

260 *BGH*, Urteil v. 11. 6. 2010, V ZR 85/09 – NJW 2010, 2873, Rn. 18; Urteil v. 16. 12. 2009, XII ZR 146/07 – BGHZ 184, 35, Rn. 19.

Haftung des Handelnden aus § 122 BGB in direkter[261] oder analoger[262] Anwendung ergibt.

2. Abhandengekommene Willenserklärung

Mit dem Begriff der abhandengekommenen Willenserklärung wird der Fall bezeichnet, in dem der Erklärende eine Willenserklärung anfertigt, sie z.B. unterschreibt, aber anschließend zurückhält, weil er sie nicht oder noch nicht abgeben möchte.[263] Durch das Vorbereiten der Willenserklärung schafft der Handelnde das erhöhte Risiko, dass der Rechtsverkehr diese Erklärung als einwandfreie Willenserklärung ansieht.[264] 476

Der Fall der abhandengekommenen Willenserklärung wird nach verbreiteter Ansicht ebenso wie der Fall des fehlenden Erklärungsbewusstseins behandelt.[265] Der Handelnde hat eine Willenserklärung geschaffen, z.B. eine Vollmachtsurkunde, die der Rechtsverkehr als solche auffassen darf, die jedoch nach oder analog zu § 119 Abs. 1 BGB anfechtbar ist und der Handelnde nach oder analog zu § 122 BGB dafür haften muss.[266] Mittlerweile kann sich die Ansicht, dass für die abhandengekommene Willenserklärung analog zu § 122 BGB gehaftet wird, auf den gesetzgeberischen Willen berufen.[267] Nur vereinzelt wird diese Haftung verneint.[268] Teilweise wird die 477

---

261 Dafür *Armbrüster*, in: MüKo-BGB[6], § 122 Rn. 5.

262 Für die objektive Ansicht: *M. Wolf/Neuner*[10], § 32 Rn. 24. Für die subjektive Ansicht: *Brox*, S. 52. Für die Ansicht der Erklärungsfahrlässigkeit: *BGH*, Urteil v. 7. 6. 1984, IX ZR 66/83 – BGHZ 91, 324, 229 f. Gegen eine Haftung aus § 122 BGB: *Medicus*[10], Rn. 608.

263 *M. Wolf/Neuner*[10], § 32 Rn. 17.

264 *Singer*, in: *Staudinger*[2012], § 122 BGB Rn. 11.

265 *Medicus*[10], Rn. 605; *Faust*, BGB AT[3], § 2 Rn. 14; *Rüthers/A. Stadler*[17], § 17 Rn. 38; **a.A.** *Bork*[3], Rn. 615.

266 *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13, 14 f.; Urteil v. 12. 1. 1984, IX ZR 83/82 – NJW 1984, 798, 2106; *Armbrüster*, in: MüKo-BGB[6], § 122 Rn. 5; *Canaris*, Vertrauenshaftung, S. 487, 548; *ders.*, JZ 1976, 132, 134; *Neuner*, JuS 2007, 401, 411; *Singer*, in: *Staudinger*[2012], § 122 BGB Rn. 11; *Rüthers/A. Stadler*[17], § 17 Rn. 38; *M. Wolf/Neuner*[10], § 50 Rn. 78.

267 Begr. FormAnpG, BT-Drucks. 14/4987, S. 11.

268 *Bork*[3], Rn. 615, 1527, der vermeintlich Erklärende habe noch kein nach außen gerichtetes Verhalten an den Tag gelehnt; *Larenz/M. Wolf*[9], § 48 Rn. 12, Wegnahme einer Vollmachtsurkunde sei mit der arglistigen Täuschung oder Drohung vergleichbar, für den abhandengekommenen Brief die Haftung jedoch bejahend, ebd., § 26 Rn. 7.

Haftung analog zu § 122 BGB und der alternative Lösungsweg über die *culpa in contrahendo* als nebeneinander anwendbar angesehen.[269]

3. Anwendung im Internet

478 Die Situation des fehlenden Erklärungsbewusstseins und der abhandengekommenen Willenserklärung haben gezeigt, dass nicht alle Merkmale einer Willenserklärung vorliegen müssen, damit der Rechtsverkehr ein schützenswertes Interesse darin entwickeln kann, dass er die Handlung als einwandfreie Willenserklärung verstehen darf. Im Gegenzug wird die Privatautonomie durch die Möglichkeit zur Anfechtung gewahrt. Beim Missbrauch von Zugangsdaten im Internet besteht ebenfalls das Spannungsfeld zwischen dem Schutz des Rechtsverkehrs sowie der Selbstbestimmung des Account-Inhabers. Es stellt sich daher die Frage, ob die Lösung des fehlenden Erklärungsbewusstseins und der abhandengekommenen Willenserklärung auf den Missbrauch von Zugangsdaten im Internet übertragen werden kann.

479 Fehlendes Erklärungsbewusstsein und abhandengekommene Willenserklärungen haben gemeinsam, dass eine Willenserklärung angenommen werden darf, wenn dem Handelnden Erklärungsfahrlässigkeit vorgeworfen werden kann. Er hat fahrlässig herbeigeführt, dass der Rechtsverkehr sein Handeln als Willenserklärung auffassen darf. Beim Missbrauch von Zugangsdaten im Internet kann die Erklärungsfahrlässigkeit auch angewendet werden. Durch den fahrlässig unsorgfältigen Umgang mit den Zugangsdaten hat der Account-Inhaber eine Situation geschaffen, durch die dem Rechtsverkehr der Anschein erwecket wird, dass eine einwandfreie Willenserklärung von ihm vorliegt. Ebenso wie beim fehlenden Erklärungsbewusstsein und der abhandengekommenen Willenserklärung kann der Rechtsverkehr beim Missbrauch von Zugangsdaten im Internet nicht erkennen, dass der Account-Inhaber die scheinbare Willenserklärung gar nicht abgeben wollte.

480 Damit enden die Gemeinsamkeiten jedoch schon. Die Rückkopplung an das Handeln des Erklärenden ist beim Missbrauch von Zugangsdaten im Internet bedeutend schwächer. Bei dem fehlenden Erklärungsbewusstsein sowie der abhandengekommenen Willenserklärung erweckt schon das Handeln des vermeintlich Erklärenden den Eindruck, es handele sich um eine einwandfreie Willenserklärung. Das Handeln des Account-Inhabers

269 *M. Wolf/Neuner*[10], § 32 Rn. 18.

beim Missbrauch von Zugangsdaten im Internet beschränkt sich jedoch auf den unsorgfältigen Umgang mit den Zugangsdaten. Der Dritte handelt und erweckt den Anschein, dass es sich um eine Willenserklärung des Account-Inhabers handelt. Die Rückkopplung an den Account-Inhaber ist dadurch erheblich abgeschwächt. Beim fehlenden Erklärungsbewusstsein fehlt das subjektive Merkmal der Willenserklärung, dessen Vorhandensein durch einen Rechtsschein begründet werden muss. Das relevante Verhalten ist eine Handlung des vermeintlich Erklärenden, von der ein hoher Rechtsschein ausgeht. Bei abhandengekommenen Willenserklärungen liegen sämtliche objektiven und subjektiven Voraussetzungen einer Willenserklärung vor. Die zur Wirksamkeit der Willenserklärung erforderliche Abgabe[270] fehlt jedoch. Die Schaffung der Willenserklärung in einer physisch einmaligen Form stellt jedoch einen starken Rechtsschein dar. Bei diesen beiden Fällen fehlt jeweils nur ein Merkmal der Willenserklärung. Beim Missbrauch von Zugangsdaten im Internet fehlt es bereits an einem Handeln des Account-Inhabers, das unmittelbar vom Rechtsverkehr als Willenserklärung aufgefasst werden kann. Sowohl sein Handeln, sein Erklärungsbewusstsein und die Abgabe der vermeintlichen Willenserklärung durch ihn fehlen und erscheinen nur für den Rechtsverkehr als gegeben. Beim Missbrauch von Zugangsdaten im Internet besteht daher eine erheblich größere Diskrepanz zwischen Realität und Schein.

Darüber hinaus ist der potentielle Empfängerkreis bei der abhandengekommenen Willenserklärung sowie dem fehlenden Erklärungsbewusstsein durch den Handelnden bestimmt. Dadurch, dass die Erklärung beim fehlenden Erklärungsbewusstsein nur von einem gewissen Empfängerkreis wahrgenommen werden kann, ist der Kreis der Personen, die auf den Schein vertrauen können, eingeschränkt. Ebenso legt der Erklärende bei der abhandengekommen Willenserklärung selbst fest, an wen sich die Erklärung richtet, sodass nur der oder die vom Erklärenden ausgesuchten Empfänger auf den Schein der Erklärung vertrauen können. Beim Missbrauch von Zugangsdaten im Internet kann jedoch der Dritte gegenüber einem beliebigen Geschäftsgegner auftreten. Die Rückkopplung an den Account-Inhaber ist bedeutend schwächer, weil dieser sich den Geschäftsgegner nicht ausgesucht hat.[271] Dadurch entstünde für den Account-Inhaber das Risiko einer Haftung gegenüber einem großen Personenkreis. Bei abhandengekom- 481

270 Vgl. dazu statt vieler *Schack*[14], Rn. 185.

271 Vgl. dazu oben Rn. 446.

mener Willenserklärung und dem fehlenden Erklärungsbewusstsein ist der Personenkreis hingegen nicht nur beschränkt, sondern vom Handelnden vorgegeben.

482 Ferner ist beim Missbrauch von Zugangsdaten im Internet der Fahrlässigkeitsvorwurf an den Account-Inhaber erheblich schwächer. Bei dem fehlenden Erklärungsbewusstsein wird dem Handelnden vorgeworfen, er hätte erkennen müssen, dass der Rechtsverkehr seine Handlung als Willenserklärung mit Rechtsbindungswillen auffasst. Bei der abhandengekommenen Willenserklärung ist dem Handelnden klar, dass seine Erklärung als einwandfreie Willenserklärung aufgefasst werden kann. Ihm wird jedoch vorgeworfen, dass sich dieses erhöhte Risiko durch seine Fahrlässigkeit verwirklicht hat. In beiden Fällen knüpft der Fahrlässigkeitsvorwurf daran an, dass der Rechtsverkehr das Handeln als Willenserklärung auffassen darf. Beim Missbrauch von Zugangsdaten im Internet bezieht sich der Fahrlässigkeitsvorwurf zunächst nur darauf, dass ein Dritter dadurch Zugang zu dem Account des Account-Inhabers erhalten hat. Zwischen seiner Fahrlässigkeit und dem Vertrauen des Rechtsverkehrs in das Vorliegen einer Willenserklärung muss erst der Dritte eine Willenserklärung selbst schaffen. Das dem Account-Inhaber vorgeworfene Verhalten führt somit nur durch einen weiteren und bedeutenden Schritt des Dritten zu einer für den Rechtsverkehr wahrnehmbaren Willenserklärung.

483 Darüber hinaus muss noch nicht einmal ein Handeln des Account-Inhabers vorliegen. Ein Unterlassen kann ebenfalls zum Missbrauch der Zugangsdaten führen. Selbst wenn sich jedes Unterlassen als Handeln und umgekehrt ansehen lässt, ermöglicht eine schwerpunktmäßige Betrachtung[272] jedoch eine – wenn auch fließende – Grenzziehung zwischen Handeln und Unterlassen. Beim Phishing[273] gibt der Account-Inhaber bewusst die Zugangsdaten auf einer Seite ein. Fahrlässigerweise verkennt er dabei, dass es sich nicht um die Seite des Authentisierungsnehmers, sondern um die eines Dritten handelt. Ein Unterlassen kann z.B. vorliegen, wenn sich ein Trojaner mit Keylogger[274] auf dem Computer des Account-Inhabers eingenistet hat. Bei der Authentisierung mit den Zugangsdaten gegenüber dem Authentisierungsnehmer ist dem Account-Inhaber nur der Vorwurf zu machen, dass er es unterlassen hat, den Trojaner zu entfernen, was häufig nicht

272 Siehe dazu die ausgeprägte Strafrechtsdogmatik *Kühl*, in: *Lackner/Kühl*[27], § 13 StGB Rn. 2 f. m.w.N.

273 Dazu oben Rn. 138 ff.

274 Dazu oben Rn. 166.

fahrlässig geschehen wird. Fälle des Unterlassens sind nicht vergleichbar mit dem fehlenden Erklärungsbewusstsein und der abhandengekommenen Willenserklärung.

Beim Missbrauch von Zugangsdaten im Internet stammen sowohl die Handlung als auch der Rechtsbindungswille vom Dritten. Eine Rückkopplung an den Account-Inhaber wie in den Fällen des fehlenden Erklärungsbewusstseins oder der abhandengekommenen Willenserklärung ist nicht möglich. 484

Darüber hinaus ist es für die Anwendung des § 122 BGB erforderlich, dass die Gründe der Ungültigkeit der Erklärung ausschließlich aus der Sphäre des Erklärenden stammen.[275] Dass dies beim Missbrauch von Zugangsdaten im Internet ebenfalls zutrifft, ist zweifelhaft. Der Authentisierungsnehmer kann durch seine Sicherheitsinfrastruktur sicherstellen, dass ein Missbrauch von Zugangsdaten erschwert wird. Fehlt es daran, kann er der Grund sein, warum die Zugangsdaten missbraucht werden konnten.[276] Der Missbrauch der Zugangsdaten liegt nicht allein in der Sphäre des Account-Inhabers, sodass eine Haftung analog zu § 122 BGB auch daran scheitert. 485

Eine Haftung analog § 122 BGB für den Missbrauch von Zugangsdaten im Internet kommt nicht in Betracht. Der Missbrauch von Zugangsdaten im Internet ist von der Stärke des Rechtsscheins kaum vergleichbar mit den Fällen des fehlenden Erklärungsbewusstseins und der abhandengekommenen Willenserklärung. 486

V. Lösung über das Deliktsrecht

1. § 823 Abs. 1 BGB

Man kann eine Lösung über die deliktische Haftung des § 823 Abs. 1 BGB erwägen, die sowohl in Zwei- als auch in Drei-Personen-Konstellationen anwendbar ist. Dessen enge Voraussetzungen[277] passen jedoch nicht zum Interesse des Geschäftsgegners. Die deliktische Haftung würde daran scheitern, dass fahrlässig verursachte Vermögensschäden nicht ersetzbar sind.[278] 487

275 *BGH*, Urteil v. 20. 3. 1986, III ZR 236/84 – NJW 1986, 2104, 2106; *Armbrüster*, in: MüKo-BGB[6], § 122 Rn. 3.
276 Oben Rn. 215 ff.
277 *Kuhn*, S. 244.
278 *Dörner*, AcP 202 (2002), 363, 391.

Ferner sind die Konturen einer deliktischen Pflicht zur Sicherung der Zugangsdaten unklar.[279] Eine Ansatz über § 823 Abs. 1 BGB kann den Missbrauch von Zugangsdaten im Internet daher nicht überzeugend lösen.[280]

2. § 823 Abs. 2 BGB

488 Die Schwäche der Lösung über § 823 Abs. 1 BGB besteht bei einer Lösung über § 823 Abs. 2 BGB nicht. Um den Missbrauch von Zugangsdaten im Internet über § 823 Abs. 2 BGB zu lösen, muss ein Schutzgesetz vorliegen. Nur wenn eine gesetzliche Regelung die Verhaltensanforderungen des Account-Inhabers an die Sicherung der Zugangsdaten statuiert, ist dies der Fall. Zwar wird dies für § 9 Abs. 1 S. 1 DeMailG angenommen.[281] Dies erscheint jedoch zweifelhaft, weil § 9 Abs. 1 S. 1 DeMailG nur den Diensteanbietern eine Pflicht auferlegt. Man kann zwar davon ausgehen, dass die Diensteanbieter ihren Kunden wegen dieser Regelung vertraglich die Sicherungspflichten auferlegen. Eine vertragliche Weiterreichung der Pflichten kann jedoch für die Kunden keine Haftung aus § 823 Abs. 2 BGB begründen. Selbst § 27 Abs. 2 PAuswG, der dem Account-Inhaber direkt Sicherungspflichten auferlegt, ist mangels Einbeziehung Dritter in den Schutzbereich kein Schutzgesetz im Sinne des § 823 Abs. 2 BGB.[282] Eine Lösung über § 823 Abs. 1 BGB oder § 823 Abs. 2 BGB kommt somit nicht in Betracht.

VI. Lösung über die allgemeinen Rechtsscheingrundsätze

489 Nach hier vertretener Auffassung ist die Haftung für den Missbrauch von Zugangsdaten im Internet durch die Anwendung der allgemeinen Rechtsscheingrundsätze[283] zu lösen.[284] Für eine Rechtsscheinhaftung nach den allgemeinen Grundsätzen, ist ein Rechtsscheintatbestand erforderlich, den

279 Unten Rn. 753.
280 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 213.
281 *Spindler*, CR 2011, 309, 313, 318.
282 *Borges*, Elektronischer Identitätsnachweis, S. 172 ff. Offen gelassen von *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 289.
283 Zu deren Voraussetzungen oben Rn. 224 ff.
284 So auch *Dörner*, AcP 202 (2002), 363, 389; *Faust*, BGB AT[3], § 26 Rn. 41; *Herresthal*, K&R 2008, 705, 707 ff.; *ders.*, in: *Taeger*/*Wiebe*, 21, 31 ff.; *ders.*, JZ 2011,

der Account-Inhaber zurechenbar gesetzt hat.[285] Ferner muss der Geschäftsgegner schutzwürdig sein und eine kausale Vermögensdisposition getroffen haben. Dieser Lösungsweg ist gleichermaßen in Zwei- und in Drei-Personen-Konstellationen anwendbar. Durch eine Differenzierung bei der Zurechenbarkeit können über die Anwendung der allgemeinen Rechtsscheingrundsätze neben den Konstellationen ohne Weitergabe auch die Konstellationen bei Weitergabe und bei Erstellen des Accounts durch einen Dritten gelöst werden.

1. Blick auf Rechtsscheintatbestände in vergleichbaren Fallkonstellationen

Vor dem Hintergrund gesetzlicher und anderer anerkannter Rechtsscheintat- **490**
bestände sowie vor dem Hintergrund vergleichbarer Fallkonstellationen soll überprüft werden, welche konkreten Voraussetzungen an die Stärke eines Rechtsscheintatbestandes sowie dessen Zurechnung gestellt werden.

a) Vollmachtsurkunde, § 172 Abs. 1 BGB

§ 172 Abs. 1 BGB schützt das Vertrauen in eine echte, ausgehändigte Voll- **491**
machtsurkunde. § 172 Abs. 1 BGB wurde bereits ausführlich betrachtet.[286] Dabei wurde gezeigt, dass entgegen zahlreicher Stimmen in der Literatur der Missbrauch von Zugangsdaten nicht überzeugend durch eine Heranziehung des Rechtsgedankens des § 172 Abs. 1 BGB begründet werden kann. § 172 Abs. 1 BGB zeigt jedoch Anhaltspunkte auf, welche Voraussetzungen ein Rechtsscheintatbestand zu erfüllen hat.

Zunächst lässt sich § 172 Abs. 1 BGB entnehmen, dass der Besitz einer **492**
physisch einmaligen Sache ein starker Rechtsscheinträger ist.[287] Die Wertung, dass der Besitz einer physisch einmaligen Sache ein starker Rechtsscheinträger ist, findet sich in sachenrechtlichen Wertungen wieder. Nach § 1006 Abs. 1 S. 1 BGB wird zugunsten des Besitzers vermutet, er sei Ei-

---

1171, 1174; *Kuhn*, S. 214 ff.; *Linardatos*, Jura 2012, 53, 55; *Rieder*, S. 194 ff.; *Spiegelhalder*, S. 124 ff.; *Sonnentag*, WM 2012, 1614, 1615.

285 Oben Rn. 226.

286 Dazu oben Rn. 303 ff.

287 Oben Rn. 310.

gentümer der Sache. Der Rechtsschein des Besitzes einer Sache ist so stark, dass er den gutgläubigen Erwerb vom Nichtberechtigten ermöglicht (vgl. §§ 929 S. 1, 932 Abs. 1 S. 1 BGB). Ferner gehören zu den vertrauensbegründenden Momenten des Rechtsscheintatbestandes des § 172 Abs. 1 BGB die durch die Schriftform erreichte Warnfunktion und erschwerte Fälschbarkeit sowie die Einschränkung der Missbrauchsmöglichkeiten.[288]

493 Der Besitz als solcher begründet jedoch nur insoweit ein schützenwertes Vertrauen, als er willentlich übergeben wurde. Eine abhandengekommene Vollmachtsurkunde begründet keinen Rechtsscheintatbestand nach oder analog zu § 172 Abs. 1 BGB.[289] Die sachenrechtliche Wertung ist gleichläufig. Die Eigentumsvermutung zugunsten des Besitzers einer Sache findet jedoch ihre Grenze, wenn die Sache abhandenkommen ist (§ 1006 Abs. 1 S. 2 BGB). In diesen Fall scheidet auch der gutgläubige Erwerb aus (§ 935 Abs. 1 S. 1 BGB). Das Abhandenkommen der Vollmachtsurkunde und der Sache kann dem Gegenstand nicht angesehen werden. Diese Erwägungen sollten daher in der Zurechenbarkeit berücksichtigt werden.[290]

494 Der gesetzliche Vertrauensschutz in gegenüber Dritten erklärten Vollmachten nach §§ 170, 171 BGB zeigt ebenfalls, dass das Verhalten, das einen Rechtsscheintatbestand begründet, rechtsgeschäftliche Bezüge aufweisen muss. Es handelt sich im Falle der Außenvollmacht um eine Willenserklärung, bei der Kundgabe einer Innenvollmacht um eine rechtsgeschäftsähnliche Handlung.[291]

b) Briefpapier, Logos und Stempel

495 Näher an der Situation des Missbrauchs von Zugangsdaten im Internet sind die Möglichkeiten, Erklärungen als von einer anderen Person stammend aussehen zu lassen. Es gibt mannigfaltige Möglichkeiten dies zu erreichen, beispielsweise das Nachahmen einer Unterschrift oder das Verwenden fremder Zeichen wie Logo, Briefbogen oder Firmenstempel. Briefpapier und Firmenstempel können wie manche Accounts ohne Überprüfung der Identität von einem Dritter erstellt werden, sodass sie von Echten kaum bis gar nicht zu unterscheiden sind. Ebenso können Briefpapier und Firmenstem-

288 Oben Rn. 313.
289 Dazu und zur Gegenauffassung oben Rn. 315.
290 Dazu unten Rn. 671 ff.
291 *M. Wolf/Neuner*[10], § 50 Rn. 70.

pel wie die Zugangsdaten von Accounts entwendet werden und dazu missbraucht werden, Willenserklärungen, die scheinbar vom angegebenen Aussteller stammen, abzugeben. Bei den Fällen von Logos und Briefpapier wird zu Recht überwiegend eine Rechtsscheinhaftung abgelehnt. Das Logo einer Autofirma auf dem Briefbogen einer Verkaufsgesellschaft reicht ebenso wenig zur Anscheinsvollmacht,[292] wie das Logo am Büro eines vermeintlichen Vertreters, der als Geschäftsstelle für die Kundenbetreuung im Ausland angegeben ist.[293] Erst die Durchführung der Geschäfte, die durch Verwendung des Briefpapiers angebahnt wurden, begründet das schützenswerte Vertrauen.[294] Daraus lässt sich für die Anerkennung von Rechtsscheintatbeständen schließen, dass Umstände, die nicht nur der Berechtigte sondern jeder mit einfachen Mitteln herbeiführen kann, wie das Verwenden von Briefpapier oder eines Accounts, kein schützenswertes Vertrauen auf Empfängerseite begründen. Einen starken Rechtsscheinträger stellen leicht nachzuahmende Sachen nicht dar. Ihnen fehlt beispielsweise das vertrauensbegründende Moment der physischen Einmaligkeit einer Sache oder einer rechtsgeschäftlichen Handlung des Geschäftsherren, wie sie die Mitteilung einer Innenvollmacht (§ 171 Abs. 1 BGB) darstellt.

Teilweise wird behauptet, dass der Rechtsschein bei rein wissensbasierten Authentisierungsmethoden ohne Überprüfung der Identität bedeutend stärker sei, als beim Briefpapier.[295] Zwar stimmt, dass das Nachahmen eines Briefpapiers einfacher ist, als Zugangsdaten auszuspähen.[296] Denn Briefe mit Briefpapier eines Geschäftsherren werden an diverse Empfänger verschickt. Es handelt sich bei Briefpapier im Gegensatz zu den Zugangsdaten um kein Geheimnis. Verkannt wird dabei jedoch, dass ein Account unter fremdem Namen von einem Dritten angelegt werden kann.[297] Dies ist so einfach möglich, wie den Briefbogen oder ein Logo nachzuahmen. Häufig reichen für das Erstellen eines Accounts, bei dem lediglich eine Plausibilitätskontrolle durchgeführt wird, unter fremdem Namen sogar die Angaben, die typischerweise auf einem Briefbogen zu finden sind. 496

---

292 *OLG Düsseldorf*, Urteil v. 4. 2. 1950, U 83/49 – BB 1950, 489; *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 35.

293 *BGH*, Urteil v. 13. 7. 1977, VIII ZR 243/75 – WM 1977, 1169, 1170.

294 Vgl. *BGH*, Urteil v. 27. 9. 1956, II ZR 178/55 – NJW 1956, 1673, 1674.

295 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18. Ähnlich *Herresthal*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 28.

296 Zu den Wegen, an Zugangsdaten zu gelangen oben Rn. 124 ff.

297 Dazu oben Rn. 210.

497 Zwischen Briefpapier, Stempel und Logo bestehen keine bedeutenden Unterschiede. Man kann sie entwenden oder mit einfachen Mitteln nachmachen. Dennoch wird das Vertrauen in Stempel scheinbar höher geschützt. Wenn behauptet wird, dass der Besitz eines Stempels für einen Rechtsscheintatbestand ausreiche, die Verwendung fremden Briefpapiers jedoch nicht,[298] verkennt der Verweis auf die *BGH*-Entscheidung deren maßgeblichen Erwägungsgründe. Maßgeblich für die Annahme einer Vertretungsmacht war in der Entscheidung, dass die AGB des Geschäftsherren sprachlich diesen und den Vertreter zu wenig differenzierten, sodass die AGB auf eine Vertretungsmacht des vermeintlich Vertretenen hindeuteten.[299] Darüber hinaus ist für die Anscheinsvollmacht entscheidend, dass der Handelnde nicht nur wie ein Vertreter ausgestattet ist, sondern auch Geschäfte von ihm mehrfach erfüllt wurden.[300] Wird in weiteren Entscheidungen ein Firmenstempel bereits bei erstmaliger Verwendung ohne weitere vertrauenserweckende Begleitumstände als Rechtsscheintatbestand angesehen,[301] so ist das auf die selektive Darstellung einzelner Aspekte der *BGH*-Entscheidung zurückzuführen.[302] Richtigerweise kann allein die ein- oder zweimalige Verwendung eines Stempels noch kein schützenswertes Vertrauen begründen.[303] Stempel sind nämlich frei verkäuflich und können von jedermann ohne Identitätsüberprüfung jederzeit besorgt werden.[304] Daraus lässt sich die Voraussetzung ableiten, dass ein starker Rechtsscheinträger nicht einfach selbst hergestellt werden kann. Ferner führt eine Identitätsüberprüfung bei Rechtsscheinträgern, die an eine Person geknüpft werden sollen, zu einem starken Vertrauensschutz.

---

298 *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 35 unter Berufung auf *BGH*, Urteil v. 12. 2. 1952, I ZR 96/51 – BGHZ 5, 111, 116.

299 Ebd., 114 ff.

300 Vgl. ebd., 116.

301 *OLG Brandenburg*, Urteil v. 14. 1. 2009, 3 U 75/08, Rn. 26; *AG Bremen*, Urteil v. 31. 3. 2011, 23 C 443/10, Rn. 13.

302 *AG Bremen*, Urteil v. 31. 3. 2011, 23 C 443/10, Rn. 13 verweist ohne nähere Begründung auf *OLG Brandenburg*, Urteil v. 14. 1. 2009, 3 U 75/08, Rn. 26, das sich auf *Schilken*, in: *Staudinger*[2009], § 167 BGB Rn. 35 beruft, ohne die Erwägungen der angesprochenen *BGH*-Entscheidung zu berücksichtigen.

303 Für den Faksimiliestempel offen gelassen *BGH*, Urteil v. 14. 3. 2000, XI ZR 55/99, Rn. 10.

304 *OLG Hamburg*, Urteil v. 27. 12. 1963, 1 U 83/63 – BB 1964, 576; zustimmend *Leptien*, in: *Soergel*[13], § 167 BGB Rn. 20.

c) Rechtsscheinhaftung bei der Benutzung von Bildschirmtext (Btx)

Beim Bildschirmtext-System handelt es sich um einen Vorgänger des Internets, sodass sich bezüglich des Missbrauchs eines Bildschirmtext-Systems die gleichen Fragen stellen, wie beim Missbrauch kontemporärer Accounts. Über das Telefonnetz wurden mittels eines Modems Textinformationen übermittelt.[305] Diese wurden anschließend als stehende Fernsehbilder, auch Bildschirmtext-Seiten genannt, auf dem Fernsehgerät angezeigt.[306] Die Informationen waren dabei direkt in der Informationsdatenbank der Bildschirmtext-Zentrale gespeichert oder wurden dynamisch von einem daran angeschlossenen externen Rechner geliefert.[307] Die Einbindung der externen Rechner machte Bildschirmtext dialogfähig. Der Bildschirmtext-Nutzer konnte Informationen durch Eingabe auf einer Tastatur übermitteln, die der externe Rechner bearbeitete und entsprechende Antworten gab.[308] Dadurch wurden Anwendungen wie Online-Banking, Bestellkataloge im Internet sowie Chats[309] möglich. 498

Der Anschlussinhaber konnte sich mit Anschlusskennung, die hardwareseitig in seinem Gerät eingespeichert war, mit seiner Teilnehmernummer sowie einem frei wählbaren Passwort einwählen.[310] Ein Einwählen von anderen Geräten aus war nur mit ausdrücklicher Einwilligung, sog. Freizügigkeitsschaltung, möglich.[311] 499

aa) Rechtsscheintatbestand

Beim Bildschirmtext stellen sich die gleichen Rechtsfragen des Missbrauchs der Zugangsdaten. Dabei ist es ebenso wie bei anderen Zugangsdaten im Internet umstritten, ob der Anschlussinhaber für den Missbrauch dieser Zugangsdaten haften muss. Einige Stimmen in der Literatur lehnen diese Haftung mangels Rechtsscheintatbestandes ab. Zum einen wird die 500

305 *Kleier*, WRP 1983, 534.
306 *Brinkmann*, BB 1981, 1183; *Kuhn*, S. 22.
307 *Kleier*, WRP 1983, 534; *Probandt*, UFITA 98 (1984), 9.
308 *Auerbach*, CR 1988, 18, 19.
309 Die Vergütung von Chats mit erotischem Inhalt war Anlass der Entscheidung des *OLG Köln*, Urteil v. 21. 11. 1997, 19 U 128/97 – NJW-RR 1998, 1277.
310 *Auerbach*, CR 1988, 18, 20; *Paefgen*, CR 1993, 559, 561; *Kleier*, WRP 1983, 534, 536.
311 *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552.

Anwendung der Anscheinsvollmacht mangels Erkennbarkeit des Handeln eines Dritten verneint.[312] Die Kritik, dass für den Geschäftsgegner das Handeln des Dritten nicht erkennbar ist und er daher nicht auf eine etwaige Vertretungsmacht vertrauen darf, ist berechtigt.[313] Die Schlussfolgerung, dass die Anscheinsvollmacht nicht anwendbar sei, ist überzeugend. Jedoch ist anschließend eine Haftung nach allgemeinen Rechtsscheingrundsätzen zu prüfen.

501 Zum anderen wird der Rechtsscheintatbestand wegen der Möglichkeiten des Ausspähens der Zugangsdaten und möglicher Manipulationen verneint.[314] Dieses Argument der mangelnden Sicherheit wird bei der Rechtsscheinhaftung für den Missbrauch von Zugangsdaten im Internet von der Rechtsprechung regelmäßig zur Verneinung der Haftung verwendet.[315] Im Gegensatz zur Rechtsscheinhaftung im Internet hat die Rechtsprechung zum Bildschirmtext sich von diesem Argument zu Recht nicht überzeugen lassen.

502 Überwiegend wird der Rechtsscheintatbestand bei missbräuchlicher Verwendung eines Bildschirmtext-Anschlusses bejaht.[316] Dogmatisch wird diese Rechtsscheinhaftung häufig an die Anscheinsvollmacht geknüpft, auf das Erfordernis des Handelns von gewisser Dauer und Häufigkeit wird jedoch teilweise implizit, teilweise explizit verzichtet.[317] Explizit wird das Merkmal der Dauer und Häufigkeit abgelehnt, weil diese nicht notwendige Voraussetzung der Anscheinsvollmacht bei der Eigenart des Bildschirmtextes nicht passe.[318] Vielmehr sei Bildschirmtext ein hinreichend sicheres Verfahren, das das Vertrauen des Geschäftsgegners in das Handeln des Anschlussinhabers schutzwürdig mache.[319] Der Grund, warum das Bildschirmtext-

312 *Probandt*, UFITA 98 (1984), 9, 17.

313 Oben Rn. 378.

314 *Borsum/Hoffmeister*, NJW 1985, 1205, 1206.

315 Oben Rn. 371.

316 *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 1401; *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552; *LG Koblenz*, Urteil v. 17. 9. 1990, 3 S 78/90 – NJW 1991, 1360; *LG Ravensburg*, Urteil v. 13. 6. 1991, 2 S 6/91 – CR 1992, 472, 473; *Canaris*, in: Bankvertragsrecht[4], Bd. 5, Rn. 527 ff.; *Kleier*, WRP 1983, 534, 537; *Lachmann*, NJW 1984, 405, 408; *Leptien*, in: *Soergel*[13], § 167 BGB Rn. 20; *Redeker*, NJW 1984, 2390, 2393.

317 Vgl. *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 1401.

318 *LG Ravensburg*, Urteil v. 13. 6. 1991, 2 S 6/91 – CR 1992, 472, 473; *Lachmann*, NJW 1984, 405, 408. An dem Erfordernis zweifelnd, es jedoch nicht ablehnend *Kleier*, WRP 1983, 534.

319 *Redeker*, NJW 1984, 2390, 2393.

System ein hinreichend sicheres Verfahren ist, wird selten deutlich gemacht. Der Zugang zum Bildschirmtext ist zum einen durch ein Passwort, eine wissensbasierte Authentisierungskomponente, geschützt. Daneben ist die Anschlusskennung zum Verbindungsaufbau nötig, die regelmäßig den physischen Zugang zum Bildschirmtext-Gerät voraussetzt, was eine Besitz-Komponente der Authentisierungsmethode darstellt. Eine solche Zwei-Faktor-Authentisierung wird als ausreichende Grundlage für einen Rechtsscheintatbestand angesehen. Der Besitz des physisch einmaligen Endgerätes stellt einen starken Rechtsscheinträger dar. Ferner ist davon auszugehen, dass die Identität der Anschlussinhaber vor Vertragsschluss durch den Vertragspartner überprüft wurde, sodass die Identität des Anschlussinhabers zuverlässig feststeht.

Eine abweichende Begründung, die weniger dogmatisch ist, basiert auf **503**
einer allgemeinen Risikoabwägung sowie auf der Schutzwürdigkeit des Vertrauens des Geschäftsgegners.[320] Teilweise wird die generelle Tendenz, die Anscheinsvollmacht nur im kaufmännischen Verkehr anzuwenden,[321] übertragen und die Rechtsscheinhaftung nur für Kaufleute angewandt.[322]

bb) Zurechenbarkeit

Bei der Frage, wann dieser Rechtsscheintatbestand dem Anschlussinhaber **504**
zurechenbar ist, werden unterschiedliche Auffassungen vertreten. Einigkeit besteht nur darin, dass dem Anschlussinhaber bei Weitergabe der Zugangsdaten der Rechtsschein zurechenbar ist.[323] Die willentliche Schaffung des Rechtsscheins durch die Ermöglichung, dass ein Dritter im Namen des Anschlussinhabers auftreten kann, begründet dabei die Zurechnung.

Werden die Zugangsdaten nicht weitergeben, werden teils hohe, teils **505**
niedrige Anforderungen an die Zurechnung gestellt. Sehr weitgehend wird vereinzelt angenommen, dass der Anschlussinhaber wegen der Schaffung des erhöhten Risikos für jeden Missbrauch verschuldensunabhängig ein-

320 *LG Koblenz*, Urteil v. 17. 9. 1990, 3 S 78/90 – NJW 1991, 1360.
321 Oben Rn. 267.
322 *Redeker*, NJW 1984, 2390, 2394 mit Verweis auf *Canaris*, Vertrauenshaftung, S. 192 ff.
323 *LG Ravensburg*, Urteil v. 13. 6. 1991, 2 S 6/91 – CR 1992, 472, 473; *Redeker*, NJW 1984, 2390, 2393.

zustehen habe.[324] Diese verschuldensunabhängige Haftung wird unter Anwendung des Verschuldensprinzips der Rechtsscheinhaftung zurückgewiesen.[325]

506 Sehr hohe Anforderungen werden hingegen von Teilen der Literatur aufgestellt. Nur bei hinreichend sicheren Authentisierungsmethoden sei der Rechtsschein zurechenbar.[326] Dazu gehöre z.B. das TAN-Verfahren, das Banken zum Online-Banking verwenden. Bei diesem Verfahren könne ein Angreifer, auch wenn er Teile der geheimen Authentisierungsmittel abfängt, wie die TAN, wegen deren einmaligen Einsatzmöglichkeit, die Zugangsdaten nicht missbrauchen.[327]

507 Vermittelnd wird herrschend angenommen, dass beim normalen kennwortgeschützten Zugang zum Bildschirmtext das fahrlässige Ermöglichen des Zugangs, die Zurechnung begründet.[328] Zum einen sei ein Missbrauch wegen der Anzeige der letzten Benutzung mit Datum und Uhrzeit leicht erkennbar und somit leicht zu verhindern.[329] Zum anderen kann der Zugriff regelmäßig nur über das eigene Bildschirmtext-Gerät erfolgen.[330] Der Anschlussinhaber habe durch diese räumliche Gebundenheit die Möglichkeit einen Missbrauch zu erkennen und zu verhindern. Das zeigt, dass der Anschlussinhaber eine Möglichkeit haben muss, den Missbrauch zu verhindern sowie einen möglichen erfolgten Missbrauch erkennen können muss.

508 Teilweise wird erwogen, die Zurechnung im privaten Rechtsverkehr wegen der damit einhergehenden Überwachungspflicht der Familienmitglieder einzuschränken. Im privaten Bereich überwiege der Schutz der Familie (Art. 6 Abs. 1 GG), sodass eine Haftung ausscheide.[331] Zwar waren Btx-Anschlüsse einer Person zugeordnet und wurden auch zum Abschließen von Verträgen über Fernkommunikation genutzt, sie dienten jedoch auch dem allgemeinen Informationsbedürfnis. Daher müsse der Geschäftspartner bei privaten Anschlüssen davon ausgehen, dass der Anschlussinhaber die Zugangsdaten mit seinem familiären Haushalt teilt, sodass kein Rechts-

---

324 *LG Koblenz*, Urteil v. 17. 9. 1990, 3 S 78/90 – NJW 1991, 1360.

325 *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 1401; *Paefgen*, CR 1993, 559, 561.

326 *Borsum/Hoffmeister*, NJW 1985, 1205, 1206; *Auerbach*, CR 1988, 18, 21.

327 *Borsum/Hoffmeister*, NJW 1985, 1205, 1206.

328 *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 1401; *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552.

329 *Auerbach*, CR 1988, 18, 19.

330 *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552.

331 *Redeker*, NJW 1984, 2390, 2394; *ders.*, IT-Recht[5], Rn. 878.

scheintatbestand bezüglich des Handelns des Anschlussinhabers bestehe.[332] Diese einschränkende Meinung konnte sich jedoch nicht durchsetzen.[333] Art. 6 Abs. 1 GG führe nicht dazu, dass das Haftungssystem ausgehebelt werde und minderjährige Kinder unbegrenzt Schaden anrichten könnten, ohne dass die Eltern dafür haften müssen.[334] Jedenfalls für Zugangsdaten zu Accounts, die ausschließlich für Rechtsgeschäfte verwendet werden, wie z.B. der Account bei einem Online-Versandhändler, kann Art. 6 Abs. 1 GG keine Einschränkung begründen.[335]

d) Bankgeschäfte

Bei unterschiedlichen Bankgeschäften stellen sich ähnliche Fragen wie beim Missbrauch von Zugangsdaten im Internet. Fehlerhafte Überweisungen sollen betrachtet werden, weil sie ebenso wie eine missbräuchlich abgegebene Willenserklärung im Internet, nicht erkennen lassen, ob der vermeintliche Absender sie tatsächlich verwendet hat. Online-Banking und ec-Karte werden betrachtet, weil zu ihrer Benutzung ebenfalls Zugangsdaten erforderlich sind. **509**

aa) Fehlerhafte Überweisungen

Führt eine Bank eine Überweisung fehlerhaft aus, stellt sich stets die Frage, ob sie das Geld direkt vom Zahlungsempfänger kondizieren kann oder ob die Rückabwicklung „über's Eck" anhand der Vertragsbeziehungen vollzogen wird.[336] Nach dem Subsidiaritätsdogma hat die Rückabwicklung anhand der Leistungsbeziehungen grundsätzlich Vorrang.[337] Nach dem bereicherungsrechtlichen Leistungsbegriff[338] liegt eine vorrangige Leistung vor, **510**

---

332 *Redeker*, NJW 1984, 2390, 2394. Zugleich wird darauf hingewiesen, dass bezüglich des Ehegatten der Geschäftspartner durch § 1357 BGB geschützt sei.

333 *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552; *Kuhn*, S. 221; *Paefgen*, CR 1993, 559, 562.

334 *Paefgen*, CR 1993, 559, 562.

335 So sogar *Redeker*, IT-Recht[5], Rn. 878.

336 Siehe dazu auch *Foerster*, AcP 213 (2013), 405, 409 f.

337 *BGH*, Urteil v. 1. 6. 2010, XI ZR 389/09 – NJW 2011, 66, Rn. 31; Urteil v. 29. 4. 2008, XI ZR 371/07 – BGHZ 176, 234, Rn. 9.

338 Diesen ablehnend *Canaris*, in: FS Larenz[1973], 799, 857 ff.

wenn der Anweisende den Rechtsschein gesetzt hat, die Leistung stamme von ihm, und der Rechtsschein ihm zurechenbar ist.[339] Bei genauer Betrachtung stellt sich dies als Ausprägung einer allgemeinen Rechtsscheinhaftung dar. Die Zurechnung wird jedoch nach dem ansonsten abgelehnten[340] Veranlassungsprinzip vollzogen.[341]

511 Eine Zurechnung scheidet somit mangels Veranlassung bei Fälschung oder Verfälschung von Überweisungsaufträgen oder Schecks wie bei Geschäftsunfähigkeit des Anweisenden aus.[342] Ebenso ist eine doppelt ausgeführte Überweisung dem Anweisenden nicht zuzurechnen.[343] Überweist die Bank fälschlicherweise mehr als vom Anweisenden gewünscht oder missachtet sie den Widerruf einer Weisung, kann dies dem Anweisenden zugerechnet werden.[344] Daraus lässt sich ableiten, dass es für jeden Einzelfall einer konkreten Veranlassung durch den Bankkunden bedarf.

512 Durch die Neuregelung des § 675u S. 1 BGB zum 31.10.2009 stellt sich jedoch die Frage, ob die Norm in der neuen Fassung eine solche Rechtsscheinhaftung ausschließt. Einerseits kann mit dem Telos von Art. 60 Abs. 1 ZDRL[345] sowie dem § 675u Abs. 1 BGB, der eine abschließende Regelung bezüglich der dort genannten Ansprüche trifft (§ 675z S. 1 BGB), davon ausgegangen werden, dass der vermeintliche Zahler vollständig aus der Abwicklung fehlgeschlagener Zahlungsvorgänge herauszuhalten ist.[346] Damit scheide eine Rechtsscheinhaftung aus. Andererseits kann die Auffassung vertreten werden, dass der Wortlaut des § 675u S. 1 BGB nur den Aufwen-

---

339 *BGH*, Urteil v. 29. 4. 2008, XI ZR 371/07 – BGHZ 176, 234, Rn. 10; Urteil v. 1. 6. 2010, XI ZR 389/09 – NJW 2011, 66, Rn. 32.

340 Oben Rn. 234.

341 *BGH*, Urteil v. 29. 4. 2008, XI ZR 371/07 – BGHZ 176, 234, Rn. 14; *M. Schwab*, in: MüKo-BGB[6], § 812 Rn. 81 ff. Gegen das Veranlassungsprinzip im Drei-Personen-Bereicherungsausgleich *v. Olshausen*, in: FS Eisenhardt, 277, 290 ff.; *Kiehnle*, EWiR 2010, 485, 486; *ders.*, Jura 2012, 895.

342 *BGH*, Urteil v. 1. 6. 2010, XI ZR 389/09 – NJW 2011, 66, Rn. 33; Urteil v. 29. 4. 2008, XI ZR 371/07 – BGHZ 176, 234, Rn. 11 jeweils m.w.N.

343 *BGH*, Urteil v. 1. 6. 2010, XI ZR 389/09 – NJW 2011, 66, Rn. 36.

344 *BGH*, Urteil v. 29. 4. 2008, XI ZR 371/07 – BGHZ 176, 234, Rn. 12, 19.

345 Richtlinie 2007/64/EG über Zahlungsdienste im Binnenmarkt.

346 *LG Hannover*, Urteil v. 21. 12. 2010, 18 O 166/10 – ZIP 2011, 1406, 1407; *Bartels*, WM 2010, 1828, 1833; *D. W. Belling/J. Belling*, JZ 2010, 708, 711; *Casper*, in: MüKo-BGB[6], § 675u Rn. 4; *Schwintowski*[3], § 7 Rn. 212; *Sprau*, in: *Palandt*[73], § 812 BGB Rn. 17a; *Winkelhaus*, BKR 2010, 441, 443.

dungsersatzanspruch ausschließe.[347] Ferner wird vertreten, dass der Zahler Ansprüche gegen den Zahlungsempfänger und gegen den Zahlungsdienstleister als Gesamtschuldner habe.[348]

bb) ec-Karte

Bei dem missbräuchlichen Einsatz einer ec-Karte steht die Frage nach der vertraglichen Haftung sowie der Beweislast im Vordergrund. Neben dem Zahlungsdiensterahmenvertrag (§ 675f Abs. 2 BGB), der zwischen Bank und Kunde besteht, bestehen gesetzliche Regelungen, die die Frage der Haftung für den Missbrauch der ec-Karte regeln. Nach § 675u S. 1 BGB hat die Bank keinen Aufwendungsersatzanspruch bei nicht autorisierter Zahlung, kann jedoch Schadensersatz nach § 675v BGB verlangen. Der in der Höhe unbegrenzte Schadensersatzanspruch nach § 675v Abs. 2 BGB setzt Vorsatz oder grobe Fahrlässigkeit des Bankkunden voraus.[349] Die Pflichtverletzung des Kunden wird unter bestimmten Voraussetzungen im Rahmen eines Anscheinsbeweises vermutet.[350] **513**

§ 675u S. 1 BGB hat hauptsächlich klarstellende Funktion, weil beim Auftragsrecht ein Aufwendungsersatzanspruch nur bei Weisung besteht.[351] Es stellt sich jedoch die Frage, ob eine Weisung durch Rechtsscheingrundsätze entstehen kann. In Zwei-Personen-Verhältnissen, bei denen jemand die ec-Karte des Bankkunden gegenüber der Bank missbraucht, komme dies wegen der vorrangigen vertraglichen Beziehungen nicht in Betracht.[352] In Drei-Personen-Verhältnissen, bei denen jemand die ec-Karte gegenüber einem Dritten, der nicht die Bank ist, missbraucht, sei eine Rechtsscheinhaf- **514**

347 *Einsele*[2], § 6 Rn. 158 ff.; *Fornasier*, AcP 212 (2012), 411, 431 ff.; *Grundmann*, WM 2009, 1109, 1117; *Kiehnle*, Jura 2012, 895, 900; *Looschelders*, Schuldrecht BT[8], Rn. 1154 f.; *Omlor*, in: *Staudinger*[2012], § 675z BGB Rn. 6; *Rademacher*, NJW 2011, 2169, 2169 ff.; *Riehm*, in: Europäisches Privatrecht[3], § 3 Rn. 30, 36.

348 *Foerster*, AcP 213 (2013), 405, 414 ff.

349 Grobe Fahrlässigkeit liegt in diesem Zusammenhang vor, wenn Karte und PIN im engen räumlichen Zusammenhang aufbewahrt werden *BGH*, Urteil v. 17. 10. 2000, XI ZR 42/00 – BGHZ 145, 337, 340 f.

350 *BGH*, Urteil v. 29. 11. 2011, XI ZR 370/10 – NJW 2012, 1277, Rn. 14 ff.; *LG Hannover*, Urteil v. 16. 3. 1998, 20 S 97/97 – WM 1998, 1123; *Kollrus*, MDR 2012, 377.

351 *Casper*, in: MüKo-BGB[6], § 675u Rn. 1.

352 *Redeker*, IT-Recht[5], Rn. 880.

tung jedoch möglich.[353] Ein Rechtsscheintatbestand sei bei Zahlungen an POS-Terminals mittels ec-Karte gegeben.[354] Eine Zurechnung komme nur bei willentlicher Übergabe in Betracht,[355] nicht jedoch bei Abhandenkommen der ec-Karte.[356] Dabei stellt sich jedoch ebenso wie bei den Überweisungsfällen die Frage, ob eine Rechtsscheinhaftung durch die Neuregelung des § 675u S. 1 BGB gesperrt ist.[357] Bei der ec-Karte stimmten manche Komponenten des Rechtsscheintatbestandes mit denen der Vollmachtsurkunde (§ 172 Abs. 1 BGB)[358] überein. Der Besitz einer physisch einmaligen ec-Karte stellt einen starken Rechtsscheinträger dar. Im Gegensatz zur Vollmachtsurkunde sind die Missbrauchsmöglichkeiten bei einer ec-Karte jedoch nicht beschränkt.

515 Die gesetzliche Wertung des § 675v BGB zeigt, dass das Vertrauen in die Zwei-Faktor-Authentisierung schützenswerter ist, als das Vertrauen in eine rein wissensbasierte Authentisierung. Während für sämtliche Zahlungsmittel ein unbegrenzter verschuldensabhängiger Schadensersatzanspruch nach § 675v Abs. 2 BGB besteht, haben Bankkunden für das Abhandenkommen von einer Besitz-Komponente verschuldensunabhängig auf einen begrenzten Betrag zu haften (§ 675v Abs. 1 BGB).[359] Diese Gesetzessystematik zeigt wiederum, dass die Rechtsordnung das Vertrauen in den Besitz physisch einmaligen Sachen schützt.

cc) Online-Banking

516 Bei der missbräuchlichen Verwendung von Online-Banking stellt sich vorrangig die Frage, ob der Bankkunde der Bank Schadensersatz nach § 675v Abs. 2 BGB schuldet.[360] Wegen der vertraglichen Beziehungen bezwei-

353 *Schinkels*, Bargeldloser Zahlungsverkehr, S. 198.
354 *Ikas*, S. 152 ff.; *Schinkels*, Bargeldloser Zahlungsverkehr, S. 189 f.
355 *Rossa*, CR 2007, 138, 143; *Schinkels*, Bargeldloser Zahlungsverkehr, S. 196.
356 *Rossa*, CR 2007, 138, 144; *Schinkels*, Bargeldloser Zahlungsverkehr, S. 196 f., 242.
357 Dazu oben Rn. 512.
358 Oben Rn. 491.
359 Dazu *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 54 Rn. 58.
360 Vgl. dazu *OLG München*, Urteil v. 23. 1. 2012, 17 U 3527/11 – MMR 2013, 163; *AG Krefeld*, Urteil v. 6. 7. 2012, 7 C 605/11 – MMR 2013, 164; *Borges*, NJW 2012, 2385; *Borges/Schwenk/Stuckenberg/Wegener*, S. 259 ff.; *Hossenfelder*, CR 2009, 790; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 92 ff.; *Schwintowski*[3], § 9 Rn. 43. Zum alten Recht *BGH*, Urteil v. 24. 4. 2012, XI ZR 96/11 – NJW 2012,

feln einige Stimmen der Literatur die Notwendigkeit einer Rechtsscheinhaftung.[361] Die Frage, ob sie nach der neuen Fassung des § 675u S. 1 BGB daneben noch möglich ist, stellt sich ebenso wie bei den Überweisungsfällen und der ec-Karte.[362] § 675u S. 1 BGB schließt dem Wortlaut nach Aufwendungsersatzansprüche für nicht autorisierte Zahlungsvorgänge aus. Mit dem Wortlaut wäre somit eine durch Rechtsscheingrundsätze begründete Autorisierung vereinbar. Daher wird angenommen, dass auch nach der neuen Rechtslage ein wirksamer Überweisungsauftrag durch Rechtsscheingrundsätze entstehen kann.[363]

Teilweise wird die Rechtsscheinhaftung beim Online-Banking vollständig abgelehnt. Bei Ablehnung der Anscheinsvollmacht mit der Rechtsfolge der Haftung auf das positive Interesse[364] ist es folgerichtig, beim Online-Banking eine entsprechende Rechtsscheinhaftung abzulehnen.[365] Wenn die Rechtsscheinhaftung wegen der Nicht-Erkennbarkeit der Vertretungskonstellation beim Handeln unter fremdem Namen abgelehnt wird,[366] begründet dies nur die Ungeeignetheit der Anscheinsvollmacht.[367] Gegen eine allgemeine Rechtsscheinhaftung kann dies nicht eingewendet werden. Eine allgemeine Rechtsscheinhaftung für den Missbrauch beim Online-Banking ist daher grundsätzlich möglich.[368] **517**

Der Rechtsscheintatbestand wird zum Teil bereits bei Verwendung eines PIN/TAN-Verfahrens bejaht.[369] Ebenso reiche eine digitale Signatur nach dem HBCI-Standard aus.[370] Vereinzelt werden die Voraussetzungen der Anscheinsvollmacht aufgegriffen, sodass ein Rechtsscheintatbestand nur in Betracht käme, wenn der Missbrauch von gewisser Dauer und Häufigkeit ist.[371] Die starken Divergenzen bezüglich der Annahme eines Rechtsschein- **518**

2422, Rn. 16 ff.; *KG Berlin*, Urteil v. 29. 11. 2010, 26 U 159/09 – MMR 2011, 338, 339 f.

361 *Langenbucher*, S. 146.

362 Dazu oben Rn. 512.

363 *Herresthal*, in: *Langenbucher/Bliesener/Spindler*, Kap. 5 § 675u BGB Rn. 7; *Grundmann*, WM 2009, 1109, 1114; *Omlor*, in: *Staudinger*[2012], § 675u BGB Rn. 3.

364 Dazu oben Rn. 267.

365 So *Erfurth*, WM 2006, 2198, 2200.

366 So *Dennis Werner*, K&R 2008, 554, 555.

367 Siehe oben Rn. 378.

368 *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 10.

369 *Brückner*, S. 87; *Mülbert*, in: FS Canaris, Bd. 2, 271, 280.

370 *Brückner*, S. 87; *Mülbert*, in: FS Canaris, Bd. 2, 271, 281.

371 *Recknagel*, S. 140.

tatbestandes beim Online-Banking lassen keine Verallgemeinerung zu, welche Merkmale einen Rechtsscheintatbestand in dieser Konstellation auszeichnen können.

519 Für die Zurechnung sei jedenfalls die willentliche Übergabe der Zugangsdaten ausreichend.[372] Bei einem Abhandenkommen der Zugangsdaten auf der anderen Seite, scheide eine Zurechnung aus.[373] Wurden die Zugangsdaten mittels Phishings[374] ausgespäht, komme eine Zurechnung der Willenserklärung zum Bankkunden nicht in Betracht.[375] Dem Kunden fehle die Möglichkeit bei Phishing den Missbrauch zu verhindern.[376] Ferner komme der Missbrauchende nicht aus dem Lager des Bankkunden, sodass eine Rechtsscheinhaftung nicht geboten sei.[377] Beim Pharming, bei dem der Bankkunde einen Missbrauch noch schwerer erkennen und verhindern kann,[378] komme daher eine Zurechnung erst recht nicht in Betracht.[379] Diese konkreten Erwägungen zur Zurechnung bei verschiedenen Missbrauchsmöglichkeiten können zur Konkretisierung der Zurechnung beim Missbrauch von Zugangsdaten im Internet verwertet werden.[380]

dd) Kreditkarte im Mail-Order-Verfahren

520 Im Mail-Order-Verfahren mittels einer Kreditkarte ist ähnlich wie bei Accounts, die lediglich eine rein wissensbasierte Authentisierung einsetzen, das Wissen der Informationen auf der Kreditkarte ausreichend. Beim Missbrauch des Mail-Order-Verfahrens haftet jedoch nur das Acquiring-Unternehmen dem Vertragspartner aufgrund seiner vertraglichen Vereinba-

372 *KG Berlin*, Urteil v. 29. 11. 2010, 26 U 159/09 – MMR 2011, 338; *Brückner*, S. 90 f.
373 *Brückner*, S. 91 ff.; *Mülbert*, in: FS Canaris, Bd. 2, 271, 282.
374 Dazu oben Rn. 142.
375 *KG Berlin*, Urteil v. 29. 11. 2010, 26 U 159/09 – MMR 2011, 338; *LG Berlin*, Urteil v. 11. 8. 2009, 37 O 4/09 – MMR 2010, 137, insoweit nicht abgedruckt Rn. 15; *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08 – MMR 2008, 626, 627 f.; *AG Krefeld*, Urteil v. 6. 7. 2012, 7 C 605/11 – MMR 2013, 164, 165; *Borges*, NJW 2005, 3313, 3314; *Borges/Schwenk/Stuckenberg/Wegener*, S. 256.
376 *Borges*, NJW 2005, 3313, 3314; *LG Berlin*, Urteil v. 11. 8. 2009, 37 O 4/09 – MMR 2010, 137, insoweit nicht abgedruckt Rn. 15.
377 *Recknagel*, S. 138.
378 Oben Rn. 147.
379 *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 10; *Borges*, NJW 2005, 3313, 3315.
380 Unten Rn. 696.

rungen.[381] Eine Rechtsscheinhaftung des Kreditkarten-Inhabers gegenüber dem Kreditkarten-Unternehmen kommt hingegen nicht in Betracht.[382] Diese Wertungen aus dem Mail-Order-Verfahren zeigen, dass eine rein wissensbasierte Authentisierung zwar bei Vorliegen entsprechender vertraglicher Vereinbarungen zu einer Haftung führen kann. Eine ausreichende Grundlage für einen Rechtsscheintatbestand bietet reines Wissen jedoch nicht. Ein starker Rechtsscheinträger wie der Besitz einer physisch einmaligen Sache fehlt bei der Überprüfung des Wissen.

e) Haftung nach § 45i Abs. 4 S. 1 TKG

Die Haftung für den Missbrauch von Telekommunikationsdienstleistungen ist spezialgesetzlich in § 45i Abs. 4 S. 1 TKG geregelt. § 45i Abs. 4 S. 1 TKG ersetzt die im Wesentlichen gleiche Vorgängerregelung des § 16 Abs. 3 TKV.[383] Zweck der Norm ist die Vereinfachung der Abrechnung im anonymen Massenverkehr der Telekommunikationsdienstleistungen.[384] Nach § 45i Abs. 4 S. 1 TKG hat der Anschlussinhaber für die missbräuchliche Verwendung einzustehen, es sei denn sie ist ihm nicht zuzurechnen. Zurechenbarkeit ist zwar eine Terminologie, die auch aus der Rechtsscheinhaftung bekannt ist. Die Zurechenbarkeit in § 45i Abs. 4 S. 1 TKG wird jedoch in Anlehnung an die Vorgängernorm § 16 Abs. 3 TKV als Verschulden analog zu §§ 276, 278 BGB verstanden.[385] Dabei hat der Anschlussinhaber die Risiken aus der eigenen Sphäre zu tragen.[386] Er ist insbesondere für die unbefugte Nutzung durch Mitglieder aus seinem Haushalt verantwortlich.[387] Der Umfang der von der Norm betroffenen Leistungen wird unterschiedlich betrachtet. Während einerseits alle Telekommunikationsleistungen erfasst

521

381 Oben Rn. 342.
382 Oben Rn. 342.
383 Begr. TKG, BT-Drucks. 15/5213, S. 22; *Schadow*, in: *Scheurle/Mayen*[2], § 45i TKG Rn. 1.
384 *Mankowski*, MMR 2009, 808, 809; *Vogt/Rayermann*, MMR 2012, 207, 208.
385 *Schadow*, in: *Scheurle/Mayen*[2], § 45i TKG Rn. 7.
386 *OLG Koblenz*, Beschluss v. 13. 9. 2010, 12 U 789/09 – CR 2014, 377; *Mankowski*, MMR 2009, 808.
387 *Ditscheid/Rudloff*, in: Beck'scher TKG-Kommentar[4], § 45i Rn. 66.

sein könnten,[388] könnten andererseits nur die Abrechnung von Verbindungen, nicht jedoch andere Vertragsschlüsse erfasst sein.[389]

522 Die dogmatische Einordnung von § 45i Abs. 4 TKG erfolgt uneinheitlich. Verbreitet wird § 45i Abs. 4 TKG als gesetzliche Beweislastregelung verstanden, die einen Anscheinsbeweis für die Richtigkeit der Abrechnung statuiert.[390] Andererseits wird diese Norm als materielle Regelung der Rechtsscheinhaftung eingeordnet.[391] Es handele sich um eine Rechtsscheinhaftung, bei der jedoch wegen des vollständig technisierten, anonymen Massengeschäftes eine individuell geschaffene Vertrauensgrundlage nicht erforderlich sei.[392] Zu weit geht das Verständnis von § 45i Abs. 4 S. 1 TKG als Ersatz einer Vertretungsmacht.[393] Die allgemeine Rechtsscheinhaftung, eventuell in Form der Duldungs- und Anscheinsvollmacht, ist jedoch neben § 45i Abs. 4 TKG anwendbar.[394] Wegen der gesetzlichen Regelung der Risikoverteilung stehen vertragliche Rechtsfragen jedoch im Vordergrund.[395]

523 Im Rahmen des Anwendungsbereiches von § 45i Abs. 4 TKG haben sich drei Fallgruppen rausgebildet, die kurz dargestellt werden sollen. Bei der ersten Fallgruppe handelt es sich um Klingelton-Verträge. Eine typische Fallgestaltung besteht darin, dass ein Elternteil für ein minderjähriges Kind einen Mobilfunk-Vertrag abschließt.[396] Das Kind nutzt das Mobiltelefon anschließend zum Abschluss eines teuren Klingelton-Abonnements. Werden 16 Monate lang die in Rechnung gestellten Abonnement-Gebühren beglichen, rechtfertigt sich dabei die Annahme einer Anscheinsvollmacht.[397] Beim erstmaligen Missbrauch habe der Diensteanbieter jedoch kein schüt-

388 So *Vogt/Rayermann*, MMR 2012, 207, 208.
389 So *Mankowski*, MMR 2009, 808, 809.
390 *Mankowski*, MMR 2009, 784; *ders.*, MMR 2009, 808; *Wiebe*, Elektronische Willenserklärung, S. 434.
391 *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 19; *AG Berlin Mitte*, Urteil v. 8. 7. 2010, 106 C 26/10 – MMR 2010, 817, 818; *J. Zimmermann*, MMR 2011, 516, 519.
392 *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 19.
393 *AG Berlin Mitte*, Urteil v. 8. 7. 2010, 106 C 26/10 – MMR 2010, 817, 818: „§ 164 Abs. 1 BGB i.V.m. § 45i Abs. 4 S. 1 TKG".
394 *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 19; *Ditscheid/Rudloff*, in: *Spindler/F. Schuster*[2], § 45i TKG Rn. 43.
395 Vgl. *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 20 ff.; Urteil v. 4. 3. 2004, III ZR 96/03 (Dialer) – BGHZ 158, 201, 204 ff. sowie *Vogt/Rayermann*, MMR 2012, 207.
396 *Vogt/Rayermann*, MMR 2012, 207.
397 *AG Berlin Mitte*, Urteil v. 8. 7. 2010, 106 C 26/10 – MMR 2010, 817, 818.

zenswertes Vertrauen darin, dass der volljährige Anschlussinhaber gehandelt hat, wenn er seine Werbung auf hauptsächlich von Minderjährigen konsumierten Medien schaltet.[398] Teilweise wird darüber hinaus bezweifelt, dass ein Handeln im oder unter fremdem Namen vorliegt.[399]

Ferner scheidet regelmäßig ein Verschulden des Anschlussinhabers mangels Möglichkeiten der Verhinderung aus. SMS bei einem Mobiltelefon gänzlich zu sperren ist nicht zumutbar.[400] Zwar lassen einige Anbieter von Klingelton-Abonnements eine Sperrung zu, eine Eintragung bei sämtlichen Anbieter ist jedoch unzumutbar.[401] Eine Sperrung beim Mobilfunkanbieter ist nicht möglich, sodass keine zumutbare Möglichkeit der Verhinderung vorhanden ist.[402] 524

Die zweite Fallgruppe betrifft R-Gespräche. Bei einem R-Gespräch hat nicht der Anrufende, sondern der Angerufene die Kosten des Gesprächs zu tragen (§ 66j Abs. 1 TKG). Zu Beginn des zunächst kostenlosen Anrufs erläutert eine Bandansage dem Angerufenen, dass er ein Gespräch zu einem gewissen Kostensatz annehmen könne, das er mittels Tastendrucks starten kann. Ein individueller Vertrauenstatbestand scheide bei dieser Bandansage aus.[403] Ferner scheitere ein Rechtsscheintatbestand daran, dass das Entgegennehmen von Anrufen regelmäßig kein rechtsgeschäftliches Verhalten darstellte.[404] Darüber hinaus passe der Vertrauenstatbestand der Anscheinsvollmacht nicht, weil für den Geschäftsgegner nicht erkennbar ist, wer handelt.[405] 525

Im Rahmen des Verschuldens können nur zumutbare Abwehrmöglichkeiten verlangt werden.[406] Fehle es an zumutbaren Möglichkeiten, scheidet ein Verschulden aus.[407] Als noch keine zentrale Sperrliste verfügbar war, war es dem Anschlussinhaber nicht zuzumuten, sich auf sämtlichen Sperr- 526

398 *AG Dieburg*, Urteil v. 31. 1. 2006, 20 C 303/05 – MMR 2006, 343, 344.
399 *Mankowski*, MMR 2009, 784.
400 *Mankowski*, MMR 2009, 808, 812.
401 Ebd., 812.
402 Ebd., 812.
403 *Mankowski*, MMR 2006, 458, 459.
404 *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 10; *Schlegel*, MDR 2006, 1021, 1022; *Mankowski*, MMR 2006, 458.
405 *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 17; *Lobinger*, JZ 2006, 1076, 1078.
406 *Klees*, MDR 2007, 185, 186.
407 *Schlegel*, MDR 2006, 1021, 1022.

listen aller Anbieter von R-Gesprächen eintragen zu lassen.[408] Die Vollsperre des Anschlusses, die Sperre gewisser Tasten oder das Ausschalten des Tonwahlverfahrens seien unzumutbar.[409] Mittlerweile ermöglicht die Eintragung auf einer Sperrliste einen wirksamen Schutz gegen R-Gespräche (vgl. § 66j Abs. 2 TKG).

527 Die dritte Fallgruppe sind die sog. Dialer. Dialer sind Computerprogramme in Form von Viren[410] oder Trojanern[411], die vom Nutzer unbemerkt Verbindungen zu teuren Premium-Diensten herstellen. Bei Dialern komme die Anscheinsvollmacht grundsätzlich in Betracht, setzt aber ein Handeln von gewisser Dauer und Häufigkeit voraus.[412] Im Rahmen der Zurechnung sind keine strengen Anforderungen zu stellen. Es sei nicht fahrlässig, einen Dialer zu erkennen, ihn aber nicht vollständig entfernen zu können.[413]

Dies zeigt, dass nur zumutbare Vorkehrungen zu treffen sind. Wenn ein Missbrauch durch zu viele Umstände ermöglicht wird, die der Account-Inhaber nicht kontrollieren kann, scheidet ein Rechtsscheintatbestand aus. Insbesondere scheidet ein Rechtsscheintatbestand aus, wenn ein Missbrauch über Schwachstellen beim Authentisierungsnehmer möglich ist,[414] und die Authentisierungsnehmer ihre Sicherungssysteme nicht aufdecken.[415]

f) Zwischenergebnis

528 Die Betrachtung der Rechtsscheinhaftung in ähnlichen Konstellationen hat gezeigt, dass ein starker Rechtsscheinträger vorhanden sein muss. Jedenfalls stellt der Besitz einer physisch einmaligen Sache einen solchen starken Rechtsscheinträger dar. Die weitere Voraussetzung gesetzlicher Rechtsscheintatbestände, dass der Rechtsscheinträger die Missbrauchsmöglichkeiten von vorne hinein beschränkt, werden in anderen Konstellationen nicht aufrecht erhalten.[416] Eine solche Voraussetzung ist bei Zugangsdaten im

---

408 *Paschke*, in: *Scheurle/Mayen*[2], § 66j TKG Rn. 2.
409 *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch) – BGHZ 166, 369, Rn. 23 f.
410 Dazu oben Rn. 189.
411 Dazu oben Rn. 193.
412 *Hanau*, Handeln unter fremder Nummer, S. 179 f.
413 *BGH*, Urteil v. 4. 3. 2004, III ZR 96/03 (Dialer) – BGHZ 158, 201, 209.
414 Dazu oben Rn. 215.
415 *Redeker*, IT-Recht[5], Rn. 875.
416 Oben Rn. 514.

Internet wegen der fehlenden Trennung von Identität und Legitimation[417] schwer umzusetzen. Ein Dritter mit den Zugangsdaten zum Account kann darüber die gleichen Handlungen wie der Account-Inhaber vornehmen. Ferner hat der Blick auf die Rechtsscheinhaftung in vergleichbaren Konstellationen gezeigt, dass der Rechtsscheinträger nicht einfach nachzumachen sein darf. Wenn ein Dritter ihn auf Anfrage erstellt, kommt ein Rechtsscheintatbestand nicht in Betracht, wenn die Identität des Geschäftsherren nicht überprüft wird.[418] Bezüglich der Zurechnung hat diese Untersuchung gezeigt, dass der Geschäftsherr eine konkrete und zumutbare Möglichkeit haben muss, einen Missbrauch zu verhindern.

2. *Rechtsscheintatbestand*

Als Rechtsscheintatbestand muss ein Sachverhalt vorliegen, der Vertrauen erweckt.[419] Dieser muss stark genug sein, um ein schützenswertes Vertrauen der Gegenseite zu begründen. Ausgangspunkt einer adäquaten Rechtsscheinhaftung muss die Schutzwürdigkeit des Vertrauens des Rechtsverkehrs sein.[420] Bei Zugangsdaten im Internet ist entscheidend, unter welchen Voraussetzungen der Erklärungsempfänger darauf vertrauen darf, dass der Account-Inhaber die Erklärung selbst oder ein Dritter mit dessen Zustimmung abgegeben hat. **529**

a) Grundsätzliche Eignung

Grundsätzlich eignen sich Zugangsdaten im Internet als Rechtsscheinträger.[421] Denn es spricht eine gewisse Plausibilität dafür, dass der Account-Inhaber mit diesen Zugangsdaten gehandelt hat.[422] Gegen das Vorliegen eines Rechtsscheins wird häufig angebracht, dass der Sicherheitsstandard im Internet zu gering sei und die Rechtsscheinhaftung wegen der Missbrauchs- **530**

417 Oben Rn. 121.
418 Oben Rn. 497.
419 Oben Rn. 227.
420 *Herresthal*, JZ 2011, 1171, 1173.
421 *Rieder*, S. 306.
422 *Oechsler*, AcP 208 (2008), 565, 578.

möglichkeiten ausscheide.[423] Dem kann in dieser Pauschalität nicht zugestimmt werden. Die Missbrauchsmöglichkeiten schließen bei anderen Rechtsscheintatbeständen deren Anerkennung nicht aus.[424] Zum Beispiel bei Blanketterklärungen kann die Unterschrift leicht gefälscht werden, was jedoch nicht zur Aberkennung des Rechtsscheintatbestandes führt. Das Fälschungsrisiko wird vielmehr dadurch berücksichtigt, dass die Vollmachtsurkunde in § 172 Abs. 1 BGB oder die Blanketterklärung echt sein muss, also der Namensträger sie ausstellen muss.[425]

531 Da mithin keine hundertprozentige Sicherheit für die Etablierung eines Rechtsscheins vorhanden sein muss, stellt sich die Frage, ab wann eine ausreichende Sicherheit vorliegt. Dabei kommt es bei der Beurteilung der Sicherheit nicht auf die Empirie an. Vielmehr ist das Vorliegen einer ausreichenden Sicherheit eine wertende Entscheidung. Das Wertungsmerkmal der Sicherheit kann sich mit der Zeit verändern.[426] Diese Zeitabhängigkeit schadet nicht.[427] Zwar lassen neue sicherere Verfahren alte Verfahren noch unsicherer wirken.[428] Das schließt jedoch nicht aus, dass ein Sicherheitsniveau kontemporär als ausreichend angesehen wird. Es ist daher eine zeitbezogene Wertungsentscheidung zu treffen, ab welchem Grad der Sicherheit ein Rechtsscheintatbestand in Betracht kommt. Juristisch muss dabei eine Ja/Nein-Entscheidung getroffen werden, wobei bei der Technik des Internets nur mit Wahrscheinlichkeiten gearbeitet werden kann.[429]

532 Für die Annahme eines Anscheinsbeweises wird häufig vorgebracht, dass das Interesse an Spaßerklärungen im Rahmen von Online-Auktionen gering sei.[430] Man kann überlegen, ob dieser Gedanke auch für die Beurteilung des Rechtsscheintatbestandes Relevanz hat. Selbst wenn die Vorteile, die

423 *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676, 1677; *Genius*, jurisPR-BGHZivilR 12/2011, Anm. 1. Dazu bereits oben Rn. 372.

424 *Faust*, BGB AT[3], § 26 Rn. 41; *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 35; *Kuhn*, S. 221; *Oechsler*, AcP 208 (2008), 565, 579; *Sonnentag*, WM 2012, 1614, 1617.

425 Oben Rn. 312.

426 *Bösing*, S. 40; *Roßnagel*, NJW 1998, 3312, 3313. Allgemein zu Ungewissheiten bei der Einschätzung von Sicherheit *BVerfG*, Beschluss v. 8. 8. 1978, 2 BvL 8/77 (Kalkar I) – BVerfGE 49, 89, 143.

427 *Rieder*, S. 270 ff.

428 *Roßnagel/Hornung*, DÖV 2009, 301, 305.

429 *Hoeren*, NJW 2008, 2615, 2617.

430 *Winter*, MMR 2002, 836; *Ernst*, MDR 2003, 1091, 1093; *Mankowski*, CR 2003, 44, 45; *M. Köhler/Arndt/Fetzer*[7], Rn. 324.

durch die Übernahme des Accounts entstehen, gering sind, hält dies irrational handelnde Angreifer nicht ab.[431] Die Praxis zeigt, dass auch ohne einen erkennbaren Vorteil, Accounts zum Nachteil des Account-Inhabers missbraucht werden.[432] Für den Rechtsscheintatbestand lässt sich aus den behaupteten mangelnden Vorteilen eines Missbrauchs kein Rückschluss ziehen. Beim Vorliegen des Rechtsscheintatbestandes kommt es darauf an, wie stark der äußere Tatbestand ist, der das Vertrauen erweckt. Die statistische Wahrscheinlichkeit eines Missbrauchs ist dabei nicht entscheidend, viel mehr kommt es darauf an, wie einfach oder schwer ein Missbrauch möglich ist. Das hängt maßgeblich von der Sicherheit der verwendeten Authentisierungsmethode ab.

b) Sicherheit der verwendeten Authentisierungsmethoden

Die erste Komponente des Rechtsscheintatbestandes beim Missbrauch von Zugangsdaten im Internet ist die Sicherheit der verwendeten Authentisierungsmethode. Die Authentisierungsmethode stellt sicher, dass derjenige, der den Account erstellt hat, diesen später auch verwenden kann, andere von der Verwendung jedoch ausgeschlossen werden. Zugangsdaten im Internet können stets weitergeben werden, sodass auch eine sichere Authentisierungsmethode nicht das Handeln eines Dritten ausschließen kann. Sie kann jedoch dafür sorgen, dass nur der Account-Inhaber oder jemand, der von ihm die Zugangsdaten erhalten hat, eine Erklärung abgegeben kann. 533

Wenn pauschal auf den Sicherheitsstandard im Internet[433] abgestellt wird, ist dies ungenau bis unzutreffend. Es kommt vielmehr darauf an, wie sicher die im Einzelfall verwendeten Authentisierungsmethoden sind. Entscheidend für die Anerkennung eines Rechtsscheintatbestandes ist nach einigen Stimmen der Literatur das Sicherungsniveau der Zugangsdaten[434] oder anders formuliert der Sicherheitsgrad des verwendeten Legitimationssystems.[435] Dabei gibt es drei Ansätze, die Sicherheitsanforderungen an die verwendeten Authentisierungsmethoden zu konkretisieren. 534

431 Vgl. *LG Konstanz*, Urteil v. 19. 4. 2002, 2 O 141/01 A – CR 2002, 609.
432 So bei *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255.
433 Dazu oben Rn. 372.
434 *Dennis Werner*, K&R 2011, 499, 500; *Redeker*, IT-Recht[5], Rn. 874. Ähnlich *Borsum/Hoffmeister*, NJW 1985, 1205, 1206.
435 *Linardatos*, Jura 2012, 53, 54; *Borsum/Hoffmeister*, NJW 1985, 1205, 1206.

535 Laut *Kuhn* bedarf es der Verlässlichkeit des Kennungszeichens.[436] Darüber hinaus bedürfe es der Gebräuchlichkeit der Kennzeichenbenutzung als Legitimationsmittel.[437] Damit wird die Voraussetzung aufgestellt, dass der Verkehr erwarten muss, dass das Kennzeichen als Legitimationsmittel zum Abschluss von Rechtsgeschäften verwendet wird und dadurch eine entsprechende Sicherung vom Inhaber des Kennzeichens zu erwarten ist. *Kuhns* zwei Merkmale lassen sich als eines zusammenfassen: die Verlässlichkeit des Authentisierungsmittels hängt maßgeblich von der Sicherung durch den Authentisierungsgeber ab. Eine Trennung dieser beiden Merkmale ist nicht sinnvoll möglich, sodass sie als Sicherheit der verwendeten Authentisierungsmethode zusammen gefasst werden können.

536 *Herresthal* möchte für die Anerkennung eines Rechtsscheintatbestandes auf die Dispositionsmöglichkeit des Account-Inhabers über das Legitimationszeichen abstellen.[438] Diese Dispositionsmöglichkeit bestimmt er anhand von drei Kriterien:[439] die Sicherung durch den Account-Inhaber, die Sicherung durch den Authentisierungsnehmer sowie die Sicherheit der Kommunikation. Diese drei Kriterien sind wichtige Anhaltspunkte, um die Sicherheit der verwendeten Authentisierungsmethode zu bestimmen. Das entscheidende Merkmal fehlt jedoch. Die Sicherheit der verwendeten Authentisierungsmethode hängt maßgeblich von den eingesetzten Authentisierungsmitteln ab.

537 Nach *Rieder* soll der Grad der Sicherheit, den die Authentisierungsmethode gegen Missbrauch bietet, entscheidend für die Anerkennung eines Rechtsscheintatbestandes sein.[440] Drei Kriterien seien bei der Wertung anhand einer Gesamtbetrachtung besonders zu berücksichtigen: Art und Beschaffenheit der verwendeten Authentisierungsmittel und deren Übermittlung, Inhalt und Bedeutung des Rechtsgeschäfts und Vereinbarungen der Parteien.[441] Die beiden letzten Kriterien von *Rieder* sind jedoch nicht geeignet einen Rechtsscheintatbestand zu begründen. Das zweite Kriterium stellt auf den Inhalt und die Bedeutung des Rechtsgeschäfts in Form der

436 *Kuhn*, S. 217 f. zustimmend *Spiegelhalder*, S. 130.
437 *Kuhn*, S. 219.
438 *Herresthal*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 28; *ders.*, JZ 2011, 1171, 1173. Ihm folgend *Sonnentag*, WM 2012, 1614, 1616.
439 *Herresthal*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 29; *ders.*, JZ 2011, 1171, 1174.
440 *Rieder*, S. 309.
441 Ebd., S. 310 ff.

finanziellen Belastung für die Parteien ab.[442] Zwar werden rational agierende Parteien dazu neigen, Rechtsgeschäfte mit einem hohen Transaktionsvolumen rechtlich abzusichern. Daraus kann jedoch nicht abgeleitet werden, dass für unbedeutendere Rechtsgeschäfte leichter ein Rechtsscheintatbestand begründet werden kann. Die Parteien gehen bei diesen Geschäften schlechthin das Risiko ein, dass der Vertrags in unwirksamer Weise zustande gekommen ist. Ebenfalls ist das dritte Kriterium ungeeignet einen Rechtsscheintatbestand zwischen zwei erstmalig aufeinander treffende Parteien zu begründen. Wenn Vertragsbeziehungen bestehen, wie beim Online-Banking, ist die Frage der Rechtsscheinhaftung wegen vorrangiger vertraglicher Regelungen weniger entscheidend.[443] Bahnen sich Vertragsbeziehungen an, dann bietet sich ein Rückgriff auf die *culpa in contrahendo* an,[444] sodass hier ebenfalls eine Rechtsscheinhaftung weniger entscheidend ist. Die Vertragsfreiheit gestattet den Parteien zwar Haftungsregeln festzulegen.[445] Einen Rechtsscheintatbestand, der geeignet sein muss, auch unter Parteien, die keinerlei Beziehungen haben, anwendbar zu sein, lässt sich daher mit *Rieders* drittem Kriterium der vertraglichen Regelungen nicht konturieren.

Zusammenfassend lässt sich feststellen, dass für die Anerkennung eines **538**
Rechtsscheintatbestandes zunächst zentral auf die Sicherheit der verwendeten Authentisierungsmethode abzustellen ist. Darüber hinaus ist zu untersuchen, ob eine sichere Authentisierung ausreicht oder ob weitere Merkmale hinzutreten müssen.[446]

Die Sicherheit der verwendeten Authentisierungsmethode muss das Ziel **539**
haben, den berechtigten Account-Inhaber zu identifizieren und die Benutzung des Accounts durch fremde und unberechtigte Dritte auszuschließen. Ein Ausschluss von berechtigten Dritten bieten höchstens biometrische Authentisierungsmittel. Die befugte Benutzung des Accounts durch einen Dritten hindert daher nicht die Anerkennung als Rechtsscheintatbestand. Für die Sicherheit der verwendeten Authentisierungsmethode kommt es auf die verwendeten Authentisierungsmittel und die drei von *Herresthal*[447] etablierten Kriterien der Sicherung durch den Authentisierungsgeber, der Sicherung

442 *Rieder*, S. 311.
443 Vergleiche dazu oben Rn. 516.
444 Hierzu oben Rn. 436.
445 *Rieder*, S. 311.
446 Zur weiteren Voraussetzung unten Rn. 595 ff.
447 *Herresthal*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 29; *ders.*, JZ 2011, 1171, 1174.

durch den Authentisierungsnehmer und der Sicherheit der Kommunikation an. Bei einem sicheren Authentisierungsvorgang hat der Authentisierungsnehmer eine Sperrmöglichkeit für die Zugangsdaten zur Verfügung zu stellen.[448] Es werden daher folgend die unterschiedlichen, gängigen Authentisierungsmethoden auf deren Sicherheit überprüft, um festzustellen, ob sie eine ausreichende Sicherheit für die Anerkennung eines Rechtsscheintatbestandes bieten.

aa) Ohne Authentisierung

540 Für die Anerkennung des Rechtsscheintatbestandes ist entscheidend, dass die verwendete Authentisierungsmethode ausreichend sicher den Account-Inhaber identifiziert. Eine logische Schlussfolgerung daraus wäre, dass ein Account, der nicht durch Zugangsdaten gesichert ist, keinen Rechtsscheintatbestand bezüglich des Handeln des Account-Inhabers begründen kann.

541 Dabei ist jedoch zu beachten, dass die weithin angenommene Anonymität im Internet[449] in dieser Form nicht vorhanden ist. Eine Kommunikation im Internet setzt die Datenübertragung zwischen zwei Rechnern, die sich anhand ihrer IP-Adresse identifizieren, voraus.[450] Der Grad der Anonymität im Internet ist daher regelmäßig nicht sehr hoch.[451] Dabei gehen die Informationen über den Besucher einer Internetseite weit über die Identifizierung mittels IP-Adresse, die eventuell sogar einen Rückschluss auf den Standort zulässt, hinaus. Internetseiten setzen auf den Rechnern eines Besuchers sog. Cookies[452] ein, die im Browser oder im Flash-Plugin gespeichert sind. Der von dem Suchmaschinenbetreiber Google verwendete Cookie lässt beispielsweise eine eindeutige Wiedererkennung über zwei Jahre hinweg zu.[453] Auch weitere Merkmale, die der Besucher einer Internetseite übermittelt, können zu dessen Wiedererkennung führen. Regelmäßig werden im HTTP-Header Informationen über den verwendeten Browser und das eingesetzte Betriebssystem übermittelt.[454] Diese Daten können dazu genutzt werden,

448 *Redeker*, IT-Recht[5], Rn. 877.
449 Siehe *Schapiro*, S. 3.
450 Oben Rn. 38.
451 *Brunst*, Anonymität im Internet, S. 25; *ders.*, DuD 2011, 618.
452 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.8.
453 Die Lebensdauer wurde von über 30 Jahren auf diesen Zeitraum verkürzt, dazu *Wilkens*, heise online v. 17. 7. 2007.
454 Der HTTP-Header „User-Agent" muss übermittelt werden *IETF*, RFC 2616, S. 144.

unterschiedliche Nutzer, die über eine IP-Adresse zugreifen, zu unterscheiden. Durch die Wiedererkennung des Nutzers kann ein Profil über diesen erstellt werden, das viel genauere Rückschlüsse auf Vorlieben zulässt, als es beispielsweise der Name und die Anschrift tun.[455]

Diese Methode ist jedoch auf die Wiedererkennung eines bestimmten Rechners beschränkt. Wird der Rechner gewechselt oder verwendet eine Person mehrere Rechner, kann dies durch das Tracking nicht erkannt werden. Darüber hinaus kann ein Nutzer den Tracking-Cookie löschen, sodass eine Wiedererkennung scheitert. 542

Diese Identifizierung hat eine paradoxe Wirkung. Zwar kann ein Internetseiten-Betreiber zahlreiche Informationen über einen Nutzer sammeln und somit ein Profil seiner Persönlichkeit erstellen.[456] Ein Rückschluss von dieser möglicherweise sehr umfangreichen virtuellen Identität auf eine numerische Identität in Form einer natürlichen Person ist jedoch nicht möglich. Die IP-Adresse identifiziert die handelnde natürliche Person nicht.[457] Andere Rückschlüsse auf die numerische Identität der handelnden natürlichen Person lassen die gesammelten Daten regelmäßig ebenfalls nicht zu. Das führt zum vermeintlich paradoxen Ergebnis, dass der Besucher einer Internetseite gläsern für dessen Betreiber sein kann, der Betreiber jedoch kaum Möglichkeiten hat, Rückschlüsse auf die numerische Identität des Nutzers zu ziehen, ohne dass er diese Daten von ihm abfragt. Ohne eine Authentisierung ist daher eine Identifizierung eines Nutzers unmöglich. Insofern bestätigt sich die eingangs aufgestellte Schlussfolgerung: Wenn kein Authentifizierungsverfahren vorhanden ist, dann ist kein Rechtsscheintatbestand, der auf ein Handeln des Account-Inhabers hindeutet, vorhanden. 543

bb) Rein wissensbasierte Authentisierung

Das am weitesten verbreitete Authentisierungsverfahren besteht in einer rein wissensbasierten Authentisierung anhand einer Kombination von Benutzername und Kennwort. Mit dem Wissen dieser zwei oder drei, wenn das Übereinstimmen von Benutzername und Kennwort als drittes Element anerkannt wird,[458] Merkmale authentisiert sich der Account-Inhaber. Die 544

455 *Brunst*, DuD 2011, 618.
456 Vgl. *Jandach*, in: FS Kilian, 443, 444 f.
457 Oben Rn. 38.
458 So *Mankowski*, CR 2007, 606, 607; *ders.*, CR 2011, 458.

rein Passwort geschützten Erklärungen werden vereinzelt als Antwort auf die Unsicherheit von E-Mails gesehen.[459]

545 Eine rein wissensbasierte Authentisierung kann auch mehrere Wissens-Komponenten verbinden. Bei einem TAN-Verfahren wird eine gleichbleibende PIN und eine transaktionsbezogene, nur einmalig einsetzbare TAN zur Authentisierung verwendet.[460] Die TANs werden dem Account-Inhaber regelmäßig in einem getrennten Schreiben zugesandt.[461] Da der Account-Inhaber sich nicht 50 sechsstellige TANs merken kann, die jeweils nur einmalig gültig sind, benötigt er daher die TAN-Liste zur Authentisierung. Dadurch wird jedoch nicht der Besitz an der TAN-Liste überprüft, sondern lediglich das Wissen, welche TANs auf der Liste stehen. Der Account-Inhaber kann die Liste beliebig vermehren, beispielsweise durch Fotokopien, Abschreiben oder Einscannen. Beim PIN/TAN-Verfahren handelt es sich somit um eine rein wissensbasierten Authentisierungsmethode, die jedoch zwei Wissenskomponenten einsetzt.[462]

aaa) Sicherheit von Passwörtern durch ihre Stärke

546 Zur Beurteilung, ob ein Rechtsscheintatbestand für passwortgeschützte Erklärungen vorliegt, kommt es zunächst auf die Sicherheit einer Authentisierungsmethode an, die als einziges Authentisierungsmittel Wissen des Authentisierungsgebers verwendet. Dabei ist zunächst zu beachten, dass es keine einheitlichen Vorgaben oder Regelungen für Passwörter gibt. Jeder kann auf seiner Internetseite Nutzer zur Eingabe von Passwörtern auffordern.[463] Dabei kann der Betreiber der Internetseite selbst entscheiden, ob er den Nutzern eine freie Wahl bei den Passwörtern lässt oder gewisse Vorgaben zur Sicherheit der Passwörter macht. Mangels vorhandener Standardisierung von Passwörtern kann keine pauschale Aussage über die Sicherheit von Passwörtern getroffen werden. Es ist anhand von Empfehlungen für sichere Passwörter zu untersuchen, ob diese für einen Rechtsscheintatbestand ausreichen.

---

459 *Mankowski*, CR 2007, 606, 607; *ders.*, CR 2011, 458.
460 *Schwintowski*[3], § 9 Rn. 34 f.
461 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 10.
462 *Bergfelder*, S. 281.
463 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.

Studien zeigen, dass bei einer freien Wahl von Passwörtern 86 % der Nutzer ein Passwort wählen, das ein Angreifer durch ausprobieren sehr einfach herausfinden kann.[464] Das Ausprobieren erfolgt mittels einer Brute-Force-Methode oder durch das Verwenden von Informationen über den Account-Inhaber.[465] Unsicher sind daher beispielsweise Zahlenkombinationen, die das Geburtsdatum des Account-Inhabers enthalten,[466] oder Zeichenketten, die aus Wörtern aus dem Wörterbuch bestehen.[467] 547

Sichere Passwörter schützen gegen das Erraten durch Ausprobieren dadurch, dass sie eine gewisse Länge haben und aus einer Kombination aus Buchstaben, Zahlen und Zeichen bestehen.[468] Diese Anforderungen lassen sich anhand einer ganzen Reihe von Kriterien konkretisieren.[469] Die gewisse Länge, die ein sicheres Passwort haben sollte, beträgt mindestens acht Zeichen.[470] Bei einem Brute-Force-Angriff wird systematisch jede mögliche Kombination ausprobiert. Die Anzahl der möglichen Kombinationen steigt exponentiell mit dem Exponenten, also der Länge des Passworts. Der Aufwand für einen Brute-Force-Angriff steigt daher mit jedem zusätzlich möglichen Zeichen um den Faktor der zur Verfügung stehenden Zeichen. Daher sollte ein Passwort aus Klein- (26 Zeichen) und Groß-Buchstaben (26 Zeichen) und Zahlen (10 Zahlen) bestehen können. Die Anzahl der möglichen Kombinationen bei einem achtstelligen Passwort steigt damit auf gut 218 Billionen[471] an. Wenn zusätzlich noch Sonderzeichen eingebaut werden,[472] erschwert dies ein Erraten erheblich. 548

Darüber hinaus schützt ein sicheres Passwort vor einem gezielten Erraten mit Hilfe von Passwort-Tabellen.[473] Ein Passwort darf daher nicht so gewählt werden, dass es im Wörterbuch steht, ein Eigenname wie Vor- oder 549

464 *Eckert*[8], S. 470 f.
465 Zu diesen Methoden oben Rn. 180, 181.
466 So verwendet vom Beklagten in *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257.
467 *Eckert*[8], S. 471.
468 *BSI*, IT-Grundschutz-Kataloge, M 2.11; *Ernst*, MDR 2003, 1091, 1094; *Rieder*, S. 310.
469 *Eckert*[8], S. 471; ähnlich auch *Rieder*, S. 310.
470 *BSI*, IT-Grundschutz-Kataloge, M 2.11; *Eckert*[8], S. 471.
471 $62^8 = 218.340.105.584.896$.
472 *Eckert*[8], S. 471.
473 Zu dieser Methode oben Rn. 180.

Nachname des Account-Inhabers ist oder aus einer Folge von Zeichen besteht, die auf der Tastatur unmittelbar nebeneinander liegen.[474]

550 Eine weitere Methode an Passwörter zu gelangen, ist bekannte Passwörter eines Nutzer bei dessen weiteren Accounts auszuprobieren.[475] Dagegen hilft, dass ein Nutzer für jeden Authentisierungsgeber ein unterschiedliches Passwort verwendet. Die Einmaligkeit des Passworts ist Voraussetzung für die wissensbasierte Sicherung von De-Mail-Accounts (§ 4 Abs. 1 S. 2 DeMailG), wodurch die Sicherheit der Authentisierung sichergestellt werden soll.[476] Die Anforderung, dass ein Passwort einmalig ist, hat einen ambivalenten Effekt. Zum einen verhindert sie, dass nach dem Erfahren eines Passworts des Account-Inhabers, dieses mit Erfolg bei seinen anderen Accounts verwendet werden kann. Auf der anderen Seite wächst das Bedürfnis des Account-Inhabers sich Passwörter aufzuschreiben mit der Anzahl der verschiedenen Passwörter. Diesem Dilemma kann ein Nutzer dadurch begegnen, indem er seine Passwörter mit einem vorne oder hinten angestellten Zeichenkette kombiniert (sog. Salting).[477] Bei dieser Methode verwendet der Nutzer das stets gleiche Passwort, stellt diesem jedoch beispielsweise den ersten Buchstabe des Namens vom Authentisierungsnehmer voran. Dadurch verwendet er bei jedem seiner Accounts ein unterschiedliches Passwort, muss sich jedoch nur das eine Kern-Kennwort merken.

551 Je mehr dieser Anforderungen ein Passwort erfüllt, desto sicherer ist es gegen das Erraten durch systematisches Ausprobieren oder Verwendung von Informationen über den Account-Inhaber. Auch das sicherste Passwort macht eine rein wissensbasierten Authentisierung nicht sicher, wenn Dritte Kenntnis vom Passwort erlangen können.

bbb) Ausspähen von Passwörtern

552 Teilweise wird behauptet ein „Diebstahl“ von Passwörtern durch Ausspähen sei unwahrscheinlich,[478] weil das Ausspähen von Passwörtern nur mit erheblichem technischen Know-How möglich wäre.[479] Dem ist zu wider-

474 *Eckert*[8], S. 471.
475 Dazu oben Rn. 181.
476 Dazu Begr. DeMailG, BT-Drucks. 17/3630, S. 28.
477 Ähnlich *B. Lorenz*, DuD 2013, 220, 223.
478 *Mankowski*, CR 2011, 458.
479 Dazu oben Rn. 128.

sprechen. Zum einen wird keine nachvollziehbare Begründung für die Unwahrscheinlichkeit des Ausspähens der Passwörter geliefert. Der Verweis auf die vielen Versuche, mittels Phishings an die Zugangsdaten zu gelangen,[480] lässt eher den gegenteiligen Schluss zu. Zum anderen gibt es zahlreiche Möglichkeiten, wie ein Dritter an das Passwort des Account-Inhabers gelangen kann. Er kann beispielsweise Zugriff auf aufgeschriebene oder auf dem Rechner oder in der Cloud gespeicherte Passwörter erhalten.[481] Oder ein Angreifer kann mittels der unterschiedlichen Varianten des Phishings wie das Pharming den Account-Inhaber zur Preisgabe überlisten.[482] Ferner könnte er auf einem infizierten Rechner mittels eines Trojaners einen Keylogger installieren und die Passwörter vom Nutzer abgreifen.[483] Möglich ist aber auch, dass er in das System des Authentisierungsnehmers eindringt und beispielsweise eine Passwort-Datenbank kopiert.[484] Darüber hinaus kann ein Angreifer Datensätze von Zugangsdaten für zahlreiche unterschiedliche Accounts aus sog. Dropzones kaufen.[485]

553 Die Möglichkeit des Ausspähens von Zugangsdaten ist eine entscheidende Schwäche der wissensbasierten Authentisierung. Die Vermehrung von Wissen ist in unbegrenztem Maße möglich. Wenn ein Dritter das Passwort von einem Account-Inhaber „stiehlt", verliert der Account-Inhaber das Passwort nicht. Der Dritte hat das Wissen um das Passwort nur vermehrt. Häufig wie in Fällen eines Keyloggers kann der Account-Inhaber noch nicht einmal bemerken, dass das Passwort einem Dritten bekannt ist. Erst nach einem Missbrauch bemerkt der Account-Inhaber regelmäßig, dass ein Dritter das Wissen um das geheime Passwort hat.

554 Eine Möglichkeit den Missbrauch mit ausgespähten Passwörtern zu verringern ist, dass der Account-Inhaber das Passwort regelmäßig ändert.[486] Das verhindert zwar nicht, dass ein Dritter ein ausgespähtes Passwort unmittelbar verwendet. Späht der Dritte das Passwort jedoch für einen geplanten, zeitlich später gelegenen Missbrauch aus, kann das regelmäßige Ändern des Passworts diesen verhindern. Wie ein Erfordernis eines einmaligen Passworts hat das häufige Ändern des selbigen einen ambivalenten Effekt.

480 *Mankowski*, CR 2011, 458.
481 Oben Rn. 132, 135.
482 Oben Rn. 138 ff.
483 Oben Rn. 166.
484 Oben Rn. 215.
485 Oben Rn. 128.
486 *Eckert*[8], S. 471.

Der Account-Inhaber muss sich die ständig wechselnden Passwörter merken. Dieser Herausforderung werden viele Nutzer mit dem Aufschreiben oder Speichern des Passworts begegnen, wodurch wiederum Möglichkeiten zum Ausspähen geschaffen werden.

555 Phishing ist auch bei den PIN/TAN-Verfahren möglich. In der einfachen Form des TAN-Verfahrens erhält der Account-Inhaber eine Liste mit TANs, die nach Verwendung verbraucht sind.[487] Erhält ein Angreifer durch Phishing-Angriff Kenntnis der PIN und einer TAN kann er nur so viele Transaktionen ausführen, wie er TANs erhalten hat. Das einfache TAN-Verfahren schützt daher den Account insoweit, als dass ein Angreifer den Account nur in begrenzter Anzahl missbrauchen kann.

556 Das iTAN-Verfahren ist noch sicherer gegen den Missbrauch durch Phishing. Beim iTAN-Verfahren fragt der Authentisierungsnehmer eine bestimmte der nummerierten (indizierten) TAN ab und nur diese kann zur Durchführung der Transaktion verwendet werden.[488] Der Angreifer muss dabei das Glück haben, dass er diejenige TAN vom Account-Inhaber abfragt, die der Authentisierungsnehmer zu einem späteren Zeitpunkt abfragt. Das erschwert die Möglichkeit auch bei erfolgtem Phishing-Angriff eine Transaktion durchzuführen erheblich. Gleichwohl lassen manche Account-Inhaber sich dazu bewegen, bis zu zehn TANs gleichzeitig preiszugeben,[489] sodass die Wahrscheinlichkeit des Erfolges beim Phishing-Angriff steigt. TAN-Verfahren können somit einen Missbrauch nicht ausschließen, erschweren ihn jedoch.

557 Der Schwäche von Passwörtern, dass sie ausgespäht werden können, kann durch eine Sicherung durch den Account-Inhaber und durch den Authentisierungsnehmer begegnet werden.

ccc) Sicherung durch den Account-Inhaber

558 Zentrale Anforderung an den Account-Inhaber zur Sicherheit der wissensbasierten Authentisierung ist die Geheimhaltung des Passworts. Fraglich ist, woher eine mögliche Geheimhaltungspflicht stammen kann. Erwägungen über die Herkunft von Geheimhaltungspflicht und Identifikationsfunktion wirken zirkulär. Im vertraglichen Bereich begründet der *BGH* die Identifika-

487 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 10.
488 Ebd., § 55 Rn. 12.
489 Vgl. *BGH*, Urteil v. 24. 4. 2012, XI ZR 96/11 – NJW 2012, 2422.

tionsfunktion mit dem Bestehen einer vertraglichen Geheimhaltungspflicht gegenüber dem Plattformbetreiber.[490] Im deliktischen Bereich hingegen leite sich die Geheimhaltungspflicht gegenüber jedermann aus der – ohne nähere Begründung behaupteten – Identifikationsfunktion des Accounts ab.[491]

559 Bei den unterschiedlichsten Accounts wird dem Inhaber eine Geheimhaltungspflicht gesetzlich auferlegt. Bei einem De-Mail-Account ist der De-Mail-Diensteanbieter verpflichtet, sicherzustellen, dass der De-Mail-Kunde sein Passwort geheim hält (§ 4 Abs. 1 S. 2 DeMailG). eBay verpflichtet seine Kunden in den AGB das Passwort geheim zu halten.[492] Bankkunden, die Online-Banking nutzen, müssen nach § 675l S. 1 BGB Vorkehrungen treffen, um die Zugangsdaten vor dem unbefugten Zugriff Dritter zu schützen.

560 Teilweise wird vertreten, dass die Verkehrserwartung an die Geheimhaltung von der Art des Accounts abhängt.[493] Während Accounts bei Informationsportalen keinen Rechtsscheintatbestand begründen sollen, komme dies für Accounts, die zum Abschluss von Rechtsgeschäften dienen, in Betracht.[494]

561 Diese Unterscheidung nach unterschiedlichen Accounts vermag nur auf den ersten Blick zu überzeugen. Zwar kann berechtigterweise erwarten werden, dass ein Bankkunde den Zugang zum Online-Banking stark schützt, wohingegen die Zugangsdaten zu einem Informationsportal wie Wikipedia weniger gut geschützt werden. Diese Erwartung kann jedoch nicht auf eine Unterscheidung zwischen Accounts auf Informationsplattformen und Accounts, die zum Abschluss von Rechtsgeschäften dienen, generalisiert werden. Denn rational agierende Account-Inhaber berücksichtigen mehr Umstände bei der Sicherung, als die Möglichkeit Rechtsgeschäfte abschließen zu können. Ein Ehemann wird beispielsweise keine Probleme haben, die Zugangsdaten zu einem Online-Versandhändler mit seiner Ehefrau zu teilen. Den Zugang zu seinem Kalender in der Cloud, beispielsweise bei

490 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18; ebenso *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 34.

491 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18.

492 Ausführlich dazu oben Rn. 405.

493 *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 34; *Sonnentag*, WM 2012, 1614, 1616.

494 *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 33.

Gmail, könnte er hingegen gegen ihren Zugriff schützen wollen, damit er sich heimliche Verabredungen mit einer Geliebten eintragen kann. Darüber hinaus kann der immaterielle Schaden, der über nicht zum Abschluss von Rechtsgeschäften bestimmten Accounts angerichtet werden kann, rational betrachtet bedeutend gewichtiger sein als der materielle Schaden, der bei Online-Versandhändlern angerichtet werden kann. Während bei einer ungewollten Bestellung ein Widerrufsrecht besteht, kann eine ungewollt von einem Dritten versendete Twitter-Nachricht den Ruf des Account-Inhabers nachhaltig schädigen.[495] Die Unterscheidung nach der Art des Accounts kann daher nicht überzeugen. Die Behauptung, dass bei Accounts, die zum Abschluss von Rechtsgeschäften dienen, regelmäßig eine Geheimhaltung der Zugangsdaten erwarten werden kann, erscheint jedoch plausibel.

562 Ein häufiges Problem besteht jedoch darin, dass sich Nutzer Passwörter aus zwei Gründen nicht merken können.[496] Der erste Grund ist, dass ein sicheres Passwort lang und komplex ist. Der zweite Grund besteht darin, dass für jeden Authentisierungsnehmer ein anderen Passwort genommen werden sollte, damit man die Zugangsdaten von einem Account nicht erfolgreich bei einem anderen Account verwenden kann. Dabei besteht ein Dilemma darin, dass diese zwei Gründe daher stammen, Passwörter sicher zu gestalten. Ein sicheres Passwort hat eine gewisse Länge.[497] Je länger das Passwort ist, desto schwieriger ist es für den Account-Inhaber sich das Passwort zu merken und desto eher schreibt er sich das Passwort auf.[498] Die Einmaligkeit oder das häufige Ändern von Passwörtern führt dazu, dass sich ein Nutzer eine Vielzahl von Passwörtern merken muss. Um sich dies zu erleichtern, neigen viele Nutzer dazu, sich die Passwörter aufzuschreiben. Sogar die PIN der ec-Karte, die regelmäßig nur aus vier Zahlen besteht, schreiben sich zahlreiche Bankkunden auf.[499] Dadurch erhalten starke Passwörter eine paradoxe Wirkung. Je sicherer diese durch ihre Länge sind, desto schwerer kann der Account-Inhaber sie sich merken. Je schwerer er sich die Passwörter merken kann, desto eher schreibt der Account-Inhaber sie sich auf, wodurch die

---

495 In dem oben Rn. 223 betrachteten Fall war das primäre Ziel der Angreifer, den Twitter-Account des Opfers zu übernehmen.

496 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 115.

497 Dazu oben Rn. 548.

498 *Pierrot*, in: *Ernst*, Rn. 38; *Schneier*, S. 136.

499 Siehe dazu *BGH*, Urteil v. 17. 10. 2000, XI ZR 42/00 – BGHZ 145, 337, 338; *LG Bonn*, Urteil v. 16. 6. 1999, 5 S 41/99 – NJW-RR 2000, 1415; *AG Kassel*, Urteil v. 16. 11. 1993, 83 C 4162/93 – NJW-RR 1994, 630; *Borges*, Verträge, S. 498 Fn. 173; *Redeker*, IT-Recht[5], Rn. 880.

Sicherheit des Passworts gefährdet wird. Ein von der Länge her sicheres Passwort veranlasst den Account-Inhaber somit dazu, sich dieses notieren. Damit schafft er eine Schwachstelle.

Es stellt sich daher die Frage, ob dem Nutzer das Speichern oder Auf- 563
schreiben des Passworts gestatten sein soll oder ob er bereits dadurch gegen seine Geheimhaltungspflicht verstößt. Um sich dieser Frage zu nähern, soll zunächst auf die Wertungen im Online-Banking zurückgegriffen werden, wo diese Frage ausführlich erörtert wird. Beim Online-Banking muss es wegen der Vielzahl an der merkenden Passwörtern dem Bankkunden erlaubt sein, die Zugangsdaten aufzuschreiben.[500] Das Aufschreiben und Belassen in einer abgeschlossenen Wohnung oder einem abgeschlossenen Geschäftsraum ist dabei eine ausreichende Sicherung des aufgeschriebenen Geheimzeichens.[501] Selbst wenn das elektronische Speichern regelmäßig durch AGB der Banken untersagt ist, soll auch dies bei hinreichend sicherer Methode zulässig sein.[502]

Der Grund, dass der Account-Inhaber wegen der Vielzahl von unter- 564
schiedlichen Passwörtern sich diese aufschreiben können muss, trifft auf sämtliche rein wissensbasierte Authentisierungsverfahren zu. Beim Online-Banking ist jedoch eine Besonderheit gegeben, die andere Authentisierungsverfahren nicht haben. Beim Online-Banking werden stets mehrere Authentisierungsmittel verwendet, beispielsweise eine PIN zum Einloggen und TANs zum Ausführen von Transaktionen. Diese unterschiedlichen Authentisierungsmittel sind stets getrennt aufzubewahren.[503] Bei einem durch Passwort geschützten Benutzerkonto ist eine Trennung wegen des Einsatzes nur eines Authentisierungsmittels nicht möglich. Im Gegensatz zum Online-Banking kann ein Dritter mit dem Wissen um ein Authentisierungsmittel die vollen Rechte des Accounts ausnutzen. Die getrennte Aufbewahrung der notierten Zugangsdaten beim Online-Banking dient der Sicherung vor unbefugten Zugriff. Dieses Ziel kann auch bei passwortgeschützten Benutzerkonten dadurch erreicht werden, dass die Notiz des Passworts ausreichend geschützt wird.

---

500 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 115. Vgl. auch *BGH*, Urteil v. 5. 10. 2004, XI ZR 210/03 – BGHZ 160, 308, 319.

501 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 130.

502 *Herresthal*, in: *Langenbucher/Bliesener/Spindler*, Kap. 5 § 675l BGB Rn. 12; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 116.

503 *Casper*, in: MüKo-BGB[6], § 675l Rn. 14.

565 Darüber hinaus kann bei einem sicheren Authentisierungsverfahren vom Account-Inhaber erwartet werden, dass er die vom Authentisierungsnehmer zur Verfügung gestellten Sperrmöglichkeiten[504] unverzüglich nutzt, um einen Missbrauch zu verhindern. Ebenso wie bei der Geheimhaltungspflicht stellt sich die Frage, ob eine Verkehrserwartung die Pflicht zur Verwendung von Sperrmöglichkeiten begründet oder ob eine Verkehrserwartung nur entstehen kann, wenn der Nutzer vertraglich dazu verpflichtet ist. Die eBay-AGB beispielsweise begründen eine Pflicht des Nutzers den Authentisierungsnehmer zu benachrichtigen, wenn es Anhaltspunkte für den Missbrauch des Accounts gibt.[505] Für Bankkunden ergibt sich diese Pflicht sogar gesetzlich aus § 675l S. 2 BGB.[506] Sofern der Account-Inhaber zur Sperrung des Accounts verpflichtet ist oder er den Authentisierungsnehmer über einen potentiellen Missbrauch zwecks Sperrung informiert, darf der Verkehr vom Authentisierungsnehmer erwarten, dass dieser den Account sperrt. Selbst bei Bestehen einer solchen Pflicht, setzt diese Pflicht regelmäßig erst nach dem ersten Missbrauch an, sodass sie ihn nicht verhindern kann. Weitere, zeitlich später gelagerte Fälle des Missbrauchs können jedoch durch eine Sperrmöglichkeit verhindert werden.

566 Zusammenfassend lässt sich festhalten, dass bei zahlreichen Accounts eine Geheimhaltung der Zugangsdaten und eine Sperrung bei Kenntnis des Passworts durch einen unbefugten Dritten vom Account-Inhaber zu erwarten ist. Zwar kann eine Sperrung der Zugangsdaten den ersten Missbrauch nicht verhindern. Eine Möglichkeit zur Sperrung sowie eine berechtigte Erwartung, dass die Account-Inhaber sie auch wahrnehmen, stärken jedoch das Vertrauen in die Sicherheit des verwendeten Authentisierungsverfahrens. Solange diese Sicherung durch den Account-Inhaber grundsätzlich zu erwarten ist, spricht dieser Teilaspekt der Authentisierungsmethode für die Anerkennung eines Rechtsscheintatbestandes.

ddd) Sicherung durch den Authentisierungsnehmer

567 Der Authentisierungsnehmer muss wie der Account-Inhaber einen Beitrag zur Sicherheit des Authentisierungsverfahrens leisten. Zentrale Anforde-

504 Zu diesen unten Rn. 569.

505 *eBay*, AGB, § 2 Nr. 7, abgedruckt oben Rn. 405.

506 Dazu *Casper*, in: MüKo-BGB[6], § 675l Rn. 12; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 147.

rungen ist dabei, dass er als Gestalter des Authentifizierungsvorgangs eine sicheres Verfahren wählt. Beispielsweise kann ein sicheres Passwort, durch das Erzwingen von einer Mindestlänge sowie der Anforderungen, dass auch Großbuchstaben und Zahlen Teil des Passworts sein müssen, seitens des Authentisierungsnehmers durchgesetzt werden.[507] Ebenso hat er für die Sicherheit der Kommunikation zu sorgen.[508]

568 Gegen das systematische Ausprobieren des Passworts im Rahmen einer Brute-Force-Attacke[509] kann der Authentisierungsnehmer dadurch Vorkehrungen treffen, dass er nach einer gewissen Anzahl missglückter Login-Versuche den Account temporär oder dauerhaft sperrt.[510] Darüber hinaus gehört zu einem sicheren Authentisierungsvorgang, dass die IT-Infrastruktur des Authentisierungsnehmers ausreichend gegen Angriffe von außen geschützt ist. Selbst wenn ein Angreifer Zugriff auf die Server des Authentisierungsnehmers hat und eine Datenbank mit den Passwörter ausspähen kann,[511] gibt es Wege, die gestohlenen und bei einem sicheren System verschlüsselten Passwörter zu sichern. One-Way-Hash-Funktionen, mit der Passwörter regelmäßig verschlüsselt in Datenbanken gespeichert werden, können mittels Brute-Force-Angriffen nur mit hohem Zeitaufwand ausprobiert werden. Daher bedienen sich Angreifer sog. Rainbow-Tables, die bereits alle möglichen Kombinationen enthalten und einen Schluss vom Hash auf den Klartext zulassen. Um dies zu vermeiden, verbindet der Authentisierungsnehmer vor der Verschlüsselung der Passwörter mittels One-Way-Hash-Funktion[512] das Passwort mit einer vor- oder nachgestellten Zeichenkette (Salting), sodass Rainbow-Tables keine Zuordnung erlauben.[513]

569 Ferner stellt der Authentisierungsnehmer bei einem sicheren Authentisierungsverfahren eine Sperrmöglichkeit zur Verfügung. Diese Sperrmöglichkeit erlaubt es dem Account-Inhaber, wenn die Zugangsdaten in der Hand eines Dritten sind, einen Missbrauch des Accounts zu verhindern. Fraglich ist, wie der Authentisierungsnehmer eine Sperrmöglichkeit bei einer rein wissensbasierten Authentisierungsmethode gestalten kann. Die Zugangsdaten zum Account sind der einzige Weg sich zu legitimieren, wenn die virtu-

---

507 *Eckert*[8], S. 471.
508 Dazu unten Rn. 574.
509 Dazu oben Rn. 181.
510 *Eckert*[8], S. 471; *Ernst*, MDR 2003, 1091, 1094; *Rieder*, S. 310.
511 Zu Angriffen auf die Infrastruktur des Authentisierungsnehmers oben Rn. 215.
512 Dazu *Schneier*, S. 94.
513 *B. Lorenz*, DuD 2013, 220, 225 f. Siehe auch oben Rn. 220.

elle Identität des Accounts nur durch eine rein wissensbasierte Authentisierung gesichert ist und keine Personendaten, noch nicht einmal eine E-Mail-Adresse, hinterlegt sind. Stellt der Account-Inhaber einen Missbrauch fest, kann er das Passwort ändern. Hat der Angreifer jedoch das Passwort zuvor geändert, hat der Account-Inhaber keine Chance mehr, sich zu legitimieren. Eine Sperrung des Accounts ist ihm in diesem Fall unmöglich. Werden wie im PIN/TAN-Verfahren mehrere Wissens-Komponenten verwendet, kann bereits die Sperrung der TAN-Liste bereits den Missbrauch verhindern.

570 Wurde bei der Registrierung eine E-Mail-Adresse verlangt und wurde diese überprüft, steht dem Account-Inhaber häufig die Möglichkeit zu, sich bei Vergessen oder nach einem Missbrauch mit Änderung des Passworts, neue Zugangsdaten per E-Mail zuschicken zu lassen. Diese Funktion bietet dem Account-Inhaber die Möglichkeit, weiteren Missbrauch durch den Account zu verhindern, wenn ein Missbrauch erstmalig erkannt wurde. Diesem Vorteil steht jedoch auch ein gravierender Nachteil gegenüber. Erlangt der Angreifer Zugriff auf den E-Mail-Account einer Person, kann er durch die „Passwort vergessen"-Funktion mit der E-Mail-Adresse verknüpfte Accounts übernehmen.[514]

571 Die Schwächen einer „Passwort vergessen"-Funktion, die nur mittels einer E-Mail-Adresse arbeitet, kann durch das Verwenden weiterer Personendaten abgesichert werden. Muss der Account-Inhaber beispielsweise eine Telefonnummer oder eine Adresse bei der Registrierung angeben, können diese Daten zur Überprüfung der Berechtigung zum Zurücksetzen verwendet werden. Der Authentisierungsnehmer kann beispielsweise bei der Telefonnummer anrufen oder neue Zugangsdaten per Post an die bekannte Adresse schicken. Das Übernehmen eines E-Mail-Accounts, welches ohne räumliche Nähe zum Account-Inhaber möglich ist, würde dann nicht mehr ausreichen. Zwar kann jemand auch fremde Briefkästen leeren oder fremde Telefone abnehmen, die dazu erforderliche räumliche Nähe macht solche Eingriffe jedoch entscheidend schwerer.

572 Authentisierungsverfahren, die neben den stetigen Zugangsdaten transaktionsbezogene Einmal-Geheimnisse verwenden, bieten bessere Möglichkeiten der Sperrung. Eine TAN- oder iTAN-Liste kann regelmäßig durch Anruf bei der ausgebenden Bank oder auf deren Internet-Seiten gesperrt werden.

573 Um abschließend bewerten zu können, ob die Sicherungsmaßnahmen eines Authentisierungsnehmers reichen, müsste er seine Sicherheitsstandards

514 So geschah es im geschilderten Fall oben Rn. 223.

offen legen.[515] Da Authentisierungsnehmer dies regelmäßig nicht tun, können zwei Schlussfolgerungen gezogen werden. Einerseits könnte das Vorliegen eines Rechtsscheintatbestandes mangels Beurteilbarkeit abgelehnt werden. Andererseits könnte das Vertrauen des Verkehrs, das durch das Eigeninteresse des Authentisierungsnehmers an der Sicherung gestärkt wird, für ausreichend erachtet werden. Eklatante Sicherheitslücken werden manchmal bekannt.[516] Dies geschieht jedoch regelmäßig erst, nachdem es zu einem Missbrauch gekommen ist. Dadurch entsteht die Gefahr, dass zum Zeitpunkt der Beurteilung des Falls von einer Sicherung durch den Authentisierungsnehmer ausgegangen wird und sich anschließend herausstellt, dass diese Beurteilung unzutreffend war. Dies spricht dafür, eine ausreichende Sicherung durch den Authentisierungsnehmer nur anzunehmen, wenn dieser seine Sicherungsmethoden offen legt oder diese anhand gesetzlicher Vorgaben konkretisiert sind.

eee) Sicherheit der Kommunikation

574 Zur Gewährleistung der Sicherheit der Kommunikation bei einer rein wissensbasierten Authentisierung sind die versendeten Daten zu verschlüsseln. Standardmäßig werden Daten über das Internet unverschlüsselt durch viele Rechner geleitet.[517] Das führt dazu, dass ein Angreifer die im Klartext übertragenen Passwörter auslesen kann (Sniffing).[518] Werden die Daten unverschlüsselt übertragen, ist die Möglichkeit das Passwort auszuspähen so groß, dass keine ausreichend sichere Authentisierungsmethode vorliegt. Erst durch Verschlüsselung der Daten, etwa durch SSL, wird die Kommunikation des Passworts so sicher, dass der Vorgang insgesamt als sicherer Authentisierungsvorgang gewertet werden kann.

575 Bei der Verwendung von Einmal-Passwörtern wie im PIN/TAN-Verfahren spielt die Sicherheit der Kommunikation eine untergeordnete Rolle. Selbst wenn ein Angreifer den Datenverkehr mitlesen würde und somit das Wissen um die verwendete TAN hätte, könnte er diese nicht zum Miss-

515 *Redeker*, IT-Recht[5], Rn. 875.
516 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211.
517 *Rieder*, S. 310.
518 Dazu oben Rn. 177. Speziell bezüglich Passwörter *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257.

brauch verwenden. Die TAN ist nach der Transaktion verbraucht, sodass ein Angreifer sie nicht für einen zukünftigen Missbrauch verwenden könnte.

fff) Schlussfolgerung für den Rechtsscheintatbestand

576 Aus einer Gesamtbetrachtung der einzelnen Aspekte der Sicherheit des Authentisierungsvorgangs ist wertungsmäßig zu entscheiden, ob der natürliche äußere Tatbestand so stark ist, dass der Erklärungsempfänger schützenswert darauf vertrauen darf, dass der Account-Inhaber gehandelt hat. Teilweise wird die Wertung getroffen, dass die Sicherungsmaßnahmen bei passwortgeschützten Accounts, bei denen eine Pflicht zur Geheimhaltung besteht, ausreichende Grundlage für einen Rechtsscheintatbestand sein können.[519] Trotz der Missbrauchsmöglichkeiten könne der Erklärungsempfänger in hinreichendem Maße auf die Verlässlichkeit vertrauen.[520] Andere Stimmen stellen nur Kriterien zur Beurteilung eines Rechtsscheintatbestandes auf, wollen jedoch die Beurteilung, ob dieser vorliegt, in die Hände der freien Beweiswürdigung der Richter geben.[521] Häufig wird jedoch angenommen, dass kein ausreichendes Sicherheitsniveau bestehe.[522] Die mantraartige Aussage, dass das Sicherheitsniveau im Internet dafür zu gering sei,[523] ist dafür zu pauschal, auch wenn sie im Ergebnis in vielen Fällen zutreffen mag.

577 Bei einem rein wissensbasierten Authentisierungsverfahren kann ein hohes Sicherheitsniveau nur schwer erreicht werden, weil sich die Sicherheit des Passworts mit dessen Schutz in einer gegenläufigen Weise verhalten. Einfache Passwörter lassen sich leicht merken, sodass der Account-Inhaber sie nicht aufschreiben muss und sie daher gut geheim gehalten werden können. Sichere Passwörter hingegen sind so komplex, dass sie aufgeschrieben werden, was die Geheimhaltung jedoch erschwert. Wegen der zahlreichen Möglichkeiten das Passwort auszuspähen besteht insgesamt keine hohe Sicherheit. Darüber hinaus hat die Betrachtung von Rechtsscheintatbeständen gezeigt, dass die Überprüfung von Wissen im Gegensatz zum starken

519 *Kuhn*, S. 219; *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 34; *Sonnentag*, WM 2012, 1614, 1616.
520 *Kuhn*, S. 219.
521 *Rieder*, S. 311 f.
522 *Biallaß*, ZUM 2007, 397, 398; *M. Wolf/Neuner*[10], § 50 Rn. 108.
523 Dazu oben Rn. 372.

Rechtsscheinträger des Besitzes einer physisch einmaligen Sache keine ausreichende Grundlage für einen Rechtsscheintatbestand ist.[524] Eine Gesamtbetrachtung bei einer rein wissensbasierten Authentisierung spricht gegen ein ausreichend sicheres Authentisierungsverfahren. Die erste Komponente eines Rechtsscheintatbestandes besteht somit bei einer rein wissensbasierten Authentisierungsmethode nicht.

cc) Zwei-Faktor-Authentisierung

Bei einer Zwei-Faktor-Authentisierung wird anstelle eines einzigen Authentisierungsmittels ein weiteres Authentisierungsmittel einer anderen Kategorie verwendet.[525] Eine Kombination zweier wissensbasierten Authentisierungskomponenten, wie sie das TAN- und iTAN-Verfahren verwenden, sind rein wissensbasierte Authentisierungsmethoden.[526] Als Zwei-Faktor-Authentisierung wird hier die am häufigsten vorkommende Methode der Kombination von Wissen und Besitz untersucht. Kombinationen aus Besitz und Sein oder Wissen und Sein sind ebenso möglich, kommen jedoch praktisch seltener vor. **578**

Bei dieser Methode kann es zwar vorkommen, dass die Authentisierung auf die Besitz-Komponente reduziert wird. Schreibt der Account-Inhaber die PIN beispielsweise auf die Chip-Karte, konterkariert er die Authentisierung anhand zweier unabhängiger Komponenten. Ebenso kann die Sicherheit des mTAN dadurch beeinträchtigt werden, dass die Transaktion auf demselben Mobiltelefon ausgeführt wird, an das die TAN geschickt wird. Die Möglichkeit, die Vorteile der Authentisierung anhand zweier getrennter Faktoren durch Nachlässigkeit des Account-Inhabers auszuhebeln, beeinträchtigt jedoch nicht die grundsätzliche Sicherheit dieser Methode. **579**

aaa) Sicherheit der Zwei-Faktor-Authentisierung

Um die Sicherheit eines Zwei-Faktor-Authentisierungsverfahrens zu beurteilen, müssen zunächst die Sicherheit der einzelnen Komponenten beurteilt werden und sodann die sich aus deren Kombination ergebende Sicherheit. **580**

524 Oben Rn. 520.
525 Oben Rn. 117.
526 Oben Rn. 545.

Die wissensbasierte Authentisierung bietet keinen besonders hohen Schutz, weil Passwörter entweder schwach und geheim oder stark und aufgeschrieben sind und das Ausspähen möglich ist.[527]

581 Eine besitzbasierte Authentisierung hat im Gegensatz dazu den Vorteil, dass der Besitz im Gegensatz zum Wissen nicht geteilt werden kann.[528] Entscheidend für die Sicherheit ist, dass die Besitz-Komponente nicht kopiert werden kann. Denn bei kopierbaren Besitz-Komponenten wäre der Besitz teilbar. Digital kann der Besitz an einer Sache zwar nicht direkt überprüft werden, ein Token kann diesen jedoch simulieren.[529]

582 Die Stärke eines auf asymmetrischer Verschlüsselung[530] basierenden Verfahrens hängt – ähnlich wie die Stärke eines Passworts – davon ab, dass ein Angreifer den Token nicht errechnen kann. Da privater und öffentlicher Schlüssel anhand von zwei Primzahlen gebildet werden, müssen diese so groß gewählt werden, dass ein Zurückrechnen nicht möglich ist.[531]

583 Der Besitz an dem Authentisierungsmittel kann gestohlen werden. Bei einer rein besitzbasierten Authentisierungsmethode stellt dies ein großes Sicherheitsrisiko dar. Häufig werden Portemonnaies, die Chip-Karten enthalten können, gestohlen. Im Gegensatz zum Ausspähen von Passwörtern bedarf der Diebstahl einer Besitz-Komponente eine räumliche Nähe zwischen Angreifer und Account-Inhaber. Eine rein besitzbasierte Authentisierung bietet jedoch ebenso wie eine rein wissensbasierte Authentisierung keinen besonders hohen Schutz. Die Kombination aus beiden Authentisierungsmitteln bietet jedoch einen hohen Schutz.

bbb) Missbrauchsmöglichkeiten bei der Zwei-Faktor-Authentisierung

584 Die Verlässlichkeit einer Zwei-Faktor-Authentisierung kann jedoch durch etwaige Missbrauchsmöglichkeiten beeinträchtigt werden. Für einen Missbrauch müsste sowohl das Passwort ausgespäht werden, als auch die dazugehörige Besitz-Komponente gestohlen werden.[532] Gelingt es einem Angrei-

527 Oben Rn. 544 ff.
528 Zu sämtlichen Vor- und Nachteilen der besitzbasierten Authentisierung oben Rn. 110.
529 Oben Rn. 119.
530 Dazu oben Rn. 78.
531 Oben Rn. 80.
532 Vgl. *Reese*, S. 53.

fer die geheime PIN einer Chip-Karte auszuspähen, beispielsweise mittels Phishing,[533] kann er mit diesem Wissen keine Handlungen über den Account vornehmen, da ihm die Besitzkomponente fehlt. Andererseits kann auch ein Dieb, der die Chip-Karte des Account-Inhabers stiehlt, keine Handlungen über dessen Account vornehmen. Denn ohne das Wissen der PIN kann dieser sich nicht erfolgreich authentisieren. Ein Angreifer muss daher sowohl das Wissen um die PIN ausspähen als auch an den Besitz der Chip-Karte gelangen. Sowohl den Besitz durch Diebstahl zu erlangen als auch das Wissen auszuspähen bereitet einen so hohen Aufwand, dass die Zwei-Faktor-Authentisierung eine hohe Sicherheit bietet. Zum einen ist das Wissen um die PIN nicht besser gegen Ausspähen geschützt als das Wissen um ein Passwort. Bei dem Einsatz von Kartenlesern der Klasse 1,[534] bei denen die PIN nicht über ein PIN-Pad, sondern über die Tastatur des Rechners eingegeben wird, kann ein Trojaner, der die Systemeingaben mittels eines Keyloggers überwacht,[535] die Eingabe der PIN mitlesen und sie somit in Erfahrung bringen. Ein Missbrauch des Accounts ist anschließend jedoch nur möglich, wenn gleichzeitig auch die Chip-Karte gestohlen wird.

585 Ein Missbrauch eines Accounts, der auf eine Zwei-Faktor-Authentisierung setzt ist jedoch ohne den Besitz der Chip-Karte möglich. Ein aktiver, in Echtzeit erfolgender Man-in-the-Middle-Angriff[536] kann die Kommunikation zwischen dem Account-Inhaber und dem Authentisierungsnehmer abfangen und verändern. Dabei kann ein Angreifer dem Account-Inhaber erwartungsgemäße Antworten des Authentisierungsnehmer vortäuschen, währenddessen er die Erklärungen des Account-Inhabers zu seinen Gunsten manipuliert und dem Authentisierungsnehmer verändert übermittelt.

ccc) Sicherung durch den Account-Inhaber

586 Bei einer Zwei-Faktor-Authentisierung kann der Account-Inhaber zunächst wie bei der rein wissensbasierten Authentisierung die Geheimhaltung der Wissenskomponente sicherstellen.[537] Die Besitz-Komponente muss er sicher verwahren, sodass ein Diebstahl nur mit Aufwand möglich ist. Beson-

533 Zum Phishing oben Rn. 138 ff.
534 Zur Klassifizierung unten Rn. 893.
535 Zu dieser Form des Ausspähens oben Rn. 166.
536 Dazu oben Rn. 168.
537 Zu deren Geheimhaltung oben Rn. 558.

ders wichtig für die Sicherheit einer Zwei-Faktor-Authentisierung ist, dass er die Besitzkomponente nicht gemeinsam mit der Notiz der PIN aufbewahrt.[538]

587 Der Authentisierungsnehmer kann zur Sicherheit des Authentisierungsvorgangs zusätzlich beitragen, indem er einen sicheren Kartenleser der Klasse 2 oder höher verwendet.[539] Dadurch stellt er sicher, dass die PIN nicht von einem Keylogger ausgespäht werden kann. Darüber hinaus muss bei einer sicheren Authentisierungsmethode darauf vertraut werden können, dass der Account-Inhaber eine vorhandene Sperrmöglichkeit[540] nutzt. Dies kann wie bei der rein wissensbasierten Authentisierung durch eine gesetzliche oder vertragliche Pflicht sichergestellt werden.[541]

ddd) Sicherung durch den Authentisierungsnehmer

588 Wie bei allen denkbaren Authentisierungsmethoden muss der Authentisierungsnehmer seine IT-Infrastruktur gegen Eingriffe von außen absichern.[542] Ferner sollte er seinen Einfluss auf den Account-Inhaber ausnutzen, diesen zur Verwendung eines sicheren Kartenlesers zu bewegen.

589 Der Authentisierungsnehmer hat bei einem sicheren Authentisierungsverfahren Sperrmöglichkeiten zur Verfügung zu stellen. Der Missbrauch der Zugangsdaten nach Diebstahl des Besitz-Elementes ist möglich. Um einen Missbrauch trotz Diebstahls zu verhindern, muss der Authentisierungsnehmer dem Account-Inhaber eine Möglichkeit zur Verfügung stellen, die Verwendung des Besitz-Elementes durch eine Sperrung zu verhindern. Nach Anzeige des Account-Inhabers hat der Authentisierungsnehmer sicherzustellen, dass eine Authentisierung mit der abhandengekommenen Besitz-Komponente nicht mehr möglich ist. Dies kann er beispielsweise durch eine Sperrliste erreichen.[543]

590 Ferner kann der Authentisierungsnehmer dazu beitragen die Sicherheit des Verfahrens zu erhöhen, indem er dem Authentisierungsgeber soweit wie möglich Transaktionsdaten mitteilt. Beim mTAN-Verfahren beispielsweise

538 Siehe dazu die umfangreichen Erfahrungen bei ec-Karten oben Rn. 513.
539 Zur Klassifizierung der Karten-Lesegeräte unten Rn. 893.
540 Zu diesen oben Rn. 589.
541 Oben Rn. 569.
542 Zu Angriffspunkten beim Authentisierungsnehmer oben Rn. 215 ff.
543 Über ein Beispiel unten Rn. 885.

kann die Sicherheit dadurch erhöht werden, dass in der SMS an den Bankkunden die Überweisungssumme sowie die letzten Zahlen des Zielkontos neben der einmaligen TAN übermittelt werden. Darüber hinaus ist die einmalige TAN nur zur Bestätigung dieser einen Transaktion gültig. Eine Änderung der Daten sollte zur Generierung einer neuen TAN führen.

eee) Sicherheit der Kommunikation

Eine unverschlüsselte Kommunikation bietet die Gefahr, dass die Daten zum einen ausgelesen und zum anderen manipuliert werden. Diese Gefahren sind bei einer Zwei-Faktor-Authentisierung nicht in gleichem Maße gegeben. Wenn eine einmalige TAN ausgespäht wird, kann mittels dieses Wissens keine Transaktion ausgeführt werden. Auch das Verändern von asymmetrisch verschlüsselten Informationen kann der Authentisierungsnehmer bemerken, sodass die Sicherheit der Kommunikation weniger entscheidend wird. Wenn die Zwei-Faktor-Authentisierung jedoch nur zu Anfang einer Session zur Authentifizierung des Nutzers verwendet wird, ist die Kommunikation nur sicher, wenn diese per SSL verschlüsselt ist.[544] **591**

fff) Schlussfolgerung für den Rechtsscheintatbestand

Die Zwei-Faktor-Authentisierung bietet ein hohes Maß an Sicherheit.[545] Authentisierungsverfahren, die auf eine Zwei-Faktor-Authentisierung setzen, bieten daher eine ausreichende Sicherheit, um möglicherweise einen Rechtsscheintatbestand anzuerkennen.[546] Dabei ist jedoch genau darauf zu achten, in welche Tatsachenlage ein Vertrauen begründet wird. Bei der elektronisch signierten Willenserklärung begründet beispielsweise nicht die Willenserklärung das Vertrauen des Erklärungsempfängers, sondern die Überprüfung seiner Signatur.[547] Bei einer Zwei-Faktor-Authentisierung, die über die Übermittlung einmaliger TANs arbeitet, bezieht sich das Vertrauen des Authentisierungsnehmers darauf, dass der Handelnde nur an die einmali- **592**

544 Dazu schon bei der rein wissensbasierten Authentisierung oben Rn. 574.

545 *Knopp/Wilke/Hornung/Laue*, MMR 2008, 723, 725.

546 *Borges*, Elektronischer Identitätsnachweis, S. 136; *ders.*, NJW 2010, 3334, 3338; *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 34; *Rieder*, S. 265 ff.

547 *Reese*, S. 52.

ge TAN gelangen kann, weil er im Besitz des Authentisierungsmittels ist. Die Anerkennung des Authentisierungsverfahrens mit zwei unabhängigen Faktoren entspricht dem Ergebnis des Blicks auf Rechtsscheintatbestände in vergleichbaren Konstellationen.[548] Der Besitz einer physisch einmaligen Sache, wie einer Chip-Karte oder einer SIM-Karte, sind ein starker Rechtsscheinträger.

dd) Zwischenergebnis

593 Die rein wissensbasierte und die Zwei-Faktor-Authentisierung bieten unterschiedliche Sicherheitsniveaus. Während die Zwei-Faktor-Authentisierung eine ausreichende Sicherheit gewährt, bietet das eine rein wissensbasierte Authentisierung nicht. Bei der Betrachtung, wer durch ein sicheres Authentisierungsverfahren identifiziert wird, zeigt sich, dass ein sicheres Authentisierungsverfahren allein noch keinen Rechtsschein eines Handelns des Account-Inhabers begründen kann.

594 Ein sicheres Authentisierungsverfahren stellt lediglich sicher, dass eine virtuelle Identität in Form des Accounts wiedererkannt werden kann. Hinter einer virtuellen Identität kann jedoch vieles stehen. Neben einer natürlichen Person, können dahinter auch mehrere Personen stehen, die sich den Account teilen. Ein Rechtsschein, der auf das Handeln einer Person in Form einer numerischen Identität hinweist, kann ein noch so sicheres Authentisierungsverfahren daher nicht bieten. Vielmehr ist erforderlich, dass die virtuelle Identität einer numerischen Identität zugeordnet ist, der Account also eine Identifikationsfunktion bezüglich einer realen Person hat.

c) Identifikationsfunktion von Accounts im Internet

595 Eine sichere Authentisierungsmethode als erste Komponente des Rechtsscheintatbestandes kann Gewähr dafür bieten, dass der Ersteller des Accounts gehandelt hat. Der Account ist jedoch nur eine virtuelle Identität. Für den Abschluss eines Rechtsgeschäftes möchte der Geschäftsgegner seinen Vertragspartner jedoch als Person in Form einer numerischen Identität identifizieren.[549] Ein Rechtsscheintatbestand kann daher nur bei Accounts be-

548 Siehe oben Rn. 528.
549 *Konrath*, S. 28.

stehen, die nicht nur eine virtuelle Identität identifizieren, sondern die auch eine Person in Form einer numerischen Identität identifizieren sollen.[550] Eine Identifikationsfunktion des Accounts wird dadurch erreicht, dass beim Erstellen des Accounts dem Account-Inhaber ermöglicht wird, durch die Angabe von Identitätsdaten, diesen Account der numerischen Identität zuzuordnen.[551] Für die Anerkennung eines Rechtsscheintatbestandes bei Zugangsdaten im Internet bedarf es daher als zweite Komponente einer zuverlässigen Identifikationsfunktion des Accounts. Eine Identifikationsfunktion, die Zuordnung der virtuellen Identität des Accounts zu einer numerischen Identität, muss beim Erstellen des Accounts oder später zuverlässig überprüft werden, damit ein Rechtsschein bezüglich des Handelns einer realen Person entstehen kann.

596 Teilweise wird erwogen, dass für Rechtsgeschäfte, die online abgeschlossen werden, ebenso wie für Bargeschäfte des alltäglichen Lebens die Grundsätze des „Geschäfts für den, den es angeht" angewendet werden können.[552] Das Interesse des Verkäufers beschränke sich dabei darauf, an sein Geld zu gelangen, wohingegen die Identität des Geschäftspartners unbedeutend sei.[553] Zur Durchsetzung von Ansprüchen[554] oder soweit die Identität des Geschäftspartners anderweitig bedeutsam ist,[555] wie etwa bei Dauerschuldverhältnissen, müsse jedoch ein identifizierbarer Vertragspartner vorliegen. Wenn der Geschäftsgegner kein Interesse an der Identität seines Geschäftspartners hätte und es ihm nur auf die Entlohnung für seine Dienste ankäme, würde sich die Frage der Rechtsscheinhaftung nicht stellen. Solange der Geschäftsgegner sicher sein Geld erhält und darum nicht nachträglich gestritten wird, benötigt er aus eigenem Interesse nicht die Identität seines Geschäftspartners. Sollte es jedoch zum Streit kommen, muss der Geschäftsgegner seinen Vertragspartner so identifiziert haben, dass er ihn rechtlich belangen kann. Dafür benötigt er den Namen des Vertragspartners sowie eine ladungsfähige Adresse.[556] Ferner ist der Geschäftsgegner gesetzlich

550 So *Redeker*, IT-Recht[5], Rn. 874. *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 34 macht dies nicht an der Identifikationsfunktion, sondern an der zu erwartenden Sicherung fest, seine Erwägungen laufen jedoch auf eine sichere Identifizierung hinaus.

551 Zur Identifikationsfunktion oben Rn. 35 ff.

552 *M. Köhler/Arndt/Fetzer*[7], Rn. 172; *Fiege*, CR 1998, 41, 46.

553 *M. Köhler/Arndt/Fetzer*[7], Rn. 172.

554 *Fiege*, CR 1998, 41, 46.

555 *M. Köhler/Arndt/Fetzer*[7], Rn. 173.

556 Dazu oben Rn. 27.

dazu verpflichtet bei Rechnungen, die Beträge von € 150 übersteigen (§ 33 S. 1 Nr. 1 UStDV), den Namen des Leistungsempfängers auf der Rechnung aufzuführen (§ 14 Abs. 4 S. 1 Nr. 1 UStG). Zur rechtmäßigen Durchführung von Rechtsgeschäften und um im Streitfall eine gerichtliche Durchsetzung erreichen zu können, muss der Geschäftsgegner daher seinen Vertragspartner identifizieren.

aa) Ohne Angabe von Personendaten

597 Zunächst ist zu untersuchen, ob ohne die Angabe von Personendaten die Zuordnung der virtuellen Identität zu einer numerischen Identität möglich ist und dadurch Grundlage eines Rechtsscheintatbestandes sein kann. Beim Erstellen des Accounts zu manchen Informationsportalen ist lediglich die Angabe eines Benutzernamens und eines Passworts, nicht aber die Eingabe von Personendaten oder einer E-Mail-Adresse erforderlich.[557] Eine Zuordnung der virtuellen Identität zu einer numerischen Identität ist dann nur durch die Auswertung von Kommunikationsdaten wie der IP-Adresse des Account-Inhabers möglich. Die IP-Adresse hat jedoch keine Identifikationsfunktion bezüglich einer numerischen Identität,[558] sodass diese Accounts nicht Grundlage einer Rechtsscheinhaftung sein können.

598 Zur Registrierung eines Accounts in Meinungsforen[559] ist regelmäßig lediglich die Angabe einer E-Mail-Adresse, die verifiziert wird, sowie die Wahl eines Pseudonyms erforderlich.[560] Die Angabe von Personendaten ist, wenn überhaupt, freiwillig.[561] Eine Zuordnung zu einer numerischen Identität kann dabei nur über die E-Mail-Adresse erfolgen. Das wird teilweise als ausreichend für die Identifikationsfunktion bezüglich der numerischen Identität angesehen.[562] Eine E-Mail-Adresse hat jedoch keine Identifikationsfunktion bezüglich einer Person in Form einer numerischen Identität,[563] von der eine Identifikationsfunktion bezüglich des Accounts abgeleitet wer-

557 So beispielsweise bei Wikipedia, dazu oben Rn. 60.
558 Oben Rn. 38.
559 Dazu oben Rn. 60.
560 *Hartmann*, S. 21; *Schapiro*, S. 18.
561 *Schapiro*, S. 18.
562 *Stöber*, JR 2012, 225, 228.
563 Oben Rn. 48. So auch *Gurmann*, S. 19. Dies erkennt *Stöber* für die E-Mail-Adresse, möchte von ihr jedoch eine Identifikationsfunktion für andere Accounts ableiten, *Stöber*, JR 2012, 225, 229.

den kann. Accounts in Meinungsforen können daher nicht Grundlage einer Rechtsscheinhaftung sein. Aus demselben Grund kommt bei E-Mails auch keine Rechtsscheinhaftung in Betracht. Wegen des frei wählbaren Absenders[564] bietet dieser keinerlei Gewähr für die Richtigkeit der Angabe.

bb) Ohne Überprüfung der Personendaten

Bei Accounts, die zum Abschluss von Rechtsgeschäften dienen, werden regelmäßig Personendaten, wie Name und ladungsfähige Anschrift abgefragt. Der Account erhält dadurch eine Identifikationsfunktion, weil als Account-Inhaber ein Namensträgers in Form einer numerischen Identität ausgewiesen wird. Wenn die angegebenen Personendaten nicht überprüft werden, kann sich der äußere Tatbestand, der Grundlage der Rechtsscheinhaftung ist, bei einer sicheren Authentisierungsmethode nur darauf beziehen, dass derjenige, der den Account erstellt hat, ihn später verwendet. Es stellt sich daher die Frage, ob eine solche Identifikationsfunktion ausreichende Grundlage für einen Rechtsscheintatbestand ist oder ob die Personendaten auch überprüft werden müssen, also nur eine zuverlässige Identifikationsfunktion Grundlage der Rechtsscheinhaftung sein kann. 599

Einige Stimmen in Rechtsprechung und Literatur meinen, es bedürfe einer Überprüfung der angegeben Personendaten, damit das Vertrauen des Erklärungsempfängers in die Zuordnung der virtuellen Identität des Accounts zur realen Person des Namensträgers möglich ist.[565] Dagegen kann eingewendet werden, dass es einer Überprüfung nicht bedürfe. Die Angabe einer Lieferadresse bei Warenbestellungen online könne bereits ausreichend eine Person identifizieren. Dem ist jedoch entgegen zu halten, dass Betrüger eine fehlende Identitätsüberprüfung ausnutzen, um Warensendungen unberechtigt unter fremdem Namen zu bestellen und die Sendungen im Anschluss abzufangen.[566] 600

Ferner könnte ein Vergleich zu § 172 Abs. 1 BGB gegen die Notwendigkeit der Überprüfung der Identität bei der Erstellung des Accounts sprechen. Nach § 172 Abs. 1 BGB ist eine unterschriebene Vollmachtsurkunde ein 601

564 Zum Mail-Spoofing oben Rn. 212.

565 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257; *Wiebe*, MMR 2002, 128, 129; *ders.*, MMR 2002, 257, 258; *Wiebe/Neubauer*, in: *Hoeren/Sieber/Holznagel*, Kap. 15 Rn. 57.

566 *Engel*, DuD 2006, 207, 208.

tauglicher Rechtsscheinträger.[567] Eine gefälschte Unterschrift kann jedoch ohne weiteres von einem Dritten auf eine Urkunde geschrieben werden.[568] Eine Überprüfung der Identität des Ausstellers der Urkunde findet beim Erstellen der Urkunde nicht statt. Eine Vollmachtsurkunde ist jedoch nur ein tauglicher Rechtsscheinträger nach § 172 Abs. 1 BGB, wenn sie echt ist, also vom benannten Aussteller ausgestellt wurde.[569]

602 Diese Wertung ist auf Accounts zu übertragen, die bei der Erstellung nicht überprüft werden. Durch die Angabe der Personendaten könnten diese Accounts grundsätzlich als Rechtsscheinträger bezüglich der Zuordnung zu dem ausgewiesenen Account-Inhaber in Betracht kommen. Ein Rechtsscheintatbestand bestünde jedoch nur, wenn der Account echt ist, also vom ausgewiesenen Account-Inhaber auch tatsächlich erstellt wurde.

603 Eine Übertragung dieser Wertung ist jedoch nur möglich, wenn Accounts und unterschriebene Vollmachtsurkunden ausreichend vergleichbar sind. Ein bedeutender Unterschied besteht jedoch in der Möglichkeit die Echtheit zu überprüfen. Die Unterschrift einer Person ist einmalig, sie ist daher aus Authentisierungssicht ein Sein-Merkmal dieser Person.[570] Eine Unterschrift muss daher nicht wie ein Account künstlich einer numerischen Identität zugeordnet werden. Die Unterschrift ist per se untrennbar mit dem Namensträger verbunden. Anhand der Unterschrift kann daher im Nachhinein überprüft werden, ob der Namensträger die Vollmachtsurkunde unterschrieben hat oder ob ein Dritter seine Unterschrift gefälscht hat.[571]

604 Bei einem Account kann hingegen im Nachhinein nicht überprüft werden, wer diesen erstellt hat. Selbst wenn der Authentisierungsnehmer noch die IP-Adresse als Verkehrsdatum gespeichert hat, ermöglicht diese aus zwei Gründen keine Überprüfung, ob der ausgewiesene Account-Inhaber den Account erstellt hat. Zum einen kann es sein, dass der ISP im Zeitpunkt, wenn die Überprüfung relevant wird, die Zuordnung der dynamischen IP-Adresse zum Inhaber des Internet-Anschlusses nicht mehr gespeichert hat.[572] Zum anderen – selbst wenn der Anschlussinhaber anhand der IP-Adresse zu ermitteln ist – bedeutet dies nicht, dass der Anschlussinhaber den Account

567 Oben Rn. 309.
568 *Mankowski*, NJW 2002, 2822, 2824.
569 Oben Rn. 312.
570 Oben Rn. 116.
571 Siehe oben Rn. 116.
572 Nach der Vorratsdatenspeicherungsrichtlinie 2006/24/EG müssen die Daten sechs Monate lang gespeichert werden.

erstellt hat, weil ein Internet-Anschluss keine Identifikationsfunktion bezüglich des Account-Inhabers besitzt.[573]

Dagegen ist zu berücksichtigten, dass beim gutgläubigen Erwerb vom Nichtberechtigten nach §§ 929 S. 1, 932 Abs. 1 S. 1 BGB eine Überprüfung, ob die Sache dem Eigentümer abhandengekommen ist, schwer bis gar nicht möglich ist. Insofern ist zu erwägen, dass für den Rechtsscheintatbestand eine Überprüfung der Identität nicht erforderlich ist. Dem ist jedoch entgegen zu halten, dass die Interessenlage beim gutgläubigen Erwerb eine andere ist. Dort bezieht sich der Rechtsschein nicht wie bei Zugangsdaten im Internet auf das Handeln eines gewissen Account-Inhabers, sondern auf die Eigenschaft des Besitzers, Eigentümer zu sein. Dafür ist der Besitz nach der Wertung des § 1006 Abs. 1 S. 1 BGB ausreichender Rechtsscheinträger. Bei den Zugangsdaten im Internet wird jedoch nicht nur auf eine Eigenschaft der Berechtigung vertraut, sondern auch darauf, dass die Identitätsbehauptung zutrifft. Auf eine Überprüfung der Identität kann somit nicht verzichtet werden. 605

Der bedeutende Unterschied zwischen einer Unterschrift und einem Account bei der nachträglichen Echtheitsüberprüfung verbietet eine Übertragung der Wertung des § 172 Abs. 1 BGB bei Accounts, bei denen die behauptete Identität beim Erstellen nicht überprüft wird. Wenn sich der Rechtsschein des § 172 Abs. 1 BGB auch dadurch begründet, dass der Vertrauende die Echtheit des Rechtsscheinträgers überprüfen kann, stellt sich die nachfolgend betrachtete Frage, ob ein Account, bei dessen Erstellen die Echtheit überprüft wurde, tauglicher Anknüpfungspunkt für einen Rechtsscheintatbestand sein kann. 606

cc) Plausibilitätskontrolle der Personendaten

Zunächst ist eine einfache Überprüfung der Personendaten in Form einer Plausibilitätskontrolle möglich. Eine Plausibilitätskontrolle kann zunächst darin bestehen, dass die eingegebenen Daten auf ihre Gültigkeit hin überprüft werden. Dazu gehört beispielsweise, dass eine deutsche Postleitzahl fünf Stellen hat. Ferner kann überprüft werden, ob eine gewisse Straße in der behaupteten Stadt existiert und ob in dieser Straße die angegebene Hausnummer vorhanden ist. Die Plausibilitätskontrolle der Personendaten 607

573 Oben Rn. 47.

erschwert einem Dritten zwar minimal die Erstellung eines Accounts auf fremden Namen. Plausible Daten kann er jedoch aus öffentlichen Quellen, wie beispielsweise einem Telefonbuch, in Erfahrung bringen. Eine Plausibilitätskontrolle bietet daher keinen entscheidenden Sicherheitsgewinn gegenüber dem kompletten Verzicht auf eine Überprüfung der Identitätsdaten.

608 Ferner ist der Abgleich der Daten mit der Schufa,[574] wie ihn beispielsweise eBay praktiziert,[575] zur Überprüfung der Identität des Account-Inhabers zu untersuchen. Bei dem Abgleich der Daten werden lediglich Name und Anschrift sowie das Geburtstag verglichen.[576] Name und Anschrift eines Dritten kann jeder bereits im Telefonbuch nachschlagen. Im Vergleich zu einer einfachen Plausibilitätskontrolle muss das Geburtsdatum zum Account-Inhaber passen. Dieses ist zwar nicht so leicht aus öffentlichen Quellen zu beschaffen wie Name und Anschrift. Das Geburtsdatum ist jedoch auch keine geheime Information. Ein Dritter kann es beispielsweise über ein soziales Netzwerk in Erfahrung bringen und mit einfachen Mitteln einen Account auf fremden Namen erstellen. So kann er sich mühelos einen mit der Schufa abgeglichenen Account unter falscher Namensangabe erstellen. Der Abgleich der Personendaten mit der Schufa ist daher nur eine erweiterte Form der Plausibilitätskontrolle. Er kann daher keine zuverlässige Identifikationsfunktion bezüglich des Account-Inhabers begründen.[577]

dd) Überprüfung der Personendaten

609 Damit der Erklärungsempfänger Vertrauen darin entwickeln kann, dass die von einem fremden Account stammende Willenserklärung vom als Account-Inhaber ausgewiesenen Namensträger stammt, muss daher dessen Identität bei der Erstellung des Accounts oder später überprüft werden.[578] Dabei stellt sich jedoch die Frage, wie sicher die Identifizierung sein muss, damit das Vertrauen des Erklärungsempfängers schützenswert ist. Um diese Frage

574 Zur Schufa-Auskunft *Bruchner/Krepold*, in: *Schimansky/Bunte/Lwowski*[4], § 41 Rn. 12.
575 Oben Rn. 65.
576 *eBay*, Überprüfung durch die Schufa.
577 So auch *Hanau*, Handeln unter fremder Nummer, S. 214; *Schapiro*, S. 14.
578 So auch *Ernst*, MDR 2003, 1091; *Roßnagel*, MMR 2002, 67, 68; *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211; *Roßnagel*, NJW 2005, 385, 388.

beantworten zu können, sollen zunächst als sicher geltende Wege der Identifizierung von Personen beleuchtet werden, um anschließend schrittweise bei weniger sicheren Wegen zu prüfen, ob deren Schutzniveau noch eine hinreichende Sicherheit bietet.

Als sicherste Methode der Identifizierung einer natürlichen Person gilt **610**
der Abgleich zahlreicher in der DNA gespeicherter Sein-Merkmale dieser Person. Dieses Verfahren wird unter anderem für die Feststellung der biologischen Abstammung von Kindern[579] oder zum Beleg für die Täterschaft des einer Straftat Beschuldigten (§ 81e Abs. 1 S. 1 StPO) verwendet.[580] Die Identitätsfeststellung mittels DNA hat eine fast hundertprozentige Wahrscheinlichkeit.[581] Eine solch aufwendige und kostspielige Identifizierung werden Teilnehmer im Rechtsverkehr typischerweise für den Abschluss eines Rechtsgeschäftes nicht aufwenden.

In einem Ausweissystem kann nur eine Trusted Authority für die Zuver- **611**
lässigkeit sorgen.[582] Diese Trusted Authority bestätigt, dass einer Person Merkmale wie Name, Vorname oder Adresse zugeschrieben werden.[583] Der Staat überprüft die Identität der Bürger bei der Ausgabe der Personalausweise. Die Identität des Antragstellers wird nicht anhand sicherer DNA-Tests überprüft, sondern der Staat verlässt sich zunächst auf Dokumente (vgl. § 9 Abs. 3 S. 3 PAuswG). Nur wenn dennoch Zweifel bezüglich der Identität des Antragstellers bestehen, greift der Staat auf die sicheren, aber auch grundrechtsrelevanten erkennungsdienstlichen Maßnahmen zurück (vgl. § 9 Abs. 4 S. 2 PAuswG). Wenn zur Ausgabe des zentralen staatlichen Ausweisdokumentes urkundliche Nachweise über die Identität, etwa die Geburtsurkunde, ausreichend sind, muss dies erst recht für den rechtsgeschäftlichen Verkehr gelten. Lässt sich der Authentisierungsnehmer daher vom Account-Inhaber Urkunden, die seine Identität beweisen, persönlich vorlegen, wird der Account-Inhaber ausreichend sicher identifiziert.

Aufbauend auf diese einmalige Prüfung der Identität bei der Ausgabe des **612**
Personalausweises als hoheitliches Ausweispapier, nutzt der Staat das Ausweispapier, um später die Identität einer Person für andere Zwecke festzu-

---

579 Dazu *Rauscher*, in: *Staudinger*[2011], Vorbem zu §§ 1591 ff. BGB Rn. 169.

580 Dazu *Pfeiffer*, in: *Pfeiffer*[5], § 81e StPO Rn. 1.

581 Die Wahrscheinlichkeit einer Fehlzuordnung wegen identischer DNA zweier Personen liegt bei 0,000025 %, *BGH*, Urteil v. 27. 7. 1994, 3 StR 225/94 – NStZ 1994, 554, 555.

582 *Bohrer*, MittBayNot 2005, 460, 461.

583 *Roßnagel/Hornung*, DÖV 2009, 301, 302.

stellen. Der Beschuldigte einer Straftat wird beispielsweise primär über hoheitliche Ausweisdokumente identifiziert (vgl. § 163b Abs. 1 S. 1 StPO).[584] Bei dieser Methode des Abgleichs von realer Person mit Bild und Daten auf dem Ausweispapier kann es zu Fehlern kommen. Sich ähnlich sehende Personen, beispielsweise eineiige Zwillinge, können sich bei diesem Verfahren als eine andere Person ausgeben. Wenn für die Zwecke der Strafverfolgung für eine Identifizierung zunächst auf hoheitliche Ausweisdokumente zurückgegriffen wird, bieten diese Dokumente erst recht eine ausreichende Sicherheit für die Identifizierung im rechtsgeschäftlichen Verkehr. Eine solche Authentisierungsmethode wird bei besonders wichtigen Rechtsgeschäften wie beim Rahmenvertrag fürs Online-Banking verwendet.[585] Der Nachteil bei dieser Überprüfung der Identität ist, dass Authentisierungsnehmer und Account-Inhaber räumlich zusammen kommen müssen. Dieser Aufwand wird bei Online-Geschäften, die gerade den Vorteil haben, dass die Geschäftspartner sich nicht am selben Ort treffen müssen, selten betrieben.

613 Eine Methode, die diesen persönlichen Kontakt zwischen Authentisierungsnehmer und Account-Inhaber beseitigt, besteht in dem PostIdent-Verfahren, das die Deutsche Post AG als Dienstleistung anbietet. Beim PostIdent-Verfahren überprüfen Mitarbeiter der Deutschen Post AG die Identität einer Person anhand von Ausweisdokumenten und teilen das Ergebnis der Prüfung dem Auftraggeber mit.[586] Wenn die Deutsche Post AG die Überprüfung der Identität mittels des Personalausweises oder eines anderen hoheitlichen Ausweisdokumentes übernimmt, entstehen keine bedeutenden zusätzlichen Fehlerquellen zu dem Verfahren, bei dem der Authentisierungsnehmer den Ausweis selbst kontrolliert. Der Authentisierungsnehmer darf sich auf die Deutsche Post AG als Trusted Authority verlassen.[587] Überprüft der Authentisierungsnehmer beim Erstellen des Accounts die Identität des Account-Inhabers daher mittels PostIdent-Verfahren, hat er eine ausreichend sichere Identifikationsmethode gewählt.

614 Die vorher genannten Methoden stellen durch den persönlichen Kontakt zwischen dem Überprüfenden und dem die Identität Behauptenden sicher, dass nur eine ähnlich aussehende Person sich als der Account-Inhaber ausgeben kann. Fraglich ist, ob es auch Methoden gibt, die ohne einen persönlichen Kontakt trotzdem als hinreichend sicher angesehen werden können.

---

584 Dazu *Pfeiffer*, in: *Pfeiffer*[5], § 163b StPO Rn. 6.
585 Oben Rn. 67.
586 *Möller*, NJW 2005, 1601.
587 Zu Trusted Authorities oben Rn. 81.

Eine solche Methode ist der elektronische Identitätsnachweis im neuen Personalausweis (§ 18 PAuswG).[588] Von der staatlichen Identitätsüberprüfung beim Ausstellen des Ausweises lässt sich ebenso wie bei der persönlichen Überprüfung grundsätzlich auf die Identität des Ausweisinhabers schließen. Der Staat nimmt dabei die Funktion der Trusted Authority war.[589] Mangels eines persönlichen Kontaktes können jedoch auch andere Personen als der Ausweisinhaber sich als dieser ausgeben. Sobald diese dritte Person die Zugangsdaten für den Ausweis erlangt und Besitz dessen hat, kann sie sich – auch ohne dass sie dem Ausweisinhaber ähnlich sieht – als dieser ausgeben. Ein Kind könnte sich somit als Erwachsener ausgeben, eine Frau als Mann. Der Authentisierungsnehmer hat dabei keine Möglichkeit festzustellen, dass der Ausweisinhaber nicht selbst handelt. Der elektronische Identitätsnachweis bietet daher weniger Sicherheit als das persönliche Überprüfen des Personalausweises mit vergleichendem Blick auf denjenigen, der die Identität behauptet.

Fraglich ist dabei, ob dieses Verfahren noch ausreichend sicher ist. Die **615**
Geheimhaltungspflicht der Zugangsdaten (§ 27 Abs. 2 PAuswG)[590] soll das Missbrauchsrisiko verringern. Zu erwägen ist jedoch, dass sich als sechsstellige PIN das Geburtsdatum eignet.[591] Insofern erscheint es nicht unwahrscheinlich, dass ein Kind sich den in der Wohnung herumliegenden Personalausweis eines Elternteils nimmt, die PIN errät oder kennt und sich als der Elternteil ausgibt. Trotz dieser Missbrauchsmöglichkeiten ergeben verschiedene gesetzliche Wertungen das Ergebnis, dass die Überprüfung mittels elektronischen Identitätsnachweises im rechtsgeschäftlichen Verkehr eine ausreichende Sicherheit bietet. Für die Identitätsüberprüfung bei der Vergabe eines qualifizierten Zertifikats für eine elektronische Signatur (§ 5 Abs. 1 SigG) reicht die Ausweisung des Signaturschlüssel-Inhabers mittels elektronischen Identitätsnachweises aus (§ 3 Abs. 1 S. 2 SigV).[592] Ebenso hat der Gesetzgeber bezüglich der De-Mail entschieden, dass die Identitätsüberprüfung mittels elektronischen Identitätsnachweises eine ausreichende Sicherheit bietet (vgl. § 3 Abs. 3 S. 1 Nr. 1 a.E. DeMailG). Diese gesetzgeberischen Wertungen gilt es zu respektieren. Eine Überprüfung der Identi-

588 Oben Rn. 88.
589 Zu Trusted Authorities oben Rn. 81.
590 Dazu unten Rn. 897.
591 Als Passwort verwenden viele das Geburtsdatum, beispielsweise der Beklagte im Fall *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255.
592 Dazu *Gramlich*, in: *Spindler/F. Schuster*[2], § 5 SigG Rn. 5.

tät des Account-Inhabers mittels elektronischen Identitätsnachweises bietet daher ausreichende Sicherheit, sodass in diesen Fällen eine Grundlage für einen Rechtsscheintatbestand besteht.[593]

616 Ebenso wie der elektronische Identitätsnachweis bietet die qualifizierte elektronische Signatur die Möglichkeit einer Erstauthentisierung gegenüber einem Authentisierungsnehmer. Dieser kann mit der Erstauthentisierung die Identität des Inhabers bei Erstellen des Accounts überprüfen. Bei der Vergabe eines qualifizierten Zertifikats für eine qualifizierte elektronische Signatur muss die Identität des Antragstellers zuverlässig überprüft werden (§ 5 Abs. 1 S. 1 SigG).[594] Der Zertifizierungsdienste-Anbieter ist dabei die Trusted Authority, auf deren Überprüfung sich der Authentisierungsnehmer verlässt.[595] Bei der elektronischen Signatur könnte aufgrund der mit dem elektronischen Identitätsnachweis vergleichbaren Missbrauchsmethoden daran zu zweifeln sein, dass die Identitätsüberprüfung ausreichend sicher ist. Hier ist jedoch ebenso die Wertung des § 3 Abs. 3 S. 1 Nr. 1 a.E. DeMailG zu berücksichtigen. Dieser stellt die qualifizierte elektronische Signatur mit dem elektronischen Identitätsnachweis für die Identitätsüberprüfung bei einem De-Mail-Account auf eine Stufe. Die Identitätsprüfung anhand einer qualifizierten elektronischen Signatur bei Erstellen des Accounts bietet daher hinreichende Sicherheit, für die Schutzwürdigkeit des Vertrauens darin, dass der Account-Ersteller auch der angegebene Namensträger ist.[596] Gleiches ist für den Identitätsbestätigungsdienst (§ 6 DeMailG) eines De-Mail-Diensteanbieters anzunehmen.

617 Als letzte Methode der Identitätsüberprüfung wird eine Überprüfung durch einen Medienbruch untersucht. Der Authentisierungsnehmer kann versuchen die Identität des Account-Inhabers dadurch zu überprüfen, dass er ihm einen Brief an die angegebene Adresse schickt oder ihn unter einer angegebenen Telefonnummer anruft.[597] Bei der Methode einen Brief an die angegebene Adresse zu schicken, wird in diesem Brief ein Geheimnis mitgeteilt, dass der Account-Inhaber anschließend eingeben muss. Dadurch

---

593 Dies stimmt überein mit dem Ergebnis, dass beim neuen Personalausweis ein Rechtsschein für das Handeln des Ausweisinhabers besteht, dazu unten Rn. 892.

594 Dazu oben Rn. 73.

595 Dazu oben Rn. 81.

596 Unter anderem deswegen besteht bei der Verwendung der qualifizierten elektronischen Signatur ein Rechtsscheintatbestand für das Handeln des Schlüssel-Inhabers, dazu unten Rn. 882.

597 *Schapiro*, S. 14.

wird der Besitz an dem Brief digitalisiert überprüft. Fraglich ist, ob das Empfangen eines Briefes ausreichend sicher den dort bezeichneten Adressaten erreicht. Zunächst ist denkbar, dass ein Mitglied des Haushalts des Adressaten den Brief abfängt. Es ist auch möglich, dass sich eine Person einen weiteren Namen an den Briefkasten klebt, um unter falschem Namen Briefe zu empfangen.[598] Briefe können auch von einer Person abgefangen werden, die sie direkt vom Briefträger entgegen nimmt oder sie aus dem verschlossenen, aber durch den Schlitz erreichbaren Briefkasten entnimmt. Ob dieses Verfahren der Identitätsprüfung für ein schützenswertes Vertrauen in die Identität des Account-Inhabers ausreicht, ist eine Wertungsentscheidung. Das Verfahren mittels eines zugesandten Briefs ist deutlich schwächer als die Überprüfung des Personalausweises oder als die Authentisierung durch den elektronischen Identitätsnachweis. Verletzungen des grundrechtlich (Art. 10 Abs. 1 GG) und strafrechtlich (§ 202 Abs. 1 StGB) geschützten Briefgeheimnisses sind zwar möglich, aber wegen der Sanktionierung kaum zu erwarten. Ein Eingriff von Außen in den Briefverkehr ist wenig wahrscheinlich. Dennoch bestehen viele Möglichkeiten im Haushalt oder durch Anbringen von zusätzlichen Namen am Briefkasten Briefe unter falschem Namen zu empfangen. Die Zusendung eines Briefes bestätigt daher nur, dass der Account unter dieser Adresse Briefe empfangen kann. Diese Methode überprüft jedoch nicht ausreichend zuverlässig, dass die virtuelle Identität einer numerischen Identität zugeordnet werden kann.[599]

Fraglich ist, ob der Anruf bei einer Telefonnummer, die beim Erstellen **618**
des Accounts angegeben wurde, den Account-Inhaber identifiziert. Dazu müsste der Telefonanschluss den Telefonierenden identifizieren. Zwar ist der Telefonanschluss auf eine Person angemeldet, deren Identität regelmäßig durch den Anbieter überprüft wurde. Ferner ist für staatliche Stellen durch den Auskunftsanspruch aus § 113 Abs. 1 S. 1 TKG nachvollziehbar auf welchen Namen der Telefonanschluss registriert ist. Ein Telefonanschluss kann jedoch innerhalb eines Haushalts geteilt werden oder für einen anderen, beispielsweise von einem Elternteil für ein Kind, angemeldet werden.[600] Einen Rückschluss auf den Telefonierenden kann der Angerufene daher anhand der Telefonnummer nicht ziehen. Ferner kann der Handelnde eine falsche Telefonnummer bei der Registrierung angeben. Der Name und

598 *Schapiro*, S. 14.
599 A.A. *Mankowski*, NJW 2002, 2822, 2825; *Ernst*, MDR 2003, 1091.
600 Dazu oben Rn. 523.

die Anschrift können anhand der Telefonnummer nur unzureichend überprüft werden. Es ist jedoch denkbar, dass bei dem Anruf nicht die Telefonnummer abgeglichen wird, sondern die Stimme des Abnehmenden. Die Stimme ist wie die Handschrift ein Sein-Merkmal, das anhand einer forensischen Untersuchung überprüft werden kann.[601] Eine solche Aufzeichnung der Stimme zur späteren Untersuchung ist jedoch ohne Einwilligung verboten (§ 201 Abs. 1 Nr. 1 StGB), sodass Authentisierungsnehmer diese Methode nicht zur Identifizierung einsetzen können.

619 Zusammenfassend lässt sich festhalten, dass die Überprüfung des Personalausweises bei persönlichem Kontakt oder über den elektronischen Identitätsnachweis sowie die Identitätsüberprüfung mittels qualifizierter elektronischer Signatur ausreichende Sicherheit dafür bieten, dass der Rechtsverkehr schützenswert darauf vertrauen kann, dass die Zuordnung des Accounts zu einer numerischen Identität korrekt erfolgt ist.

ee) Sicherstellung der Identität durch ein Reputationssystem

620 Das teilweise von Internet-Auktionsplattformen verwendete Reputationssystem soll sicherstellen, dass in die Echtheit des Accounts, also in die korrekte Zuordnung von virtueller zu numerischen Identität, Vertrauen geweckt wird.[602] Es stellt sich daher die Frage, ob ein Reputationssystem eine fehlende Überprüfung der Identität des Account-Inhabers nachträglich herstellen kann. Dazu müsste es sicherstellen, dass eine positive Bewertung nur vergeben wird, wenn der Account-Inhaber handelt.

621 Zwei Komponenten könnten dazu führen, dass auffiele, wenn nicht der Account-Inhaber handelt. Zum einen muss bei einer Transaktion bei einer Internet-Auktionsplattform Geld fließen. Wird dieser Geldtransfer über ein deutsches Konto abgewickelt, kann der Handelnde über dieses Konto identifiziert werden. Beim Anlegen eines Kontos wird die Identität des Bankkunden zuverlässig überprüft,[603] sodass ein Rückschluss auf den Accountinhaber möglich sein könnte. Selbst bei einem Geldtransfer über ein deutsches Bankkonto kann es jedoch zu auflösbaren oder unauflösbaren Identitätsverwirrungen kommen. Die Bank muss bei einer Überweisung beispielsweise den Namen des Kontoinhabers nicht überprüfen (vgl. § 675r Abs. 1 S. 1

601 Vgl. *Gfroerer*, in: *Widmaier*, § 77 Rn. 31.
602 Dazu oben Rn. 66.
603 Dazu oben Rn. 67.

BGB). Jemand könnte also eine Überweisung auf sein Konto veranlassen, dem Überweisenden jedoch über seinen wahren Namen täuschen. Diese Identitätstäuschung kann der Überweisende jedoch mit Hilfe der Bank im Nachhinein aufdecken. Ferner könnte der tatsächlich Handelnde durch den Einsatz eines Geldkuriers seine Identität verschleiern.[604] Dabei gelingt es den Tätern häufig dem Geldkurier die eigene Identität nicht zu offenbaren, sodass der Täter nicht ermittelt werden kann. Darüber hinaus werden zahlreiche Auktionen über Online-Bezahldienste abgewickelt. Bei Erstellen eines Paypal-Kontos wird zwar die Identität des Account-Inhabers mittels Kreditkarte oder Bankkonto überprüft,[605] bei Online-Bezahldiensten kann ein Betrüger jedoch ebenso einen Geldkurier einsetzen. Darüber hinaus könnte ein Angreifer durch das Ausspähen der Zugangsdaten[606] zu einem Paypal-Konto, dieses übernehmen und für nicht zu ihm zurückverfolgbare Zahlungen verwenden. Die Zahlungsabwicklung nach einer Auktion stellt somit nicht sicher, dass nur der Account-Inhaber gehandelt hat.

Zweitens ist zu erwägen, dass der Account-Inhaber anhand der Lieferadresse identifiziert werden kann. Dagegen spricht jedoch zum einen, dass man an seinen Briefkasten einen weiteren Namen anbringen kann[607] und auch Pakete an eine fiktive Person bei sich zu Hause entgegen nehmen kann. Ferner kann der Handelnde eine vom Account-Inhaber abweichende Lieferadresse angeben. Eine Person mit kriminellen Intentionen könnte sich daher durch die Reputation eine weiße Weste anlegen, um sie später zu missbrauchen.[608] Das Bewertungssystem bei einer Internet-Auktionsplattform stellt somit nicht ausreichend zuverlässig sicher, dass die virtuelle Identität des Accounts dem ausgewiesenen Account-Inhaber korrekt zugeordnet ist.[609] Auch auf Verkäuferseite kann durch den Postverkehr über die Identität getäuscht werden. Der Verkäufer kann auf das verschickte Paket eine beliebige Adresse schreiben. So kann es passieren, dass zahlreiche Käufer mit einer positiven Bewertung zum Ausdruck bringen, dass bei diesem Verkäufer die Identitätsbehauptung zutrifft, dies in Wirklichkeit jedoch nicht der Fall ist. 622

604 Zum Einsatz von Geldkurieren etwa *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08, Rn. 15 ff.; *Borges*, ZIP 2006, 1983.
605 Siehe oben Rn. 71.
606 Zu den verschiedenen Methoden oben Rn. 124 ff.
607 *Engel*, DuD 2006, 207, 208; *Schapiro*, S. 14.
608 *Hanau*, Handeln unter fremder Nummer, S. 212.
609 Ähnlich auch *LG Kassel*, Urteil v. 15. 4. 2008, 9 O 2539/06 – NJW-RR 2009, 781.

ff) Individuelle Überprüfung durch persönlichen Kontakt zum Account-Inhaber

623 Neben den soeben ausgeführten Möglichkeiten, die Zuverlässigkeit der Identifikationsfunktion durch ein Überprüfen der Identitätsbehauptung durch den Authentisierungsnehmer beim Erstellen des Accounts sicherzustellen, besteht die Möglichkeit, dass der Account-Inhaber durch Interaktionen mit einzelnen Erklärungsempfängern das Zutreffen der Identitätsbehauptung bestätigt. In diesem Fall wird, anders als bei der Überprüfung der Identität beim Erstellen des Accounts, nicht gegenüber jedem potentiellen Erklärungsempfänger, sondern nur gegenüber einzelnen im Kontakt mit dem Account-Inhaber stehenden Erklärungsempfängern die Zuverlässigkeit der Identifikationsfunktion sichergestellt. Eine solche zuverlässige Identitätsüberprüfung im Rahmen eines individuellen Vertrauenstatbestandes kann beispielsweise dadurch entstehen, dass der Account-Inhaber gegenüber einem Dritten in einem persönlichen Gespräch eine Erklärung über einen Account ankündigt, die später tatsächlich ankommt. Ebenso könnte der Account-Inhaber in einer E-Mail etwas ankündigen, was er anschließend gegenüber dem Erklärungsempfänger tatsächlich vornimmt. Dadurch bestätigt der Account-Inhaber gegenüber diesem einen Erklärungsempfänger, dass die Identitätsbehauptung des Accounts zutrifft. Dieser eine Erklärungsempfänger entwickelt somit ein Vertrauen in die korrekte Zuordnung der numerischen zu der virtuellen Identität des Accounts. Er darf sich daher auf die Identifikationsfunktion des Accounts verlassen.

gg) Zwischenergebnis

624 Für den Rechtsscheintatbestand bedarf es neben der sicheren Authentisierungsmethode der zuverlässigen Überprüfung, ob die bei der Erstellung des Accounts aufgestellte Identitätsbehauptung zutrifft. Der gesamte Rechtsverkehr darf darauf nur vertrauen, wenn der Authentisierungsnehmer die Identität bei Erstellen des Accounts oder später zuverlässig überprüft hat. Diese Überprüfung kann der Authentisierungsnehmer selbst vornehmen oder sich einer Trusted Authority bedienen. Gegenüber einzelnen Teilnehmer des Rechtsverkehrs kann ein schützenswertes Vertrauen in das Zutreffen der Identitätsbehauptung durch einen persönlichen Kontakt zu Account-Inhaber entstehen, durch den sich die Zuordnung des Accounts zum Account-Inhaber bestätigt.

d) Angemessene Verteilung der Risiken

Das Gesetz weist das Risiko der nicht vorhanden Vertretungsmacht dem Geschäftsgegner zu (vgl. § 179 BGB).[610] Soll diese gesetzliche Risikoverteilung durchbrochen werden, bedarf es zur Rechtfertigung der Durchbrechung eines gewichtigen Grundes, wie dem des überwiegenden Vertrauensschutzes.[611] Die Behauptung, teleologisch müsse das Vertrauen in den eCommerce geschützt werden,[612] reicht dazu nicht. Allein eine mögliche Unsicherheit über den Urheber einer Willenserklärung begründet diesen Vertrauensschutz nicht. Denn es besteht keine allgemeine Pflicht den Rechtsverkehr vor Irreführung zu schützen.[613] Systematisch zeigt § 123 Abs. 1 BGB, dass erst arglistige Täuschungen oder widerrechtliche Drohungen mit dem Ziel, eine andere Person zur Abgabe einer Willenserklärung zu bewegen, widerrechtlich sind. Ferner sorgt die Auslegung am objektiven Empfängerhorizont (§ 157 BGB) dafür, dass Irreführungen mit anders gemeinten, aber objektiv in eine Richtung zu verstehenden Willenserklärungen nicht möglich sind. Es stellt sich daher die Frage, ob gewichtige Gründe bestehen, die eine von der gesetzlichen Normalverteilung abweichende Risikoverteilung bei dem Missbrauch von Zugangsdaten im Internet rechtfertigen. Bei der Rechtsscheinhaftung im Internet geht es letztendlich um die Abgrenzung von Risikosphären.[614] 625

Teilweise wird gefordert, dass das Missbrauchsrisiko von Zugangsdaten nicht einseitig dem Geschäftsgegner auferlegt werden solle.[615] Beide Parteien setzten sich dem Risiko gleichermaßen aus.[616] Dagegen ist jedoch einzuwenden, dass insbesondere der Geschäftsgegner von den Vorteilen profitieren möchte. Bietet ein Verkäufer eine Ware beispielsweise in einer Internet-Auktionsplattform an, profitiert er von einem großen Käuferkreis, der potentiell zu einem höheren Verkaufserlös führt. Wird missbräuchlich mit einem fremden Account geboten, den der Account-Inhaber möglicherweise nur angelegt hat, um ihn einmalig oder gelegentlich zu benutzen, vermag es nicht 626

610 Dazu auch *BGH*, Urteil v. 13. 7. 1977, VIII ZR 243/75 – WM 1977, 1169, 1170.
611 Siehe *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 20; *Hauck*, JuS 2011, 967, 969.
612 *Mankowski*, CR 2011, 458, 459.
613 *Canaris*, Vertrauenshaftung, S. 194; *Rieder*, S. 185.
614 *Wiebe*, MMR 2002, 257, 258.
615 *Ernst*, MDR 2003, 1091, 1093; *Winter*, MMR 2002, 836.
616 *Winter*, MMR 2002, 836.

zu überzeugen, warum der Account-Inhaber das Risiko ebenso wie der Verkäufer tragen soll. Der Verkäufer hat sich im Bewusstsein der Gefahren und Unsicherheiten, aber auch mit den Vorteilen der Internet-Auktion für diese entschieden. Eine vom gesetzlichen Regelfall abweichende Risikoverteilung bedarf es für ihn daher nicht.

627 Ebenso ist eine abweichende Risikoverteilung für einen Bieter nicht angezeigt. Der Bieter stöbert auf einer Internet-Auktionsplattform nach günstigen Angeboten. Er kann sich anhand des Angebotes und den Bewertungen eines Verkäufers von dessen Vertrauenswürdigkeit überzeugen. Wurde das Angebot missbräuchlich von einem Dritten eingestellt, der in diesem Fall nicht die Vorteile der Internet-Auktionsplattform nutzen wollte, ist es ebenso angemessen, die Risiken dem Bieter aufzuerlegen.

628 Jeder Teilnehmer am Rechtsverkehr kann sich ein Medium für den Abschluss seiner Rechtsgeschäfte auswählen. Wählt er eine risikoreiche Methode, ist es billig, ihm das Risiko aufzuerlegen. Im Rahmen des Online-Banking trägt die Bank das Missbrauchsrisiko, wenn sie unsichere Authentifizierungsmethoden wie das einfache TAN-Verfahren verwendet. Sogar eine Schadensersatzhaftung der Bank ist denkbar.[617] Ebenso gehen die Geschäftspartner beim Vertragsschluss im Internet das Risiko ein, dass sie nicht mit dem gewünschten Namensträger sondern mit einer anderen Person zu tun haben. Sie können die Modalitäten des Vertragsschlusses frei wählen.[618] Die rein wissensbasierte Authentisierung ist dabei eine günstige Variante,[619] bietet jedoch im Gegenzug keinen hohen Schutz. Eine abweichende Risikoverteilung aus der Erwägung, dass beide Seiten von den Vorteilen des Vertragsschlusses über das Internet profitieren, erscheint daher nicht angebracht. Denn wer ein schnelles Medium wählt, muss die dadurch geschaffenen Unsicherheiten auf sich nehmen.[620] Wer den wirtschaftlichen Nutzen daraus trägt, muss auch die einhergehenden Risiken tragen.[621]

629 In Bezug auf Online-Auktionen wird dem Versteigerer in anderen Rechtsfragen ebenfalls das Risiko aufgebürdet, das er eingeht, um von den Chancen einer Online-Auktion zu profitieren. Entsteht durch eine Online-Auktion beispielsweise ein krasses Missverhältnis zwischen Wert der Ware und dem Kaufpreis, ist der Vertrag nach überwiegender Meinung nicht etwa we-

617 *Schulte am Hülse/Klabunde*, MMR 2010, 84, 88.
618 So auch *Borges*, NJW 2011, 2400, 2402.
619 *Mankowski*, CR 2011, 458.
620 *AG Berlin Mitte*, Urteil v. 28. 7. 2008, 12 C 52/08 – MMR 2008, 696, 697.
621 *BGH*, Urteil v. 4. 3. 2004, III ZR 96/03 (Dialer) – BGHZ 158, 201, 208.

gen eines wucherähnlichen Geschäfts nach § 138 Abs. 1 BGB nichtig.[622] Der Verkäufer habe durch die Wahl des Verkaufs über eine Online-Auktion die Chance auf einen durch Überbieten hochgetriebenen Verkaufspreis gewählt, die verbunden ist mit dem Risiko, einen niedrigen Kaufpreis zu erhalten.[623] In diesem Lichte ist es angemessen, den Versteigerer ebenfalls wegen der Chance des großen Interessentenkreises das Risiko einer missbräuchlich abgegebenen Willenserklärung tragen zu lassen.

Ferner wird angeführt, dass der Geschäftsgegner keine Möglichkeit hat zu erkennen, ob der Account-Inhaber gehandelt habe. Daher sei sein Vertrauen darin schutzwürdig.[624] Zwar kann der Geschäftsgegner der Willenserklärung selbst nicht ansehen, ob diese tatsächlich vom Account-Inhaber stammt. Er hat jedoch andere Möglichkeiten, sich zu versichern, dass der Account-Inhaber diese Willenserklärung abgeben möchte.[625] 630

aa) Die vermeintliche Notwendigkeit Schutzbehauptungen zu verhindern

Vielerorts wird die Rechtsscheinhaftung für den Missbrauch von Zugangsdaten gefordert, um Schutzbehauptungen nicht Tür und Tor zu öffnen.[626] Der Anspruchsgegner dürfe sich nicht durch eine Missbrauchsbehauptung rechtswidrig seiner vertraglichen Pflichten entziehen.[627] Gegen die Schutzbehauptungen, die gegen die Wahrheitspflicht nach § 138 Abs. 1 ZPO verstoßen, sei der Anspruchsgegner schutzlos. Zwar besteht eine Strafbarkeit nach §§ 263, 23 StGB desjenigen, der die Schutzbehauptungen aufstellt. Diese Strafbarkeit laufe jedoch regelmäßig leer.[628] 631

622 *BGH*, Urteil v. 28. 3. 2012, VIII ZR 244/10 – NJW 2012, 2723, Rn. 20; *OLG Oldenburg*, Urteil v. 30. 10. 2003, 8 U 136/03 – NJW 2004, 168, 169; *OLG Köln*, Urteil v. 8. 12. 2006, 19 U 109/06 – CR 2007, 598, 599 f.; *LG Bonn*, Urteil v. 12. 11. 2004, 1 O 307/04, Rn. 33 ff.; *LG München*, Urteil v. 7. 8. 2008, 34 S 20431/04, Rn. 19; *Ernst*, CR 2000, 304, 310; *Gooren*, MMR 2012, 453; *Hoeren*, EWiR 2012, 471; *Juretzek*, CR 2012, 462, 462.

623 *BGH*, Urteil v. 28. 3. 2012, VIII ZR 244/10 – NJW 2012, 2723, Rn. 20.

624 *Herresthal*, K&R 2008, 705, 707; *ders.*, in: *Taeger/Wiebe*, 21, 31.

625 Unten Rn. 657.

626 *Herresthal*, K&R 2008, 705, 707; *ders.*, in: *Taeger/Wiebe*, 21, 32; *ders.*, JZ 2011, 1171, 1173; *Oechsler*, AcP 208 (2008), 565, 579; *Wenn*, CR 2006, 137, 138.

627 *Wenn*, CR 2006, 137, 138.

628 *Herresthal*, K&R 2008, 705, 707; *ders.*, in: *Taeger/Wiebe*, 21, 32.

632 Schon früh wurde die Gefahr gesehen, dass sich Account-Inhaber der Haftung durch Schutzbehauptungen entziehen können.[629] Der Fall, dass ein Account-Inhaber das Handeln eines minderjährigen Kindes behauptet,[630] lässt sich in der Rechtsprechung finden. So hat ein Familienvater sich mit der Behauptung, seine minderjährige Tochter hätte seinen Bildschirmtext-Anschluss verwendet um pornographische Inhalte anzugucken, gegen den Zahlungsanspruch des Diensteanbieters gewehrt.[631]

633 Darüber hinaus wird angeführt, dass ein Dritter kein Interesse daran habe, Willenserklärungen beispielsweise im Rahmen von Online-Auktionen ohne Vertretungsmacht abzugeben.[632] Rational betrachtet lässt sich zwar kein vernünftiger Grund finden, über einen fremden Account einen Gegenstand zu ersteigern. In der Rechtsprechung lassen sich jedoch Fälle finden, in denen aus unerklärlichen Gründen über einen fremden Account Gold-Schmuck ersteigert wurde[633] oder ein vom Inhaber benötigter Imbissanhänger missbräuchlich zum Verkauf angeboten wurde.[634] Einige Dritte lassen sich aus Mutwillen oder um dem Account-Inhaber einen Streich zu spielen, zum Missbrauch der Zugangsdaten bewegen. Darüber hinaus kann ein Missbrauch von Zugangsdaten durchaus aus nachvollziehbaren Gründen erfolgen. Hat ein Dritter die Zugangsdaten zum Online-Banking oder zu einem Online-Bezahldienst, kann er sich an dem Vermögen des Account-Inhabers missbräuchlich bedienen. Das Argument, dass es Dritten an einem vernünftigen Interesse fehle, Zugangsdaten zu missbrauchen, unterstellt, dass die Behauptung eines Missbrauchs regelmäßig eine Schutzbehauptung ist.

634 Gegen die Notwendigkeit, Schutzbehauptungen durch eine materielle Lösung der Rechtsscheinhaftung zu verhindern, spricht, dass es sich um ein prozessuales Problem handelt. Insofern liegt die Suche nach einer prozessualen Lösung näher, auf die später noch eingegangen wird.[635]

---

629 *Kleier*, WRP 1983, 534, 536.
630 Wie ebd., 536 abstrakt beschrieben.
631 *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400.
632 *Winter*, MMR 2002, 836.
633 Siehe *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255.
634 Siehe *LG Köln*, Urteil v. 27. 10. 2005, 8 O 15/05 – BeckRS 2006, 07259.
635 Dazu unten Rn. 772 ff.

bb) Rechtsökonomisch sinnvolle Verteilung der Risiken

Eine vom gesetzlichen Regelfall abweichende Risikoverteilung könnte teleologisch gerechtfertigt werden, wenn der Account-Inhaber der *Cheapest Cost Avoider* ist und es daher gesamtwirtschaftlich sinnvoll ist, ihn durch die Haftung zur Sorgfalt zu bewegen. Bei der ökonomischen Analyse des Rechts werden rechtliche Regelungen danach beurteilt, in welchem Maße sie die Verschwendung von Ressourcen verhindern und damit die Effizienz erhöhen.[636] Dabei werden die Auswirkungen von Rechtsstrukturen auf die Allokationseffizienz untersucht sowie überlegt, wie die Rechtsstruktur im Hinblick auf das Ziel der Allokationseffizienz beschaffen sein sollte.[637] Die ökonomische Analyse des Rechts bietet daher zum einen die Möglichkeit die Effizienz bestehender Regelungen zu bewerten. Die Allokationseffizienz ist im Rahmen bestehender Regelungen zwar keine rechtliche Wertung. Im Rahmen einer teleologischen Auslegung kann bei entsprechendem Auslegungsspielraum jedoch die effizienteste unter möglichen Auslegungsvarianten gewählt werden. 635

Eine bedeutende Figur im Rahmen der ökonomischen Analyse des Rechts ist der *Cheapest Cost Avoider*.[638] Der *Cheapest Cost Avoider* ist derjenige, der mit den geringsten Kosten den Eintritt eines Schadens hätte verhindern können. Im Schadensrecht soll der der *Cheapest Cost Avoider* zum Abwehraufwand veranlasst werden, was durch eine Haftung erreicht wird.[639] Ebenso soll im rechtsgeschäftlichen Bereich ein Risiko, das nicht Gegenstand vertraglicher Vereinbarungen geworden ist, demjenigen zugeordnet werden, der es mit dem geringsten Aufwand beherrschen kann.[640] Er soll das Risiko jedoch nur tragen, wenn die Risikovermeidungskosten niedriger sind als der Erwartungswert des Risikos (Learned-Hand-Formel).[641] 636

636 *Cooter/Ulen*[6], S. 3 f.; *Posner*[8], S. 31 f.; *Schäfer/C. Ott*[5], S. XXXIII; *Towfigh/Petersen*, S. 5.

637 *Schäfer/C. Ott*[5], S. XLIV; *Towfigh/Petersen*, S. 5 f.

638 Dazu *Adams*[2], S. 151 ff.; *Schäfer/C. Ott*[5], S. 252, 436.

639 *Calabresi*, S. 136 ff. sowie *Adams*[2], S. 152; *Schäfer/C. Ott*[5], S. 252.

640 *Schäfer/C. Ott*[5], S. 436.

641 Entwickelt durch *United States Court of Appeals, Second Circuit*, Urteil v. 9. 1. 1947, 159 F.2d 169 (United States v. Carroll Towing Co.). Zu der Learned-Hand-Formel *Schäfer/C. Ott*[5], S. 182 f.

aaa) Die vier rechtsökonomischen Voraussetzungen der Vertrauenshaftung

637 Eine allokationseffiziente Verteilung der Ressourcen kann nur erfolgen, wenn alle Beteiligten nur vorteilhafte Verträge abschließen.[642] Um einen vorteilhaften Vertrag zu schließen ist eine möglichst vollständige Information, jedenfalls das Minimum an Informationsasymmetrien, erforderlich.[643] Dabei braucht jeder einzelne Vertragspartner jedoch nicht ein umfassendes Wissen über die Details und Hintergründe zur Transaktion, sondern nur die relevanten.[644] Hat ein Vertragspartner die Informationen nicht, können ihm hohe Kosten für deren Beschaffung entstehen.[645] Durch die hohen Informationsbeschaffungskosten kann eine ineffiziente Verteilung der eingesetzten Ressourcen entstehen. Eine Vertrauenshaftung in Form der Rechtsscheinhaftung kann dafür sorgen, dass die Informationsbeschaffung allkoationseffizient geschieht, indem der *Cheapest Cost Avoider* die Informationen zu beschaffen und offen zu legen hat. Eine solche Vertrauenshaftung kommt daher unter den folgenden vier Voraussetzungen, auf die noch im Einzelnen eingegangen werden soll, in Betracht: die asymmetrische Verteilung der Informationskosten, die Produktivität der Information, das Bestehen einer Vertrauensprämie und die Höhe der Vertrauensprämie im Vergleich zur Opportunitätsprämie.[646]

638 Keine Voraussetzung dieser Vertrauenshaftung ist, dass sich der Haftende binden möchte, für das Vertrauen einzustehen. Es ist vielmehr von einem Verpflichtetsein auszugehen.[647] Ebenso wenig ist für die Anerkennung einer Vertrauenshaftung ausreichend, dass Vertrauen faktisch gewährt und in Anspruch genommen wird.[648] Eine solche Haftung ist jedoch nur geboten, wenn die Information notwendig ist. Gibt es alternative Möglichkeiten, bedarf es eines Ausgleichs des Informationsgefälles nicht. Gibt zum Beispiel ein Verkäufer eine Garantie ab, bedarf es keiner Aufklärungspflicht über die garantiertsen Eigenschaften des Gegenstandes.[649]

---

642 *Kötz*, in: FS Drobnig, 563, 567; *Kötz/Schäfer*, S. 167.
643 *Kötz*, in: FS Drobnig, 563, 567; *Kötz/Schäfer*, S. 167.
644 *Hayek*, American Economic Review 35 (1945), 519, 527.
645 *Stigler*, The Journal of Political Economy 3/69 (1961), 213, 218.
646 *Schäfer/C. Ott*[5], S. 557, 570; dazu auch *Fleischer*, S. 165.
647 *Köndgen*, S. 251; *Schäfer/C. Ott*[5], S. 563.
648 *Schäfer/C. Ott*[5], S. 569.
649 *Posner*[8], S. 141.

(1) Asymmetrische Verteilung der Informationskosten

Die erste Voraussetzungen ist eine asymmetrische Verteilung der Informa- 639
tionskosten. Wenn beide Seiten vergleichbare Informationskosten haben, dann ist keine der beiden Seiten der *Cheapest Cost Avoider*. Wenn der Vertrauende niedrige Kosten zur Informationsbeschaffung hat, der Geschäftsgegner hingegen hohe, ist es wirtschaftlich sinnvoll, dem Vertrauenden den Anreiz zur Informationsbeschaffung in Form der Versagung einer Haftung zu schaffen. Nur wenn der Vertrauende hohe Informationskosten und der Geschäftsgegner niedrige Informationskosten hat, kann unter den weiteren Umständen ein Vertrauensschutz geboten sein.[650]

Um zu prüfen, ob die erste Voraussetzung bei dem Missbrauch von Zu- 640
gangsdaten im Internet vorliegt, müssen zunächst die Informationskosten des Vertrauenden und des Account-Inhabers gegenüber gestellt werden. Dabei stellt sich zunächst die Frage, welche Information beschafft werden soll. Die relevante Information für den Empfänger einer Willenserklärung im Internet ist, ob der Account-Inhaber die Willenserklärung selbst oder ein Dritter mit Vertretungsmacht abgegeben hat. Beim Abstellen auf diese Information hat der Account-Inhaber keine Kosten bei der Informationsbeschaffung, weil er derjenige ist, von dem die Information stammt.

Die Informationskosten beziehen sich jedoch ebenfalls darauf, dass der 641
Account-Inhaber verhindert, dass Willenserklärungen in seinem Namen ohne Vertretungsmacht abgegeben werden oder dass er den darauf potentiell Vertrauenden über die fehlende Vertretungsmacht aufklärt. Die Kosten einer solchen Aufklärung sind nicht gering. Der Account-Inhaber muss die Existenz einer durch einen Dritten in seinem Namen abgegebenen Willenserklärung erst in Erfahrung bringen. Regelmäßig hinterlassen online abgegebene Willenserklärungen Spuren in Form von gespeicherten E-Mails bei den gesendeten Objekten oder Benachrichtigungs-E-Mails über den Kauf einer Ware oder das Bieten bei einer Online-Auktion. Diese Spuren können jedoch verwischt werden, beispielsweise durch das Löschen der entsprechenden E-Mails. Einen effektiven Schutz dagegen, dass ein Dritter auf eine Erklärung des Account-Inhabers vertraut, kann nur erreicht werden, wenn der Account-Inhaber den Vertrauenden zeitnah informiert. Die dafür

650 *Schäfer*/*C. Ott*[5], S. 558. Dazu auch *Fleischer*, S. 306 f.; *Kötz*/*Schäfer*, S. 173; *C. Ott*, in: Ökonomische Probleme, 142, 157 ff.; *Schepple*, S. 121 f.; vgl. auch *Posner*[8], S. 139 f.

erforderlichen regelmäßigen und zeitnahen Kontrollen stellen mittelhohe Informationskosten dar.

642 Der Account-Inhaber kann jedoch ebenfalls auf der Stufe davor ansetzen. Durch eine sichere Verwahrung der Zugangsdaten kann er dazu beitragen, dass diese nicht missbraucht werden können.[651] Durch einen aktuellen Virenschutz,[652] eine generelle Vorsicht, eine Geheimhaltung seines Passworts und einer sorgfältigen Verwahrung einer Chip-Karte kann der Account-Inhaber das Missbrauchsrisiko vermindern. Dieser Vermeidungsaufwand stellt einen niedrigen bis mittleren Kostenaufwand für den Account-Inhaber dar. Es gibt jedoch Angriffe, gegen die sich der Account-Inhaber auch mit diesen Methoden nicht sichern kann, beispielsweise Man-in-the-Middle-Angriffen mittels Pharming in Form des DNS-Cache-Poisoning.[653] Ein Missbrauch der Zugangsdaten kann auch durch Schwachstellen in der Sicherheitsinfrastruktur des Kommunikationsübermittlers, beispielsweise im SMTP-Server oder dem Webserver eines Internetauktionshauses, ermöglicht werden.[654] Auch mit sehr hohen Informationsbeschaffungskosten kann der Account-Inhaber solche Fälle des Missbrauchs nicht verhindern. Er kann lediglich versuchen, Spuren missbräuchlich darüber abgegebener Willenserklärungen zu entdecken und ein eventuelles Vertrauen des Geschäftsgegners durch eine Aufklärung verhindern.

643 In Konstellationen, in denen die Kommunikation von einem Diensteanbieter kontrolliert wird, wie bei Internet-Auktionsplattformen, kann dieser Diensteanbieter durch Vorsorgeaufwand ebenfalls einen Missbrauch der Zugangsdaten verhindern. Er kann beispielsweise die eigene IT-Infrastruktur so absichern, dass ein Missbrauch ohne die Zugangsdaten verhindert wird.[655] Die Internet-Auktionsplattform wird vereinzelt als *Cheapest Cost Avoider* beim Missbrauch von Zugangsdaten im Internet identifiziert.[656] Diese habe es in der Hand durch die Vorgabe eines sicheren Authentisierungsverfahrens Missbrauch zu verhindern. Die Marktmacht der Online-Handelsplattformen könnte zwar ausreichend sein, um eine sicherere Authentisierungsmethode durchzusetzen. Eine effiziente Lösung muss dies dennoch nicht sein. Sicherere Authentisierungsmethoden, beispielsweise

---

651 Zur sicheren Verwahrung oben Rn. 558.
652 Oben Rn. 202.
653 Dazu oben Rn. 153.
654 Oben Rn. 211 ff.
655 Zu möglichen Schwachstellen oben Rn. 215.
656 *Wiebe*, MMR 2002, 257, 258; *ders.*, in: Internet-Auktionen^2, Kap. 4 Rn. 68.

mittels Besitz und Wissen, verursachen höhere Kosten in Form von Chip-Karten und deren Lesegeräten beim Absender, sowie einen Prüfungsaufwand durch Software auf Seiten des Empfängers. Unabhängig von der Frage, welche Authentisierungsmethode am effizientesten ist, stellt sich die Frage nach den Informationskosten bei einer rein wissensbasierten Authentisierungsmethode. Dabei hat sich gezeigt, dass die Informationskosten des Account-Inhabers keinesfalls gering sind und alleine nicht ausreichen, um Missbrauch zu verhindern.

644 Neben der höheren Sicherheit durch eine kostenaufwendigere Zwei-Faktor-Authentisierung, kann der Geschäftsgegner auch über einen zweiten, unabhängigen Kommunikationskanal die Information beschaffen. Er kann durch eine Nachfrage beim Account-Inhaber oder durch Bestehen auf Vorleistung in Erfahrung bringen, ob die Willenserklärung vom Namensträger stammt oder mit Vertretungsmacht abgegeben wurde.[657]

Eine hundertprozentige Sicherheit erreicht er dadurch zwar nicht,[658] die Wahrscheinlichkeit steigt jedoch erheblich. Der Aufwand für diese Informationsbeschaffung ist gering. Es kostet den Geschäftsgegner einen kurzen Anruf, einen nachfragenden Brief oder das Warten auf den Geldeingang. Das Gegenteil der ersten ökonomischen Voraussetzung einer Vertrauenshaftung ist somit der Fall. Der Vertrauende hat geringe Informationskosten, wohingegen der Account-Inhaber geringe bis mittlere Informationsbeschaffungskosten hat.

(2) Produktivität der Information

645 Zweite ökonomische Voraussetzungen für eine Vertrauenshaftung ist die gesamtgesellschaftliche Produktivität derjenigen Informationskosten,[659] die für das Vertrauen Ersatz sind.[660] Dabei wird beurteilt, ob der Aufwand zur Beschaffung einer Information geringer ist als der durch die Information bewirkte Nutzen bzw. als der durch eine fehlende Information verursachte

657 Unten Rn. 657.

658 *Borges*, NJW 2011, 2400, 2402.

659 Zur Produktivität von Informationen *Hirshleifer*, American Economic Review 61 (1971), 561, 563 ff.

660 *Schäfer/C. Ott*[5], S. 558 f. Dazu auch *Cooter/Ulen*[6], S. 357; *Fleischer*, S. 285; *Kötz*, in: FS Drobnig, 563, 567; *Kötz/Schäfer*, S. 175.

Schaden.[661] Diese Voraussetzung ist der Suche der ökonomischen Analyse nach Allokationseffizienz inhärent. Wenn es mehr Kosten verursacht, die Information zu beschaffen, als die Information an Schaden verhindern kann, ist es unwirtschaftlich den Informationsbeschaffungsaufwand zu betreiben.

646 Zur Verhinderung des Missbrauchs von Zugangsdaten im Internet hat der Account-Inhaber niedrige bis mittelhohe Vermeidungskosten, der Geschäftsgegner hat geringe Informationsbeschaffungskosten. Dem müssen der Nutzen, also die vermiedenen Schäden aus dem Missbrauch der Zugangsdaten im Internet gegenüber gestellt werden. Bei einem Blick auf die eingeklagten Schadenssummen erscheinen die Schäden hoch. Beispielsweise wurde in der *BGH*-Entscheidung „VIP-Bareinrichtung" eine Summe von gut € 32.000 eingeklagt.[662] Dies entspricht dem positiven Interesse, das der Geschäftsgegner an der Erfüllung des Vertrags hat. Wirtschaftlich betrachtet handelt es sich dabei lediglich um die Expektanz, den erwarteten Gewinn, den der Geschäftsgegner mit dem Vertragsschluss zu machen erwartete. Da der Account-Inhaber am Zustandekommen des Vertrags beim Missbrauch von Zugangsdaten jedoch kein Interesse hat und diesen Vertrag ursprünglich nicht wollte, kann das positive Interesse nicht als Schaden gewertet werden.

647 Vielmehr besteht der Schaden lediglich in Aufwendungen, die der Geschäftsgegner im Vertrauen auf den Vertrag macht, sowie Kosten, die ihm dadurch entstehen, dass er versucht, den vermeintlichen Vertrag durchzusetzen. Im angesprochenen Fall der „VIP-Bareinrichtung" sind dem Kläger Kosten in Höhe von gut € 1.500 bei der vorgerichtlichen Geltendmachung entstanden sowie nicht näher bezifferte Ausgaben für eine Auskunft über eine ladungsfähige Adresse der Beklagten.[663] In anderen Fällen kann das negative Interesse am Vertrag jedoch das positive übersteigen, beispielsweise wenn die eine Partei in Vorleistung tritt, die Gegenleistung jedoch nicht erhält.[664]

---

661 *Kötz*, in: FS Drobnig, 563, 567 f. *Kötz/Schäfer*, S. 175 f. *Schäfer/C. Ott*[5], S. 574.

662 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 3.

663 Vgl. das Urteil aus der ersten Instanz *LG Dortmund*, Urteil v. 23. 12. 2008, 3 O 508/08, Rn. 20 f.

664 Wie bei *LG Aachen*, Urteil v. 15. 12. 2006, 5 S 184/06 – NJW-RR 2007, 565, wo der Kläger den Kaufpreis von rund € 650 bezahlt hat, ohne die gekaufte Ware erhalten zu haben.

Die entstehenden Vertrauensschäden erreichen je nach Fallkonstellation schnell drei- bis vierstellige Beträge oder mehr. Demgegenüber stehen der mögliche Vermeidungsaufwand des Account-Inhabers, der diese Beträge nicht übersteigen wird, sowie der Informationsbeschaffungsaufwand des Geschäftsgegners, der mit den Kosten eines Anrufes, eines Briefes oder des Abwartens erheblich geringer ist. Die Informationsbeschaffung bei Missbrauch von Zugangsdaten ist somit produktiv, sodass die zweite wirtschaftliche Voraussetzung gegeben ist. 648

(3) Existenz einer Vertrauensprämie

Dritte ökonomische Voraussetzung der Vertrauenshaftung ist die Existenz einer Vertrauensprämie.[665] Eine Vertrauenshaftung ist demnach nur gerechtfertigt, wenn der Markt den Haftenden für die Haftung mit einer Vertrauensprämie, also einem höheren Entgelt für die angebotene Leistung, belohnen kann.[666] Diese Vertrauensprämie muss höher sein als die Informationskosten.[667] Diese Voraussetzung ergibt sich ebenfalls aus der Suche nach allokationseffizienten Regelungen. Erhielte ein mit einer Vertrauenshaftung Belasteter hierfür keine Vertrauensprämie, gäbe er die zur Haftung führende Aktivität auf. Eine gesamtwirtschaftlich nützliche Aktivität, wie beispielsweise eine Gefälligkeitsauskunft,[668] könnte dadurch eventuell verhindert werden. 649

Fraglich ist, ob bei online abgeschlossenen Rechtsgeschäften dem Vertragspartner eine Vertrauensprämie gewährt wird. Die Bedeutung der wahrgenommenen Zuverlässigkeit eines Vertragspartners ist bei Online-Geschäften vermutlich höher als bei offline abgeschlossenen Rechtsgeschäften. Wegen des fehlenden persönlichen Kontakts können gewöhnliche vertrauensbildende Maßnahmen nicht stattfinden. Geschäftspartner sind daher bereit einen höheren Preis zu zahlen, wenn sie den anderen Vertragspartner kennengelernt haben oder ihn durch Bewertungen anderer Vertrauen schenken können.[669] Aus diesen Grund bieten viele Internet-Auktionsplattformen ein Reputationssystem an.[670] Ein Bieter mag vor einem Kauf bei einem Verkäu- 650

665 *Schäfer/C. Ott*[5], S. 559.
666 Ebd., S. 575 f.
667 Ebd., S. 575 f.
668 Ebd., S. 560.
669 Dazu ausführlich *Jehle*, S. 51.
670 Dazu oben Rn. 66.

fer mit keinen oder nur einer Handvoll Bewertungen zurückhaltend agieren, wohingegen er ohne zu Zögern bei einem Anbieter mit einer vier- oder fünfstelligen Anzahl an positiven Bewertungen mitbieten mag. Ein Anbieter mit hoher Reputation hat somit einen höheren Interessentenkreis, sodass er bei Versteigerungen wegen der erhöhten Nachfrage teurere Preise durchsetzen kann. Bei Rechtsgeschäften, die online abgeschlossen werden, existiert daher eine Vertrauensprämie, sodass die dritte Voraussetzung der Vertrauenshaftung gegeben ist.

(4) Höhe der Opportunismusprämie im Vergleich zur Vertrauensprämie

651 Die ökonomische vierte Voraussetzung der Vertrauenshaftung ist, dass die Opportunismusprämie höher ist als die Vertrauensprämie.[671] Lohnt es sich für einen Marktteilnehmer mehr sich opportunistisch zu verhalten, so ist eine Vertrauenshaftung ökonomisch sinnvoll. Opportunistisches Verhalten[672] kann sich bei Marktversagen wie dem „Market for Lemons“[673] ergeben. Bei der Unfähigkeit der Käufer die Qualität der Ware einzuschätzen oder bei wechselndem Kundenstamm und einer fehlenden Sanktionsmöglichkeit des Anbieters kann dieser opportunistisch handeln und die Qualität der Güter senken. Eine sich daraus ergebende Abwärtsspirale von sinkender Qualität und niedrigeren Preisen, eine adverse Selektion, kann sogar zum Marktversagen führen.[674] Dieser adversen Selektion mit der Gefahr des Marktversagens kann mit der Vertrauenshaftung dadurch begegnet werden, dass die Opportunismusprämie durch die Haftung unter die Vertrauensprämie gesenkt wird.

652 Im Internet ist das unternehmensspezifische Kapital, das aufgewendet werden muss, um Onlinehandel zu betreiben gering, sodass eine Voraussetzung für die Möglichkeit des opportunistischen Handelns grundsätzlich gegeben ist.[675] Die Marktein- und -austrittsbarrieren sind beim Onlinehandel ebenfalls niedrig. So kann es vorkommen, dass ein Anbieter bei eBay binnen weniger Tage in betrügerischer Absicht Waren anbietet, die er nicht

671 *Schäfer/C. Ott*[5], S. 562. Ähnlich *Fleischer*, S. 278 ff.
672 Dazu ausführlich *Williamson*, S. 54 ff.
673 Beschrieben von *Akerlof*, Quarterly Journal of Economics 84 (1970), 488, 488 ff. Dazu *Towfigh/Petersen*, S. 121; *Cooter/Ulen*[6], S. 41.
674 *Schäfer*, in: Ökonomische Probleme, 117, 127; *Towfigh/Petersen*, S. 121.
675 Vgl. *Schäfer/C. Ott*[5], S. 562.

zu liefern plant, und damit einen mittleren fünfstelligen Betrag einnimmt und verschwindet.[676]

Andererseits muss die Rolle des Vertrauens ebenfalls berücksichtigt werden. Dieses muss über einen langen Zeitraum erarbeitet werden und kann schnell verloren gehen. Die Reputation eines Anbieters ist eine entscheidende Komponente für den Onlinehandel.[677] Beim Onlinehandel ist die Sanktionsmöglichkeit gegenüber dem Anbieter bedeutend höher als beim Einzelhandel, weil es dem Kunden einfacher fällt, den Anbieter zu wechseln. Während beim Einzelhandel ein Kunde längere Wege in Kauf nehmen müsste, wenn er zu einem Konkurrenten wechseln möchte, sind beim Onlinehandel alle Anbieter unabhängig von ihrer geographischen Lage für den Kunden gleich gut erreichbar. Er kann mittels Mausklicks bestellen und erhält die Ware zur Haustür geliefert. Ein Onlinehändler kann zwar jederzeit einen neuen Account anlegen oder sogar Onlineshop eröffnen, um eine schlechte Reputation los zu werden. Und neue Teilnehmer im Markt des Onlinehandels werden von Kunden akzeptiert. Gleichwohl spielt das Vertrauen in einen Geschäftspartner sowie dessen Reputation im Onlinehandel eine große Rolle.[678] Viele Geschäftspartner wählen, wenn möglich, bekannte Anbieter. Die Vertrauensprämie ist bei online geschlossenen Rechtsgeschäften somit höher als die Opportunismusprämie, sodass die vierte Voraussetzung nicht gegeben ist. 653

(5) Zwischenergebnis

Von den vier rechtsökonomischen Voraussetzungen für eine Vertrauenshaftung liegt die Hälfte nicht vor. Aus rechtsökonomischer Sicht ist eine rechtsgeschäftliche Haftung für den Missbrauch von Zugangsdaten dem Grunde nach nicht notwendig. 654

bbb) Die Ausgestaltung einer Haftung aus rechtsökonomischer Sicht

Obwohl die Haftung rechtsökonomisch dem Grunde nach nicht erforderlich ist, soll dennoch auf eine rechtsökonomische Betrachtung der Ausgestal- 655

676 Wie bei *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08.
677 *Jehle*, S. 70.
678 Ebd., S. 51 ff.

tung einer möglichen Haftung eingegangen werden. Ist die wie bei § 172 Abs. 1 BGB gesetzlich vorgegeben oder ist das Vertrauen des Erklärungsempfänger wegen der Stärke des Rechtsscheins wie beispielsweise bei elektronischen Signaturen schutzwürdig, stellt sich die Frage nach der Ausgestaltung der Haftung auf Rechtsfolgenseite.

656 Bei einer Haftung für die willentliche Duldung eines *falsus procutrators* gibt es ökonomisch einen Zielkonflikt.[679] Die Haftung auf das negative Interesse kann nur eine optimale Abschreckung und dadurch einen optimalen Kontrollaufwand garantieren.[680] Die Haftung auf das positive Interesse hingegen leistet dies nicht, verhindert jedoch, dass Ressourcen fehlgeleitet und Schäden hochgetrieben werden.[681] Bei der Haftung für ein fahrlässiges Ermöglichen des Auftretens ohne Vertretungsmacht kann sowohl eine ex-ante- als auch ex-post-Effizienz durch die Haftung auf das negative Interesse hergestellt werden.[682]

cc) Alternative Möglichkeiten der Absicherung gegen Missbrauch

657 Bisher wurde betrachtet, wie sicher Authentisierungsmethoden sind und was Account-Inhaber sowie gegebenenfalls Plattformbetreiber zur Verhinderung des Missbrauchs unternehmen. Für die angemessene Verteilung der Risiken beim Missbrauch von Zugangsdaten im Internet ist jedoch entscheidend, was der Erklärungsempfänger als Absicherung gegen den Missbrauch tun kann. Er hat zwar keine Möglichkeiten einen Missbrauch zu verhindern, er kann sich jedoch durch verschiedene Maßnahmen dagegen absichern, dass er auf eine missbräuchlich abgegebene Willenserklärung vertraut. Dabei sind zwei Arten von Maßnahmen zu unterscheiden. Der Geschäftsgegner kann sowohl vor Empfang einer Willenserklärung als auch nach dem Empfang Maßnahmen ergreifen.

658 Vor dem Empfang der Willenserklärung kann der Geschäftsgegner bereits Kontakt mit dem späteren Vertragspartner haben. Solcher Kontakt kann zum einen durch ein Kennenlernen in der Offline-Welt bestehen sowie durch vorherige Erfahrungen bei Online-Geschäften. Wenn sich jemand beispielsweise telefonisch bei einem Vertragspartner nach einem Angebot

679 *Kötz/Schäfer*, S. 237.
680 Ebd., S. 237.
681 Ebd., S. 237.
682 Ebd., S. 238 ff.

erkundigt, der Vertragsschluss dann anschließend per mittels E-Mail ausgetauschten Willenserklärungen stattfindet, wie es bei geschäftlich handelnden Personen häufig vorkommt,[683] ist trotz der einfachen Manipulationsmöglichkeiten bei E-Mails[684] ein Missbrauch kaum möglich. Selbst wenn sich die Vertragspartner vorher nicht aus der analogen Welt kennen, sondern stets nur online kommuniziert haben, hat der Erklärungsempfänger anhand charakteristischer Merkmale der Erklärung Indizien dafür, ob sie vom Account-Inhaber stammt oder nicht. Wortwahl, Zeichensetzung, typische Ausdrücke oder spezifisches Wissen können dem Erklärungsempfänger Rückschlüsse auf den Urheber der Erklärung geben. Durch das Kontrahieren mit bekannten Vertragspartnern kann jeder Teilnehmer des Rechtsverkehrs Möglichkeiten eines Missbrauchs reduzieren.

659 Ob die Kommunikation zwischen sich bekannten Personen überwiegt oder im Internet anonyme Massenkommunikation vorherrscht,[685] ist nicht entscheidend. Auch bei einer anonymen Massenkommunikation hat der Erklärungsempfänger Möglichkeiten sich gegen Missbrauch abzusichern. Jedem Teilnehmer am Rechtsverkehr steht es frei, für jedes Rechtsgeschäft eine Authentisierungsmethode zu wählen, die seinen Sicherheitsvorstellungen entspricht.[686] Bei der Wahl kann der Teilnehmer die Bedeutung und den Wert des Rechtsgeschäfts und eine unsichere, günstige oder eine sicherere, kostenaufwendigere Authentisierungsmethode wählen. Die sehr kostengünstige und leicht zu fälschende E-Mail steht am Anfang, gefolgt von der leicht sichereren Stufe der passwortgeschützten Erklärung. Darüber hinaus stehen mit der aufwendigeren und tendenziell kostspieligen elektronischen Signatur, die in vier unterschiedlich sicheren Formen existiert,[687] verschiedene Abstufungen an Sicherheit und Kostenaufwand zur Verfügung, auf deren qualifizierten Formen der Erklärungsempfänger ein schützenswertes Vertrauen hat.[688] Der Teilnehmer am Rechtsverkehr kann daher vor Anbahnung eines Vertrags die Wahl treffen, wie sicher die Authentisierungsmethode sein soll, und für den konkreten Zweck zu unsichere Authentisierungsmethoden ausschließen.

---

683 Vgl. *Hoeren*, CR 2002, 295, 296.
684 Dazu oben Rn. 212.
685 Letzteres behauptet *Bösing*, S. 43.
686 So auch *Borges*, NJW 2011, 2400, 2402; *Roßnagel*, MMR 2003, 164, 170.
687 Zu den Formen der elektronischen Signatur oben Rn. 74.
688 Oben Rn. 578 ff.

660 Ferner kann der Teilnehmer am Rechtsverkehr sich vorab über die Reputation des späteren Vertragspartners informieren. Im und außerhalb des Internets bestehen zahlreiche Möglichkeiten sich über die Reputation eines Geschäftspartners zu informieren wie Testberichte, Meinungen von Bekannten oder Kundenforen.[689] Bei Internet-Auktionsplattformen gibt es regelmäßig ein institutionalisiertes Reputationssystem, das mittels zweier Zahlen, der Anzahl an positiven Bewertungen sowie der Prozentzahl an positiven Bewertungen gemessen an den gesamten Bewertungen, die Vertrauenswürdigkeit eines Vertragspartners einschätzbar zu machen versucht.[690]

661 Ist dem Handelnden die Reputation eines potentiellen Vertragspartners nicht ausreichend genug, hat er die Möglichkeit auf einer Identitätsüberprüfung zu bestehen. Diese kann er beispielsweise mittels des elektronischen Identitätsnachweises[691] oder des PostIdent-Verfahrens[692] machen. Ebenso kann sich der Handelnde Auskünfte über die Solvenz des potentiellen Vertragspartners beispielsweise über Banken oder die Schufa besorgen.

662 Der Empfänger einer Willenserklärung kann stets rückfragen, ob die Willenserklärung vom Account-Inhaber selbst oder von einem Dritten mit dessen Einverständnis abgegeben wurde. Stellt der Empfänger der Willenserklärung diese Rückfrage auf demselben Kommunikationsweg, auf dem er die Erklärung erhalten hat, schützt er sich nur minimal gegen Missbrauch. Bricht er jedoch das Medium und stellt die Rückfrage telefonisch oder postalisch, besteht eine große Chance einen möglichen Missbrauch aufzudecken.[693] Der Medienbruch stellt dabei zwar ein Hemmnis dar,[694] das das online abgewickelte Geschäft verlangsamt. Er bietet jedoch eine effektive und kostengünstige Methode, Schäden durch den Missbrauch von Zugangsdaten zu reduzieren. Der Behauptung, dass im elektronischen Rechtsverkehr vielfach eine solche Möglichkeit fehle,[695] kann nicht zugestimmt werden. Fehlen dem Erklärungsempfänger tatsächlich solche Möglichkeiten und möchte er sich stets durch Rückfragen absichern, muss er in letzter Konsequenz von einem konkreten Rechtsgeschäft Abstand nehmen.

---

689 *Jehle*, S. 69 f.
690 Oben Rn. 64.
691 Dazu oben Rn. 88.
692 Siehe oben Rn. 613.
693 Siehe *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 729. Dies geschah beispielsweise bei *LG Frankfurt*, Urteil v. 15. 12. 2004, 3-13 O 28/04 (nicht veröffentlicht).
694 *Bösing*, S. 43; *Knopp/Wilke/Hornung/Laue*, MMR 2008, 723, 725.
695 *Herresthal*, K&R 2008, 705, 707; *ders.*, in: *Taeger/Wiebe*, 21, 31.

Eine weitere Möglichkeit für den Vertragspartner besteht darin, auf der Vorleistung des Geschäftsgegners zu bestehen. Bei Online-Auktionen sichert sich der Verkäufer regelmäßig dadurch ab, dass der Käufer in Vorleistung treten muss. Verkäufer begegnen dadurch der Problematik von Spaßbietern, sodass sie höchstens den Schaden in Höhe des negativen Interesses, also den Aufwand das Angebot einzustellen, tragen müssen. 663

Letztlich hat der Teilnehmer am Rechtsverkehr noch die Möglichkeit, die Identität des Geschäftspartners außer Acht zu lassen und sich gegen einen Missbrauch zu versichern. Solange der Teilnehmer seine Leistung sicher erhält oder wenigstens seine Gegenleistung behält, kann ihm die Identität des Gegenübers oder die Berechtigung eines Dritten in seinem Namen zu handeln egal sein.[696] Der Verkäufer kann beispielsweise das Delkredererisiko auf einen Zahlungsdiensteanbieter verlagern. Online-Händler verlagern das Delkredererisiko häufig auf Kreditkarten-Acquiring-Unternehmen, die dieses Risiko aufgrund des Gesetzes der großen Zahlen zu tragen haben.[697] Selbst Privatpersonen haben Möglichkeiten, das Delkredererisiko abzusichern. PayPal bietet Verkäufern beispielsweise an, unter bestimmten Voraussetzungen das Delkredererisiko für über das System empfangene Zahlungen zu übernehmen.[698] Ebenso haben Käufer die Möglichkeit sich von PayPal gegen das Risiko abzusichern, dass der Verkäufer trotz Zahlungseingang die Ware nicht liefert.[699] Das Risiko die Gegenleistung nicht zu erhalten, können die Vertragsparteien auch durch die Einschaltung eines Treuhänders absichern. 664

Viele der Möglichkeiten der Absicherung gegen den Missbrauch haben gemeinsam, dass sie den elektronischen Geschäftsverkehr, der sich durch seine Geschwindigkeit und ständige Verfügbarkeit auszeichnet, verlangsamen. Möchte ein Teilnehmer am Rechtsverkehr von den Chancen der Geschwindigkeit des Online-Rechtsverkehrs profitieren, so muss er auch das damit einhergehende Missbrauchsrisiko tragen. 665

696 Vgl. *M. Köhler/Arndt/Fetzer*[7], Rn. 172.

697 *BGH*, Urteil v. 16. 4. 2002, XI ZR 375/00 – BGHZ 150, 286, 297 ff. sowie oben Rn. 342.

698 Vgl. *PayPal*, Verkäuferschutzrichtlinie.

699 Vgl. *PayPal*, Käuferschutzrichtlinie.

dd) Zwischenergebnis

666 Der Verkehrsschutz gebietet hier weder aus teleologischen noch aus rechtsökonomischen Erwägungen eine Rechtsscheinhaftung zu etablieren, wenn deren Voraussetzungen eigentlich nicht vorliegen.

e) Widerspruch zur herrschenden Ansicht bei Weitergabe der Zugangsdaten

667 Bei Ablehnung eines Rechtsscheintatbestandes kann bei Weitergabe[700] der Zugangsdaten eine Haftung des Account-Inhabers nicht begründet werden. Im Ergebnis wird jedoch herrschend angenommen, dass der Account-Inhaber nach Weitergabe der Zugangsdaten für einen Missbrauch hafte.[701] Dieses Ergebnis wird zum Teil über die Duldungsvollmacht[702] zum Teil über eine analoge Anwendung des § 172 Abs. 1 BGB[703] begründet. Beide Lösungen zur Begründung der Haftung setzen voraus, dass ein Rechtsscheintatbestand dahingehend besteht, dass der Account-Inhaber oder ein Dritter mit seinem Einverständnis eine Erklärung über den Account abgegeben hat. Dieser Rechtsscheintatbestand existiert jedoch weder bei der hier vertretenen Anwendung der allgemeinen Rechtsscheinhaftung noch nach herrschender Meinung bei Anwendung der Anscheinsvollmacht.[704] Die Konstellationen mit und ohne Weitergabe unterscheiden sich nicht im vom Geschäftsgegner wahrnehmbaren Rechtsschein. Er erhält in beiden Fällen eine Erklärung, die aussieht, als habe sie der Account-Inhaber abgegeben. Der Erklärung kann der Empfänger jedoch nicht ansehen, wer sie tatsächlich abgegeben hat. Nur im für den Erklärungsempfänger nicht erkennbaren Verhalten des Account-Inhabers besteht bei den Konstellationen ein Unterschied. Dieses Verhalten des Account-Inhabers ist Anknüpfungspunkt für eine unterschiedliche Beurteilung der Zurechnung in den beiden Konstellationen. Der Rechtsscheintatbestand ist mit und ohne Weitergabe der Zugangsdaten der Gleiche. Die beiden herrschenden Ansichten zur Haftung bei Weitergabe und ohne Weitergabe widersprechen sich daher.

---

700 Zum Begriff der Weitergabe oben Rn. 295.
701 Oben Rn. 293.
702 Oben Rn. 297 ff.
703 Oben Rn. 303 ff.
704 Oben Rn. 371 ff.

Vor diesem Hintergrund ist zu überlegen, in welche Richtung dieser Widerspruch aufzulösen ist. Teilweise wird gefordert, man müsse in beiden Konstellationen den Rechtsschein anerkennen, weil ansonsten die Haftung bei bewusster Weitergabe nicht begründet werden kann.[705] Die bewusste Schaffung der Möglichkeit einer Identitätstäuschung rechtfertige die Haftung des Account-Inhabers.[706] Weder aus rechtlichen noch aus rechtsökonomischen Gründen ist diese angestrebte Risikoverteilung jedoch zu rechtfertigen.[707] Für eine Anerkennung des Rechtsscheintatbestandes in beiden Konstellationen spreche ferner, dass ohne eine Haftung bei Weitergabe ansonsten eine Anreizstruktur fehle, die Weitergabe von Passwörtern zu unterlassen.[708] Dagegen spricht jedoch, dass der Account-Inhaber auch ohne eine Rechtsscheinhaftung Anreize hat seine Zugangsdaten geheim zu halten. Beispielsweise hat er ein Interesse daran, dass kein Dritter seine E-Mails lesen kann oder die Reputation seines eBay-Accounts durch nicht ernst gemeinte Angebote oder nicht ernst gemeintes Mitbieten zerstört. 668

Überzeugend ist hingegen, den Widerspruch dahin gehend aufzulösen, dass ein Rechtsscheintatbestand sowohl in der Konstellation ohne Weitergabe als auch mit Weitergabe der Zugangsdaten gleichermaßen abgelehnt wird. Bei einer rein wissensbasierten Authentisierungsmethode besteht ein Rechtsscheintatbestand somit in beiden Konstellationen nicht.[709] Diesen Rechtsscheintatbestand bei Weitergabe zu bejahen, entstammt Billigkeitserwägungen, die sich dogmatisch nicht rechtfertigen lassen. Nur die Zurechnung lässt sich bei der Weitergabe der Zugangsdaten überzeugend begründen. Durch die Annahme einer Haftung des Account-Inhabers schafft die herrschende Meinung dadurch bei Weitergabe der Zugangsdaten eine Rechtsscheinhaftung ohne Rechtsschein.[710] Die herrschende Meinung bezüglich der Haftung bei Weitergabe der Zugangsdaten[711] ist daher abzulehnen. Mangels eines Rechtsscheintatbestandes haftet der Account-Inhaber dem Geschäftsgegner auch bei Weitergabe der Zugangsdaten zu einem Ac- 669

705 *Borges*, NJW 2011, 2400, 2402.
706 Ebd., 2402.
707 Oben Rn. 625 ff.
708 *Borges*, NJW 2011, 2400, 2402.
709 Oben Rn. 544 ff.
710 Dies ist den Ansichten, die eine Haftung bei rein wissensbasierter Authentisierung bejahen vorzuwerfen oben Rn. 365, 380.
711 Oben Rn. 293.

count nicht, wenn der Account eine rein wissensbasierte Authentisierungsmethode verwendet.

f) Zwischenergebnis

670 Ein Rechtsscheintatbestand besteht beim Missbrauch von Zugangsdaten im Internet nur, wenn eine sichere Authentisierungsmethode gewählt wurde und der Account-Inhaber bei Erstellen des Accounts zuverlässig überprüft wurde. Eine ausreichend sichere Authentisierungsmethode stellt die Zwei-Faktor-Authentisierung dar.[712] Eine rein wissensbasierte Authentisierung bietet hingegen keine hinreichende Gewähr dafür, dass der Account-Inhaber gehandelt hat.[713] Die Zuordnung zwischen virtueller Identität des Accounts und dem Namensträger muss zuverlässig durch die Überprüfung seiner Identität vorgenommen werden.[714] Dafür reicht eine Plausibilitätskontrolle,[715] der Abgleich der Daten mit der Schufa[716] oder die Zusendung eines Briefes nicht aus.[717] Die Anerkennung eines Rechtsscheintatbestandes für rein wissensbasierte Authentisierungsmethoden ist auch nicht aus rechtsökonomischen Erwägungen[718] oder zur angemessenen Verteilung der Risiken erforderlich.[719]

3. Zurechenbarkeit

671 Der Rechtsscheintatbestand muss dem Account-Inhaber auch zurechenbar sein. Objektiv ist dafür erforderlich, dass er eine Möglichkeit hat, diesen zu zerstören. Subjektiv muss ihm der Rechtsschein je nach vertretener Ansicht nach dem Verschuldens- oder Risikoprinzip zurechenbar sein.[720]

712 Oben Rn. 534 ff.
713 Oben Rn. 544 ff.
714 Oben Rn. 595 ff.
715 Oben Rn. 607 ff.
716 Oben Rn. 608.
717 Oben Rn. 617.
718 Oben Rn. 635 ff.
719 Oben Rn. 625 ff.
720 Oben Rn. 233 ff.

a) Möglichkeit den Rechtsschein zu zerstören

Ein Rechtsscheintatbestand kann nur dann zurechenbar sein, wenn derjenige, der den Rechtsscheintatbestand geschaffen hat, eine Möglichkeit hat, den Rechtsschein zu beseitigen.[721] Der Namensträger muss beim Missbrauch von Zugangsdaten im Internet die Möglichkeit haben, den Rechtsscheintatbestand zu zerstören, also zu verhindern, dass ein Dritter mit seinem Account handelt. Diese Anforderungen kann beispielsweise durch eine Sperrmöglichkeit des Accounts erfüllt werden.[722] Diese Sperrmöglichkeiten sichern auch das Authentisierungsverfahren ab, denn sie dienen ähnlich wie die Sicherung der Zugangsdaten dafür, dass nur der Account-Inhaber mit dem Account handeln kann.[723] Nur wenn der Account dem Account-Inhaber zu jeder Zeit die Möglichkeit bietet, den Account zu sperren oder wieder alleinige Kontrolle über ihn zu übernehmen, kommt die Zurechnung eines möglichen Rechtsscheintatbestand in Frage. Die Zerstörung des Rechtsscheins im digitalen Verkehr ist nicht immer möglich, so kann beispielsweise das Revidieren einer digital signierten Willenserklärung nicht sicher durch ihr Löschen erfolgen.[724] 672

Aus dem Grund, dass der Account-Inhaber eine Möglichkeit haben muss, einen vorhanden Rechtsschein zu zerstören, kommt die Zurechnung nicht in Betracht, wenn es Angreifern durch Schwachstellen beim Authentisierungsnehmer möglich ist, ohne die Zugangsdaten sich in den Account des Inhabers einzuloggen.[725] Sollte das Authentifizierungssystem des Authentisierungsnehmers durch Schwachstellen der Server-Infrastruktur oder SQL-Injections, durch Cross-Site-Scripting (XSS) kompromittierbar sein, scheidet somit eine Zurechnung zum Account-Inhaber aus. Ebenso scheidet eine Zurechnung zu ihm aus, wenn ein Angreifer ohne Zutun des Account-Inhabers an die Zugangsdaten gelangt ist. Das kann zum einen durch Brute-Force-Attacken[726] oder durch die unauthorisierte Weitergabe der Zugangsdaten durch den Authentisierungsnehmer[727] erfolgen. 673

721 Siehe oben Rn. 246.
722 *Redeker*, IT-Recht[5], Rn. 877.
723 Die Sperrmöglichkeiten bei verschiedenen Authentisierungsmethoden wurden daher schon im Rahmen deren Sicherheit behandelt, vgl. oben Rn. 534 ff.
724 *provet/GMD*, S. 132.
725 Zu diesen Schwachstellen oben Rn. 215 ff.
726 Dazu oben Rn. 181.
727 Dazu oben Rn. 221.

b) Beschränkung auf grobe Fahrlässigkeit?

674 Mit unterschiedlichen Anknüpfungspunkten kann erwogen werden, dass der Account-Inhaber nur bei Vorliegen von grober Fahrlässigkeit beim Missbrauch der Zugangsdaten haften muss. Diese Erwägungen setzen zunächst voraus, dass die Zurechnung nach dem Verschuldensprinzip[728] erfolgt, weil ansonsten kein Raum für einen Verschuldensmaßstab vorhanden ist. Zunächst ist die Erwägung aufzugreifen, dass sich eine Rechtsscheinhaftung im Bürgerlichen Recht nur bei Vorliegen von grober Fahrlässigkeit rechtfertigt.[729] Die scharfe Rechtsfolge der Erfüllungshaftung rechtfertige sich im Bürgerlichen Recht im Gegensatz zum Handelsrecht nur bei Erfüllung dieser strengen Voraussetzung. Liege diese nicht vor, komme nur eine Haftung aus *culpa in contrahendo* in Betracht.[730] Es mag zwar dem Rechtsempfinden entsprechen, die scharfe Rechtsfolge der Erfüllungshaftung nur bei Vorliegen der strengeren Voraussetzung der groben Fahrlässigkeit zu gewähren. Dogmatisch lässt sich diese Ansicht jedoch kaum begründen. Die gesetzlichen Rechtsscheintatbestände setzen eine willentliche Schaffung voraus.[731] Wenn mit einer *BGH*-Entscheidung begründet wird, dass dort die Erfüllungshaftung wegen einfacher Fahrlässigkeit verneint wurde,[732] begründet dies nicht eine Haftung auf das positive Interesse bei grober Fahrlässigkeit. In der Entscheidung wird klargestellt, dass § 172 Abs. 1 BGB mit dem „Aushändigen“ die willentliche Schaffung eines Rechtsscheintatbestandes voraussetzt und unterhalb dieser Voraussetzungen nur eine Haftung nach den „Grundsätzen, wie sie zu der Haftung auf das negative Interesse entwickelt worden sind“ in Betracht komme.[733]

675 Andere Überlegungen dagegen wollen den Haftungsmaßstab der groben Fahrlässigkeit anwenden. Wenn mangels Vorsatzes die Haftung auf das positive Interesse scheitert solle im Rahmen einer Haftung aus *culpa in contrahendo* der Verschuldensmaßstab auf grobe Fahrlässigkeit beschränkt werden.[734] Systematisch solle dabei vorsichtig der § 675v Abs. 2 BGB her-

728 Dazu oben Rn. 237.
729 *Hübner*[2], Rn. 1289.
730 Ebd., Rn. 1289.
731 Dazu oben Rn. 249.
732 *Hübner*[2], Rn. 1289; unter Verweis auf *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13.
733 *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13, 14 f.
734 *Oechsler*, MMR 2011, 631, 633, ihm folgend *Linardatos*, Jura 2012, 53, 55; *Sonnentag*, WM 2012, 1614, 1619 f.

angezogen werden.[735] Dieser finde beim Missbrauch von Kreditkarten im Mail-Order-Verfahren Anwendung, was mit Zugangsdaten im Internet vergleichbar sei.[736] Viele Accounts im Internet haben mit dem Mail-Order-Verfahren gemeinsam, dass eine rein wissensbasierte Authentisierungsmethode verwendet wird. Wenn zur Begründung darauf auf die hohe Missbrauchsanfälligkeit sowie die komplexen technischen Rahmenbedingungen abgestellt wird,[737] kann dem nur eingeschränkt zugestimmt werden. Zugangsdaten im Internet funktionieren über einen komplexen technischen Ablauf, das Mail-Order-Verfahren jedoch nicht. Zwar wird mit Verweis auf die Intention des Gesetzgebers[738] verneint, dass Kreditkarten im Mail-Order-Verfahren ein Zahlungsauthentifizierungsinstrument im Sinne des § 1 Abs. 5 ZAG, wie von § 675v BGB vorausgesetzt, seien.[739] Im Ergebnis besteht jedoch Einigkeit darin, dass § 675v BGB auch bei Kreditkarten im Mail-Order-Verfahren angewendet wird.[740] Insbesondere ist jedoch § 675v BGB auf den Missbrauch beim Online-Banking anwendbar.[741] Beim Online-Banking handelt es sich sogar um Zugangsdaten im Internet, sodass der Rechtsgedanke des § 675v BGB überzeugend zur Lösung des Missbrauchs von anderen Zugangsdaten im Internet herangezogen werden kann.

676 Folgend soll daher geprüft werden, ob die Voraussetzungen einer Analogie, eine planwidrige Gesetzeslücke sowie eine vergleichbare Interessenlage,[742] vorliegen. Die planwidrige Gesetzeslücke liegt in Form einer nachträglichen Regelungslücke vor.[743] Fraglich erscheint jedoch, ob die Interessenlage vergleichbar ist. Dafür spricht zunächst, dass beim Online-Banking ebenso wie bei anderen Accounts im Internet Zugangsdaten verwendet werden. Man könnte somit einen Erst-Recht-Schluss ziehen. § 675u Abs. 1 BGB schließt einen Aufwendungsersatzanspruch der Bank gegen ihren Kunden aus. Die Banken verwenden teilweise AGB, die den Kunden bei fahrlässigem Umgang mit den Zugangsdaten in die Haftung nehmen.[744] § 675v Abs. 2 BGB gebietet eine Beschränkung der Haftung auf Fälle von

735 *Oechsler*, MMR 2011, 631, 633.
736 Ebd., 633.
737 So ebd., 633.
738 Begr. ZAG, BT-Drucks. 14/11613, S. 36.
739 *Casper/Pfeifle*, WM 2009, 2343, 2347; dagegen *Oechsler*, WM 2010, 1381, 1382.
740 *Casper/Pfeifle*, WM 2009, 2343, 2345 f.; *Oechsler*, WM 2010, 1381, 1328 f.
741 Dazu ausführlich *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 92 ff.
742 Oben Rn. 329 ff.
743 Dazu oben Rn. 330.
744 *Casper*, in: MüKo-BGB[6], § 675v Rn. 6.

grober Fahrlässigkeit. Daraus könnte geschlossen werden, dass wenn schon privatautonom der Account-Inhaber sich nicht verpflichten kann für den leicht fahrlässigen Umgang mit Zugangsdaten zu haften, dies erst recht im Rahmen der Rechtsscheinhaftung gelten müsse.

677 Gegen die vergleichbare Interessenlage spricht, dass § 675v BGB auf die Besonderheiten der Interessen der Beteiligten beim Einsatz von Zahlungsauthentisierungsinstrumenten zugeschnitten ist und sich nicht übertragen lässt. Erstens wirkt die Beschränkung der Haftung auf grobe Fahrlässigkeit nach § 675u Abs. 2 BGB für sämtliche Authentisierungsmethoden, also sowohl für rein wissensbasierte als auch für Zwei-Faktor-Methoden. Während bei rein wissensbasierten Authentisierungsmethoden ein Rechtsschein nicht vorliegt,[745] sodass dieser auch bei grober Fahrlässigkeit nicht zugerechnet werden kann, besteht beim Einsatz der Zwei-Faktor-Authentisierung ein Rechtsscheintatbestand, bei dem eine Beschränkung auf grobe Fahrlässigkeit den Account-Inhaber entlastet. Zweitens sind die Zahlungsauthentisierungsinstrumente ein häufiges Ziel von Angreifern. Bei ihnen handelt es sich um ein Massengeschäft und sie werden häufig missbraucht. § 675v BGB trifft für diese besondere Konstellation eine Regelung, die die Interessen von beiden Seiten berücksichtigt und Rechtssicherheit schafft. Diese Interessenlage weicht von Zugangsdaten für andere Accounts im Internet ab.

678 Drittens und entscheidend schafft § 675v BGB eine ausdifferenzierte Lösung, die als Gesamtkonzept zu verstehen ist. Zwar wird der Bankkunde durch die Beschränkung der unbegrenzten Haftung auf grobe Fahrlässigkeit (§ 675v Abs. 2 BGB) entlastet. Im Gegenzug wird er beim Verlust von Besitz-Authentisierungsmitteln auf einen begrenzten Geldbetrag mit einer verschuldensunabhängigen Haftung belastet (§ 675v Abs. 1 S. 1 BGB). Dieses Gesamtkonzept lässt sich jedoch nicht übertragen. Eine verschuldensunabhängige Haftung für den Missbrauch von Zugangsdaten im Internet lässt sich nicht begründen. Die mit der verschuldensunabhängigen begrenzten Haftung einhergehende Beschränkung auf grobe Fahrlässigkeit für die unbegrenzte Haftung lässt sich wertungsstimmig nicht isolieren. Eine vergleichbare Interessenlage liegt somit nicht vor. § 675 Abs. 2 BGB lässt sich somit nicht auf Zugangsdaten zu anderen Accounts im Internet übertragen.[746]

---

745 Oben Rn. 544 ff.

746 So auch *Borges*, NJW 2012, 2385, 2387; *Borges/Schwenk/Stuckenberg/Wegener*, S. 294; **a.A.** *Hossenfelder*, Pflichten von Internetnutzern, S. 255.

c) Maßstab der Zurechnung

Die willentliche Schaffung eines Rechtsscheintatbestandes begründet stets dessen Zurechenbarkeit.[747] Dies zeigt sich unter anderem in der Wertung des § 172 Abs. 1 BGB,[748] der ein Aushändigen der Vollmachtsurkunde erfordert.[749] Die Weitergabe der Zugangsdaten begründet daher die Zurechenbarkeit eines etwa vorhandenen Rechtsscheintatbestandes.[750] **679**

Sodann stellt sich die Frage, ob eine Zurechnung auch ohne willentliche Weitergabe der Zugangsdaten erfolgen werden kann.[751] Dafür spräche, dass jeder Teilnehmer am Rechtsverkehr für das aus seiner Risikosphäre stammende zurechenbare Verhalten Dritter einzustehen habe.[752] **680**

Andererseits könnte die Zurechnung des Rechtsscheintatbestandes auf die willentliche Weitergabe der Zugangsdaten beschränkt sein.[753] Erstens spricht dafür, dass die gesetzlichen Rechtsscheinvollmachten in §§ 170 ff. BGB stets eine willentliche Schaffung des Rechtsscheintatbestandes voraussetzen.[754] Zweitens ist eine Rückkopplung der konkreten Willenserklärung an den Account-Inhaber schwierig. Bei abhandengekommenen Willenserklärungen[755] sowie dem fehlenden Erklärungsbewusstsein[756] hat der Geschäftsherr den Großteil der Erklärung selbst geschaffen. Der Rechts- **681**

747 Oben Rn. 249.

748 Darauf begründen einige ihre Meinung zur Haftung für den Missbrauch von Zugangsdaten im Internet, dazu oben Rn. 303 ff.

749 Oben Rn. 314.

750 Vgl. nur *Oechsler*, MMR 2011, 631, 632; *Reese*, S. 76; *Sonnentag*, WM 2012, 1614, 1617; *Ultsch*, DZWir 1997, 466, 473.

751 So *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 518 f.; *Herresthal*, K&R 2008, 705, 708 f.; *ders.*, in: *Taeger/Wiebe*, 21, 37; *Kuhn*, S. 230 ff.; *Stöber*, EWiR 2011, 521, 552; *ders.*, JR 2012, 225, 229; *Verse/Gaschler*, Jura 2009, 213, 215. Für die elektronische Signatur *Bergfelder*, S. 390; *Dörner*, AcP 202 (2002), 363, 392 f.; *M. Köhler/Arndt/Fetzer*[7], Rn. 227; *Reese*, S. 133 ff.; *Rieder*, S. 284 ff.; *Spiegelhalder*, S. 160 ff.

752 *Herresthal*, K&R 2008, 705, 708 f.; *ders.*, in: *Taeger/Wiebe*, 21, 37.

753 So *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 181; *Faust*, BGB AT[3], § 26 Rn. 41; *M. Köhler/Arndt/Fetzer*[7], Rn. 324; *Langenbucher*, S. 146; *Linardatos*, Jura 2012, 53, 55; *Redeker*, IT-Recht[5], Rn. 875; *Rieder*, S. 315; *Ultsch*, DZWir 1997, 466, 473. Für die Zurechnung nur nach einem erweitertem Weitergabebegriff *Borges*, Elektronischer Identitätsnachweis, S. 136; *ders.*, NJW 2011, 2400, 2403; *Sonnentag*, WM 2012, 1614, 1618.

754 Für § 172 Abs. 1 BGB oben Rn. 314.

755 Oben Rn. 476.

756 Oben Rn. 472.

verkehr bekommt seine Handlungen oder deren Ergebnisse unmittelbar mit, sodass ein schutzwürdiges Vertrauen darin besteht. Dies ist bei Zugangsdaten im Internet nicht der Fall. Die Weitergabe oder das Ausspähen der Zugangsdaten ist für den Rechtsverkehr nicht einsehbar und bei ihm fehlt es am rechtsgeschäftlichen Bezug. Ferner zeigen die Wertungen aus den sog. Überweisungsfällen bei Bankgeschäften, dass es an der notwendigen Rückkopplung fehlt. Führt eine Bank eine Überweisung doppelt aus, fehlt es an einem Verhalten des Bankkunden mit Bezug auf das konkrete Rechtsgeschäft, an das angeknüpft werden kann.[757] Ebenso fehlt dieses Verhalten des Account-Inhabers beim Missbrauch der Zugangsdaten.

682 Drittens zeigt die Wertung des § 935 BGB, dass das fahrlässige Abhandenkommen von Sachen nur bei überragendem Verkehrsschutz eine Zurechnung begründet. Regelmäßig muss der Eigentümer einer Sache diese willentlich aus der Hand geben, damit ein gutgläubiger Erwerb aufgrund des Rechtsscheins des Besitzes möglich ist (vgl. § 935 Abs. 1 S. 1 BGB). Nur bei Wertpapieren bedarf es dieser Zurechnung zum Eigentümer nicht, sodass diese auch bei Abhandenkommen gutgläubig erworben werden können (§ 935 Abs. 2 BGB). Ein den Wertpapieren entsprechendes Verkehrsschutzbedürfnis besteht bei Vollmachtsurkunden[758] und Blanketten nicht.[759] Diese Erwägungen treffen ebenso auf Zugangsdaten im Internet zu, sodass die Wertung des § 935 BGB für eine Beschränkung der Zurechnung auf die Weitergabe der Zugangsdaten spricht.

683 Viertens lässt die Beschränkung der Zurechnung auf die willentliche Schaffung durch einen Erst-Recht-Schluss zu § 172 Abs. 1 BGB begründen. Der Rechtsschein des § 172 Abs. 1 BGB ist je nach verwendeter Authentisierungsmethode leicht bis erheblich stärker als ein solcher bei Zugangsdaten im Internet.[760] Bei diesem starken Rechtsscheintatbestand ist die Zurechnung nach herrschender Ansicht nur bei willentlicher Übergabe der Vollmachtsurkunde möglich.[761] Wenn die Zurechnung beim stärkeren Rechtsscheintatbestand schon auf die willentliche Schaffung begrenzt ist, muss dies erst recht für den schwächeren Rechtsscheintatbestand der Zugangsdaten im Internet gelten. Die Zurechnung ist somit begrenzt auf die willentliche Schaffung des Rechtsscheintatbestandes. Eine Zurechnung

757 Oben Rn. 511.
758 Oben Rn. 317.
759 Oben Rn. 327.
760 Oben Rn. 345 ff.
761 Dazu und zur Gegenauffassung oben Rn. 315.

kommt somit nur in Betracht, wenn der Account-Inhaber die Zugangsdaten weitergeben hat.

d) Fälle der Zurechnung

Für das Risiko- und Verschuldensprinzip soll untersucht werden, wie unterschiedliche Fallkonstellationen zu beurteilen sind. Bei dieser Untersuchung wird unterstellt, dass nicht nur die willentliche Weitergabe der Zugangsdaten eine Zurechnung begründet,[762] weil ansonsten bei keiner der folgenden Konstellationen eine Zurechnung zu bejahen wäre. Ebenso soll mit untersucht werden, ob ein Verhalten grob fahrlässig ist, worauf die Zurechnung nach einer hier abgelehnten Meinung beschränkt ist.[763] **684**

Nach dem Risikoprinzip[764] hat der Account-Inhaber für alle Risiken einzustehen, die er eher beherrschen kann als der andere Teil.[765] Nach dem Verschuldensprinzip[766] kommt eine Zurechnung bei Abhandenkommen in Betracht, wenn der Account-Inhaber schuldhaft, also fahrlässig im Sinne des § 276 Abs. 2 BGB, umgegangen ist. Bestehen gesetzliche Regelungen über den Umgang mit den Zugangsdaten, wie die Obliegenheit der Geheimhaltung bei der elektronischen Signatur (vgl. § 5 Abs. 4 S. 2 SigG), richtet sich der Sorgfaltsmaßstab nach diesen. Bestehen keine gesetzlichen oder vertraglichen Regeln zur Aufbewahrung der Zugangsdaten, richtet sich das Verschulden nach einem „Verschulden gegen sich selbst“.[767] Einschränkend ist nach dem Verschuldensprinzip zu fordern, dass der Account-Inhaber mit einem Missbrauch gerechnet hat oder bei pflichtgemäßem Verhalten hätte rechnen müssen.[768] **685**

Für eine Zurechnung reicht noch nicht die Einrichtung des Accounts.[769] Damit wird lediglich die Möglichkeit zur Kommunikation geschaffen. Für **686**

762 Entgegen der hier vertretenen Auffassung, oben Rn. 679 ff.
763 Oben Rn. 674.
764 Dazu oben Rn. 243.
765 Im Rahmen des Missbrauchs von Zugangsdaten vertreten von *Spiegelhalder*, S. 153; *Reese*, S. 133 ff.; *Rieder*, S. 230 ff.
766 Dazu oben Rn. 237.
767 Siehe oben Rn. 238.
768 *Borges*, NJW 2011, 2400, 2403; *Herresthal*, K&R 2008, 705, 709; *ders.*, in: *Taeger/Wiebe*, 21, 38; *Stöber*, EWiR 2011, 521, 552; *ders.*, JR 2012, 225, 229.
769 *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676, 1677; *Borges*, in: Internet-Auktion, 214, 216.

eine Zurechnung ausreichend ist hingegen, wenn der Account-Inhaber nach Kenntnis vom Missbrauch der Zugangsdaten nichts gegen einen weiteren Missbrauch unternimmt.[770]

aa) Sorgfalts- und Verkehrspflichten des Account-Inhabers

687 Bevor Einzelfälle der Zurechnung für die unterschiedlichen Möglichkeiten, die Zugangsdaten zu missbrauchen,[771] untersucht werden, sollen allgemeine Sorgfaltspflichten des Account-Inhabers bezüglich der Absicherung seines Rechners betrachtet werden, weil sie für eine Zurechnung nach dem Verschuldensprinzip[772] relevant sind. Insgesamt ist der Umfang der Sorgfaltspflichten bezüglich der IT-Sicherheit noch nicht genau herausgearbeitet.[773] Nachfolgend werden daher Anforderungen an die Account-Inhaber betrachtet, die diesen aus unterschiedlichen Gründen auferlegt werden. Sowohl deliktische Verkehrspflichten als auch Sorgfaltspflichten innerhalb von Vertragsbeziehungen werden herangezogen.

688 Grundsätzlich stellt sich die Frage, wie hoch die Anforderungen an einen Account-Inhaber sind. Fachspezifisches IT-Hintergrundwissen kann von ihm nicht verlangt werden. Vielmehr ist auf einen durchschnittlichen Nutzer abzustellen, der über solches Wissen nicht verfügt.[774] Insgesamt darf der Sorgfaltsmaßstab nicht all zu hoch angesetzt werden, weil die elektronischen Prozesse der Datenverarbeitung nur mit besonderem Fachwissen verstanden werden können. Im Gegensatz zu anderen Bereichen wie dem Straßenverkehr finden die Datenverarbeitungsprozesse innerhalb des Rechners unzugänglich für die Wahrnehmung durch Sinnesorgane statt.[775] Ein Nutzer kann somit nicht durch Beobachtung des Rechners erkennen, welche Rechenoperationen dieser gerade durchführt. Die Tendenz an diejenigen, die IT-Systeme für private Zwecke nutzen, keine zu hohen Anforderungen zu stellen, lässt sich auch in der höchstrichterlichen Rechtsprechung wiederfinden. Die höchstrichterlichen Anforderungen an den technischen

770 *Borges*, in: Internet-Auktion, 214, 216; *ders.*, NJW 2011, 2400, 2403.
771 Dazu oben Rn. 124.
772 Dazu oben Rn. 237.
773 *Spindler*, MMR 2008, 7, 13.
774 *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08 – MMR 2008, 626, 628; *Erfurth*, WM 2006, 2198, 2201.
775 *Erfurth*, WM 2006, 2198, 2201.

Sachverstand bei der Bestimmung der im Verkehr erforderlichen Sorgfalt sind nicht sehr hoch. Bei der Sicherung eines Routers muss dieser beispielsweise auf dem Stand der Sicherungstechnik beim Kauf sein.[776] Bezüglich Trojanern muss der durchschnittliche Nutzer nicht damit rechnen, dass sich Schadprogramme in harmlos erscheinenden Dateien befinden.[777]

689 Für die Anerkennung einer Verkehrs- oder Sorgfaltspflicht ist der Bekanntheitsgrad der Gefahr entscheidend.[778] Die Account-Inhaber müssen die Gefahren, die von ihren Rechnern und Accounts ausgehen, nur durch Sorgfaltsmaßnahmen abwenden, soweit diese Gefahren allgemein bekannt sind. Die Nutzer müssen sich über aktuelle Gefahren nicht in Fachzeitschriften oder Fachseiten im Internet informieren. Das Verfolgen von aktuellen Meldungen in allgemeinen und klassischen Medien reicht aus.[779] Darüber hinaus müssen Account-Inhaber die Warnungen des jeweiligen Authentisierungsnehmers zur Kenntnis nehmen.[780]

690 Bei der Konfiguration seines Rechners können vom Account-Inhaber keine spezifischen Fachkenntnisse verlangt werden. Die sichere Konfiguration seiner Umgebung ist ihm nur insoweit zumutbar, als dass die Einstellmöglichkeiten in einer für den Nutzer verständlichen Sprache erklärt sind.[781] Anderenfalls ist ihm die sichere Konfiguration technisch nicht zumutbar. Insbesondere kann von ihm nicht erwartet werden, dass er bestehende System- oder Netzwerkeinstellungen bewertet.[782] Sicherheitsrelevante Einstellungen im Betriebssystem und Browser können von einem privaten IT-Nutzer nicht erwartet werden.[783] Wirtschaftlich sind ihm nur Maßnahmen zumutbar, die er ohne fremde Hilfe realisieren kann.[784] Die Kosten für einen

776 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 23.

777 *BGH*, Urteil v. 4. 3. 2004, III ZR 96/03 (Dialer) – BGHZ 158, 201, 209.

778 *Mantz*, K&R 2007, 566, 568; *Spindler*, BSI-Studie, Rn. 286.

779 *Bender*, WM 2008, 2049, 2054; *Spindler*, BSI-Studie, Rn. 288; *Dennis Werner*, Verkehrspflichten, S. 174.

780 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261.

781 *Dennis Werner*, Verkehrspflichten, S. 153.

782 Ebd., S. 153.

783 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261; *Spindler*, BSI-Studie, Rn. 307 f.; *Dennis Werner*, Verkehrspflichten, S. 166 ff.; **a.A.** *Bender*, WM 2008, 2049, 2054.

784 *Spindler*, BSI-Studie, Rn. 292; *Dennis Werner*, Verkehrspflichten, S. 154.

IT-Fachmann, die unverhältnismäßig hoch sein können, muss er zur Sicherung seines Rechners nicht aufwenden.[785]

691 Viele Möglichkeiten die Zugangsdaten des Account-Inhabers auszuspähen basieren auf einer Infektion des Rechners mit Malware.[786] Er kann die Risiken einer solchen Infektion seines Rechners durch die Verwendung eines Antiviren-Programms verringern.[787] Antiviren-Programme setzten bei der Installation keine Fachkenntnisse voraus und sie sind kostengünstig oder kostenlos verfügbar.[788] Die Kenntnis, dass mit Antiviren-Programmen der Rechner geschützt werden kann, ist weit verbreitet.[789] Vom Account-Inhaber kann daher erwartet werden, dass er einen ständig aktualisierten Antiviren-Schutz verwendet.[790] Die Details der Pflicht zum Einsatz einer Antiviren-Software bei Windows sind nicht abschließend geklärt. Beim Signaturerkennungsverfahren, das die wichtigste Komponente von Antiviren-Software ist,[791] besteht ein Schutz nur, soweit die jeweilige Malware in der Datenbank des Antiviren-Herstellers erfasst ist. Die Datenbank aktualisiert der Hersteller regelmäßig, um seine Kunden vor aktuellen Bedrohungen zu schützen. Einige Stimmen in der Literatur betrachteten eine wöchentliche Aktualisierung zur Erfüllung der Pflicht eines ständig aktualisierten Antiviren-Programms als ausreichend.[792] Andere Vertreten erwarten vom Nutzer, dass dieser seinen Antiviren-Schutz täglich aktualisiert.[793] Die Verwen-

---

785 *Mantz*, K&R 2007, 566, 570; *Spindler*, BSI-Studie, Rn. 292; *Dennis Werner*, Verkehrspflichten, S. 154; **a.A.** *LG Hamburg*, Beschluss v. 21. 4. 2006, 308 O 139/06 – MMR 2007, 131, 132.

786 Oben Rn. 182.

787 Oben Rn. 202.

788 *Hossenfelder*, Pflichten von Internetnutzern, S. 127.

789 *Dennis Werner*, Verkehrspflichten, S. 156.

790 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261; *Bender*, WM 2008, 2049, 2054; *Borges*, MMR 2008, 262, 264 f.; *Borges/Schwenk/Stuckenberg/Wegener*, S. 273 f., 284; *B. Lorenz*, DuD 2013, 220, 225; *Herresthal*, in: *Langenbucher/Bliesener/Spindler*, Kap. 5 § 675l BGB Rn. 11; *Hossenfelder*, Pflichten von Internetnutzern, S. 180, 202, 231, 244; *ders.*, CR 2009, 790, 793; *R. Koch*, NJW 2004, 801, 804; *F. A. Koch*, CR 2009, 485, 488; *Libertus*, MMR 2005, 507, 510; *Mantz*, K&R 2007, 566, 570; *Redeker*, IT-Recht[5], Rn. 1063; *Spindler*, BSI-Studie, Rn. 295 ff.; *Dennis Werner*, Verkehrspflichten, S. 155 ff.; **a.A.** *Kind/Dennis Werner*, CR 2006, 353, 355.

791 Oben Rn. 203.

792 *Dienstbach/Mühlenbrock*, K&R 2008, 151, 154 f.; *Libertus*, MMR 2005, 507, 510; *Spindler*, BSI-Studie, Rn. 296; *Dennis Werner*, Verkehrspflichten, S. 157.

793 *Bender*, WM 2008, 2049, 2054; *Borges/Schwenk/Stuckenberg/Wegener*, S. 274, 284; *F. A. Koch*, CR 2009, 485, 489 f.; *B. Lorenz*, DuD 2013, 220, 225.

dung eines kostenfreien Antiviren-Programms ist zur Erfüllung der Sorgfaltspflicht ausreichend.[794] Verwendet ein Nutzer kein Antiviren-Programm handelt er grob fahrlässig.[795]

Diese Pflicht zum Einsatz eines Antiviren-Programms bezieht sich – auch wenn dies in der Diskussion nicht explizit zum Ausdruck kommt – auf das Absichern des Betriebssystems Windows mit einem Virenschutz. Ob auch ein Nutzer von Linux oder Mac OS X[796] seinen Rechner absichern muss, ist ungeklärt. Diese Betriebssysteme gelten wegen ihrer von Windows abweichenden Systemarchitektur als sicherer. Angriffe mit Malware sind in der Vergangenheit nur vereinzelt aufgetreten, durch Sicherheitsupdates jedoch zügig unterbunden worden. Ferner ist die Auswahl an Antiviren-Programmen gering. Ob eine Pflicht für Nutzer von Linux und Mac OS X besteht, ihren Rechner mit einem Antiviren-Programm zu schützen, ist zu bezweifeln. 692

Der Einsatz einer Firewall[797] ist zwar ein wichtiger Bestandteil der Absicherung von IT-Systemen. Firewalls besitzen jedoch nur in sehr begrenztem Maße die Fähigkeit, eine Infektion der hinter der Firewall befindlichen Rechner mit Malware zu verhindern.[798] Diese ambivalenten Eigenschaften der Firewall spiegeln sich auch in den Ansichten zur Pflicht des Account-Inhabers eine Firewall einzusetzen nieder. Teilweise wird vertreten, dass der Einsatz einer Firewall zumutbar und daher zu erwarten ist.[799] Zahlreiche Stimmen der Literatur lehnen jedoch eine Pflicht zur Einsatz einer Firewall ab.[800] Zum einen sei die Möglichkeit sich mit einer Firewall zu schützen noch zu wenig bekannt.[801] Zum anderen ist sichere Konfiguration nur mit Spezialkenntnissen möglich, wodurch es privaten Anwendern technisch 693

794 *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08 – MMR 2008, 626, 629; *Mühlenbrock/Dienstbach*, MMR 2008, 630, 631.

795 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 134; differenzierend nach der Art des Accounts *Hossenfelder*, Pflichten von Internetnutzern, S. 203, 232.

796 14,4 % der Nutzer verwenden diese Betriebssysteme, *Schnarz/Seeger*, DuD 2012, 253, 254.

797 Oben Rn. 207.

798 Oben Rn. 209.

799 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261; *Hossenfelder*, Pflichten von Internetnutzern, S. 180; *ders.*, CR 2009, 790, 793; *F. A. Koch*, CR 2009, 485, 488.

800 *Borges/Schwenk/Stuckenberg/Wegener*, S. 274; *Spindler*, BSI-Studie, Rn. 298 ff.; *Dennis Werner*, Verkehrspflichten, S. 161 ff..

801 *Spindler*, BSI-Studie, Rn. 301; *Dennis Werner*, Verkehrspflichten, S. 162.

nicht zumutbar sei, eine Firewall einzusetzen.[802] Eine auf dem Betriebssystem vorinstallierte Firewall darf jedoch nicht deaktiviert werden.[803]

694 Sicherheitslücken in dem verwendetem Betriebssystem sowie den eingesetzten Programmen können ebenfalls eine Infektion des Rechners mit Malware ermöglichen.[804] Regelmäßige Updates von Betriebssystemen und den Anwendungen können dieses Risiko verringern.[805] In welchem Maße die Installation von Updates Nutzern zumutbar ist, ist nicht abschließend geklärt. Manche Stimmen der Literatur sehen den Nutzer nur dann als zur Installation von Updates verpflichtet an, wenn diese sich automatisch oder halb-automatisch installieren.[806] Teilweise wird eine Pflicht zur Aktualisierung ohne diese Einschränkung angenommen.[807] Bei der Zumutbarkeit lässt sich ebenfalls bezüglich des Aufwands der Updates differenzieren. Einzelne Stimmen in der Literatur verneinen die Pflicht zum Herunterladen von Updates mit einem großen Datenvolumen.[808] Andererseits wird den Nutzern zugemutet auch große Datenmengen an Updates herunter zu laden, das Warten oder das Umstellen auf eine schnellere Internet-Verbindung sei zumutbar.[809]

695 Zusammenfassend lässt sich festhalten, dass der Umfang der Sorgfalts- und Verkehrspflichten an den Nutzer eines Rechners noch nicht ausreichend konkretisiert ist. Es lässt sich jedoch die Tendenz feststellen, dass private Nutzer nicht allzu hohe Anforderungen erfüllen müssen. Sie müssen sich jedoch jedenfalls vor Gefahren schützen, die allgemein bekannt sind, weil beispielsweise die klassischen Medien über sie berichten. Der Einsatz eines Antiviren-Programms kann jedenfalls von Windows-Nutzern erwartet werden.

---

802 *Spindler*, BSI-Studie, Rn. 300; *Dennis Werner*, Verkehrspflichten, S. 162.

803 *Mühlenbrock/Dienstbach*, MMR 2008, 630, 631; *Dennis Werner*, Verkehrspflichten, S. 162.

804 Oben Rn. 184.

805 Oben Rn. 201.

806 *Spindler*, BSI-Studie, Rn. 302 ff.; *Dennis Werner*, Verkehrspflichten, S. 164 ff. Zwei Drittel der Nutzer verlassen sich auf diese automatischen Updates, *Schnarz/Seeger*, DuD 2012, 253, 255.

807 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261; *Hossenfelder*, Pflichten von Internetnutzern, S. 204, 244.

808 *Dennis Werner*, Verkehrspflichten, S. 165.

809 *F. A. Koch*, CR 2009, 485, 489.

bb) Einzelfälle

Die Betrachtung vergleichbarer Konstellationen hat gezeigt, dass eine Zurechnung nur in Betracht kommt, wenn dem Account-Inhaber zumutbare Möglichkeiten zur Verfügung stehen, den Missbrauch zu verhindern.[810] Er muss keinesfalls alle erdenklichen Maßnahmen zur Verhinderung eines Missbrauchs treffen. Es reicht aus, dass er bekannte und wirtschaftlich zumutbare Sicherungsmaßnahmen trifft. 696

Ermöglicht der Account-Inhaber den physikalischen Zugang zu aufgeschriebenen Zugangsdaten,[811] ist zu erwägen, dass dies in seine Risikosphäre fällt. Nach dem Risikoprinzip muss abgegrenzt werden, ob der Diebstahl noch in die neutrale Sphäre oder schon in die Sphäre des Account-Inhabers fällt. Das grundsätzliche Diebstahlrisiko kann der Account-Inhaber ebenso wenig wie der Geschäftsgegner kontrollieren.[812] Nur wenn er die Zugangsdaten unsorgfältig aufbewahrt, schafft er dadurch ein erhöhtes Risiko, für das er einzustehen hat.[813] Nach dem Verschuldensprinzip ist im Einzelfall zu überprüfen, ob die Form der Notiz der Zugangsdaten fahrlässig ist. Es kann nicht verlangt werden, dass jeder Nutzer seine Passwörter auswendig lernt.[814] Ihm muss also grundsätzlich möglich sein, sich seine Passwörter aufzuschreiben.[815] Notiert er sie sich, muss dies an einem sicheren Ort erfolgen.[816] Ein am Monitor befindlicher Klebezettel mit den Zugangsdaten ist dabei möglicherweise sogar als grob fahrlässig anzusehen,[817] ebenso das offene Herumliegenlassen von Passwort oder Chip-Karte und PIN.[818] Hat der Account-Inhaber das Passwort jedoch ohne Zusammenhang zum Account versteckt, ist dies nicht als sorgfaltswidrig anzusehen.[819] 697

Speichert der Account-Inhaber das Passwort ungesichert auf seinem Rechner in einer Schlüsselbund-Verwaltung[820] und erlaubt er anderen Personen die Nutzung seines Computers, ist dies ein Risiko, das in seine Sphäre 698

---

810 Oben Rn. 527.
811 Zu dieser Konstellation oben Rn. 132.
812 *Spiegelhalder*, S. 164.
813 *Spiegelhalder*, S. 164; *Rieder*, S. 285.
814 *B. Lorenz*, DuD 2013, 220, 223.
815 Oben Rn. 132.
816 *B. Lorenz*, DuD 2013, 220, 223.
817 *Borges*, NJW 2011, 2400, 2403.
818 *Dörner*, AcP 202 (2002), 363, 393.
819 *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 181.
820 Dazu oben Rn. 135.

fällt und somit nach dem Risikoprinzip zurechenbar ist. Ebenfalls nach dem Verschuldensprinzip ist das Speichern in der Schlüsselbund-Verwaltung zuzurechnen, weil es grob fahrlässig ist, ein Passwort ungeschützt auf einem Rechner zu speichern und diesen einen Dritten nutzen zu lassen.[821] Verwendet ein Account-Inhaber einen Passwortspeicher auf seinem Rechner muss er den Zugang dazu mit einem Passwort absichern und die darin gespeicherten Passwörter verschlüsseln.[822] Nutzt der Account-Inhaber hingegen einen Cloud-Speicher[823] für seine Passwörter und werden dem Cloud-Anbieter die Zugangsdaten entwendet, kommt eine Zurechnung zum Nutzer nicht in Betracht. Den einzigen Vorwurf, dem man ihm in diesem Fall machen könnte, ist, dass er den Cloud-Anbieter nicht sorgfältig ausgewählt hat. Für den Nutzer ist jedoch kaum bis gar nicht nachvollziehbar, wie gut die Daten beim Anbieter geschützt sind.[824]

699 Gelangt ein Angreifer durch einen Phishing-Angriff an die Zugangsdaten des Account-Inhabers,[825] stellt sich ebenfalls die Frage der Zurechnung. Nach dem Risikoprinzip kann beim klassischen Phishing die Zurechnung zum Account-Inhaber bejaht werden. Es fällt in seine Risikosphäre die Zugangsdaten nicht, auch nicht unbemerkt, weiterzugeben. Durch die unbewusste Weitergabe erhöht er das Missbrauchsrisiko so erheblich, dass ihm die Folgen dieser Risikoerhöhung zuzurechnen sind. Im Rahmen des Verschuldensprinzips ist nach den Umständen des Einzelfalls zu prüfen, ob der Account-Inhaber bei Beachtung der ordnungsgemäßen Sorgfalt hätte erkennen können, dass die Phishing-Seite nicht vom Authentisierungsnehmer stammt und dass deswegen durch Eingabe der Zugangsdaten mit einem Missbrauch zu rechnen sei.

700 Zur Herausarbeitung eines Sorgfaltsmaßstabes kann auf die umfangreichen Fälle des Phishings im Rahmen des Online-Bankings zurückgegriffen werden.[826] Man könnte in Anlehnung an die zum Online-Banking vertretenen Ansichten die Zurechnung aus zwei Gründen ausschließen: dem Account-Inhaber fehlen die Möglichkeiten den Missbrauch im Voraus zu erkennen und zu verhindern und weil der Missbrauchende nicht aus dem

821 *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 519; *Oechsler*, AcP 208 (2008), 565, 582.
822 *B. Lorenz*, DuD 2013, 220, 225.
823 Dazu oben Rn. 136.
824 *Schulz/Bosesky/C. Hoffmann*, DuD 2013, 95, 99.
825 Zu den verschiedenen Formen des Phishings oben Rn. 138 ff.
826 Siehe hierzu oben Rn. 519.

Lager des Account-Inhabers stammt, sei eine Rechtsscheinhaftung nicht geboten.[827] Letzteres Argument überzeugt nicht. Die Rechtsscheinhaftung entscheidet darüber, welches Vertrauen des Rechtsverkehrs schutzwürdig ist. Bei der Zurechnung kommt es auf die Verbindung von Haftenden zum Rechtsscheintatbestand an, nicht aus welchem Lager ein möglicher Handelnder stammt. Das erste Argument, dass die Möglichkeit den Missbrauch im Voraus zu erkennen fehle, trifft häufig aber nicht immer zu. Es gibt einige Anzeichen an Phishing-Seiten, die diese als betrügerischen Versuch erkennen lassen, sodass der Account-Inhaber erkennen kann, dass damit die ausgespähten Zugangsdaten später missbraucht werden sollen. Da Banken so präsent warnen, dass bei jeder Transaktion jeweils nur eine TAN abgefragt wird, ist jedenfalls die Eingabe von mehr als einer TAN einer indizierten Liste[828] als fahrlässig einzustufen. Die Eingabe einer gesamten Liste ist als grob fahrlässig einzustufen.[829] Es ist gemeinhin bekannt, dass Zugangsdaten zum Online-Banking zur späteren Plünderung des Kontos gephisht werden, sodass bei Verdachtsmomenten ebenfalls damit gerechnet werden muss, dass die Zugangsdaten nach Eingabe missbraucht werden. Offensichtliche Betrugsversuche, beispielsweise bei Phishing-Seiten mit eklatanten Rechtschreib- und Grammatikfehlern, nicht zu erkennen, ist fahrlässig.[830] Fahrlässig handelt beispielsweise auch, wer als Bankkunde der Aufforderung in einem Pop-up-Fenster, die mit der Androhung der Sperrung des Online-Banking-Zugangs verbunden ist, einen Geldbetrag zu überweisen nachkommt und die Bank auf solche Angriffsszenarien aufmerksam gemacht hat.[831] Das Fehlen einer HTTPS-Verbindung ist jedoch nicht fahrlässig, weil auch trotz der unterschiedlichen Anzeige im Browser die Unterscheidung zwischen einer HTTP- und einer HTTPS-Verbindung von einem durchschnittlichen Nutzer nicht erwartet werden kann.[832] Nach dem Verschuldensprinzip kann es daher beim klassischen Phishing zur Zurechnung kommen.

---

827 Oben Rn. 519.

828 *BGH*, Urteil v. 24. 4. 2012, XI ZR 96/11 – NJW 2012, 2422.

829 *OLG München*, Urteil v. 23. 1. 2012, 17 U 3527/11 – MMR 2013, 163; **a.A.** *LG Landshut*, Urteil v. 14. 7. 2011, 24 O 1129/11, Rn. 26.

830 *Hossenfelder*, CR 2009, 790, 793.

831 *AG Köln*, Urteil v. 26. 6. 2013, 119 C 143/13 – BKR 2013, 482, 483.

832 *Erfurth*, WM 2006, 2198, 2203; *Hossenfelder*, Pflichten von Internetnutzern, S. 204 f.; *ders.*, CR 2009, 790, 793; *Kind/Dennis Werner*, CR 2006, 353, 356; **a.A.** *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261.

701 Beim Pharming[833] kommt eine Zurechnung nur bei gewissen Konstellationen in Betracht. Beim DNS-Poisoning sowie dem DNS-Cache-Poisoning liegt die Ursache für die Ermöglichung des Pharming-Angriffs beim Betreiber des DNS-Servers. Der Account-Inhaber hat darauf keinen Einfluss,[834] sodass eine Zurechnung bereits nach dem allgemeinen Grundsatz ausscheidet, dass der Account-Inhaber eine Möglichkeit haben muss, den Rechtsschein zu verhindern.[835] Geschieht das Pharming in Form einer Veränderung der Hosts-Datei oder als Drive-By-Pharming stammt die Ursache für die Ermöglichung des Pharmings aus der Sphäre des Account-Inhabers, sodass ihm ein späterer Missbrauch nach dem Risikoprinzip zuzurechnen ist. Bei Anwendung des Verschuldensprinzips kommt es darauf an, ob bei Beachtung der ordnungsgemäßen Sorgfalt das Ausspähen der Daten sowie der spätere Missbrauch hätte verhindert werden können. Diese beiden Formen des Pharmings funktionieren durch eine Infektion des Rechners oder des Routers des Accounts-Inhabers.[836] Fahrlässig handelt der Account-Inhaber insbesondere dann, wenn er durch Nachlässigkeit die Infektion seines Computers mit Schadsoftware verursacht hat, zum Beispiel durch einen fehlenden aktuellen Virenschutz beim Einsatz des Windows-Betriebssystems. Ein Verschulden kann in diesem Fall darüber hinaus begründet werden, dass die Phishing-Seite aufgrund ihrer Gestaltung ernsthafte Zweifel daran begründet, dass sie vom Authentisierungsnehmer stammt.[837] Eine grobe Fahrlässigkeit kommt beim Pharming nur in Betracht, wenn die Phishing-Seite aufgrund ihrer Gestaltung eindeutig als Fälschung zu identifizieren ist, beispielsweise durch Text in gebrochenem Deutsch oder offensichtlichen Layout-Fehlern. Manche Phishing-Seiten sind jedoch den Internetseiten des Authentisierungsnehmers so ähnlich, dass ein Opfer sie kaum vom Original unterscheiden kann.[838] Bei solchen Täuschungen handelt der Account-Inhaber nicht fahrlässig. Eine Zurechnung nach dem Verschuldensprinzip scheidet somit regelmäßig aus.[839]

---

833 Zu den verschiedenen Arten des Pharmings oben Rn. 147 ff.

834 Daher trifft den Nutzer auch keine Pflicht das DNS-System vor Angriffen zu schützen, *Dennis Werner*, Verkehrspflichten, S. 169 f.

835 Oben Rn. 672.

836 Zu den Infektionswegen oben Rn. 182 ff.

837 *Hossenfelder*, CR 2009, 790, 793.

838 *Hossenfelder*, Pflichten von Internetnutzern, S. 197.

839 Diese Ergebnis stimmt überein mit den Wertungen beim Online-Banking, dazu oben Rn. 519.

Späht ein Angreifer mittels eines Keyloggers die Zugangsdaten des Ac- 702
count-Inhabers aus,[840] stellt sich beim Risikoprinzip die Frage, aus welcher Sphäre das Risiko stammt. Handelt es sich um einen physischen Keylogger, lässt sich die Risikosphäre anhand dessen Einsatzortes bestimmen. Wurde beispielsweise ein Adapter zwischen Tastatur und Anschluss am Rechner des Account-Inhabers installiert, der die Tastatureingaben aufzeichnet, ist dies dem Account-Inhaber nach dem Risikoprinzip zurechenbar. Wurde der Keylogger jedoch als zusätzliches PIN-Eingabefeld auf dem Geldautomaten einer Bank installiert, fällt dies in den Risikobereich des Authentisierungsnehmers. Nach dem Verschuldensprinzip kommt eine Zurechnung nur in Betracht, wenn der Account-Inhaber den Keylogger bei ordnungsgemäßer Sorgfalt hätte erkennen können. Ist der Keylogger in der räumlichen Sphäre des Authentisierungsnehmers installiert, wie beispielsweise das zusätzliche PIN-Eingabefeld beim Geldautomaten, handelt der Account-Inhaber regelmäßig nicht fahrlässig, wenn er dies nicht erkennt. Er darf darauf vertrauen, dass der Authentisierungsnehmer den Authentisierungsvorgang sicher gestaltet. Nur bei sich aufdrängenden Verdachtsmomenten, beispielsweise einem schiefen PIN-Eingabefeld, kann das schützenswerte Vertrauen des Account-Inhabers beeinträchtigt sein. Bei physischen Keyloggern in der eigenen räumlichen Sphäre handelt der Account-Inhaber fahrlässig, wenn er den Keylogger bei der Beachtung der ordnungsgemäßen Sorgfalt hätte erkennen können. Handelt es sich um einen Adapter, der zwischen Tastatur und Anschluss am Rechner gesteckt ist, ist das Erkennen schwer. Regelmäßig befinden sich die Anschlüsse hinten am Rechner, der so gedreht ist, dass der Verwender des Rechners diese nicht sehen kann. Der Account-Inhaber hat zwar die Möglichkeit diesen Adapter zu erkennen, es entspricht jedoch nicht der im Verkehr erforderlichen Sorgfalt seinen Rechner regelmäßig auf Keylogger zu untersuchen. Ein fahrlässiges Handeln scheidet somit regelmäßig aus.

Software-Keylogger hingegen fallen in die Risikosphäre des Account-In- 703
habers, sodass nach dem Risikoprinzip eine Zurechnung stattfindet. Sie installieren sich durch eine Infektion des Rechners, sodass der Account-Inhaber fahrlässig handelt, sofern er seinen Rechner nicht hinreichend gegen eine Infektion gesichert hat.[841] Ferner hat der Account-Inhaber keine zumutbare Möglichkeit zu überprüfen, ob und welche Zugangsdaten proto-

840 Zu Keyloggern oben Rn. 166.
841 Oben Rn. 691.

kolliert werden und an wen diese gesendet werden. Einen Missbrauch kann er so bei Beachtung der im Verkehr erforderlichen Sorgfalt nicht vorhersehen. Leichte oder grobe Fahrlässigkeit ist ihm insofern regelmäßig nicht vorzuwerfen.

704 Das Erlangen der Zugangsdaten mittels Social Engineerings[842] fällt in die Risikosphäre des Account-Inhabers, sodass nach dem Risikoprinzip eine Zurechnung erfolgen kann. Nach dem Verschuldensprinzip ist im Einzelfall zu entscheiden, ob das Verhalten des Account-Inhabers bei der Weitergabe der Zugangsdaten fahrlässig war und ob er einen späteren Missbrauch hätte vorhersehen können. Wird der Account-Inhaber durch Social Engineering auf eine Phishing-Seite geleitet (Spear-Phishing), stellt sich wie beim Phishing und Pharming die Frage, ob er aufgrund der Gestaltung der Seite Verdacht schöpfen muss. Ist dies nicht der Fall, handelt der Account-Inhaber fahrlässig, wenn er die Täuschung und die böse Absicht des Angreifers hätte erkennen können. Nach den Umständen des Einzelfalls kommt eine grobe Fahrlässigkeit in Betracht, wenn der Account-Inhaber zu leichtgläubig dem Angreifer unglaubwürdige Behauptungen geglaubt hat.[843]

705 Bei einem Man-in-the-Middle-Angriff[844] kommt es auf die Angriffsmethode an, um zu bestimmen, welcher Risikosphäre der Angriff zuzuordnen ist. Bei einem Angriff mittels DNS-Spoofing auf zentrale DNS-Server fällt dies in die neutrale Sphäre. Das Zwischenschalten eines WLAN-Hotspots oder einer GSM-Basisstation als Evil Twin kann der Account-Inhaber nicht beeinflussen, sodass dies ebenfalls in die neutrale Sphäre fällt. Lediglich wenn der Angreifer beim Man-in-the-Middle-Angriff den Verkehr über seinen Rechner deswegen umleiten konnte oder lediglich dessen Inhalt verändert, fällt dies in die Risikosphäre des Account-Inhabers, weil er am besten seinen Rechner vor solchen Angriffen schützen kann. Nur in diesem Fall ist der Missbrauch mittels eines Man-in-the-Middle-Angriffs dem Account-Inhaber nach dem Risikoprinzip zuzurechnen. Nach dem Verschuldensprinzip kommt eine Zurechnung bei einem Man-in-the-Middle-Angriff regelmäßig nicht in Betracht. Wird der Angriff mittels DNS-Spoofing oder Evil Twin vollzogen, konnte der Account-Inhaber die Umleitung des Datenverkehrs nicht beeinflussen, sodass ihm daraus kein Verschuldensvorwurf gemacht werden kann. Im Gegensatz zum Phishing und Pharming werden bei einem

842 Siehe dazu oben Rn. 162.
843 Vgl. etwa *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08, Rn. 28.
844 Dazu oben Rn. 168 ff.

Man-in-the-Middle-Angriff die Zugangsdaten entweder unbemerkt mitgehört oder direkt zum Missbrauch verwendet, häufig unter Vortäuschung des gewollten Vorgangs. Während der Account-Inhaber Auffälligkeiten bei der Phishing-Seite bemerken könnte, hat er beim Man-in-the-Middle-Angriff häufig keine Anzeichen, dass seine Daten mitgelesen oder missbraucht werden. Ein Verschuldensvorwurf ist ihm daher nicht zu machen. Sichert der Account-Inhaber seinen Rechner nicht ausreichend gegen eine Infektion ab, benutzt er beispielsweise einen Windows-Rechner ohne Antiviren-Schutz, ermöglicht er den Man-in-the-Middle-Angriff fahrlässig. Den späteren Missbrauch wird der Account-Inhaber bei der mangelnden Sicherung jedoch häufig nicht erkennen, sodass ihm diesbezüglich keine Fahrlässigkeit vorzuwerfen ist. Grobe Fahrlässigkeit wird beim Man-in-the-Middle-Angriff regelmäßig erst recht nicht vorliegen. Nach dem Verschuldensprinzip ist der Missbrauch nach einem Man-in-the-Middle-Angriff somit häufig nicht zurechenbar.

706 Beim Sniffing[845] kommt es nach dem Risikoprinzip darauf an, wer das Sniffing durch den Einsatz einer unverschlüsselten Verbindung ermöglicht hat. Die Absicherung der eigenen WLAN-Verbindung fällt in die Risikosphäre des Account-Inhabers. Setzt der Authentisierungsnehmer jedoch beim Authentisierungsvorgang eine nicht verschlüsselte Verbindung ein, ist dieser Umstand seiner Risikosphäre zuzurechnen. Wird der Mobilfunkverkehr mitgelesen, fällt dies in die neutrale Sphäre. Nach dem Risikoprinzip ist somit nur der Einsatz einer unverschlüsselten WLAN-Verbindung dem Account-Inhaber zuzurechnen. Bei Anwendung des Verschuldensprinzips ergibt sich das Gleiche. Wird der Mobilfunk-Verkehr mitgelesen oder setzt der Authentisierungsnehmer eine unverschlüsselte Verbindung ein, sind dies Umstände, die der Account-Inhaber nicht beeinflussen kann, sodass ein Verschuldensvorwurf daraus nicht erwachsen kann. Bereits seit mehreren Jahren ist es verkehrsüblich ein WLAN zu verschlüsseln,[846] sodass der Einsatz eines schlecht gesicherten WLANs gegen die im Verkehr erforderliche Sorgfalt verstößt. Während der Einsatz einer unsicheren Verschlüsselungsmethode wie WEP als fahrlässig eingestuft werden kann, ist das Fehlen einer Verschlüsselungsmethode beim Wireless LAN als

845 Siehe oben Rn. 177.

846 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 33.

grob fahrlässig anzusehen. Eine Zurechnung nach dem Verschuldensprinzip kommt in diesem Fall in Betracht.

707 Errät der Angreifer die Zugangsdaten durch das Ausprobieren bekannter Daten,[847] stellt sich nach dem Risiko die Frage, welcher Sphäre dies zuzuordnen ist. Bei dem Herausfinden durch einen Brute-Force-Angriff fällt es jedenfalls nicht in den Risikobereich des Account-Inhabers, weil dieser keine Möglichkeit hat dies zu verhindern. Durch das Verwenden des immer gleichen Passworts bei verschiedenen Authentisierungsnehmern könnte er jedoch ein erhöhtes Risiko setzen. Das Risiko, das der Account-Inhaber dadurch setzt, ist jedoch sehr gering. Die Kombination der Zugangsdaten muss erst ausgespäht werden, damit ein Angriff auf einer anderen Seite funktioniert. Man kann daher erwägen, dies der neutralen Sphäre zuzuordnen. Dagegen spricht jedoch, dass dieses minimale Risiko vom Account-Inhaber besser beherrscht werden kann. Dass das Risiko klein ist, schmälert lediglich die Wahrscheinlichkeit des Missbrauchs, hat jedoch keinen Einfluss auf die Haftung des Account-Inhabers. Begünstigt der Account-Inhaber somit durch das Verwenden der stets selben Kombination bei den Zugangsdaten ein Erraten, ist ihm dies nach dem Risikoprinzip zuzurechnen. Nach dem Verschuldensprinzip stellt sich die Frage, ob es verkehrsüblich ist, bei jedem Authentisierungsnehmer eine unterschiedliche Kombination von Zugangsdaten zu verwenden. Angesichts der Tatsache, dass die Mehrheit der Account-Inhaber nur drei oder weniger unterschiedliche Passwörter bei den zahlreichen Accounts,[848] die sie besitzt verwendet, ist bereits an der Verkehrsüblichkeit zu zweifeln. Doch nur weil eine Mehrheit sich nicht an ein Sicherheitsniveau hält, entspricht das unsichere Verhalten nicht der im Verkehr erforderlichen Sorgfalt. Nur weil sehr viele Autofahrer sich nicht an die zulässige Höchstgeschwindigkeit (vgl. § 3 Abs. 3 StVO) halten, entfällt die Fahrlässigkeit ihres Verhaltens durch die schiere Anzahl an Überschreitungen nicht. Das durch die Verwendung der gleichen Zugangsdaten bei unterschiedlichen Authentisierungsnehmern gesetzte Risiko ist jedoch nicht so hoch, dass eine Pflicht zur Verwendung unterschiedlicher Benutzernamen oder Passwörter besteht.[849] Zwar kann dem Account-Inhaber somit unter Umständen Fahrlässigkeit vorgeworfen werden, wenn er das immer gleiche Passwort bei unterschiedlichen Authentisierungsnehmern verwen-

847 Dazu oben Rn. 180.
848 Vgl. *Wefel*, S. 3.
849 *B. Lorenz*, DuD 2013, 220, 223.

det. Eine Zurechnung nach dem Verschuldensprinzip scheitert jedoch daran, dass er mit einem konkreten Missbrauch nicht rechnen braucht. Erst wenn er Kenntnis davon erlangt, dass die Zugangsdaten möglicherweise in die Hände eines Angreifers gelangt sind,[850] besteht für ihn Anlass sein Passwort zu ändern.[851]

Darüber hinaus erwägen einzelne Stimmen der Literatur weitere Anfor- **708**
derungen an den Account-Inhaber bezüglich seiner Zugangsdaten. Der Account-Inhaber sei verpflichtet, ein Passwort mit ausreichender Länge zu wählen, das nicht durch einen Wörterbuch-Angriff angreifbar ist.[852] Diese Anforderung an den Account-Inhaber überzeugt nicht. Der Authentisierungsnehmer muss durch entsprechende Vorgaben vielmehr sicherstellen, dass die Authentisierungsgeber sichere Passwörter wählen. Ferner solle eine Pflicht des Account-Inhabers bestehen, die Passwörter regelmäßig zu ändern.[853] Um diese Pflicht zu erfüllen müssen die Passwörter nicht alle drei, sondern alle ein bis zwei Jahre geändert werden.[854] Zwar kann der Account-Inhaber durch das häufige Ändern des Passworts Missbrauch durch ausgespähte Zugangsdaten verhindern. Es ist ihm jedoch nicht zumutbar, die Passwörter für alle seine Accounts jedes Jahr oder auch nur alle zwei Jahre zu ändern, weil er wahrscheinlich über so viele Accounts verfügt, dass diese Pflicht ihn zu stark belasten würde.

e) Zwischenergebnis

Der Rechtsscheintatbestand ist dem Account-Inhaber nur bei willentlicher **709**
Schaffung, also der Weitergabe der Zugangsdaten zuzurechnen.[855] Der Account-Inhaber muss im konkreten Fall die Möglichkeit gehabt haben, den Missbrauch zu verhindern.[856]

---

850 Wenn bekannt wird, dass die Authentisierungsdaten des Authentisierungsnehmers gestohlen wurden, besteht Anlass dazu. Dies passierte beispielsweise dem Notiz-Dienst Evernote Anfang 2013, dazu *J. Schuster*, heise online v. 3. 3. 2013.

851 *B. Lorenz*, DuD 2013, 220, 224.

852 Ebd., 223.

853 Ebd., 224.

854 Ebd., 224.

855 Oben Rn. 679 ff.

856 Oben Rn. 672.

4. Schutzwürdigkeit des Geschäftsgegners

710 Die allgemeine Voraussetzung der Schutzbedürftigkeit des Geschäftsgegners muss auch bei der Haftung für den Missbrauch von Zugangsdaten im Internet erfüllt sein.[857] Da die Stärke des Rechtsscheins über den Grad des schädlichen Wissens entscheidet, muss für den Missbrauch von Zugangsdaten im Internet das schädliche Wissen bestimmt werden. Zwar ist beim Missbrauch von Zugangsdaten im Internet wegen des Handelns unter fremdem Namen die Vertretungskonstellation nicht offensichtlich. Eine Nähe zu den Rechtsscheinvollmachten besteht jedoch. In Anlehnung an § 173 BGB schadet daher bereits leicht fahrlässige Unkenntnis.[858]

5. Disposition im Vertrauen auf den Rechtsschein

711 Die allgemeine Voraussetzung der Rechtsscheinhaftung, dass der Geschäftsgegner im Vertrauen auf den Rechtsschein eine Disposition getroffen hat,[859] ist bei dem Missbrauch von Zugangsdaten im Internet ebenfalls anwendbar.

6. Rechtsfolge

712 Grundsätzlich erhält der Vertrauende bei der Rechtsscheinhaftung das, was seinem Vertrauen entspricht.[860] Vertraut der Empfänger einer Willenserklärung, die über das Internet verschickt wurde, schützenswert darauf, dass diese vom Account-Inhaber stammt, ist er vom Account-Inhaber so zu stellen, als ob dies zutrifft. Dies läuft auf eine Erfüllungshaftung auf das positive Interesse hinaus.

713 Der Haftende kann seine Haftung jedoch auf das negative Interesse begrenzen, wenn die Anfechtung des Rechtsscheintatbestandes möglich wäre.[861] Auch wenn dies nicht immer mit der Anfechtungsmöglichkeit des Rechtsscheins begründet wird, lassen sich Vertreter dieser Ansicht

857 Allgemein zu dieser Voraussetzung oben Rn. 252.
858 Im Ergebnis auch *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 36; *Kuhn*, S. 226; *Reese*, S. 56 f.; *Spiegelhalder*, S. 165 f.
859 Oben Rn. 254.
860 Oben Rn. 257.
861 Dazu oben Rn. 258.

finden.[862] Wegen der Nähe zu den Rechtsscheinvollmachten, wo eine Anfechtungsmöglichkeit herrschend ausgeschlossen wird,[863] ist dies jedoch bei der Haftung für den Missbrauch von Zugangsdaten abzulehnen.[864]

714 Ebenso wie bei jeder Rechtsscheinhaftung stellt sich die Frage, ob der Geschäftsgegner ein Wahlrecht zwischen der scheinbaren und der wirklichen Lage besitzt.[865] Wegen der Nähe zu den Rechtsscheinvollmachten ist zu erwägen, die herrschende Meinung, dass bei diesen ein Wahlrecht nicht besteht,[866] zu übertragen. Dagegen spricht jedoch, dass der Geschäftsgegner, falls zweifelhaft ist, ob eine Rechtsscheinhaftung im Einzelfall gegeben ist, nicht das Prozessrisiko tragen soll, sondern sich direkt an den Handelnden wenden können soll.[867] Daher hinaus steht dem Vertrauenden bei der Rechtsscheinhaftung grundsätzlich ein Wahlrecht zwischen dem Schein und der Wirklichkeit zu.[868] Der Geschäftsgegner hat daher beim Missbrauch von Zugangsdaten im Internet die Wahl den Schein gelten zu lassen und den Account-Inhaber in Anspruch zu nehmen oder die tatsächliche Lage zu Grunde zu legen und sich an den Handelnden zu wenden.

7. Zwischenergebnis

715 Nach den Grundsätzen der allgemeinen Rechtsscheinhaftung besteht ein Rechtsscheintatbestand dafür, dass der Account-Inhaber eine Erklärung über seinen Account abgegeben hat, wenn eine sichere Authentisierungsmethode wie die Zwei-Faktor-Authentisierung verwendet und die Identität des Account-Inhabers bei Erstellung des Accounts überprüft wird.[869] Zurechenbar ist dem Account-Inhaber dieser Rechtsscheintatbestand nur, wenn er die Zugangsdaten willentlich übergeben hat.[870]

---

862 *Herresthal*, K&R 2008, 705, 709; *ders.*, in: *Taeger/Wiebe*, 21, 39; *Klees*, MDR 2007, 185, 188; *Kuhn*, S. 239; *Spiegelhalder*, S. 174.
863 Siehe oben Rn. 259.
864 So auch *Rieder*, S. 317.
865 Allgemein dazu oben Rn. 260.
866 Siehe oben Rn. 260.
867 Vgl. *Canaris*, Vertrauenshaftung, S. 519; *M. Wolf/Neuner*[10], Kap. 51 Rn. 112.
868 So *Canaris*, Vertrauenshaftung, S. 519.
869 Oben Rn. 670.
870 Oben Rn. 709.

VII. Zwischenergebnis

716 Der Missbrauch von Zugangsdaten im Internet lässt sich nicht überzeugend über die Anscheinsvollmacht lösen, weil mangels Erkennbarkeit des Dritten kein Rechtsschein bezüglich dessen Berechtigung zu handeln besteht.[871] Sofern vertragliche Beziehungen zwischen dem Account-Inhaber und dem Authentisierungsnehmer vorliegen, kann das Problem über diese vertraglichen Vereinbarungen und Pflichten gelöst werden.[872] Solche vertraglichen Vereinbarungen fehlen jedoch häufig, beispielsweise bei Drei-Personen-Konstellationen, bei denen Authentisierungsnehmer und Geschäftsgegner auseinanderfallen.[873] Für diese Konstellationen kann über eine Lösung über die *culpa in contrahendo* nachgedacht werden, die jedoch regelmäßig an einem vorvertraglichen Schuldverhältnis scheitert.[874] Der vertraglichen Beziehung zwischen Account-Inhaber und Authentisierungsnehmer Schutzwirkungen zu Gunsten des Geschäftsgegners zuzusprechen, kann in Drei-Personen-Konstellationen wegen der mangelnden Leistungsnähe des Geschäftsgegners und der fehlenden Erkennbarkeit für den Account-Inhaber das Problem nicht überzeugend lösen.[875] Eine Lösung über die analoge Anwendung des § 122 BGB scheitert an der fehlenden Vergleichbarkeit der Interessenlage.[876] Eine deliktische Lösung über § 823 Abs. 1 BGB scheitert an der fehlenden Ersatzfähigkeit fahrlässig verursachter Vermögensschäden.[877] Eine Lösung über § 823 Abs. 2 BGB scheitert an dem Vorliegen von Schutzgesetzen.[878]

717 Die Haftung für den Missbrauch von Zugangsdaten im Internet lässt sich überzeugend mit den allgemeinen Grundsätzen der Rechtsscheinhaftung lösen.[879] Ein Rechtsscheintatbestand besteht nur bei Verwendung einer hinreichend sicheren Authentisierungsmethode und bei hinreichend zuverlässiger Identifikationsfunktion des Accounts. Eine hinreichend sichere Authentisierungsmethode stellt die Zwei-Faktor-Authentisierung dar.[880] Die rein

871 Oben Rn. 370 ff.
872 Oben Rn. 397.
873 Oben Rn. 292.
874 Oben Rn. 428 ff.
875 Oben Rn. 403 ff.
876 Oben Rn. 471 ff.
877 Oben Rn. 487.
878 Oben Rn. 487.
879 Oben Rn. 489 ff.
880 Oben Rn. 578 ff.

wissensbasierte Authentisierung hingegen begründet keinen Rechtsschein für das Handeln des Account-Inhabers.[881] Eine Haftung für die Weitergabe der Zugangsdaten bei einer rein wissensbasierten Authentisierung scheidet somit entgegen der dazu vertretenen Ansichten aus. Die Lösung über die Duldungsvollmacht[882] oder über eine analoge Anwendung des § 172 Abs. 1 BGB[883] überzeugen somit weder in der Begründung des Lösungswegs noch im Ergebnis. Bei welchen Account-Typen eine Haftung des Account-Inhabers in Betracht kommt, wird noch ausführlich untersucht.[884]

881 Oben Rn. 544 ff.
882 Oben Rn. 297 ff.
883 Oben Rn. 303 ff.
884 Unten Rn. 830.

§ 7 Haftung des Account-Inhabers bei Erstellen des Accounts durch Dritten

Erstellt ein Dritter einen Account, bei dem er einen anderen als Account-Inhaber ausweist,[1] stellt sich die Frage, ob der Namensträger für einen Missbrauch des Accounts haften muss. Als Lösungswege für diese Frage kommen die Gleichen wie bei der Haftung ohne Weitergabe der Zugangsdaten in Betracht.[2] Die Anwendung der Anscheinsvollmacht[3] überzeugt nicht, weil mangels Erkennbarkeit des Handelns des Dritten kein Rechtsschein diesbezüglich entsteht.[4] Diese Fallkonstellation ist ebenso über eine allgemeine Rechtsscheinhaftung zu lösen.[5] **718**

Bezüglich des Rechtsscheins reicht es nicht aus, dass pauschal auf Missbrauchsmöglichkeiten verwiesen wird.[6] Die Missbrauchsmöglichkeiten schließen die Anerkennung des Rechtsscheintatbestandes nicht aus.[7] Vielmehr kommt es auf eine sichere Authentisierungsmethode sowie auf eine sichere Überprüfung der behaupteten Identität an.[8] Eine rein wissensbasierte Authentisierung stellt dabei keine ausreichende Sicherheit für die Anerkennung eines Rechtsscheintatbestandes dar.[9] In den Fällen, bei denen eBay-Accounts unter fremdem Namen erstellt wurden,[10] ist daher ein Rechtsscheintatbestand zu verneinen. **719**

Ferner müsste für einen Rechtsscheintatbestand die behauptete Identität zuverlässig überprüft werden.[11] Zwar bietet ein zuverlässiges Identifi- **720**

---

1 Oben Rn. 210.
2 Dazu oben Rn. 370 ff.
3 Beim Erstellen des Accounts durch einen Dritten angewandt von *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676, 1677; *LG Kassel*, Urteil v. 15. 4. 2008, 9 O 2539/06 – NJW-RR 2009, 781; *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08, Rn. 24.
4 Oben Rn. 378.
5 Dazu oben Rn. 489.
6 So jedoch *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676, 1677.
7 Oben Rn. 530.
8 Oben Rn. 534 ff.
9 Oben Rn. 544 ff.
10 Wie *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676, 1677; *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08, Rn. 28.
11 Oben Rn. 595 ff.

zierungsverfahren keine hundertprozentige Sicherheit. Würde es dies tun, könnte ein Dritter nicht unbefugt den Account eines Dritten erstellen und die Frage der Haftung würde sich nicht stellen. Das Verfahren muss jedoch ausreichend sicher sein, damit das Vertrauen des Geschäftsgegners darin schützenswürdig ist. Wenn keine Identitätsüberprüfung stattfindet, ist kein sicheres Identifizierungsverfahren vorhanden.[12] Wird nur eine Plausibilitätskontrolle durchgeführt, wie bei eBay,[13] besteht kein schützenswertes Vertrauen in die Identität des Account-Inhabers.[14] Wenn für einen eBay-Account trotzdem ein Rechtsscheintatbestand bejaht wurde,[15] liegt dies an einer Besonderheit des Falls. Der Dritte, der den Account erstellt hat, hat diesen von eBay überprüfen lassen. Bei diesem mittlerweile eingestellten Verfahren überprüfte eBay die Identitätsbehauptung im PostIdent-Verfahren.[16] Dieses Verfahren stellt eine zuverlässige Überprüfung der Identität dar, sodass die zweite Voraussetzung des Rechtsscheins damit erfüllt wird.[17] Eine Bejahung des Rechtsscheintatbestandes[18] scheitert jedoch an der ersten Voraussetzung, dem Einsatz eines hinreichend sicheren Authentisierungsverfahrens. Trotz der sicheren Überprüfung der Identitätsbehauptung kommt ein Rechtsscheintatbestand wegen der eingesetzten rein wissensbasierten Authentisierungsmethode nicht in Betracht.

721 Der vom Erklärungsempfänger wahrnehmbare Rechtsschein unterscheidet sich nicht von den Fallkonstellationen des Missbrauchs nach Weitergabe der Zugangsdaten oder ohne Weitergabe dieser. Die Registrierung und die Identitätsüberprüfung findet für ihn nicht wahrnehmbar statt. Insofern besteht beim Rechtsscheintatbestand bei der Erstellung des Accounts durch einen Dritten kein Unterschied zu den anderen Fallkonstellationen.

722 Die Zurechnung macht jedoch den bedeutenden Unterschied. Die Erstellung des Accounts mit Zustimmung oder im Auftrag des Account-Inhabers stellt eine willentliche Schaffung des Rechtsscheintatbestandes dar. Diese ist wie die willentliche Weitergabe der Zugangsdaten[19] zuzurechnen. Die Überlassung von öffentlich bekannten oder zumindest nicht geheimen Da-

12 *Borges/J. Meyer*, EWiR 2006, 419, 420.
13 *Hanau*, Handeln unter fremder Nummer, S. 212.
14 Ebd., S. 214 sowie oben Rn. 607 ff.
15 *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08, Rn. 28.
16 *eBay*, Werden Sie „Geprüftes Mitglied".
17 Oben Rn. 613.
18 Wie angedeutet von *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08, Rn. 28.
19 Oben Rn. 679.

ten, wie Name, Anschrift, Geburtstag sowie einer Bankverbindung reicht dafür nicht aus.[20] Weil diese Daten nicht geheim sind, kann ihr Wissen keinen Rückschluss auf die Identität oder Berechtigung geben.[21] Eine einfache Kopie des Personalausweises reicht aus demselben Grund nicht aus. Die beglaubigte Kopie eines Personalausweises hingegen, ähnlich wie eine Ausfertigung einer Vollmachtsurkunde,[22] ist ein Dokument, das den Rückschluss auf die Identität oder zumindest eine Berechtigung zulässt. Hat der Account-Inhaber eine solche Kopie dem Dritten ausgehängt, kommt eine Zurechnung in Betracht.[23]

723 Erstellt der Dritte ohne Auftrag des Account-Inhabers den Account und nutzt der Account-Inhaber den Account später, führt diese „Anerkennung" des Accounts zu einer Zurechnung.[24] Hat der Account-Inhaber hingegen kein Wissen von der Existenz des Accounts, kann er diesem auch nicht zugerechnet werden. Ein denkbarer Fall ist, dass ein Dritter einen Account erstellt, bei dem die E-Mail-Adresse mittels einer Aktivierungsmail überprüft wird.[25] Bestätigt der Account-Inhaber den Account ohne Erfassen des Inhalts der E-Mail aus Nachlässigkeit, indem er auf den Aktivierungslink klickt, erscheint fraglich, ob eine Zurechnung in Betracht kommt. Bei dieser Nachlässigkeit schafft der Account-Inhaber nicht willentlich einen Rechtsscheintatbestand, sodass eine Zurechnung nur in Betracht kommt, wenn die nachlässige Schaffung eines Rechtsscheintatbestandes dafür ausreicht.[26] Stellt die Überprüfung der E-Mail-Adresse die einzige Form der Überprüfung der Identität des Account-Inhabers dar, scheitert eine Haftung des Namensträgers jedoch bereits an dem fehlenden Rechtsscheintatbestand.[27]

724 Ein Rechtsscheintatbestand, der zugerechnet werden kann, besteht jedoch bei einer zuverlässigen Überprüfung der Identitätsbehauptung. Nutzt jemand beispielsweise die gelockerten Anforderungen des § 5 Abs. 1 S. 2 SigG, um eine qualifizierte elektronische Signatur auf einen fremden Na-

---

20 In diese Richtung jedoch *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08, Rn. 28.

21 Ähnlich *Hanau*, Handeln unter fremder Nummer, S. 212.

22 Vgl. dazu oben Rn. 310.

23 *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08, Rn. 28; *Härting*[4], Rn. 574.

24 *Oechsler*, AcP 208 (2008), 565, 580; *ders.*, MMR 2011, 631, 632; *Sonnentag*, WM 2012, 1614, 1618.

25 Zu dieser Methode oben Rn. 61.

26 Entgegen der hier vertretenen Auffassung, zu dieser oben Rn. 679.

27 Oben Rn. 598.

men zu erstellen[28] oder benutzt er den elektronischen Identitätsnachweis im neuen Personalausweis ohne Wissen des Account-Inhabers, um sich als dieser bei der Registrierung auszugeben, kommt eine Zurechnung nicht in Betracht, weil der Namensträger den Rechtsschein in diesen Fällen nicht willentlich geschaffen hat. Dabei ist jedoch stets zu beachten, dass die Erstellung im fremden Namen bei der zuverlässigen Überprüfung der Identitätsbehauptung nur schwer möglich ist. Bei der analogen Überprüfung der Identität muss der Dritte dem Namensträger ähnlich sehen, um als dieser gelten zu können oder den Rechtsschein einer Berechtigung setzen.[29] Bei der digitalen Überprüfung mittels qualifizierter elektronischer Signatur oder elektronischem Identitätsnachweis muss der Dritte beide Authentisierungskomponenten besitzen, was möglich, aber schwer ist. Hat der Account-Inhaber sie ihm zugänglich gemacht, liegt eine willentliche Schaffung vor, sodass wiederum zugerechnet werden kann.

725 Eine rechtsgeschäftliche Haftung des Account-Inhabers kommt somit in Betracht, wenn beim Account ein sicheres Authentisierungsverfahren eingesetzt wird, die Identitätsbehauptung bei der Registrierung zuverlässig überprüft wird und der Account-Inhaber willentlich dem Dritten durch Übergabe von Dokumenten oder Geheimnissen ermöglicht hat, einen Account im fremden Namen zu registrieren.

28 Unten Rn. 887.
29 Oben Rn. 614.

§ 8 Deliktische Haftung des Account-Inhabers

Die rechtsgeschäftliche Haftung steht im Mittelpunkt dieser Untersuchung. 726
Die deliktische Haftung für den Missbrauch der Zugangsdaten im Internet soll jedoch ebenfalls kurz beleuchtet werden. Einerseits wird die Auffassung vertreten, dass die Wertungen der deliktischen Haftung auf die rechtsgeschäftliche Haftung zu übertragen sei.[1] Um diese Meinung angemessen würdigen zu können, ist die Untersuchung der zu übertragenden Grundsätze erforderlich. Andererseits stellt sich die Frage, ob ein Vergleich der rechtsgeschäftlichen mit der deliktischen Haftung gewinnbringend ist. Bei einer Vergleichbarkeit der Haftungsgründe könnten die Wertungen der beiden Bereiche aneinander angepasst werden.

Bei der deliktischen Haftung des Account-Inhabers für den Missbrauch 727
der Zugangsdaten ist insbesondere die „Halzband"-Entscheidung[2] des *BGH* relevant, bei dem der Missbrauch ohne die Weitergabe der Zugangsdaten stattfand. Den Entscheidungen „Halzband" sowie „VIP-Bareinrichtung"[3] des *BGH* liegen gleiche Sachverhaltskonstellationen zu Grunde, die jedoch rechtlich einmal die Frage der deliktischen Haftung und ein anderes Mal die Frage der rechtsgeschäftlichen Haftung aufwerfen. Bei beiden Fällen nutzte der eine Lebenspartner die schlecht gesicherten Zugangsdaten des anderen Lebenspartners, um Waren bei einer eBay-Auktion zu versteigern. Nachfolgend soll daher das in der Halzband-Entscheidung entwickelte Haftungsmodell vorgestellt und untersucht werden.

I. Eigener Zurechnungstatbestand

Der Account-Inhaber müsse bei unzureichender Sicherung der Zugangsda- 728
ten zum Benutzerkonto auf einer Internetseite für einen darüber erfolgten Missbrauch haften.[4] Dabei handele es sich um einen selbstständigen Zurechnungstatbestand, wobei der Account-Inhaber sich so behandeln lassen

1 Oben Rn. 388.
2 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134.
3 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346.
4 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 16.

muss, als habe er selbst gehandelt.[5] Die Pflicht zur Sicherung bestehe nicht, weil mit der Erstellung des Accounts eine erhöhte Gefahr für Rechtsverletzungen geschaffen werde.[6] Vielmehr könne sich jeder selbst einen eigenen Account anlegen, um damit Rechtsverletzungen zu begehen. Der Grund für die Haftung bestehe vielmehr in der erhöhten Gefahr, dass der Handelnde bei Benutzerkonten im Internet nicht identifiziert werden kann.[7]

729 Diese Haftung des Account-Inhabers setze kein Verschulden voraus.[8] Entgegen einer in der Rechtsprechung verbreiteten Ansicht[9] sei die deliktische Haftung für den Missbrauch von Zugangsdaten im Internet nicht über die Störerhaftung zu lösen.[10] Auf eine Verletzung von Prüfpflichten komme es somit nicht an.[11] Der Grund für diesen neuen Zurechnungstatbestand sei darin zu sehen, dass die Privilegierung der Störerhaftung, erst nach Hinweis auf Unterlassen zu haften, dadurch umgangen wird.[12] Eine Haftung komme bereits beim ersten Missbrauchsfall in Betracht.[13] In der Literatur vertreten vereinzelte Stimmen einschränkend, dass eine Haftung im engen Familienkreis erst nach positiver Kenntnis von Verstößen ausgelöst werde.[14]

730 Bei dieser Haftung handelt es sich nicht um eine verschuldensunabhängige Gefährdungshaftung mit der Rechtsfolge des Schadensersatzes.[15] Für eine Schadensersatzhaftung bedarf es eines Verschuldensvorwurfs an den Account-Inhaber, dass er mit dem späteren Missbrauch rechnen musste.[16] Somit handelt es sich um eine verschuldensunabhängige Beseitigungshaftung, die bei Vorliegen von Verschulden zum Schadensersatz führen kann. Diese differenzierte und neuartige Konstruktion wird teilweise als „delik-

---

5 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 16.
6 Ebd., Rn. 18.
7 Ebd., Rn. 18. Zustimmend *Beyerlein*, EWiR 2009, 453, 454; *Härting*[4], Rn. 2250.
8 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 20.
9 *OLG Frankfurt*, Beschluss v. 13. 6. 2005, 6 W 20/05 – CR 2005, 655; Urteil v. 16. 5. 2006, 11 U 45/05, Rn. 19; *OLG Stuttgart*, Beschluss v. 16. 4. 2007, 2 W 71/06 – NJW-RR 2008, 199, 200; *LG Bonn*, Urteil v. 7. 12. 2004, 11 O 48/04 – WRP 2005, 640, 641; *LG Köln*, Urteil v. 18. 10. 2006, 28 O 364/06 – MMR 2007, 337, 338; *AG München*, Urteil v. 24. 4. 2007, 161 C 24310/05 – CR 2007, 816, 816.
10 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 10.
11 Ebd., Rn. 20.
12 *Rössel*, CR 2009, 453, 454.
13 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 20.
14 *Leistner*, GRUR-Beil. 2010, 1, 8.
15 *Rössel*, CR 2009, 453, 454.
16 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 20.

tische Rechtsscheinhaftung“ bezeichnet.[17] Diese Bezeichnung ist jedoch unglücklich gewählt. Bei der rechtsgeschäftlichen Rechtsscheinhaftung ist eine Disposition im Vertrauen auf den Rechtsschein Voraussetzung.[18] Bei einer deliktischen Haftung kommt es darauf jedoch nicht an, weil der Geschädigte sich nicht im Vertrauen auf den Rechtsschein den Täter der Verletzungshandlung aussucht.[19]

II. Keine überzeugende dogmatische Begründung und Begründbarkeit

Problematisch an dieser Haftungskonstruktion ist, dass der *BGH* sie weder **731**
begründet noch herleitet,[20] sondern vielmehr deren Bestehen und Voraussetzungen postuliert. Zahlreiche Einzelaspekte bei den Voraussetzungen erscheinen dogmatisch unstimmig. Ferner erscheint die gesamte Konstruktion dogmatisch fragwürdig. Auf beide Probleme soll nachfolgend eingegangen werden.

1. Fehlender Schutzzweckzusammenhang

Zunächst ist gegen die Haftung einzubringen, dass der Schutzzweckzusam- **732**
menhang nicht gegeben ist.[21] Bei der Bestimmung des Haftungsumfangs muss der Schutzzweck der haftungsbegründenden Norm berücksichtigt werden. Eine Haftung für einen bestimmten Schaden kommt nur in Betracht, wenn die Norm den Schutzzweck hat, gerade diesen Schaden zu verhindern.[22] Haftungsgrund für die Inanspruchnahme des Account-Inhabers ist die Möglichkeit der Identitätsverwirrung.[23] Dogmatisch konsequent wäre somit die Erfassung derjenigen Kosten, die durch die Identitätsverwirrung und Aufklärung der Tatsache, wer gehandelt hat, notwendig sind.[24]

Bei der Erweiterung des Haftungsgrunds wären entsprechende Schäden **733**
vom Schutzzweck erfasst. Daher richtet sich andere Kritik nicht gegen den

17 *Rössel*, CR 2009, 453, 454; dagegen *Leistner*, GRUR-Beil. 2010, 1, 6.
18 Oben Rn. 254.
19 *Leistner*, GRUR-Beil. 2010, 1, 7.
20 *Volkmann*, K&R 2010, 368, 373; *v. Ungern-Sternberg*, GRUR 2010, 386, 392.
21 *Rössel*, CR 2009, 453, 454.
22 *Oetker*, in: MüKo-BGB[6], § 249 Rn. 124 m.w.N.
23 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18.
24 Dazu auch *Leistner*, GRUR-Beil. 2010, 1, 7.

fehlenden Schutzzweckzusammenhang, sondern gegen die unvollständige Herausarbeitung des Haftungsgrunds. Die Identitätsverwirrung allein könne nicht Grund für die Haftung sein.[25] Auf Seiten des klagenden Rechteinhabers solle es nicht auf eine mögliche Kenntnis bezüglich des tatsächlich Handelnden ankommen.[26] Somit solle bei diesem neuen Zurechnungstatbestand eine Haftung zwar durch die Identitätsverwirrung begründet sein, eine Identitätsverwirrung müsse jedoch nicht vorgelegen haben. Das ist widersprüchlich. Der Haftungsgrund müsse daher auf die Schaffung einer Gefahrenquelle zur Verletzung von Immaterialgüterrechten sowie deren effektiver Durchsetzung erweitert werden.[27] Damit kann die Ausformung der Haftungskonstruktion des *BGH* nur mit einem Haftungsgrund erklärt werden, den er selbst ablehnt.[28]

2. *Dogmatische Unstimmigkeiten*

734 Darüber wecken spätere Entscheidungen des ersten Senats des *BGH* Zweifel an dem Verständnis der dogmatischen Konstruktion als materielle Lösung. Die Formulierung bei der Entwicklung der Konstruktion, dass es sich um einen „selbstständigen Zurechnungsgrund“ handele,[29] zeigt, dass der erste Senat des *BGH* das Problem materiell-rechtlich gelöst hat. In einer späteren Entscheidung versteht der erste Senat diese Lösung jedoch als „unwiderlegliche Vermutung“.[30] Damit weicht er nicht nur von der Konstruktion des Zurechnungsgrunds zur Vermutung ab. Er wendet sich auch von einer materiell-rechtlichen Lösung ab, hin zu einer prozessualen Lösung. Dieser Widerspruch zeigt, dass für diese Lösung keine dogmatisch überzeugende Grundlage besteht.

735 Dogmatisch inkonsequent ist ebenfalls die Ausgestaltung der Konstruktion bei der Zurechnung, wobei das Verhalten des Dritten, nicht jedoch sein Verschulden zugerechnet wird.[31] Zwar sei die Wertung, dass eine Schadensersatzhaftung nur bei eigenem Verschulden des Account-Inhabers in

25 *Leistner*, GRUR-Beil. 2010, 1, 6.
26 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 19.
27 *Leistner*, GRUR-Beil. 2010, 1, 6 f.
28 Siehe *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18.
29 Ebd., Rn. 16.
30 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 15.
31 *Hecht*, K&R 2009, 462, 463.

Betracht kommt, zu begrüßen.[32] Diese dogmatische Unstimmigkeit zeigt jedoch, dass die Konstruktion dogmatisch kaum zu halten ist.

736 Der Blick auf einzelne dogmatische Unstimmigkeiten beim Haftungssystem des *BGH* hat gezeigt, dass Begründung und Voraussetzungen der Lösung kaum zusammen passen und dass die dogmatische Konstruktion äußert zweifelhaft ist. Hinzu kommt, dass in einem größeren Kontext betrachtet diese Lösung der Verhaltenszurechnung dem Deliktsrecht fremd ist.[33] Bei der Haftung für den Verrichtungsgehilfen nach § 831 BGB wird dem Geschäftsherren nicht etwa die Handlung oder das Verschulden des Verrichtungsgehilfen zugerechnet. § 831 BGB statuiert vielmehr eine Haftung des Geschäftsherren für das eigene Verschulden, der mangelnden Sorgfalt bei Auswahl oder Überwachung des Dritten.[34]

737 Um die Schwächen der Entlastungsmöglichkeit des § 831 Abs. 1 S. 2 BGB auszugleichen, wurde die Haftung für Organisationsverschulden nach § 823 Abs. 1 BGB entwickelt.[35] Bei dieser Konstruktion wird dem Geschäftsherren ebenfalls nicht das Verhalten seiner Mitarbeiter zugerechnet. Er haftet für das eigene Verschulden, beispielsweise für eine Verletzung der Pflicht, innerbetriebliche Abläufe so zu organisieren, dass Schädigungen Dritter im gebotenen Umfang vermieden werden oder dass Organisationspflichten mit haftungsbefreiender Wirkung delegiert wurden.[36] Lediglich § 31 BGB statuiert eine deliktische Verhaltenszurechnung. Diese Norm gilt direkt und in analoger Anwendung[37] jedoch nur für juristische Personen. Diese haben die Besonderheit, dass sie nicht selbst, sondern nur durch natürlichen Personen handeln können.[38] Die deliktische Haftung des BGB kennt somit nur die Haftung für eigenes Handeln. Eine Zurechnung findet nur statt, wenn das Haftungssubjekt nicht selbst handeln kann.

32 *Hecht*, K&R 2009, 462, 463.
33 Ähnlich aber ungenau *Rössel*, CR 2009, 453, 454.
34 *D. W. Belling*, in: *Staudinger*[2012], § 831 BGB Rn. 2 ff. m.w.N.
35 *G. Wagner*, in: MüKo-BGB[6], § 823 Rn. 76 ff. m.w.N.
36 Ebd., § 823 Rn. 78 f.
37 *Reuter*, in: MüKo-BGB[6], § 31 Rn. 11.
38 Oben Rn. 31.

3. Möglichkeit der Herleitung über andere Normen, die Verhalten zurechnen

a) Verhaltenszurechnung bei Pflichtverletzungen in Sonderverbindungen

738 Eine Zurechnung des Verhaltens eines Dritten kennt das BGB beim Bestehen von Sonderverbindungen (§ 278 BGB). Nach dem Wortlaut § 278 S. 1 BGB wird direkt nur das Verschulden des Erfüllungsgehilfen zugerechnet. In entsprechender Anwendung ist dem Geschäftsherren jedoch auch das Verhalten in Form der Handlungen des Erfüllungsgehilfen zuzurechnen.[39] Die Systematik des BGB zeigt somit, dass eine Verhaltenszurechnung nur bei bestehenden Sonderverbindungen in Betracht kommt. Der eigene Zurechnungstatbestand des *BGH* ist somit der Systematik des Deliktsrechts im BGB fremd.

b) Verhaltenszurechnung bei der Haftung des Unternehmensinhabers

739 Vereinzelt wird behauptet, die Konstruktion der Haftung für den Account-Inhaber beruhe auf der Haftung des Unternehmensinhabers, wie sie nach § 8 Abs. 2 UWG, § 14 Abs. 7 MarkenG und § 99 UrhG besteht.[40] Um zu überprüfen, ob sich die Haftungskonstruktion aus der Haftung des Unternehmensinhabers dogmatisch überzeugend herleiten lässt, werden zunächst die unterschiedlichen Haftungsnormen des Unternehmensinhabers untersucht.

740 Nach § 8 Abs. 2 UWG haftet der Unternehmensinhaber für Zuwiderhandlungen seiner Mitarbeiter oder Beauftragten. Dabei handelt es sich wie bei § 831 Abs. 1 BGB um einen eigenen, zusätzlichen Anspruch.[41] Im Gegensatz zu § 831 Abs. 1 S. 2 BGB steht dem Unternehmensinhaber ein Entlastungsbeweis nicht zu, sodass es sich um einen verschuldensunabhängigen Anspruch handelt.[42] Ein weiterer Unterschied zu § 831 Abs. 1 BGB besteht in der Rechtsnatur. Im Gegensatz zu § 831 Abs. 1 BGB begründet § 8 Abs. 2 UWG eine Haftung für fremdes und nicht für eigenes Verhal-

---

39 Siehe *Dauner-Lieb*, in: NK-BGB[2], § 278 Rn. 6.

40 *v. Ungern-Sternberg*, GRUR 2010, 386, 392.

41 *Büscher*, in: *Fezer*[2], § 8 UWG Rn. 229; *H. Köhler*, in: *H. Köhler/Bornkamm*[31], § 8 UWG Rn. 2.32; *Ohly*, in: *Piper/Ohly/Sosnitza*[5], § 8 UWG Rn. 143.

42 *Bergmann/Goldmann*, in: *Harte-Bavendamm/Henning-Bodewig*[3], § 8 UWG Rn. 301.

ten.[43] Dabei werden dem Unternehmensinhaber die Rechtsverletzungen des Dritten als eigene zugerechnet.[44] Der Grund für die Haftung des Unternehmensinhabers nach § 8 Abs. 2 UWG liegt darin, dass er sich nicht hinter von ihm abhängigen Dritten verstecken können soll.[45] Durch den Einsatz von Mitarbeitern und Beauftragten erweitert er seinen Geschäftskreis und schafft damit das Risiko von Zuwiderhandlungen.[46] Seine Inanspruchnahme der Vorteile der arbeitsteiligen Organisation soll seine Verantwortung für das Verhalten im Wettbewerb nicht beseitigen.[47] Dementsprechend ist eine Voraussetzung der Haftung, dass die Verletzungshandlungen einen inneren Zusammenhang zu dem Unternehmen aufweisen.[48] Anwendbar ist § 8 Abs. 2 UWG nur auf Unterlassungs- und Beseitigungsansprüche, nicht auf Schadensersatzansprüche.[49]

Im Markenrecht existiert mit § 14 Abs. 7 MarkenG eine Parallelnorm zu **741**
der Haftung des Unternehmensinhabers nach § 8 Abs. 2 UWG. Wegen der Parallelität sind beide Normen im gleichen Sinne auszulegen.[50] Bei § 14 Abs. 7 MarkenG handelt es sich auch um einen eigenständigen, verschuldensunabhängigen Anspruch.[51] Ein Entlastungsbeweis wie bei § 831 Abs. 1 S. 2 BGB ist in § 14 Abs. 7 MarkenG nicht vorgesehen.[52] Im Gegensatz zu § 8 Abs. 2 UWG sind von § 14 Abs. 7 MarkenG nicht nur Unterlassungs- und Beseitigungsansprüche sondern auch Schadensersatzansprüche erfasst,

---

43 *Bergmann/Goldmann*, in: *Harte-Bavendamm/Henning-Bodewig*[3], § 8 UWG Rn. 300.

44 Ebd., § 8 UWG Rn. 300.

45 *H. Köhler*, in: *H. Köhler/Bornkamm*[31], § 8 UWG Rn. 2.33; *Ohly*, in: *Piper/Ohly/Sosnitza*[5], § 8 UWG Rn. 143.

46 *Bergmann/Goldmann*, in: *Harte-Bavendamm/Henning-Bodewig*[3], § 8 UWG Rn. 302; *H. Köhler*, in: *H. Köhler/Bornkamm*[31], § 8 UWG Rn. 2.33; *Ohly*, in: *Piper/Ohly/Sosnitza*[5], § 8 UWG Rn. 143.

47 *Büscher*, in: *Fezer*[2], § 8 UWG Rn. 215; *H. Köhler*, in: *H. Köhler/Bornkamm*[31], § 8 UWG Rn. 2.33; *Ohly*, in: *Piper/Ohly/Sosnitza*[5], § 8 UWG Rn. 143.

48 *Büscher*, in: *Fezer*[2], § 8 UWG Rn. 217.

49 *Bergmann/Goldmann*, in: *Harte-Bavendamm/Henning-Bodewig*[3], § 8 UWG Rn. 300; *Büscher*, in: *Fezer*[2], § 8 UWG Rn. 218 f.; *H. Köhler*, in: *H. Köhler/Bornkamm*[31], § 8 UWG Rn. 2.33 f.; *Ohly*, in: *Piper/Ohly/Sosnitza*[5], § 8 UWG Rn. 144.

50 *Fezer*, in: MarkenR[4], § 14 MarkenG Rn. 1055; *Ingerl/Rohnke*, in: MarkenG[3], Vor §§ 14-19d Rn. 43.

51 *Fezer*, in: MarkenR[4], § 14 MarkenG Rn. 1056; *Hacker*, in: *Ströbele/Hacker*[10], § 14 MarkenG Rn. 543; *Ingerl/Rohnke*, in: MarkenG[3], Vor §§ 14-19d Rn. 48.

52 *Fezer*, in: MarkenR[4], § 14 MarkenG Rn. 1055.

sofern der Angestellte oder Beauftragte schuldhaft gehandelt hat.[53] Der Haftungsgrund des § 14 Abs. 7 MarkenG stimmt mit der der Parallelnorm überein. Der Unternehmensinhaber darf sich nicht hinter von ihm abhängigen Dritten verstecken, wenn er die Vorteile der arbeitsteiligen Organisation in Anspruch nimmt.[54]

742 Im Urheberrecht gibt es mit § 99 UrhG ebenfalls eine Haftungsnorm für den Unternehmensinhaber, die dem § 8 Abs. 2 UWG nachgebildet ist.[55] Sie begründet auch einen eigenständigen, verschuldensunabhängigen Anspruch gegen den Unternehmensinhaber.[56] Wie § 8 Abs. 2 UWG ist die Haftung des Unternehmensinhabers nach § 99 UrhG auf Unterlassen und Beseitigung beschränkt, sodass Schadensersatz nach der Norm nicht verlangt werden kann.[57] Haftungsgrund ist wiederum, dass der Unternehmensinhaber sich nicht hinter abhängigen Dritten verstecken können soll.[58] Daher setzt § 99 UrhG voraus, dass der Unternehmer Vorteile aus der Handlung zieht.[59]

743 Die Betrachtung der unterschiedlichen Ausformungen der Haftung des Unternehmensinhabers in UWG, MarkenG und UrhG zeigt, dass eine Haftungsform mit der Rechtsnatur und den Rechtsfolgen existiert, die der Haftungskonstruktion des *BGH* zu Grunde liegt. Bei diesen Ansprüchen handelt es sich um eigene, zusätzliche Ansprüche, die verschuldensunabhängig, also ohne Verletzung von Prüfpflichten bestehen.[60] Im Gegensatz zu den deliktischen Normen des BGB haftet bei diesen Normen der Geschäftsinhaber für fremdes Verhalten.[61] Ebenfalls sind die Ansprüche – mit Ausnahme des § 14 Abs. 7 MarkenG – auf Unterlassung und Beseitigung beschränkt.[62] Die Lösung des *BGH* greift somit Rechtsnatur und Rechtsfolge einer Haftungsform auf, die außerhalb des BGB existiert.

---

53 *Fezer*, in: MarkenR[4], § 14 MarkenG Rn. 1056; *Hacker*, in: *Ströbele/Hacker*[10], § 14 MarkenG Rn. 543; *Ingerl/Rohnke*, in: MarkenG[3], Vor §§ 14-19d Rn. 48.

54 *Fezer*, in: MarkenR[4], § 14 MarkenG Rn. 1055; *Ingerl/Rohnke*, in: MarkenG[3], Vor §§ 14-19d Rn. 43.

55 *Wild*, in: *Schricker/Loewenheim*[4], § 99 UrhG Rn. 1.

56 *Dreier*, in: *Dreier/Schulze*[4], § 99 UrhG Rn. 1; *Wild*, in: *Schricker/Loewenheim*[4], § 99 UrhG Rn. 1.

57 *Dreier*, in: *Dreier/Schulze*[4], § 99 UrhG Rn. 1.

58 Ebd., § 99 UrhG Rn. 1; *Wild*, in: *Schricker/Loewenheim*[4], § 99 UrhG Rn. 1.

59 *Dreier*, in: *Dreier/Schulze*[4], § 99 UrhG Rn. 5.

60 Wie *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 16.

61 Wie ebd., Rn. 16.

62 Wie ebd., Rn. 20. Dazu auch *v. Ungern-Sternberg*, GRUR 2010, 386, 392.

Die Voraussetzungen der Haftung des Unternehmensinhabers sowie der dahinterstehende Haftungsgrund sind jedoch beim Missbrauch von Zugangsdaten im Internet nicht gegeben. Daran scheitert die dogmatisch überzeugende Übertragung des Rechtsgedankens. Zunächst liegt nicht notwendig ein unternehmerisches Handeln des Account-Inhabers vor. Wie der Name der Haftung des Unternehmensinhabers deutlich zeigt, ist diese nur für den Inhaber eines Unternehmens anwendbar. Wie die Sonderregelungen des HGB und BGB zeigen, können an Unternehmer höhere Anforderungen im Hinblick auf Selbstverantwortung und Beherrschung von Risiken gestellt werden. Dies trifft auf Account-Inhaber nicht per se zu.[63] Diese können unternehmerisch oder nicht unternehmerisch tätig sein. Der Behauptung, dass der Account-Inhaber mit dem Benutzerkonto einen ihm vorbehaltenen Geschäftsbereich unterhalte,[64] kann nicht zugestimmt werden. Mit der Eröffnung des Accounts schafft der Account-Inhaber lediglich eine Möglichkeit zur Kommunikation und Teilnahme.[65] Die Erweiterung seines Geschäftsbereichs geht damit nicht notwendigerweise einher. 744

Darüber hinaus fehlt es an dem zentralen Rechtsgrund für die Haftung des Unternehmensinhabers. Der Unternehmensinhaber soll nicht einseitig von den Vorteilen der arbeitsteiligen Organisation profitieren können. Nutzt er diese, muss er als Korrelat auch die Nachteile der Verantwortlichkeit für die Haftungen der von ihm abhängigen Dritten tragen. Der Account-Inhaber richtet das Benutzerkonto zunächst auf seinen Namen ein. Eine arbeitsteilige Organisation schafft er mit der Einrichtung von Kommunikationsmöglichkeiten zunächst nicht. Diese besteht oder besteht nicht unabhängig von der Einrichtung des Accounts. Mit der Einrichtung des Accounts nutzt der Account-Inhaber somit nicht die Vorteile der arbeitsteiligen Organisation, die der zentrale Gedanke der Haftung des Unternehmensinhabers sind. Der Wertung, der Account-Inhaber solle haften, obwohl er aus Rechtsverletzungen von Dritten, die über seinen Account erfolgen, keine Vorteile erlangt,[66] kann nicht zugestimmt werden. Bei der Haftung des Unternehmensinhabers ist dies ein wesentlicher Grund für die Verantwortlichkeit des Unternehmensinhabers. Deswegen muss er von der Rechtsverletzung profitieren[67] 745

63 Im vom *BGH* zu entscheidenden Fall war der Account-Inhaber kein Unternehmer *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 15.

64 *v. Ungern-Sternberg*, GRUR 2010, 386, 392.

65 Oben Rn. 437.

66 *v. Ungern-Sternberg*, GRUR 2010, 386, 392.

67 *Dreier*, in: *Dreier/Schulze*[4], § 99 UrhG Rn. 5.

oder sie muss zumindest einen inneren Zusammenhang zum Unternehmen aufweisen.[68]

746 Ferner unterscheiden sich die Haftung des Unternehmensinhabers und des Account-Inhabers entscheidend im Verhältnis zum Dritten. Der Unternehmensinhaber setzt den Dritten willentlich ein. Er stellt ihn an oder beauftragt ihn, regelmäßig unter Abschluss eines Schuldverhältnisses mit ihm. Er geht somit bewusst das Risiko ein, dass der Dritte Rechtsverletzungen begeht. Der Account-Inhaber auf der anderen Seite hat, wenn er die Zugangsdaten nicht weitergibt, keine relevante Verbindung zum Dritten. Wenn der Dritte die Zugangsdaten ausspäht,[69] weiß der Account-Inhaber regelmäßig nicht, dass ein Dritter für ihn handeln kann. Er hat nicht bewusst das Risiko geschaffen, dass der Dritte über den Account Rechtsverletzungen begehen kann. Da der Account-Inhaber den Dritten nicht willentlich eingesetzt hat, sondern nur eine Möglichkeit zur Kommunikation und Teilnahme für sich geschaffen hat, unterscheiden sich die beiden Konstellationen wesentlich.

747 Darüber hinaus besteht ein erheblicher Unterschied in der Beherrschbarkeit der Risikosphäre. Der Unternehmer kann zwar die Handlungen der Angestellten und Beauftragten nicht lückenlos überwachen. Er kann diese jedoch zu einem gewissen Maße überprüfen. Er hat die volle Kontrolle darüber, wen er willentlich einsetzt und ob und wann er die Dienste des Dritten für ihn beendet. Rechtsverletzungen des Dritten spielen sich somit in seiner Risikosphäre ab. Beim Account-Inhaber ist dies nicht der Fall. Zwar kann er seinerseits beispielsweise durch die Geheimhaltung der Zugangsdaten[70] das Risiko eines Missbrauchs senken. Es gibt jedoch zahlreiche Wege wie Brute-Force-Attacken[71] oder Schwachstellen beim Authentisierungsnehmer,[72] die sich außerhalb seiner Risikosphäre abspielen. Die wesentlichen Gründe für die Haftung des Unternehmensinhabers sind somit beim Account-Inhaber nicht gegeben. Eine Übertragung der Haftungskonstruktion ist somit nicht möglich.

---

68 *Büscher*, in: *Fezer*[2], § 8 UWG Rn. 217.
69 Oben Rn. 124 ff.
70 Oben Rn. 558.
71 Oben Rn. 181.
72 Oben Rn. 215.

4. Herleitung des Unterlassungsanspruches aus § 1004 Abs. 1 BGB

748 Ferner ist zu erwägen, die Rechtsfolge des Unterlassens ohne Schadensersatz analog zu § 1004 Abs. 1 BGB zu konstruieren. Der Account-Inhaber könnte als Zustandsstörer auf die Unterlassung gewisser Handlungen über den Account analog zu § 1004 Abs. 1 BGB haften. In seiner direkten Anwendung gewährt § 1004 Abs. 1 BGB nur Unterlassungsansprüche bei der Beeinträchtigung von Eigentum. Sein Anwendungsbereich wird jedoch in analoger Anwendung auf absolute Rechte, das allgemeine Persönlichkeitsrecht und weitere deliktisch geschützte Interessen ausgedehnt.[73] Bei dieser analogen Anwendung wird der Anspruch als quasi-negatorisch bezeichnet.[74] Es sind somit viele Fälle des Missbrauchs von Zugangsdaten im Internet möglich, bei denen der Geschädigte die Unterlassung von Beeinträchtigungen von analog zu § 1004 Abs. 1 BGB geschützte Interessen mit einem quasi-negatorischen Anspruch verlangen könnte. Verursacht der Account-Inhaber diese selbst, kann er als Handlungsstörer[75] in Anspruch genommen werden.

749 In der entscheidenden Konstellation des Missbrauchs ohne Weitergabe der Zugangsdaten verursacht der Account-Inhaber die Beeinträchtigung jedoch nicht unmittelbar durch sein Verhalten, sodass ein quasi-negatorischer Unterlassungsanspruch gegen ihn nur besteht, wenn er Zustandsstörer wäre. Die Verantwortlichkeit des Zustandsstörers beruht darauf, dass die volle Sachherrschaft mit der Verantwortlichkeit des Eigentümers für diesen Zustand korreliert.[76] Neben der Möglichkeit den Zustand zu beseitigen oder zu verhindern,[77] muss die Beeinträchtigung mittelbar auf den Willen des Eigentümers zurückgehen,[78] damit dieser Zustandsstörer ist. An dieser Voraussetzung scheitert eine analoge Anwendung des § 1004 Abs. 1 BGB bei der deliktischen Haftung des Account-Inhabers ohne Weitergabe der Zugangsdaten. Der Missbrauch ist nicht auf den mittelbaren Willen des Account-Inhabers zurückzuführen, sodass er kein Zustandsstörer ist. Ferner

---

73 *Fuchs*/*Pauker*[8], S. 130.

74 *Fuchs*/*Pauker*[8], S. 130; *Looschelders*, Schuldrecht BT[8], Rn. 1428.

75 Zum Handlungsstörer *Baldus*, in: MüKo-BGB[6], § 1004 Rn. 152 ff.; *Fuchs*/*Pauker*[8], S. 132 f.

76 *Gursky*, in: *Staudinger*[2013], § 1004 BGB Rn. 102.

77 *Baldus*, in: MüKo-BGB[6], § 1004 Rn. 155.

78 *BGH*, Urteil v. 20. 11. 1992, V ZR 82/91 (Froschlärm) – BGHZ 120, 239, 254; *Bassenge*, in: *Palandt*[73], § 1004 BGB Rn. 19; *Fuchs*/*Pauker*[8], S. 133.

ist daran zu zweifeln, dass ein Account mit einer Sache, über die der Eigentümer wegen der physischen Einmaligkeit die volle Sachherrschaft ausüben kann, vergleichbar ist. Über eine analoge Anwendung des § 1004 Abs. 1 BGB mit dem Account-Inhaber als Zustandsstörer lässt sich die vom *BGH* angenommene Haftung somit ebenfalls nicht dogmatisch überzeugend konstruieren.

5. Zwischenergebnis

750 Zusammenfassend lässt sich festhalten, dass der *BGH* eine Haftungskonstruktion gewählt hat, die mit der Haftung für fremdes Verhalten dem Deliktsrecht im BGB fremd ist. Die Rechtsnatur der Haftung für fremdes Verhalten lässt sich mit den Rechtsfolgen dieser Haftungskonstruktion zwar bei der Haftung des Unternehmensinhabers nach § 8 Abs. 2 UWG, § 14 Abs. 7 MarkenG und § 99 UrhG wiederfinden. Die Haftungsgründe für die Haftung des Unternehmensinhabers sind jedoch beim Account-Inhaber nicht gegeben. Der *BGH* hat somit einen Anspruch konstruiert, der weder dogmatisch begründet noch begründbar ist.

751 Dogmatisch überzeugend könnte die Haftung des Account-Inhabers beim Missbrauch der Zugangsdaten womöglich über ein einheitliches Haftungskonzept mit Verkehrspflichten gelöst werden. In der Literatur möchten zahlreiche Stimmen von der Störerhaftung auf ein einheitliches System mit Verkehrspflichten wechseln.[79] Dieses einheitliche Haftungskonzept könnte sowohl für die Haftung des Account-Inhabers beim Missbrauch der Zugangsdaten als auch ohne deren Weitergabe eine Lösung bieten.[80]

III. Zweifelhafte Identifikationsfunktion

752 Neben der fehlenden dogmatischen Begründung und Begründbarkeit der Haftung des Account-Inhabers für den Missbrauch von Zugangsdaten über

---

79 *Ahrens*, WRP 2007, 1281, 1286 ff.; *Gräbig*, MMR 2011, 504, 508 f.; *Leistner*, GRUR-Beil. 2010, 1, 18; *Leistner/Stang*, WRP 2008, 533, 541 ff.; *dies.*, LMK 2010, 297473; *Schapiro*, S. 124 ff.; *Spindler*, GRUR 2011, 101, 103; *Spindler/Volkmann*, WRP 2003, 1, 6 ff.; *Stang/Hühner*, GRUR 2010, 636, 637; *Volkmann*, Störer im Internet, S. 131 ff.; **a.A.** *Hollenders*, S. 190 ff.

80 Vgl. *Gräbig*, MMR 2011, 504, 508 f.; *Leistner*, GRUR-Beil. 2010, 1, 18.

die Zurechnung des Verhaltens des Dritten als eigenes, überzeugen die teleologischen Erwägungen zur Rechtfertigung der Haftung nicht. Für die Haftung des Account-Inhabers spreche, dass das Benutzerkonto ein „besonderes Identifikationsmittel" für das Handeln unter einem bestimmten Namen nach außen hin sei.[81] Einem Benutzerkonto auf einer Internet-Auktionsplattform mit Reputationssystem kommt zwar grundsätzlich eine Identifikationsfunktion zu. Die Identitätsüberprüfung von eBay mit dem Abgleich der eingegeben Daten bei der Schufa[82] stellt jedoch keine ausreichend zuverlässige Methode dar.[83] Die Abfrage von teilweise öffentlichen und teilweise nicht geheimen Daten lässt keinen zuverlässigen Rückschluss auf den Account-Inhaber zu.[84] Das Argument, dass Erklärungen unter fremdem Namen über Benutzerkonten erheblich schwerer nachgeahmt werden können als Briefpapier,[85] trifft nicht zu.[86] Auch die teleologische Erwägung, die rechtliche Zuverlässigkeit der besonderen Identifikationsmittel solle gestärkt werden,[87] rechtfertigt kein anderes Ergebnis. Es ist nicht ersichtlich, warum unsichere Authentisierungsmethoden wie die rein wissensbasierte Authentisierung[88] rechtlich als zuverlässig eingestuft werden soll.

IV. Ausgestaltung einer möglichen Geheimhaltungspflicht

Teilweise wird im Rahmen dieser Haftung des Account-Inhabers angenom- **753**
men, es bestehe eine neue Verkehrspflicht gegenüber jedermann mit dem Inhalt die Zugangsdaten zu sichern.[89] Wie diese Verkehrspflicht ausgestaltet ist und welche Anforderungen der im Verkehr erforderlichen Sorgfalt entsprechen, soll nachfolgend untersucht werden. Eine Anlehnung der Ausgestaltung an die Verkehrspflichten bei der ec-Karte sowie dem Online-Banking[90] kommt aus zwei Gründen nicht in Betracht. Zum einen sind die

81 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18.
82 Oben Rn. 65.
83 A.A. *Hecht*, K&R 2009, 462, 464; wohl auch *AG München*, Urteil v. 24. 4. 2007, 161 C 24310/05 – CR 2007, 816, 817.
84 Unten Rn. 848.
85 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18.
86 Oben Rn. 496.
87 *Hecht*, K&R 2009, 462.
88 Oben Rn. 544 ff.
89 *Härting*[4], Rn. 2250; *Hecht*, K&R 2009, 462.
90 So *Hecht*, K&R 2009, 462, 463.

Anforderungen teilweise spezialgesetzlich im BGB geregelt. Zum anderen bestehen zwischen der Bank und ihrem Kunden vertragliche Beziehungen, bei denen regelmäßig Sorgfaltspflichten in den AGB der Banken ausgeformt sind. Die vertraglichen Vereinbarungen des Account-Inhabers mit dem Authentisierungsnehmer gelten wegen der Relativität der Schuldverhältnisse[91] nur zwischen den beiden Vertragspartnern. Sie begründen nach außen keine deliktische Pflicht gegenüber jedermann.[92]

754 Andere Ansätze basieren darauf innerhalb einer möglichen deliktischen Pflicht konkrete Maßstäbe zu entwickeln. Die Weitergabe des Passworts verstoße dabei gegen eine gegenüber jedermann zu achtende Geheimhaltungspflicht.[93] Auch das Speichern des Passworts in der Schlüsselbund-Verwaltung[94] verstoße gegen diese Verkehrspflicht.[95] Die Begründung, dass mit der unzureichenden Sicherung der Zugangsdaten die Gefahr für die Verletzung von absolut geschützten Rechten gesteigert wird,[96] vermag nicht zu überzeugen. Der Schutzzweckzusammenhang zwischen der Geheimhaltungspflicht und der Rechtsgutsverletzung fehlt dabei.[97] Denn die Möglichkeit, dass ein Dritter den Account des Account-Inhabers mit den Zugangsdaten verwenden kann, erhöht nicht die Gefahr der Rechtsgutsverletzung, weil der Dritte sich regelmäßig ebenfalls einen Account erstellen kann.[98] Der Grund der Haftung besteht vielmehr darin, dass es zu einer Identitätsverwirrung kommen kann, weil er ohne das Wissen, wer gehandelt hat, in der Geltendmachung seiner Ansprüche beeinträchtigt ist.[99]

755 Eine Geheimhaltungspflicht kann daher als Verkehrspflicht gegenüber jedermann nur bestehen, wenn die allgemeinen Voraussetzungen dazu vorliegen. An dem Vorliegen dieser Voraussetzungen ist jedoch zu zweifeln. Entscheidende Grundvoraussetzung für die Entstehung einer deliktischen Verkehrspflicht ist, die tatsächliche und rechtliche Möglichkeit zur Steue-

---

91 *Olzen*, in: *Staudinger*[2009], § 241 BGB Rn. 296 ff. m.w.N.

92 *Leistner*, GRUR-Beil. 2010, 1, 8.

93 *OLG Frankfurt*, Beschluss v. 13. 6. 2005, 6 W 20/05 – CR 2005, 655; *OLG Stuttgart*, Beschluss v. 16. 4. 2007, 2 W 71/06 – NJW-RR 2008, 199, 200; *LG Köln*, Urteil v. 18. 10. 2006, 28 O 364/06 – MMR 2007, 337, 338.

94 Oben Rn. 135.

95 *LG Köln*, Urteil v. 18. 10. 2006, 28 O 364/06 – MMR 2007, 337, 338.

96 Implizit *OLG Frankfurt*, Beschluss v. 13. 6. 2005, 6 W 20/05 – CR 2005, 655; *OLG Stuttgart*, Beschluss v. 16. 4. 2007, 2 W 71/06 – NJW-RR 2008, 199.

97 Oben Rn. 732.

98 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18.

99 Ebd., Rn. 18.

rung einer Gefahr aus der eigenen Sphäre.[100] Der Blick auf den Schutzzweck der Identitätsverwirrung offenbart jedoch, dass der Account-Inhaber nur eine beschränkte Möglichkeit hat, Identitätsverwirrungen zu verhindern. Selbst wenn sich bei dem Account, der die Identitäsverwirrung hervorruft, um einen Account des Account-Inhabers handelt, bestehen Möglichkeiten, wie ein Dritter ohne das Zutun des Account-Inhabers an die Zugangsdaten gelangen kann. Errät ein Angreifer die Zugangsdaten des Accounts durch eine Brute-Force-Attacke[101] oder nutzt er Schwachstellen beim Authentisierungsnehmer[102] aus, hat der Account-Inhaber keine tatsächliche Möglichkeit einen Missbrauch zu verhindern. Selbst wenn der Account vom Namensträger erstellt wurde, kann er nicht jegliche Identitätsverwirrung selbst verhindern.[103] Darüber hinaus können Identitätsverwirrungen dadurch entstehen, dass der Dritte den Account unberechtigt unter dem Namen des Namensträgers erstellt.[104] Verwendet der Authentisierungsnehmer keine hinreichend sichere Methode zur Überprüfung der Identitätsbehauptung[105] kann es somit zu einer Identitätsverwirrung kommen, die der Namensträger und vermeintliche Account-Inhaber nicht verhindern kann.

Bei konsequenter Anwendung des Haftungsgrundes der Identitäsverwir- **756**
rung kann eine Verkehrspflicht des Account-Inhabers nur sehr differenziert begründet werden. Wegen der zahlreichen Möglichkeiten, wie es zu Identitätsverwirrungen kommen kann, auf die der Account-Inhaber keinen Einfluss hat, muss man trennen zwischen solchen Gefahren, auf die der Account-Inhaber einen Einfluss hat, und solchen Gefahren, bei denen das nicht der Fall ist. Die Gefahr der Identitätsverwirrung kann der Account-Inhaber durch eine Sicherung der Zugangsdaten zwar verringern, die Gefahr stammt jedoch nicht nur aus seiner Sphäre, sondern auch aus der des Authentisierungsnehmers. Eine Verkehrspflicht des Account-Inhabers kann sich somit nur auf Gefahren seiner Sphäre beschränken. Eine Pflicht zur Sicherung der Zugangsdaten kommt daher zunächst nur für Accounts in Betracht, die der Account-Inhaber selbst angelegt hat. Ferner kann diese Pflicht nur Maßnahmen umfassen, die dem Account-Inhaber tatsächlich möglich und zumutbar sind. Angesichts der geringen Schadenshöhe, die durch eine Identitäts-

100 *G. Wagner*, in: MüKo-BGB[6], § 823 Rn. 316 m.w.N.
101 Oben Rn. 181.
102 Oben Rn. 215.
103 Dies verkennt *Leistner*, GRUR-Beil. 2010, 1, 8.
104 Oben Rn. 210.
105 Zu den unterschiedlichen Methoden oben Rn. 595.

verwirrung entstehen kann, sowie des hohen Aufwands,[106] den eine starke Sicherung der Zugangsdaten erfordert, lässt sich höchstens eine deliktische Verkehrspflicht des Account-Inhabers insoweit statuieren, als dass er die Zugangsdaten nicht wissentlich einem Dritten weitergeben darf. Selbst an dem Bestehen dieser Pflicht ist zu zweifeln.[107] Denn die Situation, in denen der Geschädigte Schwierigkeiten mit der Ermittlung eines Schädigers hat, kommen im Deliktsrecht häufig vor. Besprüht jemand die Wand eines Hauseigentümers oder zerkratzt jemand den Lack eines Autos mit einem Schlüssel, fällt es dem Geschädigten in der Regel schwer, den Täter zu ermitteln. Dass beim Einsatz von Accounts im Internet eine Identitätsverwirrung, die es erschwert den Schädiger zu ermitteln, eine Verkehrspflicht hervorrufen soll, vermag daher nicht zu überzeugen.

757 Verkehrspflichten außerhalb von Pflichten zur Geheimhaltung und Sicherung der Zugangsdaten lassen sich hingegen gut nach den allgemeinen Voraussetzungen begründen. Den Account-Inhaber trifft daher beispielsweise die Verkehrspflicht Beeinträchtigungen absolut geschützter Rechte, die über seinen Account erfolgen, unverzüglich zu unterbinden, sofern er die Möglichkeiten dazu besitzt. Macht ein Geschädigter den Account-Inhaber auf eine solche Verletzung eines absolut geschützten Rechts aufmerksam, muss er sie somit beseitigen.

V. Belastung des Account-Inhabers

758 Ferner ist zu untersuchen, wie stark die Haftung für den Missbrauch eines Accounts bei unzureichender Sicherung der Zugangsdaten den Account-Inhaber belastet. Die Behauptung, dass diese Haftung keine übermäßige Belastung darstelle, weil für Gefahren aus dem eigenen Verantwortlichkeitsbereich gehaftet werden muss,[108] trifft nicht zu. Das Gegenteil ist der Fall. Die Haftung ist außerordentlich weitreichend.[109] Erstens geht sie erheblich über das Maß hinaus, für das der Unternehmensinhaber haften muss.[110] Dieser muss nur für ausgesuchte Angestellte oder Beauftrage haften und auch

106 Zum Verhältnis von Nutzen und Kosten zur Begründung von Verkehrspflichten *G. Wagner*, in: MüKo-BGB[6], § 823 Rn. 338 f.
107 A.A. *Leistner*, GRUR-Beil. 2010, 1, 8.
108 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 23.
109 *Rössel*, CR 2009, 453, 454.
110 *Leistner*, GRUR-Beil. 2010, 1, 6.

nur, wenn er grundsätzlich Vorteile durch deren Handeln zieht.[111] Zweitens gibt es zahlreiche Möglichkeiten, den Account zu missbrauchen, ohne dass der Account-Inhaber dies verhindern kann oder Einfluss darauf hat. Weder die Schwachstellen beim Authentisierungsnehmer,[112] noch die unbefugte Weitergabe der Zugangsdaten durch diesen,[113] noch Brute-Force-Attacken[114] kann der Account-Inhaber verhindern oder beeinflussen. Die Haftung für den Missbrauch von Zugangsdaten belastet den Account-Inhaber somit möglicherweise mit Risiken, die außerhalb seines Verantwortungsbereichs liegen. Dies trifft insbesondere dann zu, wenn die Unaufklärbarkeit des konkreten Missbrauchs zu seinem Nachteil gewertet wird. Die deliktische Haftung für den Missbrauch von Zugangsdaten belastet den Account-Inhaber somit in großem Maße.

VI. Zwischenergebnis

Dem deliktischen Haftungsmodell des Account-Inhabers über die Zurechnung fremden Verhaltens fehlt sowohl eine dogmatisch saubere Konstruktion sowie eine überzeugende Begründung der Notwendigkeit. Für eine Übertragung dieses Haftungsmodells auf die rechtsgeschäftliche Haftung eignet es sich daher nicht. Überzeugend kann die deliktische Haftung des Account-Inhabers über ein einheitliches Haftungsmodell basierend auf Verkehrspflichten gelöst werden.[115] **759**

Darüber hinaus lassen sich grundsätzlich die deliktischen Wertungen nicht auf rechtsgeschäftliche Fragen[116] und umgekehrt[117] übertragen. Während es bei der deliktischen Haftung um absolut geschützte Rechte geht, ist im rechtsgeschäftlichen Bereich eine Interessenabwägung zwischen der Privatautonomie und dem Verkehrsschutz möglich. Insofern verwundert es nicht, dass die Wertungen teilweise entgegen gesetzt getroffen werden. Bei der Haftung ohne Weitergabe der Zugangsdaten besteht bei rechtsgeschäftlichen Sachverhalten wegen der fehlenden Rückkopplung an den **760**

111 Oben Rn. 745 ff.
112 Oben Rn. 215.
113 Oben Rn. 221.
114 Oben Rn. 181.
115 Oben Rn. 751.
116 *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 19.
117 *LG Köln*, Urteil v. 18. 10. 2006, 28 O 364/06 – MMR 2007, 337, 338.

Account-Inhaber die Tendenz, die Haftung abzulehnen.[118] Bei deliktischen Sachverhalten hingegen begründe die Schaffung des Risikos durch eine Identitätsverwirrung oder erhöhte Gefahrenquelle insbesondere ohne eine Weitergabe der Zugangsdaten die Haftung.[119] Bei der Haftung nach Weitergabe der Zugangsdaten geht die rechtsgeschäftliche Wertung herrschend von einer Haftung des Account-Inhabers aus.[120] Deliktisch ergibt sich ein uneinheitliches Bild je nach Art des Accounts. Bei Accounts, die dem Abschluss von Rechtsgeschäften dienen, hafte der Account-Inhaber wegen der Möglichkeiten den Missbrauch zu verhindern.[121] Ist jedoch das Teilen des Accounts zu erwarten, wie bei Internet-Anschlüssen, solle der Account-Inhaber nach umstrittener Ansicht darauf vertrauen dürfen, dass der Dritte keine Rechtsverletzungen begeht, sodass eine Haftung nur bei Verdachtsmomenten in Betracht kommt.[122]

761 Der Vergleich der rechtsgeschäftlichen mit der deliktischen Haftung für den Missbrauch von Zugangsdaten im Internet bringt somit wegen der unterschiedlichen grundlegenden Wertungen keine neuen Erkenntnisse. Eine Angleichung der Haftung in beiden Bereichen erscheint weder zweckmäßig noch notwendig.

---

118 Vgl. oben Rn. 370 ff.

119 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18; Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 18.

120 Oben Rn. 293 ff.

121 *OLG Frankfurt*, Beschluss v. 13. 6. 2005, 6 W 20/05 – CR 2005, 655; *OLG Stuttgart*, Beschluss v. 16. 4. 2007, 2 W 71/06 – NJW-RR 2008, 199; *LG Bonn*, Urteil v. 7. 12. 2004, 11 O 48/04 – WRP 2005, 640. Zu den Fällen auch *Härting*[4], Rn. 2247.

122 *BGH*, Urteil v. 15. 11. 2012, I ZR 74/12 (Morpheus) – NJW 2013, 1441, Rn. 20 f. m.w.N. In diese Richtung auch *BVerfG*, Beschluss v. 12. 3. 2012, 1 BvR 2365/11 (Filesharing) – NJW 2012, 1715, Rn. 25 f.

§ 9 Haftung der anderen Beteiligten

I. Haftung des Handelnden

Die Haftung des handelnden Dritten kommt gegenüber dem Geschäftsgegner sowie dem Account-Inhaber in Betracht. **762**

1. Haftung gegenüber dem Geschäftsgegner

Bei der Haftung gegenüber dem Geschäftsgegner sind zwei Fälle zu unterscheiden. Zunächst wird der Fall betrachtet, in dem der Account-Inhaber dem Geschäftsgegner nicht nach Rechtsscheingrundsätzen auf das positive Interesse haftet. Weil die Regeln über die Stellvertretung (§§ 164 ff. BGB) auf das Handeln unter fremdem Namen entsprechend angewendet werden,[1] werden konsequenterweise die §§ 177 ff. BGB ebenfalls analog angewendet.[2] Bei mangelnder Genehmigung haftet der Handelnde also dem Geschäftsgegner analog zu § 179 BGB. Dabei wird regelmäßig § 179 Abs. 1 BGB einschlägig sein.[3] **763**

Problematisch an dem Anspruch ist für den Geschäftsgegner, dass der Handelnde nur schwer zu ermitteln ist.[4] Der Geschäftsgegner sieht nur, von welchem Account eine Erklärung stammt. Eventuell kann er mittels der IP-Adresse den Anschlussinhaber ermitteln. Über diese kann jedoch nicht bestimmt werden, wer im konkreten Fall gehandelt hat.[5] Die Behauptung, dass nur mit Hilfe des Account-Inhabers der Handelnde identifiziert werden kann,[6] darf nicht dahingehend verstanden werden, dass er stets helfen kann. Zwar kann der Account-Inhaber die Identität des Dritten offenbaren, **764**

---

1 Oben Rn. 283 ff.

2 *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676; *Faust*, JuS 2011, 1027, 1029; *Herresthal*, JZ 2011, 1171, 1172; *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 13.

3 *Hauck*, JuS 2011, 967, 970.

4 *Süßenberger*, S. 124; *Herresthal*, JZ 2011, 1171, 1172; *ders.*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 24; *Kuhn*, S. 206.

5 Oben Rn. 47.

6 *Herresthal*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 26; *ders.*, JZ 2011, 1171, 1172.

wenn er die Zugangsdaten in einer Schlüsselbund-Verwaltung gespeichert hat oder er einen Klebezettels mit dem Passwort auf seinem Monitor angebracht hat[7] und einen Dritter seinen Rechner benutzten lässt, sofern der Missbrauch im zeitlichen Zusammenhang damit auftritt. In vielen Fällen kennt der Account-Inhaber eventuell nur Umstände, die auf einen Dritten hindeuten, wie der Befall seines Rechners mit einem Trojaner.[8] Diese Information deutet jedoch nur auf einen Missbrauchsweg hin und nicht auf den handelnden Dritten. Darüber hinaus kann der Account-Inhaber bei Brute-Force-Angriffen[9] oder bei unbefugter Weitergabe der Zugangsdaten durch den Authentisierungsnehmer[10] noch nicht einmal Hinweise auf den Missbrauchsweg geben, weil diese Missbrauchswege nicht aus seiner Sphäre stammen. Ein Anspruch analog zu § 179 Abs. 1 BGB gegen den Handelnden ist somit regelmäßig schwer bis nicht durchsetzbar.[11]

765 Der zweite Fall ist, dass der Account-Inhaber dem Geschäftsgegner nach Rechtsscheingrundsätzen haftet. Dabei hat der Geschäftsgegner bereits einen Anspruchsgegner. Wenn dem Geschäftsgegner entgegen der herrschenden Meinung ein Wahlrecht zwischen wahrer und scheinbarer Rechtslage zusteht,[12] kommt in diesem Fall eine Haftung des Handelnden analog zu § 179 Abs. 1 BGB in Betracht. Darüber hinaus kann eine Haftung des Handelnden wegen einer vorsätzlichen sittenwidrigen Schädigung (§ 826 BGB) des Geschäftsgegners nach den Umständen des Einzelfalls in Betracht kommen. Ebenso kann eine Haftung des Handeln nach § 823 Abs. 2 BGB i.V.m. § 263 Abs. 1 StGB bestehen, weil ein sog. Eingehungsbetrug mit dem Erlangen einer Verpflichtung bei einer nur minderwertigen, da vom Account-Inhaber nicht gewollten, Gegenleistung vorliegen kann.[13] Bei dem hier abgelehnten Lösungsweg über die *culpa in contrahendo* mit einer Haftung des Accounts-Inhabers auf das negative Interesse,[14] kann daneben der Handelnde analog zu § 179 Abs. 1 BGB in Anspruch genommen werden.[15]

---

7 Siehe oben Rn. 132 ff.
8 Oben Rn. 193.
9 Oben Rn. 181.
10 Oben Rn. 221.
11 *Herresthal*, JZ 2011, 1171, 1172.
12 Oben Rn. 714.
13 Zum Eingehungsbetrug *T. Fischer*, in: StGB-Kommentar[60], § 263 Rn. 176 m.w.N.
14 Dazu oben Rn. 428 ff.
15 *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 13.

2. Haftung gegenüber dem Account-Inhaber

Eine Haftung des Handelnden gegenüber dem Account-Inhaber kommt ebenso in Betracht. Hat der Account-Inhaber dem Dritten die Zugangsdaten weitergegeben und missbraucht dieser sie, so kommt eine Haftung aufgrund des Innenverhältnisses zwischen den beiden in Betracht. Eine solche Haftung besteht insbesondere dann, wenn der Account-Inhaber wirksam verpflichtet wird oder er dem Geschäftsgegner anderweitig schadensersatzpflichtig ist. Darüber hinaus können dem Account-Inhaber Kosten durch die unberechtigte Inanspruchnahme durch den Geschäftsgegner entstehen, die er vom Handelnden ersetzt verlangen kann. 766

Fehlt es an einem Vertragsverhältnis, kommt eine deliktische Haftung in Betracht. Bei reinen Vermögensschäden scheidet eine solche Haftung nach § 823 Abs. 1 BGB jedoch aus. Der Dritte haftet nach § 823 Abs. 1 BGB nur, wenn er durch den Missbrauch des Accounts das absolut geschützte Rechte des Account-Inhabers verletzt. Das wird regelmäßig nicht der Fall sein. In Betracht kommt jedoch, die §§ 202a, 202b StGB sowie § 263 Abs. 1 StGB als Schutzgesetze im Rahmen des § 823 Abs. 2 BGB anzuerkennen. Bei denjenigen Missbrauchswegen, die unter diese Strafgesetze fallen, könnte demnach eine Haftung in Betracht kommen. Beim Betrug nach § 263 Abs. 1 StGB kommt ein solcher Anspruch nur in Betracht, sofern der Betrug zu Lasten des Account-Inhabers geschah. Hat der Dritte die Zugangsdaten mit der Absicht missbraucht, den Account-Inhaber beispielsweise aus Mutwillen zu schädigen,[16] kommt eine Haftung aus § 826 BGB in Betracht. 767

II. Haftung des Authentisierungsnehmers

Die Haftung des Authentisierungsnehmers kommt gegenüber zwei anderen Beteiligten, dem Account-Inhaber und dem Geschäftsgegner, in Betracht. Mit dem Account-Inhaber hat der Authentisierungsnehmer ein Vertragsverhältnis, aus dem sich die Pflicht ergibt, auf die Interessen des Account-Inhabers Rücksicht zu nehmen (§ 241 Abs. 2 BGB). Teilweise ergeben sich aus den Verträgen oder aus dem Gesetz spezifische Leistungspflichten. Bei Verletzung dieser Pflichten haftet der Authentisierungsnehmer dem Account- 768

16 Siehe dazu oben Rn. 634.

Inhaber nach §§ 280 Abs. 1, 241 Abs. 2 BGB bzw. nach §§ 280 Abs. 1, Abs. 3, 283 S. 1 BGB.

769 Eine mögliche Pflichtverletzung besteht darin, dass der Authentisierungsnehmer seine Pflicht zur Sicherung der Zugangsdaten, insbesondere deren Geheimhaltung, verletzt. Denkbar ist dabei die unbefugte Offenbarung der Zugangsdaten an einen Unberechtigten.[17] Ebenso stellt es eine Pflichtverletzung dar, wenn der Authentisierungsnehmer seine IT-Infrastruktur nicht ausreichend sichert.[18]

770 Die mangelnde Information des Account-Inhabers über grundsätzliche oder aktuelle Risiken kann ebenfalls eine Pflichtverletzung des Authentisierungsnehmers darstellen. Insbesondere im Rahmen des Online-Bankings werden Aufklärungspflichten der Bank gegenüber ihrem Kunden angenommen, weil diese einen überlegenen Sachverstand besitzt und aktuelle Entwicklungen besser nachverfolgen kann.[19] Ebenso muss der Authentisierungsnehmer sicherstellen, dass ausreichend sichere Authentisierungsmethoden verwendet werden. Bei Banken wird beispielsweise angenommen, dass diese eine Pflicht trifft, Authentisierungsmethoden zu verwenden, die ein angemessenen Schutz gegen Missbrauch bieten.[20]

771 Mit dem Geschäftsgegner hat der Authentisierungsnehmer häufig keine vertragliche Verbindung, auf die eine Haftung gestützt werden könnte. Man könnte erwägen, das Verhältnis des Account-Inhabers mit dem Authentisierungsnehmer, als Schuldverhältnis mit Schutzwirkungen zu Gunsten des Geschäftsgegners anzusehen.[21] Dies wird jedoch regelmäßig an der Erkennbarkeit der einbezogenen Personen für den Authentisierungsnehmer scheitern.[22] Für qualifizierte elektronische Signaturen besteht eine spezialgesetzliche Haftungspflicht des Zertifizierungsdiensteanbieters nach § 11 Abs. 1 S. 1 SigG.[23] Im Rahmen des DeMailG gibt es eine solche Haftung nicht, sodass nur die Anerkennung der Pflichten der Diensteanbieter als Schutzge-

17 Oben Rn. 221.

18 *Borges*, Elektronischer Identitätsnachweis, S. 195; *Borges/Schwenk/Stuckenberg/Wegener*, S. 294; *Spindler*, CR 2011, 309, 317; *Bergfelder*, S. 397.

19 *Borges/Schwenk/Stuckenberg/Wegener*, S. 295; *Borges*, Elektronischer Identitätsnachweis, S. 198 ff.; *ders.*, NJW 2012, 2385, 2388; *Hanau*, Handeln unter fremder Nummer, S. 70; *Kind/Dennis Werner*, CR 2006, 353, 356.

20 *Hanau*, Handeln unter fremder Nummer, S. 71 f.; *Kind/Dennis Werner*, CR 2006, 353, 359; *Schulte am Hülse/Klabunde*, MMR 2010, 84, 88.

21 Ebenso wie bei der Haftung des Account-Inhabers oben Rn. 403 ff.

22 *Spindler*, CR 2011, 309, 317.

23 Dazu *Bergfelder*, S. 395.

setz zu einer Haftung nach § 823 Abs. 2 BGB führen kann.[24] Fehlen gesetzliche Haftungstatbestände oder Pflichten für den Authentisierungsnehmer, kommt eine Haftung von ihm gegenüber dem Geschäftsgegner nicht in Betracht.

24 Diese befürwortend *Spindler*, CR 2011, 309, 317.

§ 10 Beweiserleichterungen bei der Haftung für den Missbrauch von Zugangsdaten im Internet

Neben der materiellen Rechtslage ist für den Geschäftsgegner entscheidend, 772
ob er seinen Anspruch beweisen kann. Die grundsätzliche Regel bei der Beweislastverteilung im Zivilprozess ist, dass jede Partei, die sie begünstigenden Tatsachen zu beweisen hat.[1] Der Geschäftsgegner muss nach diesem Grundsatz beweisen, dass der Account-Inhaber selbst oder ein Dritter mit dessen Einverständnis eine elektronische Willenserklärung abgegeben hat. Dieser Beweis ist dem Geschäftsgegner durch den Augenscheinsbeweis mit dem elektronischen Dokument (§ 371 Abs. 1 S. 2 ZPO) schwer bis gar nicht möglich. Die Echtheit der Erklärung kann der Geschäftsgegner nur in den seltensten Fällen im Rahmen eines Vollbeweises beweisen.[2] Zum Beweis der Echtheit einer elektronischen Erklärung gehört sowohl die Authentizität, also die Urheberschaft der Erklärung, sowie deren Integrität, ein Ausschluss von nachträglichen Veränderungen.[3] Durch umfassende Informationen zum verwendeten Rechner, der IP-Adresse und der Sicherheitsinfrastruktur des Authentisierungsnehmers wäre ein Vollbeweis möglich.[4] Diese Informationen sind jedoch häufig nur staatlichen Behörden zugänglich.[5] Die Echtheit der Erklärung lässt sich nur durch Begleitumstände, nicht durch die Erklärung selbst beweisen.[6] Dies hat zur Folge, dass ein elektronischer Vertragsschluss faktisch nicht mit einem Vollbeweis geführt werden kann.[7]

Diese Beweisschwierigkeiten sind insbesondere bei der Inanspruchnah- 773
me des Account-Inhabers relevant. Ohne eine Beweiserleichterung kann er sich durch Bestreiten vom Vertrag lösen, er hat quasi ein „Widerrufs-

---

1 Diese sog. Rosenbergsche Formel wurde entwickelt von *Rosenberg*[5], S. 98 ff. und ist nunmehr allgemein anerkannt *BGH*, Urteil v. 18. 5. 2005, VIII ZR 368/03 – NJW 2005, 2395, 2396; *Adolphsen*[4], § 23 Rn. 61; *Jauernig/Hess*[30], § 50 Rn. 11; *Lüke*[10], Rn. 277; *Paulus*[4], Rn. 416.

2 *Borges*, Verträge, S. 486; *ders.*, Elektronischer Identitätsnachweis, S. 230; *Borges/Schwenk/Stuckenberg/Wegener*, S. 302.

3 *Bergfelder*, S. 87 ff.

4 *Borges*, Verträge, S. 487.

5 Ebd., S. 487.

6 Ebd., S. 488.

7 *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180; *Borges*, NJW 2005, 3313, 3316.

recht kraft Beweislastverteilung“[8]. Diese Problematik von Schutzbehauptungen kann über die freie richterliche Beweiswürdigung (§ 286 Abs. 1 S. 1 ZPO) oder über Beweiserleichterungen gelöst werden. Nachfolgend sollen zunächst Lösungen über mögliche Beweiserleichterung untersucht werden. Der Behauptung, der Haftung für den Missbrauch von Zugangsdaten sei kein materielles, sondern nur ein prozessuales Problem,[9] kann nicht zugestimmt werden. Über eine prozessuale Lösung kann nur Schutzbehauptungen und Ausreden des sich vom Vertrag lösen wollenden Account-Inhaber begegnet werden. Materiell stellen sich auch bei wahrheitsgemäß aufgeklärtem Sachverhalt Fragen der Zurechnung. Wegen der Beweisschwierigkeiten des Geschäftsgegners ist zu erwägen, ob Beweiserleichterungen für den Vertragsschluss über Accounts im Internet in Betracht kommen. Dazu sollen zunächst unterschiedliche Formen der Beweiserleichterung betrachtet werden, um zu prüfen, ob deren Voraussetzungen beim Missbrauch von Zugangsdaten im Internet vorliegen.

I. Formen der Beweiserleichterung

774 Es existieren verschiedene Formen der Beweiserleichterung. Unter dem Begriff der Beweiserleichterung werden hier sämtliche Formen der Abweichung von der Grundregel, dass eine Partei sie begünstigende Tatsachen zu beweisen hat, verstanden.[10] Dem engen Verständnis, dass nur Erleichterungen bei der Beweiswürdigung erfasst sind,[11] wird nicht gefolgt. Folgend werden Beweiserleichterungen in Form der Beweislastumkehr, des Anscheinsbeweises und der sekundären Darlegungslast untersucht.

1. Beweislastumkehr mit und ohne tatsächlicher Vermutung

775 Die stärkste Form der Beweiserleichterung ist die Umkehr der Beweislast, weil derjenige zu dessen Lasten die Beweislast umgekehrt wurde, den vol-

8 *Mankowski*, CR 2003, 44; *ders.*, MMR 2004, 181.
9 *Probandt*, UFITA 98 (1984), 9, 18.
10 So auch *BGH*, Urteil v. 7. 6. 1988, VI ZR 91/87 (Limonadenflasche) – BGHZ 104, 323, 333; Urteil v. 27. 4. 2004, VI ZR 34/03 (Beckenringfraktur) – BGHZ 159, 48, 53.
11 *Laumen*, NJW 2002, 3739, 3743; *Prütting*, in: *Baumgärtel*[2], § 19 Rn. 7.

len Gegenbeweis erbringen muss. In der Rechtsprechung haben sich zwei Formen der Beweislastumkehr herausgebildet, die folgend vorgestellt werden sollen.

a) Umkehr der Beweislast

Eine Beweislastumkehr kommt in seltenen Fällen in Betracht, in denen methodisch eine Abweichung vom Gesetz begründbar ist.[12] Für die Umkehr der Beweislast haben sich in der Rechtsprechung verschiedene Fallgruppen herausgebildet,[13] die folgend kurz vorgestellt werden, um anschließend herauszufiltern, mit welcher Begründung eine Beweislastumkehr erfolgen kann. 776

Eine Fallgruppe der Beweislastumkehr ist die Produzentenhaftung.[14] Dabei erfolgt eine Beweiserleichterung durch die Abgrenzung der Gefahrenbereiche.[15] Der Produzent könne seinen komplexen Herstellungsprozess mit verschachtelter Arbeitsteilung sowie verwickelten technischen, chemischen oder biologischen Vorgängen, im Gegensatz zu seinem Prozessgegner, überblicken.[16] Ferner sei die hinter §§ 831, 836 BGB stehende Wertung, dass dem Beherrscher einer Gefahrenquelle das Risiko der Unaufklärbarkeit anzulasten ist, auf die Produzentenhaftung übertragbar.[17] Auch für kleine Betriebe mit einem überschaubaren Herstellungsprozess sei die Beweislastumkehr anwendbar, weil der Herstellungsvorgang in die Organisationssphäre des Herstellers fällt, in die der Prozessgegner keinen Einblick hat.[18] Ferner müsse der Hersteller eines Produkts dessen Fehlerfreiheit durch Ausgangskontrollen überprüfen, weil ansonsten die Beweisführung für den Zeitpunkt 777

12 *Prütting*, in: *Baumgärtel*[2], § 19 Rn. 8.
13 Dazu *Musielak*, Grundlagen, S. 132 ff.
14 Dazu *Jauernig/Hess*[30], § 50 Rn. 34; *Prütting*, in: *Baumgärtel*[2], § 19 Rn. 13; *Riehm*, JZ 2006, 1035, 1042 ff.; *Rosenberg/K. H. Schwab/Gottwald*[17], § 115 Rn. 28 f.
15 *Prütting*, in: *Baumgärtel*[2], § 19 Rn. 16.
16 *BGH*, Urteil v. 26. 11. 1968, VI ZR 212/66 (Hühnerpest) – BGHZ 51, 91, 105.
17 *BGH*, Urteil v. 26. 11. 1968, VI ZR 212/66 (Hühnerpest) – BGHZ 51, 91, 106; Urteil v. 24. 11. 1976, VIII ZR 137/75 (Schwimmschalter) – BGHZ 67, 369, 362; Urteil v. 19. 11. 1991, VI ZR 171/91 (Hochzeitsessen) – BGHZ 116, 104, 108.
18 *BGH*, Urteil v. 19. 11. 1991, VI ZR 171/91 (Hochzeitsessen) – BGHZ 116, 104, 109; noch offen gelassen im Urteil v. 26. 11. 1968, VI ZR 212/66 (Hühnerpest) – BGHZ 51, 91, 107.

der Mangelhaftigkeit des Produkts schwer fällt.[19] Unterlässt er Ausgangskontrollen finde ebenfalls eine Beweislastumkehr statt.[20] Mit dieser Beweislastumkehr bei der Produkthaftung besteht ökonomisch betrachtet eine Lage, die einer Gefährdungshaftung für diese Produkte sehr nahe kommt.[21] Insofern erklärt sich die teleologische Begründung, dass der Hersteller diese Gefahren besser versichern könne als der Verwender des Produkts.[22]

778 Die zweite Fallgruppe betrifft eine Umkehr der Beweislast für den Kausalitätsbeweis bei der Arzthaftung.[23] Diese Beweislastumkehr für den Kausalitätsbeweis komme in Betracht, wenn der Arzt einen groben Behandlungsfehler begangen hat.[24] Zwar kann der Arzt die Kausalität nur ebenso schwer beweisen wie der Patient.[25] Durch einen groben Fehler schaffe der Arzt jedoch eine Lage, in der nicht mehr erkennbar ist, was den Fehler verursacht hat, was ihm zu Lasten fällt.[26] Selbst beim Vorliegen eines groben Behandlungsfehlers sei die Beweislastumkehr jedoch ausnahmsweise ausgeschlossen, wenn der Ursachenzusammenhang äußerst unwahrscheinlich ist.[27] Ebenso scheidet bei fehlendem Risikozusammenhang die Beweislastumkehr aus.[28] Das Vorliegen dieser Ausnahmen hat jedoch der Arzt zu beweisen.[29] Eine Beweislastumkehr bei der Arzthaftung komme ebenfalls in Betracht, wenn der Arzt seine Dokumentationspflicht verletzt.[30] Der Patient leide bei mangelnder Dokumentation an einer Beweisnot bezüglich möglicher Behandlungsfehler, sodass ihm durch eine Beweislastumkehr der schwierige Beweis erleichtert wird.[31]

---

19 *BGH*, Urteil v. 7. 6. 1988, VI ZR 91/87 (Limonadenflasche) – BGHZ 104, 323, 334.
20 Ebd., 334.
21 *Schäfer/C. Ott*[5], S. 224. Ohne die rechtsökonomischen Erwägungen auch *Prütting*, in: *Baumgärtel*[2], § 19 Rn. 21.
22 *BGH*, Urteil v. 26. 11. 1968, VI ZR 212/66 (Hühnerpest) – BGHZ 51, 91, 104 f.; *Prütting*, in: *Baumgärtel*[2], § 19 Rn. 18.
23 Dazu *Jauernig/Hess*[30], § 50 Rn. 38; *Musielak*, in: FG 50 Jahre BGH, Bd. 3, 193, 217; *Prütting*, in: *Baumgärtel*[2], § 19 Rn. 25; *Rosenberg/K. H. Schwab/Gottwald*[17], § 115 Rn. 24 ff.
24 *BGH*, Urteil v. 27. 4. 2004, VI ZR 34/03 (Beckenringfraktur) – BGHZ 159, 48, 55; Urteil v. 12. 2. 2008, VI ZR 221/06 – NJW 2008, 1381, Rn. 13.
25 *BGH*, Urteil v. 19. 11. 1955, VI ZR 214/54 – VersR 1956, 499, 500.
26 Ebd., 500.
27 *BGH*, Urteil v. 27. 4. 2004, VI ZR 34/03 (Beckenringfraktur) – BGHZ 159, 48, 55.
28 Ebd., 55.
29 Ebd., 55.
30 *Prütting*, in: *Baumgärtel*[2], § 19 Rn. 32.
31 *BGH*, Urteil v. 27. 6. 1978, VI ZR 183/76 – BGHZ 72, 132, 136 ff.

Die dritte Fallgruppe ist die Beweislastumkehr bei Beweisvereitelung.[32] **779**
Zerstört oder entzieht jemand einem aktuellen oder potentiellen Prozessgegner schuldhaft Beweise, tritt eine Beweislastumkehr zu Lasten desjenigen ein, der die Beweise zerstört oder entzogen hat.[33] Diese Beweislastumkehr bei der Beweisverteilung lasse sich aus dem Rechtsgedanken der §§ 427, 441 Abs. 3 S. 3, 444, 446, 453 Abs. 2, 454 Abs. 1 ZPO ableiten.[34] Das schuldhafte Beeinträchtigen der Beweislage des Gegners in einem aktuellen oder künftigen Prozess rechtfertige es, den Beweisvereiteler die Nachteile der entstehenden Beweisnot tragen zu lassen.[35] Der daraus entstehende Schuldvorwurf muss sich dabei sowohl auf die Zerstörung oder Entziehung des Beweisobjekts als auch auf die Benachteiligung des Gegners in einem Prozess beziehen.[36]

Als Gemeinsamkeit der drei Fallgruppen lässt sich herausfiltern, dass die **780**
Partei, zu Gunsten derer die Beweislastumkehr in Ausnahmefällen angenommen wird, unter der schweren Beweisnot leidet, dass sie gewisse Tatsachen nicht beweisen kann. Bei der Produzentenhaftung entsteht die Beweisnot dadurch, dass sich der Vorgang komplett in der Sphäre des Herstellers abspielt, in die die Gegenpartei keinen Einblick hat, und der Hersteller diese Vorgänge jedoch gestalten und überblicken kann. Bei der Beweisvereitelung entsteht die Beweisnot durch ein vorwerfbares Verhalten der Gegenseite. Der Vernichter von Beweisen solle aus Billigkeitserwägungen keine Vorteile durch sein schuldhaftes Handeln erhalten. Die Begründung bei der Arzthaftung ähnelt jener der Beweisverteilung, weil entscheidend ist, dass der Arzt durch seinen groben Behandlungsfehler den Beweis des Patienten erschwert. Aus den drei Fallgruppen ist noch eine unausgesprochene Voraussetzung abzuleiten. Dem Begünstigten darf es nicht möglich sein, die Beweise selbst herzustellen. Ansonsten könnte ihm die Beweisnot ebenso vorgeworfen werden wie der anderen Partei. Zusammenfassend lässt sich festhalten, dass eine Beweislastumkehr in Betracht kommt, wenn der Begünstigte an einer Beweisnot dadurch leidet, dass der Prozessgegner diese

---

32 Dazu *Jauernig/Hess*[30], § 50 Rn. 30; *Leipold*, in: *Stein/Jonas*[22], § 286 ZPO Rn. 187 ff.; *Prütting*, in: *Baumgärtel*[2], § 19 Rn. 36; *Rosenberg/K. H. Schwab/Gottwald*[17], § 115 Rn. 19 ff.; *Schilken*, Zivilprozessrecht[6], Rn. 507.

33 *BGH*, Urteil v. 23. 9. 2003, XI ZR 380/00 – NJW 2004, 222; Urteil v. 23. 11. 2005, VIII ZR 43/05 – NJW 2006, 434, Rn. 23.

34 *BGH*, Urteil v. 23. 11. 2005, VIII ZR 43/05 – NJW 2006, 434, Rn. 23.

35 *BGH*, Urteil v. 23. 11. 2005, VIII ZR 43/05 – NJW 2006, 434, Rn. 23; *Musielak*, Grundlagen, S. 136.

36 *BGH*, Urteil v. 23. 9. 2003, XI ZR 380/00 – NJW 2004, 222.

schuldhaft hervorgerufen hat oder dass sich die Vorgänge in der Sphäre des Prozessgegners ohne Einblicksmöglichkeit des Begünstigen abspielen und der Begünstigte die Beweisnot nicht anderweitig verhindern kann.

b) Tatsächliche Vermutung

781 Ferner lassen sich in der Rechtsprechung Fälle finden, bei denen eine Beweislastumkehr als Folge einer tatsächlichen Vermutung angenommen wird. Beispielsweise besteht eine tatsächliche Vermutung, dass eine Privaturkunde vollständig ist[37] oder dass die GEMA zur Wahrnehmung der Rechte an öffentlich aufgeführten Musiktiteln berechtigt ist.[38] Tatsächliche Vermutungen sind von gesetzlichen Vermutungen (§ 292 S. 1 ZPO)[39] zu unterscheiden. Im Gegensatz zu diesen sind jene nicht von § 292 ZPO erfasst.[40] Der Begriff der tatsächlichen Vermutung wird unterschiedlich verwendet.[41] Zum einen kann eine tatsächliche Vermutung als Grundlage eines Anscheinsbeweises verstanden werden.[42] Zum anderen wird eine tatsächliche Vermutung zur Begründung einer sekundären Darlegungslast verwendet.[43] Ferner kann als tatsächliche Vermutung die Umkehr der Beweislast verstanden werden.[44] Letzterem Verständnis der tatsächlichen Vermutung wird vorgeworfen, dass eine Erwägung mit Erfahrungswissen ausschließlich im Bereich der Beweiswürdigung und nicht der Beweislast anzusiedeln sei.[45] Ein Umkehren der Beweislast mit Hilfe der tatsächlichen Vermutung

37 *BGH*, Urteil v. 11. 11. 1977, V ZR 105/75 – WM 1978, 244.

38 *BGH*, Urteil v. 5. 6. 1985, I ZR 53/83 (GEMA-Vermutung I) – BGHZ 95, 274, 276 f.

39 Dazu *Lüke*[10], Rn. 266; *Paulus*[4], Rn. 427; *Musielak*, Grundkurs[11], Rn. 480.

40 *Lüke*[10], Rn. 266; *Musielak*, JA 2010, 561; *Prütting*, in: MüKo-ZPO[4], § 292 Rn. 7; **a.A.** *Bruns*[2], Rn. 171c.

41 *Allner*, S. 21 ff.; *Prütting*, Gegenwartsprobleme, S. 57.

42 So *BGH*, Urteil v. 9. 10. 2009, V ZR 178/08 – NJW 2010, 363, Rn. 15; *Schellhammer*[14], Rn. 519; *Baumgärtel*, in: FS Schwab, 43, 50.

43 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 12; Urteil v. 15. 11. 2012, I ZR 74/12 (Morpheus) – NJW 2013, 1441, Rn. 33 f.

44 So *BGH*, Urteil v. 11. 11. 1977, V ZR 105/75 – WM 1978, 244; Urteil v. 5. 6. 1985, I ZR 53/83 (GEMA-Vermutung I) – BGHZ 95, 274, 276.

45 *Allner*, S. 55 ff.; *Laumen*, in: *Prütting/Gehrlein*[5], § 292 ZPO Rn. 7; *Prütting*, Gegenwartsprobleme, S. 55; *Rosenberg/K. H. Schwab/Gottwald*[17], § 113 Rn. 37.

umgehe häufig die Voraussetzungen der Rechtsfortbildung.[46] Unabhängig davon, wie berechtigt diese Kritik ist, wird die tatsächliche Vermutung im Folgenden im Bereich der Beweislast angesiedelt. Vielfach lässt sich in der Rechtsprechung eine tatsächliche Vermutung mit der Folge einer Beweislastumkehr finden. Für diese wird hier der Begriff der tatsächlichen Vermutung verwendet. Dadurch wird eine begriffliche Trennung zwischen dem Problem der Beweiswürdigung mit dem Anscheinsbeweis und der Beweislastverteilung durch die tatsächliche Vermutung ermöglicht.

782 Eine tatsächliche Vermutung mit der Folge der Umkehr der Beweislast wird von der Rechtsprechung häufig ohne nähere Begründung angenommen. Dadurch kann die dogmatische Herleitung der tatsächlichen Vermutung ebenso wie deren Voraussetzungen nur schwer bestimmt werden. Beispielsweise wird ohne nähere Begründung bei Wettbewerbsverstößen die Wiederholungsgefahr tatsächlich vermutet und kann insbesondere durch eine strafbewehrte Unterlassungserklärung widerlegt werden.[47] Eine inhaltsgleiche tatsächliche Vermutung besteht auch bei der Wiederholungsgefahr bezüglich der Verwendung unwirksamer AGB.[48] Bei 20-jähriger Durchführung einer vom OHG-Gesellschaftsvertrag abweichenden Gewinnverteilung spreche eine tatsächliche Vermutung für die verbindliche Abänderung unter Verzicht auf die Schriftform.[49] Bei Verstoß gegen eine DIN-Norm besteht eine tatsächliche Vermutung dafür, dass Risiken, die die Norm verhindern soll, kausal auf der Verletzung der Norm beruhen.[50] Erschwerend kommt bei der Bestimmung der Voraussetzungen hinzu, dass der Begriff, der tatsächlichen Vermutung nicht einheitlich verwendet wird. Teilweise wird eine tatsächliche Vermutung im Bereich der Produkthaftung angenommen,[51] obwohl dort bereits aus anderem Grund eine Beweislastumkehr angenommen wird.

783 Einige Entscheidungen geben jedoch Einblick in die Erwägungsgründe, unter welchen Voraussetzungen eine tatsächliche Vermutung anzunehmen ist. Beispielsweise die tatsächliche Vermutung, dass eine Privaturkunde

46 *Laumen*, in: *Baumgärtel*[2], § 14 Rn. 21; *Prütting*, Gegenwartsprobleme, S. 54 f.; *ders.*, in: MüKo-ZPO[4], § 292 Rn. 28.

47 *BGH*, Urteil v. 8. 2. 1980, I ZR 22/78 (Grand Prix) – NJW 1980, 1793, 1794.

48 *BGH*, Urteil v. 9. 7. 1981, VII ZR 123/80 – BGHZ 81, 222, 225 f.

49 *BGH*, Urteil v. 17. 1. 1966, II ZR 8/64 – NJW 1966, 826, 827.

50 *BGH*, Urteil v. 19. 4. 1991, V ZR 349/89 – BGHZ 114, 273, 276, wobei jedoch nur von einer „widerleglichen Vermutung" gesprochen wird.

51 So *BGH*, Urteil v. 12. 11. 1991, VI ZR 7/91 (Kindertee) – BGHZ 116, 60, 73.

vollständig ist,[52] wurde so begründet, dass sich daraus Voraussetzungen für deren Annahme herausarbeiten lassen. Eine tatsächliche Vermutung beruht auf allgemeinen Erfahrungssätzen aus der Lebenserfahrung.[53] Häufig wird die tatsächliche Vermutung über Wahrscheinlichkeitserwägungen begründet.[54] Der Behauptung, dass eine überwiegende Wahrscheinlichkeit bereits zur Annahme einer tatsächlichen Vermutung ausreiche,[55] kann nicht zugestimmt werden.[56] Bei der GEMA-Vermutung beruht die überwiegende Wahrscheinlichkeit an der Quasi-Monopolstellung der GEMA bei der Wahrnehmung von Urheberrechten an gewissen Werken, sodass mit hoher Wahrscheinlichkeit bei der Verwendung von Musik von der GEMA wahrgenommene Rechte betroffen sind.[57] Ferner solle der gesetzgeberische Wille leistungsfähige Verwertungsgesellschaften zu schaffen, mit der Beweiserleichterung verwirklicht werden.[58] Als Voraussetzung lässt sich somit herausfiltern, dass aufgrund der Lebenserfahrung mit hoher Wahrscheinlichkeit auf eine Tatsache geschlossen werden kann. Die effektive Rechtsdurchsetzung wegen ansonsten bestehender Beweisnot kann ebenfalls zur Begründung herangezogen werden.

784 Die tatsächliche Vermutung führt objektiv zu einer Umkehr der Beweislast für das Vorliegen der vermuteten Haupttatsachen.[59] Um die tatsächliche Vermutung zu entkräften, muss der volle Gegenbeweis erbracht werden.[60] Eine solche Beweispflicht kommt daher nur in Betracht, wenn eine Tatsache außerhalb des von der darlegungspflichtigen Partei zu klärendem Geschehensablaufs stattfindet, während der Prozessgegner Kenntnis habe und auch Aufklärung von ihm verlangt werden kann.[61] Die tatsächliche Vermutung

52 *BGH*, Urteil v. 11. 11. 1977, V ZR 105/75 – WM 1978, 244; Urteil v. 5. 7. 2002, V ZR 143/01 – NJW 2002, 3164, 3165. Dazu *Allner*, S. 42 ff.

53 *Allner*, S. 37, 65; *Huber*, in: *Musielak*[10], § 292 ZPO Rn. 1; *Lüke*[10], Rn. 266; *Musielak*, Grundkurs[11], Rn. 480.

54 *Wassermeyer*, S. 35 m.w.N.

55 *Bruns*[2], Rn. 171c.

56 *Laumen*, in: *Baumgärtel*[2], § 14 Rn. 7.

57 *BGH*, Urteil v. 5. 6. 1985, I ZR 53/83 (GEMA-Vermutung I) – BGHZ 95, 274, 277; Urteil v. 13. 6. 1985, I ZR 35/83 (GEMA-Vermutung II) – BGHZ 95, 285, 290.

58 *BGH*, Urteil v. 13. 6. 1985, I ZR 35/83 (GEMA-Vermutung II) – BGHZ 95, 285, 290 f.

59 *Förschler/Steinle*[7], Rn. 817; *Laumen*, in: *Prütting/Gehrlein*[5], § 292 ZPO Rn. 6; *Musielak*, JA 2010, 561.

60 *BGH*, Urteil v. 11. 11. 1977, V ZR 105/75 – WM 1978, 244.

61 *Musielak*, Grundkurs[11], Rn. 403; *Prütting*, in: MüKo-ZPO[4], § 286 Rn. 131.

muss dem Beweis des Gegenteils zugänglich sein.[62] Wenn der Gegner nicht die Möglichkeit hat, das Gegenteil zu beweisen, kommt eine tatsächliche Vermutung somit nicht in Betracht. Alternative Möglichkeiten schließen die Vermutung nicht aus, wie beispielsweise das häufige Falschbeurkunden eines Grundstückkaufvertrags.[63] Sie sind der Gegenstand eines möglichen Gegenbeweises. Im Gegensatz zur gesetzlichen Vermutung muss bei der tatsächlichen Vermutung nicht nur die Vermutungsbasis vorgetragen werden, sondern auch die vermutete Tatsache.[64]

2. *Anscheinsbeweis*

Der Anscheinsbeweis, auch Beweis des ersten Anscheins oder *prima-facie*-Beweis genannt,[65] ist eine Form der mittelbaren Beweisführung im Rahmen der freien Beweiswürdigung (vgl. § 286 Abs. 1 S. 1 ZPO) durch den Richter im Zivilprozess.[66] Beim Anscheinsbeweis wird von einem typischen Geschehensverlauf nach der allgemeinen Lebenserfahrung auf das Vorliegen einer bestimmten Ursache oder Folge geschlossen.[67] Der Anscheinsbeweis ist nicht gesetzlich normiert, wird aber in § 371a ZPO vorausgesetzt.[68] Er statuiert keine Beweislastumkehr, sondern verhindert eine *non-liquet*-Situation.[69] Für die Begründung eines Anscheinsbeweises wird häufig der Gedanke der Sphären herangezogen, dass jede Partei für ihren Gefahrenbereich verantwortlich ist und Nachteile zu tragen hat, die durch die Unaufklärbarkeit der aus ihrer Sphäre stammenden Tatsachen entstehen.[70] Dabei erfüllt der Anscheinsbeweis häufig die Funktion eines Irgendwie-Beweises.[71] Kann beispielsweise das Verschulden nicht voll bewiesen werden, führen jedoch die meisten und die wahrscheinlichen Möglichkeiten zum gleichen rechtlichen Ergebnis, wird angenommen, dass ein Verschulden, egal welcher Art, vorliegt. **785**

62 *BGH*, Urteil v. 5. 7. 2002, V ZR 143/01 – NJW 2002, 3164, 3165.
63 *BGH*, Urteil v. 11. 11. 1977, V ZR 105/75 – WM 1978, 244.
64 *BGH*, Urteil v. 9. 10. 2009, V ZR 178/08 – NJW 2010, 363, Rn. 13.
65 *Adolphsen*[4], § 23 Rn. 38; *Musielak*, Grundlagen, S. 83.
66 *Prütting*, in: MüKo-ZPO[4], § 286 Rn. 48; *Schellhammer*[14], Rn. 518.
67 *Lüke*[10], Rn. 279; *Foerste*, in: *Musielak*[10], § 286 ZPO Rn. 23; *Paulus*[4], Rn. 424.
68 *Jauernig/Hess*[30], § 50 Rn. 11; *Musielak*, Grundkurs[11], Rn. 468.
69 *Adolphsen*[4], § 23 Rn. 40.
70 *Hanau*, Handeln unter fremder Nummer, S. 53.
71 *Prütting*, Gegenwartsprobleme, S. 110; *Kollhosser*, AcP 165 (1965), 46, 62 f.

786 Ein Erfahrungssatz, der einen Anscheinsbeweis begründet, basiert auf der Beobachtung, dass beim Eintreten einer bestimmten Tatsache nicht zwingend, aber mit hoher Wahrscheinlichkeit oder aufgrund eines Musters auf das Vorliegen einer Ursache oder Folge zu schließen ist.[72] Er muss so stark sein, dass er die volle Überzeugung des Gerichts von der behaupteten Tatsache begründet.[73] Typisch ist ein Geschehensablauf, wenn er nach der Erfahrung des täglichen Lebens durch das Regelmäßige, Übliche, Gewöhnliche und Häufige seines Ablaufs sein Gepräge erhält.[74] Ein solcher Erfahrungssatz entsteht durch die induktive Verallgemeinerung.[75] Dieser Erfahrungssatz ist zu unterscheiden von einem einfachen Erfahrungssatz, der sich dadurch auszeichnet, dass die Wahrscheinlichkeit, wenn die eine Tatsache vorliegt, auch die Ursache oder Folge vorliegt, nicht ausreichend hoch ist, um für die volle richterliche Überzeugung auszureichen.[76]

787 Für die Begründung eines Erfahrungssatzes für einen Anscheinsbeweis kommt es nicht auf eine empirische Statistik an.[77] Bei der Wahrscheinlichkeit handelt es sich nämlich um eine Aussage bezüglich einer statistischen Masse, wohingegen im Einzelfall die Aussage entweder zutrifft oder nicht zutrifft.[78] Vielmehr kommt es darauf an, dass nach logischen Erwägungen, die von der allgemeinen Lebenserfahrung gedeckt sind, eine hohe Wahrscheinlichkeit für den typischen Geschehensablauf spricht.[79] Es reiche nicht aus, dass bei zwei verschiedenen Möglichkeiten eine wahrscheinlicher ist als die andere.[80] Diese Anforderung wird jedoch in der Rechtsprechung nicht konsequent durchgehalten. Ein Anscheinsbeweis kommt nicht in Betracht, wenn der Begünstigte seine Beweisnot anderweitig verhindern kann. Bei einem versendeten Brief steht dem Absender beispielsweise durch die

72 *Laumen*, in: *Baumgärtel*[2], § 12 Rn. 12; *Musielak*, Grundlagen, S. 94 ff.; *Prütting*, in: MüKo-ZPO[4], § 286 Rn. 58.

73 *Laumen*, in: *Prütting/Gehrlein*[5], § 286 ZPO Rn. 26; *Leipold*, in: *Stein/Jonas*[22], § 286 ZPO Rn. 130.

74 *BGH*, Urteil v. 27. 5. 1957, II ZR 132/56 (Einschreibbrief) – BGHZ 24, 308, 312; Urteil v. 18. 3. 1987, IVa ZR 205/85 – BGHZ 100, 214, 216.

75 *Jungmann*, ZZP 120 (2007), 459, 461; *ders.*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 344.

76 *Prütting*, Gegenwartsprobleme, S. 108; *ders.*, in: MüKo-ZPO[4], § 286 Rn. 60.

77 *BGH*, Urteil v. 27. 5. 1957, II ZR 132/56 (Einschreibbrief) – BGHZ 24, 308, 312; *Prütting*, Gegenwartsprobleme, S. 94.

78 *Musielak*, in: FG 50 Jahre BGH, Bd. 3, 193, 204 f.

79 *Prütting*, Gegenwartsprobleme, S. 106.

80 *BGH*, Urteil v. 27. 5. 1957, II ZR 132/56 (Einschreibbrief) – BGHZ 24, 308, 313.

förmliche Zustellung oder ein Einschreiben mit Rückschein die Möglichkeit zu, einen sicheren Beweis zu schaffen.[81] Daher besteht insoweit kein Bedürfnis ihm mit einer Beweiserleichterung zu helfen.

Andererseits lassen sich auch Fälle feststellen, bei denen unter zwei oder mehr vergleichbar wahrscheinlichen Möglichkeiten, die leicht überwiegend wahrscheinliche gewählt wurde. Dies geschieht dort, wo Beweisnot herrscht und wo Erfahrungssätze, die sich durch Häufigkeit, Üblichkeit und Gleichmäßigkeit auszeichnen, fehlen. Dabei werden im Ausschlussverfahren unwahrscheinliche Geschehensabläufe eliminiert.[82] Dieser „Anscheinsbeweis ohne ersten Anschein“[83] lässt sich in diversen Entscheidungen des *BGH* wiederfinden.[84] Beim lautlosen Ertrinken eines Nichtschwimmers spreche beispielsweise ein Anscheinsbeweis für die Ursächlichkeit einer fehlenden Absperrung, wobei körperliche Mängel als Alternativmöglichkeit unwahrscheinlich sind, aber den Anscheinsbeweis erschüttern könnten.[85] Bei der nicht vollbewiesenen Erkrankung mit Lues spreche ein Anscheinsbeweis dafür, dass gewisse Symptome für eine Lues und keine andere Krankheit sprechen und dass die Infektion auf eine fünf Jahre zurückliegende Bluttransfusion zuzuführen sei.[86] Dabei reiche es aus, dass der vermeintlich typische Geschehensablauf in „Gutachten der Sachverständigen nicht ausgeschlossen“ wurde und dass zu der Frage wenig Erfahrungsmaterial vorliegt.[87] Ebenso spreche ein Anscheinsbeweis dafür, dass eine Ehefrau ihren Mann bei einer Bluttransfusion mit Lues angesteckt hat, obwohl nicht feststand, dass die Frau sich vor der Transfusion mit Lues angesteckt hatte.[88] Ferner spreche ein Anscheinsbeweis dafür, dass sich der Unfall eines Gaststättenbesuchers beim Verlassen der Gaststätte und nicht bei einer späteren Rückkehr ereignete.[89] Diese Fälle haben gemeinsam, dass zahlreiche ver- 788

81 *BGH*, Urteil v. 27. 5. 1957, II ZR 132/56 (Einschreibbrief) – BGHZ 24, 308, 313; *Prütting*, Gegenwartsprobleme, S. 105.

82 *Jungmann*, ZZP 120 (2007), 459, 465; *ders.*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 346.

83 *Jungmann*, ZZP 120 (2007), 459.

84 Zu den Fällen *Jungmann*, ZZP 120 (2007), 459, 462 ff.; *Kollhosser*, AcP 165 (1965), 46, 75; *Musielak*, Grundlagen, S. 99 ff.

85 *BGH*, Urteil v. 3. 2. 1954, VI ZR 332/52 (Nichtschwimmer) – NJW 1954, 1119, 1119 f.

86 *BGH*, Urteil v. 14. 12. 1953, III ZR 183/52 (Lues I) – BGHZ 11, 227, 230 f.

87 Ebd., 231.

88 *BGH*, Urteil v. 12. 2. 1957, VI ZR 303/56 (Lues II) – VersR 1957, 252.

89 *BGH*, Urteil v. 17. 12. 1953, III ZR 136/52 – VersR 1954, 401, 402.

schiedene Möglichkeiten des Geschehensablaufs in Betracht kommen und sich keine überwiegend wahrscheinliche Möglichkeit herausbildet. Wahrscheinlich aus der einhergehenden Beweisnot wurde dennoch zu Gunsten des Geschädigten ein Anscheinsbeweis angenommen. Problem ist, dass wenn eine Tatsache für beide Seiten schwer zu beweisen ist, das Problem des Beweises und somit auch das Risiko, die Tatsache nicht beweisen zu können, auf die Gegenpartei verlagert wird.[90] Deswegen muss bei dem Anscheinsbeweis ohne ersten Anschein die sich auf den Anscheinsbeweis berufende Partei die Unwahrscheinlichkeit der auszuschließenden anderen Möglichkeiten beweisen.[91]

789 Die Anwendung des Anscheinsbeweises ist durch das Revisionsgericht überprüfbar,[92] wodurch der Anscheinsbeweis die freie Beweiswürdigung unter die Kontrolle des Revisionsgerichts in typisierbaren Fällen stellt.[93] Der Grund für die Bindung des Revisionsgerichts an die Tatsachenfeststellungen ist die Sachnähe bei der unmittelbaren Beweisaufnahme.[94] Bei typischen Sachverhalten hingegen ist keines der Gerichte sachnäher und es besteht ein Bedürfnis, typische Erfahrungssätze ebenso wie Rechtssätze in der Rechtsprechung zu vereinheitlichen.[95]

790 Für die Entkräftung des Anscheinsbeweises mittels eines Gegenbeweises, muss die Gegenseite den Anscheinsbeweis *erschüttern*,[96] indem sie konkrete Tatsachen behauptet, die in der Überzeugung des Gerichtes einen vom Erfahrungssatz abweichenden Geschehensablauf möglich erscheinen lässt.[97] Eine Beweislastumkehr, die den Beweis des Gegenteils zur Folge hätte, statuiert der Anscheinsbeweis gerade nicht.[98] Erhebliche Zweifel am Beweis können durch die ernsthafte Möglichkeit eines atypischen Gesche-

---

90 *Prütting*, Gegenwartsprobleme, S. 211.

91 *Jungmann*, ZZP 120 (2007), 459, 471; **a.A.** *BGH*, Urteil v. 14. 12. 1953, III ZR 183/52 (Lues I) – BGHZ 11, 227, 231.

92 *BGH*, Urteil v. 4. 10. 1983, VI ZR 98/82 – NJW 1984, 432, 433; *Prütting*, in: MüKo-ZPO[4], § 286 Rn. 66; *Riehm*, Abwägungsentscheidungen, S. 186; *Laumen*, in: *Baumgärtel*[2], § 12 Rn. 41.

93 *Riehm*, Abwägungsentscheidungen, S. 91.

94 Ebd., S. 216.

95 Ebd., S. 216; **a.A.** wohl *Kollhosser*, AcP 165 (1965), 46, 55.

96 *Adolphsen*[4], § 23 Rn. 42; *Jauernig/Hess*[30], § 50 Rn. 25.

97 *Laumen*, in: *Baumgärtel*[2], § 12 Rn. 34; *Schellhammer*[14], Rn. 519; *Prütting*, in: MüKo-ZPO[4], § 286 Rn. 65.

98 *BGH*, Urteil v. 5. 2. 1987, I ZR 210/84 (Raubpressungen) – BGHZ 100, 31, 34.

hensablaufs im konkreten Fall begründet werden.[99] Dazu müssen konkrete Tatsachen vorgetragen werden.[100]

Anscheinsbeweis und tatsächliche Vermutung erleichtern somit die Be- **791**
weisführung für die beweisbelastete Partei. Der Unterschied zwischen den beiden ist, dass zum Widerlegen des Anscheinsbeweises das Erschüttern der Vermutungsgrundlage ausreicht, wohingegen bei der tatsächlichen Vermutung der volle Gegenbeweis erbracht werden muss. Die Voraussetzungen für das Anerkennen dieser beiden Beweiserleichterungen ähneln sich durch das Abstellen auf Erfahrungssätze der Lebenserfahrung und auf Wahrscheinlichkeiten. Wegen der Unklarheit der Herleitung und des Anwendungsbereichs der tatsächlichen Vermutung[101] sowie der vorgeworfenen Nähe zum Anscheinsbeweis lassen sich die beiden Beweiserleichterungen in ihren Voraussetzungen nicht klar von einander abtrennen. Die tatsächliche Vermutung hat jedoch mit der Beweislastumkehr eine stärkere Rechtsfolge, sodass aufgrund der ähnlichen Voraussetzungen festgehalten werden kann, dass an die Anerkennung einer tatsächlichen Vermutung höhere Anforderungen als an das Anerkennen eines Anscheinsbeweises zu stellen sind.

3. Sekundäre Darlegungslast

Die Darlegungslast, auch Behauptungslast genannt,[102] regelt, welche Par- **792**
tei eine Behauptung aufstellen muss, um prozessuale Nachteile zu vermeiden.[103] Die Notwendigkeit begünstigende Tatsachen selbst vorzutragen, ergibt sich aus der Verhandlungsmaxime.[104] Behauptungs- und Beweislast stimmen grundsätzlich überein,[105] sodass jede Partei für sie begünstigende Umstände zu behaupten und zu beweisen hat.[106] Ausnahmsweise kann sich jedoch eine sekundäre Darlegungslast, auch Substantiierungslast genannt,[107] ergeben.

---

99 *Leipold*, in: *Stein/Jonas*[22], § 286 ZPO Rn. 139; *Reichold*, in: *Thomas/Putzo*[34], § 286 ZPO Rn. 13.
100 *Leipold*, in: *Stein/Jonas*[22], § 286 ZPO Rn. 139.
101 *Laumen*, in: *Baumgärtel*[2], § 14 Rn. 1.
102 *Paulus*[4], Rn. 413; *Prütting*, in: MüKo-ZPO[4], § 286 Rn. 134.
103 *Jauernig/Hess*[30], § 50 Rn. 1.
104 *Laumen*, in: *Prütting/Gehrlein*[5], § 286 ZPO Rn. 70.
105 *Jauernig/Hess*[30], § 50 Rn. 1.
106 Oben Rn. 772.
107 *Laumen*, in: *Prütting/Gehrlein*[5], § 286 ZPO Rn. 73.

793 Voraussetzung für eine solche sekundäre Darlegungslast ist, dass die beweisbelastete Partei Informationen nicht hat oder deren Beschaffung unzumutbar ist.[108] Dafür reicht es noch nicht aus, dass es der einen Partei wesentlich schwerer fällt als der anderen Partei.[109] Sie muss vielmehr alles Mögliche und Zumutbare tun, damit von der Gegenpartei eine Aufklärung verlangt werden kann.[110] Die Gegenpartei hingegen muss genaue Kenntnis von diesen bestimmten rechtserheblichen Tatsachen haben oder ihr muss die Beschaffung der Informationen leicht sein und ihr muss ein Vortrag zu den Tatsachen zumutbar sein.[111] Die Informationen müssen sich auf Vorgänge im Wahrnehmungsbereich der Gegenpartei beziehen.[112] Allein die Tatsache, dass die Darlegung der beweisbelasteten Partei wesentlich schwerer fällt als der Gegenpartei, reicht nicht aus.[113]

794 Die Partei mit der Darlegungslast muss lediglich pauschal eine Tatsache behaupten,[114] für die jedoch eine gewisse Wahrscheinlichkeit sprechen muss.[115] Die Gegenpartei muss anschließend durch ein substantiiertes Vorbringen diese Behauptung bestreiten.[116] Falls ihr dies nicht gelingt, gelten die Behauptungen der beweisbelasteten Partei als nach § 138 Abs. 3 ZPO zugestanden.[117] Wenn die Partei es jedoch ohne überzeugenden Grund unterlässt einen Beweis zu erbringen, obwohl nur sie über die Möglichkeit verfügt, spricht die Lebenserfahrung dafür, dass ein solcher nicht vorhanden sind.[118] Der Umfang des substantiierten Bestreitens hängt vom Wechselspiel zwischen Vortrag und Gegenvortrag ab.[119] Gelingt hingegen das substantiierte Bestreiten, geht die Beweislast nicht über.[120] Die beweisbe-

---

108 *BGH*, Urteil v. 7. 12. 1998, II ZR 266/97 – BGHZ 140, 156, 158; *Leipold*, in: *Stein/Jonas*[22], § 138 ZPO Rn. 37.

109 *BGH*, Urteil v. 17. 10. 1996, IX ZR 293/95 – NJW 1997, 128, 129.

110 *Musielak*, in: FG 50 Jahre BGH, Bd. 3, 193, 197.

111 *BGH*, Urteil v. 1. 12. 1982, VIII ZR 279/81 – BGHZ 86, 23, 29; *Musielak*, Grundkurs[11], Rn. 403; *Prütting*, in: MüKo-ZPO[4], § 286 Rn. 103; *Reichold*, in: *Thomas/Putzo*[34], Vorbem § 284 ZPO Rn. 18.

112 *Leipold*, in: *Stein/Jonas*[22], § 138 ZPO Rn. 37.

113 Ebd., § 138 ZPO Rn. 37.

114 *Laumen*, in: *Prütting/Gehrlein*[5], § 286 ZPO Rn. 73; *Jauernig/Hess*[30], § 50 Rn. 3.

115 *Musielak*, Grundkurs[11], Rn. 403.

116 *Laumen*, in: *Prütting/Gehrlein*[5], § 286 ZPO Rn. 73; *Jauernig/Hess*[30], § 50 Rn. 3.

117 *Jauernig/Hess*[30], § 50 Rn. 3; *Musielak*, Grundkurs[11], Rn. 403; *Prütting*, in: MüKo-ZPO[4], § 286 Rn. 103.

118 *Musielak*, Grundkurs[11], Rn. 403.

119 *Prütting*, in: MüKo-ZPO[4], § 286 Rn. 136.

120 *Leipold*, in: *Stein/Jonas*[22], § 138 ZPO Rn. 38.

lastete Partei muss dann beweisen, dass die beim substantiierten Bestreiten vorgebrachten Tatsachen nicht zutreffen.[121]

II. *Schutzbehauptungen durch freie richterliche Beweiswürdigung verhindern*

Die Notwendigkeit für Beweiserleichterungen wird dadurch begründet, dass sich der Account-Inhaber ohne solche durch eine einfache Behauptung vom Vertrag lösen könnte. Eine Alternative zur Beweiserleichterung besteht jedoch darin, dass diese Schutzbehauptung als solche entlarvt wird und unberücksichtigt bleibt. Über die freie richterliche Beweiswürdigung (§ 286 Abs. 1 S. 1 ZPO) können solche Schutzbehauptungen verhindert werden.[122] Wird eine Behauptung spät vorgetragen, beispielsweise erst im Prozess, so kann ein Richter diese als Schutzbehauptung entlarven und unberücksichtigt lassen.[123] Bei der Zurückweisung von Schutzbehauptungen besteht das allgemeine Problem, dass ein Richter nicht gegen den Anspruch auf rechtliches Gehör verstoßen darf (Art. 103 Abs. 1 GG). Erhebt er bezüglich Ausführungen einer Partei, die er als Schutzbehauptung ansieht, keinen Beweis, verstößt er gegen den Anspruch der behaupteten Partei auf rechtliches Gehör.[124] Erhebt er jedoch Beweis bezüglich der Behauptung kann er im Rahmen seiner freien Beweiswürdigung zum Schluss kommen, dass es sich um eine Schutzbehauptung handelt. **795**

In der Rechtsprechung lassen sich Fälle finden, bei denen eindeutig keine Schutzbehauptungen vorliegen. Das *LG Köln* hat im Rahmen der freien Beweiswürdigung einem Besitzer eines Imbissanhängers geglaubt, dass ihm ein übler Streich gespielt wurde, als der Anhänger auf einer Internet-Auktionsplattform zum Verkauf angeboten wurde, obwohl der Besitzer den Wagen auf weiteren Vergnügungsmärkten einzusetzen beabsichtigte.[125] Beispielsweise konnte sich das *LG Kassel* davon überzeugen, dass der Enkel und nicht dessen 82-jährige Großmutter, die glaubhaft über keine techni- **796**

121 *BAG*, Urteil v. 12. 8. 1976, 2 AZR 237/75 – NJW 1977, 167; *LG Düsseldorf*, Urteil v. 21. 3. 2012, 12 O 579/10 – NJW 2012, 3663, 3663 f.; *Leipold*, in: *Stein/Jonas*[22], § 138 ZPO Rn. 38.

122 So auch *KG Berlin*, Urteil v. 10. 3. 2005, 8 U 122/04 – MDR 2005, 1431.

123 Siehe *OLG Hamm*, Beschluss v. 22. 8. 2006, 2 Ss OWi 528/06 – NZV 2007, 96, 97.

124 Vgl. *KG Berlin*, Urteil v. 10. 3. 2005, 8 U 122/04 – MDR 2005, 1431.

125 *LG Köln*, Urteil v. 27. 10. 2005, 8 O 15/05 – BeckRS 2006, 07259.

schen Kenntnisse verfügt, den auf die Großmutter lautenden Account verwendet hat.[126]

797 Im Gegensatz lassen sich Schutzbehauptungen nach einer Abwägungen der Umstände im Einzelfall auch entlarven. Die Annahme einer Schutzbehauptung liegt beispielsweise nahe, wenn ein Anschlussinhaber behauptet, nicht er sondern seine minderjährige Tochter hätte pornographische Inhalte über den Bildschirmtext-Anschluss abgerufen.[127] Ein Indiz für eine Schutzbehauptung kann ebenfalls sein, wenn der Anschluss-Inhaber eines Internetanschlusses behauptet, der illegale Download von Musik sei durch seinen dreizehnjährigen Sohn ohne Wissen des Anschlussinhabers erfolgt, sich jedoch auf dem Computer des Sohns ein Ordner namens „Papas Music" befindet, in dem Musik gespeichert ist, die von Jugendlichen im Alter des Sohns regelmäßig nicht gehört wird.[128]

798 Die Umstände des Einzelfalls können auch in weiteren Fällen auf Schutzbehauptungen hindeuten. Ein spätes Bestreiten der Abgabe oder das späte Behauptung eines Missbrauchs können Indizien für eine Schutzbehauptung sein. Ein vorheriger Kontakt mit dem Geschäftsgegner, bei dem die später erfolgte Erklärung angekündigt wurde, kann bei späterem Bestreiten ein Indiz für eine Schutzbehauptung sein. Wenn durch reihenweises Bestreiten verschiedener Tatsachen an der Glaubwürdigkeit dieser Behauptungen ernsthafte Zweifel bestehen, kann ein Gericht dadurch Schutzbehauptungen erkennen. In einem Fall glaubte das *AG München* dem Beklagten nicht.[129] Er hatte behauptet, dass er die Willenserklärung über den Account nicht abgegeben habe und dass er den Account nicht erstellt habe. Darüber hinaus bestritt er den Empfang für ein Dokument, dessen Empfang er schriftlich quittiert hatte. Wegen dieser Lüge wertete das *AG München* die anderen Behauptungen auch als Schutzbehauptungen.[130] Dies zeigt, dass die freie richterliche Beweiswürdigung durchaus in der Lage ist, durch die Gesamtheit des Vortrags einer Partei und deren Glaubwürdigkeit Schutzbehauptungen zu erkennen und deren Auswirkungen zu verhindern. Weitere Indizien für Schutzbehauptungen liegen vor, wenn die Willenserklärung mittels einer IP-Adresse abgegeben wurde, die geographisch dem Bereich des Account-Inhabers zuzuordnen und auf seinen Internet-Anbieter registriert ist. Wei-

126 *LG Kassel*, Urteil v. 15. 4. 2008, 9 O 2539/06 – NJW-RR 2009, 781.
127 Vgl. *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400.
128 *OLG Köln*, Urteil v. 23. 3. 2012, 6 U 67/11 – MMR 2012, 387, 389.
129 *AG München*, Urteil v. 24. 4. 2007, 161 C 24310/05 – CR 2007, 816, 817.
130 Ebd., 817.

tere Indizien können sein, dass in einem Text Spezialwissen oder für den Account-Inhaber typische Ausdrücke verwendet wurden.

Die Möglichkeit, Schutzbehauptungen über die freie richterliche Beweis- 799
würdigung zu entlarven, zeigt, dass das Problem nicht notwendigerweise über Beweiserleichterungen gelöst werden muss. Für den Geschäftsgegner sind Beweiserleichterungen jedoch vorteilhafter, weil die Situation für die Schutzbehauptungen umgedreht wird. Der Geschäftsgegner muss grundsätzlich beweisen, dass eine Erklärung vom Account-Inhaber stammt und gegebenenfalls, dass sein Bestreiten eine Schutzbehauptung darstellt. Bei einer Beweiserleichterung muss der Account-Inhaber darlegen oder beweisen, dass er die Erklärung nicht abgegeben hat.

III. Anerkannte Beweiserleichterungen in ähnlichen Konstellationen

Nachfolgend sollen zunächst anerkannte Beweiserleichterungen von Fällen, 800
die dem Missbrauch von Zugangsdaten im Internet ähnlich sind, betrachtet werden, um anschließend Schlussfolgerungen für Beweiserleichterung bei Missbrauch von anderen Zugangsdaten im Internet zu ziehen.

1. Elektronische Signatur

Bei der elektronischen Signatur[131] hat der Gesetzgeber die Beweiserleichte- 801
rung gesetzlich normiert. Der Beweiswert von qualifizierten elektronischen Signaturen ist in § 371a Abs. 1 S. 2 ZPO, der § 292a ZPO a.F. ablöst,[132] geregelt. Bei der Regelung handelt es sich um einen gesetzlich normierten Anscheinsbeweis.[133] Es entsprach dem gesetzgeberischen Willen, die allgemeinen richterrechtlichen Voraussetzungen für einen Anscheinsbeweis für diesen Einzelfall zu kodifizieren.[134] Teilweise wird bezweifelt, dass dies gelungen ist.[135] Erfahrungssätze bei der elektronischen Signatur lägen nicht

131 Dazu oben Rn. 73 ff.
132 *Musielak*, in: FG Vollkommer, 237, 249.
133 *Reichold*, in: *Thomas/Putzo*[34], § 371a ZPO Rn. 2; *A. Stadler*, ZZP 115 (2002), 413, 432; *W. Zimmermann*, in: MüKo-ZPO[4], § 371a Rn. 4.
134 Begr. FormAnpG, BT-Drucks. 14/4987, S. 23; Begr. JKomG, BT-Drucks. 15/4067, S. 34; *Huber*, in: *Musielak*[10], § 371a ZPO Rn. 6.
135 *Huber*, in: *Musielak*[10], § 371a ZPO Rn. 7.

vor, sodass die notwendige Vermutungsbasis fehle.[136] Dagegen lässt sich jedoch einwenden, dass in diesem Fall ein Anscheinsbeweis ohne ersten Anschein[137] ohne vorhandene Erfahrungssätze begründet werden könnte. Darüber hinaus wird gegen die Plausibilität der Vermutungsbasis eingebracht, dass eine Delegation der Signierung an Mitarbeiter zu erwarten sei.[138] Es liegt somit kein echter Anscheinsbeweis vor, sondern vielmehr eine gesetzliche Beweisregel.[139] Der Beweis des Vorliegens der Voraussetzungen von § 371a Abs. 1 S. 2 ZPO ist bei qualifizierten elektronischen Signaturen von Anbietern ohne Akkreditierung schwer zu führen.[140] Die einfache elektronische Signatur und die fortgeschrittene elektronische Signatur sind von § 371a Abs. 1 S. 2 ZPO nicht erfasst.[141] Für fortgeschrittene elektronische Signaturen ist ein Anscheinsbeweis nach den richterrechtlichen Grundsätzen je nach konkreter technischer Ausgestaltung jedoch möglich.[142]

802 Hinter dieser Kodifizierung des Anscheinsbeweises steckt der Sphärengedanke. Der Erklärungsempfänger kann zu den Umständen der Abgabe einer elektronisch signierten Erklärung nicht substantiiert vortragen.[143] Dem Erklärungsempfänger wird somit der Beweis von Tatsachen erleichtert, die er kaum beweisen kann. Doch bei qualifizierten elektronischen Erklärungen besteht das Problem, dass es schwierig ist, den Beweis über lange zurückliegende Erklärungen zu führen.[144] Teilweise wird einschränkend vertreten, dass der Anscheinsbeweis des § 371a Abs. 1 S. 2 ZPO nur dann zum Tragen kommt, wenn feststeht, dass der Schlüssel-Inhaber die Erklärung selbst signiert hat.[145] Dagegen spricht jedoch, dass die eigenhändige Signierung kein konstitutives Merkmal der qualifizierten elektronischen Signatur ist.[146] § 2 Nr. 2 lit. c SigG setzt nach seinem Wortlaut nur voraus, dass der

136 *Schemmann*, ZZP 118 (2005), 161, 181; *A. Stadler*, ZZP 115 (2002), 413, 434.
137 Oben Rn. 788.
138 *Schemmann*, ZZP 118 (2005), 161, 182; dagegen *Musielak*, in: FG Vollkommer, 237, 249 f.
139 *Berger*, in: *Stein/Jonas*[22], § 371a ZPO Rn. 15; *W. Zimmermann*, in: MüKo-ZPO[4], § 371a Rn. 4; *Czeguhn*, JuS 2004, 124, 126.
140 *Roßnagel*, MMR 2000, 451, 459 f.
141 *Huber*, in: *Musielak*[10], § 371a ZPO Rn. 3; *Trautwein*, in: *Prütting/Gehrlein*[5], § 371a ZPO Rn. 2.
142 *Ernst*, MDR 2003, 1091, 1092.
143 *Trautwein*, in: *Prütting/Gehrlein*[5], § 371a ZPO Rn. 5.
144 Vgl. *Roßnagel*, MMR 2002, 215, 218 f.
145 *Jandt*, K&R 2009, 548, 554.
146 Anders jedoch ebd., 550 f. In diese Richtung auch *Roßnagel*, MMR 2008, 22, 27.

Schlüssel-Inhaber die Zugangsdaten grundsätzlich „unter seiner alleinigen Kontrolle halten kann“, nicht dass er es im konkreten Fall auch getan hat. Dies entspricht auch dem Willen des Gesetzgebers, nach dem § 2 Nr. 2 lit. c SigG sicherstellt, dass der Schlüssel-Inhaber „seine Signaturerstellungseinheit vor unbefugter Nutzung schützen können muss.“[147] Demnach reicht die Möglichkeit des Schutzes. Dass der Schlüssel-Inhaber die Signaturerstellungseinheit auch im konkreten Einzelfall gegen unbefugte Nutzung geschützt hat, ist gerade nicht erforderlich. § 371a Abs. 1 S. 2 ZPO soll nach dem Normzweck gerade auch die Fälle erfassen, bei denen nicht geklärt werden kann, wer die Erklärung elektronisch signiert hat.[148]

Der Wortlaut des § 371a Abs. 1 S. 2 ZPO verwendet die richterrechtliche Voraussetzung des Widerlegens des Anscheinsbeweises mit dem Rückgriff auf das Erschüttern[149] durch Tatsachen, die ernstliche Zweifel an der Vermutungsbasis begründen. Welche Anforderungen an das Erschüttern zu stellen sind, ist unklar. Teilweise wird behauptet, es dürfen keine zu hohen Anforderungen gestellt werden.[150] Andererseits wird behauptet, der Zweck, den sicheren Rechtsverkehr durch qualifizierte elektronische Signaturen zu gewähren, soll durch hohe Anforderungen an das Erschüttern erreicht werden.[151] Zum Erschüttern reichen jedenfalls rein theoretische Möglichkeiten alternativer Geschehensabläufe nicht aus.[152] Das Erschüttern der Vermutungsbasis des § 371a Abs. 1 S. 2 ZPO ist schwerer als das Erschüttern der Vermutungsbasis bei Einsatz einer ec-Karte[153], weil der Missbrauch regelmäßig später auffallen wird und dadurch die Beweisführung erschwert wird.[154] Dadurch lässt dieser Anscheinsbeweis den Schlüssel-Inhaber das Missbrauchsrisiko tragen.[155] Problematisch ist, dass die Sicherheitsanforderungen fest ins Gesetz geschrieben sind, sodass der Anscheinsbeweis mit neuen Erkenntnissen im Wege der richterlichen Würdigung keiner neuen Bewertung unterworfen werden kann. Dadurch werden die Systemrisiken

803

147 Begr. SigG, BT-Drucks. 14/4662, S. 18.
148 *Huber*, in: *Musielak*[10], § 371a ZPO Rn. 6; *Schemmann*, ZZP 118 (2005), 161, 167.
149 Oben Rn. 790.
150 *Armgardt/Spalka*, K&R 2007, 26, 29; *Bergfelder*, S. 308; *Greger*, in: *Zöller*[30], § 371a ZPO Rn. 2.
151 *Trautwein*, in: *Prütting/Gehrlein*[5], § 371a ZPO Rn. 6.
152 *Greger*, in: *Zöller*[30], § 371a ZPO Rn. 2.
153 Dazu unten Rn. 812 ff.
154 *Borges*, Verträge, S. 509.
155 *Berger*, in: *Stein/Jonas*[22], § 371a ZPO Rn. 6.

der qualifizierten elektronischen Signatur dem Schlüssel-Inhaber aufgebürdet.[156]

804 Das Erschüttern der Vermutungsbasis § 371a Abs. 1 S. 2 ZPO ist in folgenden Fällen denkbar. Kann der Schlüssel-Inhaber beweisen, dass ein Dritter die Erklärung signiert hat, entfällt die Vermutungsbasis, die sich nur auf die Echtheit der Erklärung bezieht.[157] Dazu muss der Schlüssel-Inhaber nur vortragen, dass er die Chip-Karte samt der PIN weitergeben hat.[158] Anders war noch die Regelung des § 292a ZPO a.F., wonach sich die Vermutungsbasis auf die Abgabe mit Willen des Schlüssel-Inhabers bezog. Den Anscheinsbeweis des § 292a ZPO a.F. konnte der Schlüssel-Inhaber somit nicht durch die Weitergabe der Chip-Karte erschüttern. Der Anscheinsbeweis des § 371a Abs. 1 S. 2 ZPO hingegen ist bereits erschüttert, wenn der Schlüssel-Inhaber die Chip-Karte aus der Hand gegeben hat. Ferner kann der Schlüssel-Inhaber die Vermutungsbasis dadurch erschüttern, dass ihm ein anderes Dokument, als jenes, das er signieren wollte, untergeschoben wurde.[159] Dies kann durch einen Angriff mittels Trojaners[160] auf die Software zur Erstellung der Signatur erfolgen.[161] Der Schlüssel-Inhaber muss dann darlegen, dass der Rechner infiziert war, sodass die externe Manipulation möglich war.[162] Ebenso kann der Beweis des Diebstahls der Signaturkarte sowie des Ausspähens der PIN die Vermutungsbasis erschüttern.[163] Vereinzelt wird behauptet, dass wegen des stets möglichen Einsatzes von Trojanern der Anscheinsbeweis schon erschüttert sei, wenn der betreffende Rechner des Schlüssel-Inhabers mit dem Internet oder anderen Rechnern verbunden ist.[164]

805 Darüber hinaus können Fehler bei der Überprüfung der Identitätsbehauptung des Schlüssel-Inhabers beim Ausstellen des Signaturschlüssels auftre-

---

156 *Borges*, Verträge, S. 509 f.

157 *Bergfelder*, S. 309; *Berger*, in: *Stein/Jonas*[22], § 371a ZPO Rn. 17.

158 *Berger*, in: *Stein/Jonas*[22], § 371a ZPO Rn. 17; *Huber*, in: *Musielak*[10], § 371a ZPO Rn. 10; *Schemmann*, ZZP 118 (2005), 161, 174.

159 *Huber*, in: *Musielak*[10], § 371a ZPO Rn. 10; *Schemmann*, ZZP 118 (2005), 161, 173; *Roßnagel/Fischer-Dieskau*, NJW 2006, 806, 807.

160 Oben Rn. 193.

161 *Armgardt/Spalka*, K&R 2007, 26, 29.

162 *Gassen*, S. 245.

163 *Berger*, in: *Stein/Jonas*[22], § 371a ZPO Rn. 17; *Bergfelder*, S. 311; *Redeker*, IT-Recht[5], Rn. 915; *Schemmann*, ZZP 118 (2005), 161, 173; *W. Zimmermann*, in: MüKo-ZPO[4], § 371a Rn. 4.

164 *Armgardt/Spalka*, K&R 2007, 26, 32.

ten. Kann der vermeintliche Schlüssel-Inhaber diese beweisen, wird dadurch die Vermutungsbasis erschüttert.[165] Der Behauptung, dass dies kaum vorkommen werde,[166] ist zu widersprechen. Insbesondere durch die Lockerung der Anforderungen an die Identifizierung,[167] ist das Erstellen einer qualifizierten elektronischen Signatur auf einen fremden Namen einfacher möglich geworden. Die technische Unsicherheit des Systems kann ebenfalls die Vermutungsbasis erschüttern. Beim Beweis eines Algorithmenverfalls, also der Möglichkeit den privaten Schlüssel anhand des öffentlichen Schlüssels mit geringem Aufwand zu erreichen,[168] ist die Vermutungsbasis ebenfalls erschüttert.[169]

Scheitert der Anscheinsbeweis des § 371a Abs. 1 S. 2 ZPO daran, dass **806**
der Schlüssel-Inhaber die Vermutungsbasis erschüttert, kann sich dessen Haftung aus dem materiellen Recht ergeben.[170] Nach den allgemeinen Rechtsscheingrundsätzen haftet der Schlüssel-Inhaber unter gewissen Umständen für den Missbrauch seines qualifizierten elektronischen Signaturschlüssels.[171] So kann der Schlüssel-Inhaber zwar durch die Weitergabe der Zugangsdaten und die anschließende Signierung durch einen Dritten die Vermutungsbasis der Echtheit der Erklärung zerstören. Bei einer qualifizierten elektronischen Signatur wird ihm die Erklärung des Dritten dabei jedoch nach Rechtsscheingrundsätzen zugerechnet.

Aus der Betrachtung der gesetzlich normierten Beweiserleichterung des **807**
§ 371a Abs. 1 S. 2 ZPO lassen sich grundsätzliche Wertungen herausarbeiten. Zum einen ist es für den Anscheinsbeweis entscheidend, dass das Authentisierungsverfahren einen hohen Sicherheitsstandard aufweist. Die qualifizierte elektronische Signatur reicht nach dem gesetzgeberischen Willen dafür aus.[172] Die Sicherheit der elektronischen Signatur zeichnet sich durch zwei Merkmale aus. Erstens setzt sie auf eine Zwei-Faktor-Authentisierung.[173] Für eine erfolgreiche Authentisierung ist neben dem Wissen des PIN der Besitz der physisch einmaligen Chip-Karte erforderlich,

165 *Schemmann*, ZZP 118 (2005), 161, 172.
166 *Dästner*, NJW 2001, 3469.
167 Unten Rn. 887.
168 Oben Rn. 80.
169 *Schemmann*, ZZP 118 (2005), 161, 175.
170 *Berger*, in: *Stein/Jonas*[22], § 371a ZPO Rn. 18.
171 Unten Rn. 882 ff.
172 Begr. FormAnpG, BT-Drucks. 14/4987, S. 23.
173 Unten Rn. 883.

was einen Missbrauch erheblich erschwert.[174] Zweitens muss die Identität des Schlüssel-Inhabers bei Ausstellung des Zertifikats zuverlässig überprüft werden.[175] Aus der Wertung des § 371a Abs. 1 S. 2 ZPO kann daher abgeleitet werden, dass für ähnlich sichere Authentisierungsverfahren bei einer unveränderten Lage von Missbrauchsmöglichkeiten im Vergleich zum Zeitpunkt der gesetzgeberischen Entscheidung ein Anscheinsbeweis in Betracht kommt. Zum anderen lässt sich aus der Gesetzesbegründung zu § 371a Abs. 1 S. 2 ZPO entnehmen, dass die Schutzwürdigkeit des Geschäftsgegners und das Sicherstellen des Vertrauens des Marktes in die elektronische Signatur, bei der Erwägung eines Anscheinsbeweises eine Rolle spielen können.[176]

2. Bildschirmtext (Btx)

808 Beim Bildschirmtext[177] wurden Beweiserleichterungen herrschend angenommen. Nur vereinzelt wurden sie abgelehnt.[178] Gegen diese Beweiserleichterung wird eingebracht, dass sich der Authentisierungsnehmer die Authentisierungsmethoden auswählen könnte.[179] Ferner fehlten dem Account-Inhaber positive sowie negative Nachweismöglichkeiten des elektronischen Vertragsschlusses.[180] Eine Beweiserleichterung könnte sich nur aus der Beweisnot der anderen Partei ergeben.[181] Dies verbiete sich jedoch bei den in Frage stehenden Erfüllungsansprüchen, weil bei diesen der Geschäftsgegner einen sicher beweisbaren Vertragsschluss herbeiführen könnte[182] und weil er die negative Tatsache, dass er den Vertragsschluss nicht herbeigeführt habe, nur schwer beweisen könne.[183]

809 Beweiserleichterungen werden jedoch in unterschiedlicher Form angenommen. Überwiegend wird eine tatsächliche Vermutung beim Missbrauch

174 Oben Rn. 584.
175 Unten Rn. 886.
176 Vgl. Begr. JKomG, BT-Drucks. 15/4067, S. 34.
177 Zu dessen technischen Grundlagen oben Rn. 498.
178 *Auerbach*, CR 1988, 18; *Clemens*, NJW 1985, 1998, 2005; *Kleier*, WRP 1983, 534, 536.
179 *Auerbach*, CR 1988, 18.
180 *Clemens*, NJW 1985, 1998, 2005.
181 *Kleier*, WRP 1983, 534, 536.
182 Ebd., 536. Zu alternativen Sicherungsmöglichkeiten oben Rn. 657.
183 *Kuhn*, S. 255.

des Bildschirmtext-Anschlusses angenommen.[184] Dabei wird die tatsächliche Vermutung wie hier[185] als Beweislastumkehr verstanden.[186] Die Sicherung durch die in das Endgerät eingespeicherte Anschlussziffer sowie das Passwort begründen diese Vermutung.[187] Die tatsächliche Vermutung bestehe darin, dass eine missbräuchliche Nutzung des Bildschirmtext-Anschlusses nur durch Zutun des Account-Inhabers ermöglicht wurde.[188] Den Inhalt des Vertrags müsse jedoch der Geschäftsgegner beweisen.[189] Durch die Notwendigkeit das spezielle Bildschirmtext-Gerät des Anschlussinhabers zu verwenden, ist ein Missbrauch nur in der räumlichen Sphäre des Account-Inhabers möglich, sodass dieser den Missbrauch gut kontrollieren kann.[190]

In der Literatur wird hingegen häufig die schwächere Form der Beweiserleichterung in Form des Anscheinsbeweises bevorzugt.[191] Das Vorliegen des Anscheinsbeweises wird entweder durch das Vorliegen des Regelfalls, dass berechtigt gehandelt wurde,[192] oder durch die hinreichende Sicherung des Authentisierungsvorgangs[193] begründet. Ein Beweis der Vermutungsbasis sei dabei jedoch nur bei nicht manipulierbaren Aufzeichnungen möglich.[194] Teilweise wird dieser Anscheinsbeweis auf Sekundäransprüche beschränkt.[195] **810**

Aus den Beweiserleichterungen beim Bildschirmtext lässt sich die Erkenntnis gewinnen, dass eine starke Beweiserleichterung wie die tatsäch- **811**

184 *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552; Urteil v. 21. 11. 1997, 19 U 128/97 – NJW-RR 1998, 1277, 1279; *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 1406; *Borsum/Hoffmeister*, BB 1983, 1441, 1446; *dies.*, NJW 1985, 1205, 1207; *Brinkmann*, BB 1981, 1183, 1187.

185 Oben Rn. 781.

186 *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 1406, nicht explizit, aber durch den Verweis auf die *BGH*-Entscheidung eindeutig: *BGH*, Urteil v. 18. 9. 1984, VI ZR 223/82 – BGHZ 92, 143, 146 f.

187 *OLG Köln*, Urteil v. 21. 11. 1997, 19 U 128/97 – NJW-RR 1998, 1277, 1279; *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 1406.

188 *OLG Köln*, Urteil v. 21. 11. 1997, 19 U 128/97 – NJW-RR 1998, 1277, 1279; *Borsum/Hoffmeister*, BB 1983, 1441, 1446; *dies.*, NJW 1985, 1205, 1207.

189 *Borsum/Hoffmeister*, BB 1983, 1441, 1446; *dies.*, NJW 1985, 1205, 1207.

190 *OLG Köln*, Urteil v. 30. 4. 1993, 19 U 134/92 – CR 1993, 552.

191 *Kuhn*, S. 253; *Probandt*, UFITA 98 (1984), 9, 18.

192 *Probandt*, UFITA 98 (1984), 9, 18.

193 *Kuhn*, S. 253.

194 Ebd., S. 253.

195 Ebd., S. 254 f.

liche Vermutung bei einem sicheren Authentisierungsverfahren in Betracht kommt. Das Bildschirmtext-System setzt auf eine Zwei-Faktor-Authentisierung dadurch, dass zum Einwählen neben dem geheimen Kennwort die im Endgerät eingespeicherte Anschlusskennung notwendig ist.[196] Die Besitzkomponente beim Bildschirmtext, die sich ebenfalls durch eine physische Einmaligkeit auszeichnet, ist jedoch besonders gesichert. Da es sich um ein großes und sperriges Gerät handelt, verlässt es regelmäßig nicht die räumliche Sphäre des Anschlussinhabers. Im Gegensatz zu einer Chip-Karte, die der Inhaber im Portemonnaie stets mit sich tragen kann, kann der Anschlussinhaber das in seiner räumlichen Sphäre befindliche Bildschirmtext-Gerät besser kontrollieren. Da ein Teilen des Bildschirmtext-Anschlusses in der häuslichen Gemeinschaft zu erwarten ist,[197] bezieht sich die Beweiserleichterung nur darauf, dass die Nutzung des Anschlusses nur mit Zutun des Anschlussinhabers ermöglicht wurde.[198] Ferner zeigt die Diskussion um die Beweiserleichterungen, dass die Grenzen zwischen einem Anscheinsbeweis und einer tatsächlichen Vermutung schwer zu ziehen sind.[199]

3. ec-Karte

812 Der Anscheinsbeweis beim Missbrauchs von ec-Karte, der auf Kreditkarten ebenso angewendet wird, bietet in Rechtsprechung und Literatur ausführliches Anschauungsmaterial. Einige Stimmen aus Literatur und Rechtsprechung meinen, dass die am 31.10.2009 in Kraft getretene Neuregelung in § 675w S. 3 BGB die Beibehaltung des Anscheinsbeweises verbiete.[200] Überwiegend wird jedoch gestützt auf den Willen des Gesetzgebers[201] angenommen, dass die Neuregelung keine Veränderung der Rechtslage bezweckte und der entwickelte Anscheinsbeweis weiterhin angewendet werden kann.[202] Unabhängig davon, ob der Anscheinsbeweis in seiner alten

196 Oben Rn. 498.
197 Oben Rn. 300.
198 *OLG Oldenburg*, Urteil v. 11. 1. 1993, 13 U 133/92 – NJW 1993, 1400, 1401.
199 Dazu bereits abstrakt oben Rn. 791.
200 So im Ergebnis *AG Berlin Mitte*, Urteil v. 25. 11. 2009, 21 C 442/08 – NJW-RR 2010, 407, 408; *Franck/Massari*, WM 2009, 1117, 1126; *Scheibengruber*, BKR 2010, 15, 20 f.
201 BT-Drucks. 16/11643, S. 114.
202 *LG Berlin*, Urteil v. 22. 6. 2010, 10 S 10/09 – NJW-RR 2011, 352, 354; *AG Frankfurt*, Urteil v. 10. 11. 2010, 29 C 1461/10-85 – WM 2011, 496, 497; *AG Hamburg*,

Form weiter Bestand hat, lassen sich aus der Diskussion um dessen Voraussetzungen wertvolle Schlüsse für einen Anscheinsbeweis beim Missbrauch von Zugangsdaten im Internet ziehen.

Wird mit einer ec-Karte unter Verwendung der korrekten Zugangsdaten **813**
Geld an einem Automaten abgehoben, besteht ein Anscheinsbeweis dafür, dass der Kartenbesitzer diese selbst vorgenommen hat oder dass ein Dritter nach Entwendung der Karte wegen des unsorgsamen Umgangs mit der PIN Kenntnis von dieser erlangen konnte und dieser das Geld abgehoben hat.[203] Der Grund für die Anerkennung des Anscheinsbeweises ist, dass quasi nicht beweisbar ist, dass der Bankkunde oder ein Berechtigter gehandelt hat.[204] Der Anscheinsbeweis hat eine ausdifferenzierte Ausformung. Ist beispielsweise unstrittig, dass der Karteninhaber die Abhebung nicht selbst vorgenommen hat, bezieht sich der Anscheinsbeweis nur darauf, dass dieser die PIN zusammen mit der Karte aufbewahrt hat.[205] Wird nicht die Originalkarte sondern eine Dublette verwendet, wie beim Skimming der Fall,[206] kommt der Anscheinsbeweis nicht in Betracht.[207] Weil die Bank die Vermutungsbasis vollständig beweisen muss, liegt die Beweislast der Verwendung der Originalkarte bei ihr.[208]

Der Bankkunde kann die Vermutungsbasis des Anscheinsbeweises durch **814**
die konkrete Darlegung eines alternativen Geschehensablaufs erschüttern.[209] Rein theoretische, alternative Möglichkeiten, die jedoch höchst unwahrscheinlich sind, reichen dafür nicht. Eine solche theoretische aber unwahrscheinliche Möglichkeit ist, dass ein Bankmitarbeiter als Innentäter

---

Urteil v. 28. 9. 2010, 4 C 178/10 – WM 2011, 498; *Bunte*[3], SB girocard Rn. 85; *Casper/Pfeifle*, WM 2009, 2343, 2347; *Günther*, WM 2013, 496, 497 f.; *Grundmann*, WM 2009, 1157, 1164; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 54 Rn. 49, 109; *Oechsler*, WM 2010, 1381, 1382; *Spindler*, in: FS Nobbe, 215, 232 f.; *v. Westphalen*, in: *Erman*[13], § 675w BGB Rn. 13.

203 *BGH*, Urteil v. 5. 10. 2004, XI ZR 210/03 – BGHZ 160, 308, 314 ff.; Urteil v. 14. 11. 2006, XI ZR 294/05 – BGHZ 170, 18, Rn. 31; unbeanstandet von *BVerfG*, Beschluss v. 8. 12. 2009, 1 BvR 2733/06 – NJW 2011, 1129, Rn. 16.

204 *Borges*, Verträge, S. 496; *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 331.

205 *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 331.

206 Zum Skimming *Schulte am Hülse/Welchering*, NJW 2012, 1262, 1264.

207 *BGH*, Urteil v. 29. 11. 2011, XI ZR 370/10 – NJW 2012, 1277, Rn. 16; *Kollrus*, MDR 2012, 377, 379; *Günther*, WM 2013, 496, 498; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 54 Rn. 116.

208 *BGH*, Urteil v. 29. 11. 2011, XI ZR 370/10 – NJW 2012, 1277, Rn. 16.

209 *Kollrus*, MDR 2012, 377, 380.

den Institutsschlüssel ausspäht oder die Sicherheitsinfrastruktur beeinträchtigt.[210] Ebenso theoretisch möglich, aber sehr unwahrscheinlich sei, dass der Dritte die mit 128-Bit verschlüsselten PIN errechnet hat.[211] Wegen der zunehmenden Rechenleistung moderner Computer sowie der Aggregation dieser in Botnetzen, die Hacker für solche Operationen nutzen können, wird daran gezweifelt, dass die 128-Bit-Verschlüsselung noch einen ausreichenden Schutz bietet.[212] Dies zeigt, dass die Vermutungsbasis eines Anscheinsbeweises einer ständigen Überprüfung und Anpassung an neue Entwicklungen bedarf. Er unterliegt einer Dynamik, bei der die geänderte Lebenserfahrung das ständige Hinterfragen der Erfahrungssätze notwendig macht.[213]

815 Erschüttern kann der Karteninhaber den Anscheinsbeweis jedoch dadurch, dass er einen Diebstahl der Karte darlegt.[214] Dazu muss er nicht den Vollbeweis eines Diebstahls erbringen, sondern vielmehr nur äußere Umstände beweisen, die auf einen Diebstahl hindeuten. Dafür kommt es auf die Umstände des Einzelfalls an.[215] Der Anscheinsbeweis kann ebenfalls dadurch erschüttert werden, dass eine konkrete Möglichkeit des Ausspähens der PIN bewiesen wird. Dies setze jedoch einen engen zeitlichen Zusammenhang zwischen dem Einsatz der ec-Karte mit dem späteren Missbrauch voraus.[216] Zwar wird der Ausspäher nach dem Diebstahl die ec-Karte schnell missbrauchen, um einer Sperrung zuvor zu kommen, bei anderen Konstellationen kann jedoch das Ausspähen und der Missbrauch Wochen oder Monate auseinander liegen.[217] Man kann daher an dem Erfordernis des zeitlichen Zusammenhangs zweifeln.

816 Eine Besonderheit des Anscheinsbeweises beim ec-Karten-Missbrauch besteht in der Begründung der Vermutungsbasis. Zwar lassen sich durchaus Erwägungen finden, die den typischen Geschehensablauf durch Empi-

---

210 *BGH*, Urteil v. 5. 10. 2004, XI ZR 210/03 – BGHZ 160, 308, 318; *Schulte am Hülse/Welchering*, NJW 2012, 1262, 1265.

211 *BGH*, Urteil v. 5. 10. 2004, XI ZR 210/03 – BGHZ 160, 308, 316; *Bunte*[3], SB girocard Rn. 86.

212 *Scheibengruber*, BKR 2010, 15, 21.

213 *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 354.

214 *Hanau*, Handeln unter fremder Nummer, S. 141; *Bergfelder*, S. 272.

215 *Bergfelder*, S. 272; *Borges*, Verträge, S. 502.

216 *BGH*, Urteil v. 5. 10. 2004, XI ZR 210/03 – BGHZ 160, 308, 317 f.; *Hanau*, Handeln unter fremder Nummer, S. 142 f.; *ders.*, VersR 2005, 1215, 1219.

217 *Schulte am Hülse/Welchering*, NJW 2012, 1262, 1264.

rie zu belegen oder widerlegen versuchen.[218] Dies verkennt jedoch, dass der Anscheinsbeweis ohne einen empirischen Befund über den Erfahrungssatz begründet wird.[219] Weil kein Erfahrungssatz besteht, wird der Anscheinsbeweis vielmehr durch den Ausschluss alternativer Möglichkeiten begründet.[220] Es handele sich dabei um einen „Anscheinsbeweis ohne ersten Anschein".[221] Bei dieser Form durch Ausschluss alternativer Möglichkeiten gehört es jedoch zu der zu beweisenden Vermutungsgrundlage, dass die auszuschließenden Möglichkeiten, von der Bank bewiesen werden müssen.[222] Dabei besteht jedoch das Problem, dass für die abschließende Bewertung der Möglichkeiten Auskünfte über die Sicherheit erforderlich sind, die jedoch die Sicherheit beeinträchtigen können.[223]

817 Die Annahme des Anscheinsbeweises bei der ec-Karte zeigt, dass die verwendete Zwei-Faktor-Authentisierung unter gewissen Umständen eine ausreichende Wahrscheinlichkeit für die Anerkennung der Beweiserleichterung darstellt. Dass der Anscheinsbeweis nur beim Einsatz der Originalkarte und nicht einer Dublette in Betracht kommt, zeigt, dass die physische Einmaligkeit der Besitz-Komponenten entscheidend ist. Sie erlaubt dem Karten-Inhaber Missbrauchsmöglichkeiten zu entdecken. Ist ihm die Karte abhandengekommen, beispielsweise beim Diebstahl des Portemonnaies, kann er die Gefahr eines Missbrauchs entdecken und durch Sperrung der Karte verhindern. Unausgesprochen, aber dennoch bedeutend für die Annahme des Anscheinsbeweis ist, dass bei der ec-Karte wegen der gesetzlich erforderlichen Überprüfung der Identität des Kunden bei Eröffnung des Kontos[224] die Identität des Karten-Inhabers feststeht.

818 Ebenso zeigt die Diskussion um den Anscheinsbeweis, dass die materielle Rechtslage für die Frage, ob der Account-Inhaber selbst oder jemand mit seinem Einverständnis gehandelt hat, zunächst irrelevant ist. Erst wenn feststeht, dass dies nicht der Fall war, werden weitere Beweisthemen für die materielle Rechtslage, bei der ec-Karte die Frage der groben Fahrlässigkeit bei der Pflichtverletzung, relevant. Die Tatsache, dass bei der ec-Karte

218 *Kollrus*, MDR 2012, 377, 379; *Schulte am Hülse/Welchering*, NJW 2012, 1262, 1265.
219 *BGH*, Urteil v. 5. 10. 2004, XI ZR 210/03 – BGHZ 160, 308, 316.
220 *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 345 f.; *ders.*, ZZP 120 (2007), 459, 464.
221 *Jungmann*, ZZP 120 (2007), 459, 463 f. Dazu oben Rn. 788.
222 *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 347.
223 Ebd., 349.
224 Vgl. oben Rn. 67.

vertragliche Beziehungen zwischen Karten-Inhaber und der Bank bestehen, was beim Missbrauch von Zugangsdaten im Internet häufig nicht der Fall ist, schadet daher einem Erkenntnisgewinn aus der Rechtslage bei der ec-Karte nicht.

4. Online-Banking

819 Wegen der hohen praktischen Relevanz des Missbrauchs beim Online-Banking[225] soll die Diskussion um Beweiserleichterungen der Bank für vermeintlich vom Kunden durchgeführte Transaktionen betrachtet werden, um Beweiserleichterungen für andere Zugangsdaten im Internet damit abgleichen zu können. Grundsätzlich kommt ein Anscheinsbeweis beim Online-Banking nur in Betracht, wenn mit der herrschenden Meinung § 675w S. 3 BGB so verstanden wird, dass er die Rechtsfigur des Anscheinsbeweises nicht ausschließt.[226] Wegen der unterschiedlichen im Einsatz befindlichen Authentisierungsmethoden beim Online-Banking ist der Anscheinsbeweis differenziert zu betrachten.

820 Beim iTAN-Verfahren[227] wird in Teilen der Literatur ein Anscheinsbeweis dafür angenommen, dass bei einer Transaktion mit den Zugangsdaten der Bankkunde selbst oder ein Vertreter mit Berechtigung behandelt hat.[228] Dies ergebe sich aus der Übertragung des für die Verwendung der ec-Karte entwickelten Anscheinsbeweises,[229] weil das Online-Banking mit iTAN-Verfahren ein vergleichbaren Sicherheitsstandard besitze. Überwiegend wird der Anscheinsbeweis beim Online-Banking unter Verwendung des

225 Oben Rn. 67.

226 Oben Rn. 812 sowie explizit zum Online-Banking *Herresthal*, in: *Langenbucher/Bliesener/Spindler*, Kap. 5 § 675w BGB Rn. 13.

227 Dazu oben Rn. 556.

228 *Gössmann/Sönke*, in: FS Nobbe, 93, 110; *Hanau*, Handeln unter fremder Nummer, S. 77; *ders.*, VersR 2005, 1215, 1219 f.; *Herresthal*, in: *Langenbucher/Bliesener/Spindler*, Kap. 5 § 675w BGB Rn. 14; *Karper*, DuD 2006, 215, 218; *Recknagel*, S. 149 ff.; *S. Werner*, MMR 1998, 232, 235; *ders.*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.5 Rn. 63; *van Gelder*, in: FS Nobbe, 55, 66 f.

229 Oben Rn. 812.

iTAN-Verfahrens abgelehnt.[230] Der Sicherheitsstandard reiche nicht aus,[231] weil es sich beim iTAN-Verfahren um eine unsichere, rein wissensbasierte Authentisierungsmethode handelt.[232] Die Möglichkeiten des Phishings und Pharmings[233] sowie von Man-in-the-Middle-Angriffen[234] würden eine entsprechende Lebenserfahrung des Anscheinsbeweises widerlegen. Empirische Belege dafür, dass die Zugangsdaten häufig missbraucht werden, sprechen ferner gegen die Annahme eines Erfahrungssatzes, dass stets der Kontoinhaber oder ein Berechtigter gehandelt haben.[235]

Darüber hinaus sei die Bank am besten in der Lage, die Risiken eines **821**
Missbrauchs zu steuern, weswegen ein Anscheinsbeweis für unsichere Authentisierungsmethoden auszuschließen sei.[236] Dagegen wird eingewendet, dass die Bank keinen Einfluss auf die Konfiguration des Systems des Nutzers, wie Browser und Antivirensoftware nehmen könne.[237] Ihr bleibt es jedoch unbenommen, Verfahren durchzusetzen, bei denen die Ausnutzung entsprechender Schwachstellen nicht möglich ist. Zusätzlich ist es dem Bankkunden faktisch schwer möglich einen Anscheinsbeweis zu erschüttern, weil er zur IT-Infrastruktur der Bank keine Angaben machen könne.[238]

Das mTAN- sowie das eTAN-Verfahren setzen hingegen auf eine Zwei- **822**
Faktor-Authentisierung.[239] Dadurch bieten sie einen besseren Schutz gegen Angriffe als eine rein wissensbasierte Authentisierung. Deswegen wird ein Anscheinsbeweis bei diesen Verfahren häufig angenommen.[240] Weil je-

---

230 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261; *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08 – MMR 2008, 626, 628; *Bergfelder*, S. 283; *Biallaß/Borges/Dienstbach* u. a., in: Innovationsmotor IT-Sicherheit, 495, 507; *Borges*, NJW 2005, 3313, 3317; *ders.*, BKR 2009, 85, 87; *Casper*, in: MüKo-BGB[6], § 675w Rn. 20; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 85; *Mühlenbrock/Dienstbach*, MMR 2008, 630; *Omlor*, in: *Staudinger*[2012], § 675w BGB Rn. 10; *Schulte am Hülse/Klabunde*, MMR 2010, 84, 87; *v. Westphalen*, in: *Erman*[13], § 675w BGB Rn. 21.

231 *Schulte am Hülse/Klabunde*, MMR 2010, 84, 87.

232 Oben Rn. 545.

233 Oben Rn. 138 ff.

234 Oben Rn. 168.

235 *Erfurth*, WM 2006, 2198, 2205; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 83; *Recknagel*, S. 142.

236 *Erfurth*, WM 2006, 2198, 2206.

237 *Gössmann/Sönke*, in: FS Nobbe, 93, 110.

238 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 81.

239 Dazu Oben Rn. 117.

240 *Casper*, in: MüKo-BGB[6], § 675w Rn. 20; *Borges*, BKR 2009, 85, 87; *Mühlenbrock/Dienstbach*, MMR 2008, 630; *Borges/Schwenk/Stuckenberg/Wegener*, S. 313.

doch auch Zwei-Faktor-Authentisierungsmethoden mit einem Man-in-the-Middle-Angriff angreifbar sind,[241] wird vereinzelt der Anscheinsbeweis dafür abgelehnt.[242] Nur das optimierte eTAN-Verfahren mit zwei komplett unabhängigen Komponenten reiche aus, um eine solche Beweiserleichterung anzunehmen.[243] Anderes Stimmen der Literatur erkennen den Anscheinsbeweis nicht nur beim eTAN- sondern auch beim mTAN-Verfahren an.[244] Wie das mTAN- und eTAN-Verfahren setzt das HBCI-Verfahren auch auf eine Zwei-Faktor-Authentisierung. Ein Anscheinsbeweis für das Handeln des Bankkunden solle daher bei diesem Verfahren bestehen.[245] Dies wird insbesondere mit der Nähe zur elektronischen Signatur begründet.[246] Teilweise wird jedoch ein Anscheinsbeweis beim HBCI-Verfahren abgelehnt,[247] weil sich die Definition des Sicherheitsstandards zu weit von der elektronischen Signatur bewegt habe.

823 Wird der Anscheinsbeweis beim Online-Banking abgelehnt oder schafft es der Bankkunde einen solchen Anscheinsbeweis zu erschüttern, kommt eine Haftung wegen grob fahrlässigen Umgangs mit den Zugangsdaten nach § 675v Abs. 2 BGB in Betracht. Dabei kann ebenfalls ein Anscheinsbeweis für die Pflichtverletzung des Bankkunden erwogen werden. Im Gegensatz zur Rechtslage bei der ec-Karte[248] wird dieser Anscheinsbeweis für die Pflichtverletzung beim Online-Banking überwiegend abgelehnt.[249]

824 Eine Beweiserleichterung in Form des Anscheinsbeweises steht der Bank somit bei einer rein wissensbasierten Authentisierung nach einer überwiegenden Ansicht nicht zur Verfügung. Eine Beweiserleichterung der Bank in Form einer sekundären Darlegungslast solle ihr jedoch für solche Tatsachen zu Gute kommen, die dem Bankkunden, jedoch nicht ihr, bekannt sind.[250]

---

241 Oben Rn. 146.
242 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 86.
243 Ebd., § 55 Rn. 86.
244 *Herresthal*, in: *Langenbucher/Bliesener/Spindler*, Kap. 5 § 675w BGB Rn. 15.
245 *Gössmann/Sönke*, in: FS Nobbe, 93, 110; *Omlor*, in: *Staudinger*[2012], § 675w BGB Rn. 10; *Recknagel*, S. 150.
246 *Gössmann/Sönke*, in: FS Nobbe, 93, 113; *Recknagel*, S. 150.
247 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 84; *Bergfelder*, S. 287; *v. Westphalen*, in: *Erman*[13], § 675w BGB Rn. 21.
248 Oben Rn. 813.
249 *KG Berlin*, Urteil v. 29. 11. 2010, 26 U 159/09 – MMR 2011, 338; *LG Mannheim*, Urteil v. 16. 5. 2008, 1 S 189/07 – MMR 2008, 765; *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 166 ff.; **a.A.** *Gössmann/Sönke*, in: FS Nobbe, 93, 110.
250 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 88.

Der differenzierten Diskussion um den Anscheinsbeweis beim Online-Banking lassen sich Wertungen entnehmen, die für Beweiserleichterungen bei anderen Zugangsdaten im Internet relevant werden können. Die rein wissensbasierte Authentisierung bietet keine ausreichende Grundlage für die Anerkennung eines Anscheinsbeweises. Bei einer Zwei-Faktor-Authentisierung kann ein solcher jedoch durchaus angenommen werden. Wegen verbleibender Angriffsmöglichkeiten wird jedoch an der Anerkennung des Anscheinsbeweises gezweifelt. Dabei wird stets ein Vergleich zu der Situation des § 371a Abs. 1 S. 2 ZPO bemüht und die Vergleichbarkeit mit dem Sicherheitsstandard der qualifizierten elektronischen Signatur angestellt. Wie bei der ec-Karte ist für den Anscheinsbeweis beim Online-Banking zwar unausgesprochen aber entscheidend, dass die Identität des Bankkunden bei der Eröffnung des Konto zuverlässig überprüft wird.[251] Die Zuordnung des Kontos zu seinem Inhaber steht damit ausreichend sicher fest. Ebenso wie bei der ec-Karte[252] beschäftigt sich der Anscheinsbeweis nur mit der tatsächlichen Frage, ob der Bankkunde oder ein Dritter mit seinem Einverständnis gehandelt hat, sodass die vertraglichen Beziehungen, die bei anderen Zugangsdaten im Internet häufig nicht vorliegen, für die Beweiserleichterung keine Rolle spielen. **825**

5. Zwischenergebnis

Aus der Betrachtung verschiedener anerkannter Beweiserleichterungen bei ähnlichen Konstellationen lassen sich einige Wertungen herausfiltern, die für Beweiserleichterungen beim Missbrauch von Zugangsdaten im Internet relevant werden. Zunächst dreht sich ein Großteil der Diskussionen um die Frage, ob ein Anscheinsbeweis in Betracht kommt. Andere Formen der Beweiserleichterungen werden kaum diskutiert. Über die Gründe, warum stärkere Beweiserleichterungen wie die tatsächliche Vermutung außer Acht gelassen werden, kann nur spekuliert werden. Vermutlich erfolgt die Abgrenzung von Anscheinsbeweis und tatsächlicher Vermutung wegen der ähnlichen Voraussetzungen[253] insbesondere anhand der Rechtsfolge. Trifft dies zu, kann aus den Diskussionen der soeben behandelten Fälle geschlossen **826**

251 Oben Rn. 67.
252 Oben Rn. 818.
253 Oben Rn. 791.

werden, dass die Rechtsfolge der Beweislastumkehr bei den ähnlichen Konstellationen für unangemessen erachtet wird.

827 Für den Anscheinsbeweis lassen die soeben untersuchten Konstellationen einige Schlüsse zu. Eine rein wissensbasierte Authentisierung reicht für die Anerkennung des Anscheinsbeweises wegen der zahlreichen Missbrauchsmöglichkeiten nicht aus. Eine Zwei-Faktor-Authentisierung hingegen kann wegen der erhöhten Sicherheit, insbesondere wegen der Kombination aus der physischen Einmaligkeit der Besitz-Komponente und der Geheimhaltung des Wissens-Komponente, eine ausreichende Grundlage sein. Diese Wertung deckt sich mit den Erkenntnissen zum Rechtsscheintatbestand.[254] Ebenso hat die Analyse der verschiedenen Beweiserleichterungen gezeigt, dass die Identifizierung des Account-Inhabers eine wichtige Rolle spielt. Dies deckt sich ebenfalls mit den Erkenntnissen des Rechtsscheintatbestandes.[255]

828 Ferner lässt sich aus den untersuchten Konstellationen die unausgesprochene Tatsache herausfiltern, dass die Erklärung im Nachhinein nicht verändert wurde. Die elektronische Signatur dient primär dazu, dass überprüft werden kann, dass ein Text unverändert ist. Bei der ec-Karte bieten das Journal des Geldautomaten sowie die Autorisierungsprotokolle[256] ausreichende Gewähr dafür, dass die Buchungsvorgänge nicht nachträglich verändert wurden. Für die Anerkennung eines Erfahrungssatzes, der einen Anscheinsbeweis begründen kann, ist daher ebenso wie beim Rechtsscheintatbestand erforderlich, dass eine ausreichend sichere Authentisierungsmethode verwendet wird, die die virtuelle Identität des Accounts durch eine Identitätsüberprüfung zuverlässig einer numerischen Identität zuordnet.[257] Darüber hinaus muss eine nachträgliche Fälschung der abgegebenen Erklärung unwahrscheinlich sein.

829 Aus den betrachteten Konstellationen lässt sich daher die folgende Schlussfolgerung ziehen: Wenn eine ausreichend sichere Authentisierungsmethode wie die Zwei-Faktor-Authentisierung verwendet wurde, die virtuelle Identität des Accounts zuverlässig der numerischen Identität des Account-Inhabers zugeordnet ist und eine nachträgliche Fälschung der Er-

254 Oben Rn. 534 ff.
255 Oben Rn. 595 ff.
256 Dazu *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 54 Rn. 10, 115.
257 Ohne das Erfordernis der Identitätsprüfung auch *Borges*, Elektronischer Identitätsnachweis, S. 230. Nur die Authentisierungsmethode sei entscheidend *Kuhn*, S. 254.

klärung unwahrscheinlich ist, besteht ein Anscheinsbeweis dafür, dass der Account-Inhaber die in Frage stehende Erklärung über den Account selbst abgegeben hat. Sind diese hohen Anforderungen für den Anscheinsbeweis bei der Art des Accounts nicht gegeben, kann eine Beweiserleichterung in Form der sekundären Darlegungslast nach deren allgemeinen Voraussetzungen in Betracht kommen.

Kapitel 3 Anwendung und Zusammenfassung der Ergebnisse

§ 11 Anwendung der Ergebnisse auf verschiedene Account-Typen

Nachfolgend wird die entwickelte Lösung über die allgemeine Rechtsscheinhaftung[1] zu den Beweiserleichterungen[2] auf die unterschiedlichen Accounts angewandt. Die verschiedenen Account-Typen sind nach der Sicherheit ihrer verwendeten Authentisierungsmethode geordnet. **830**

I. Internetanschluss, IP-Adresse

1. Rechtsscheinhaftung

Es ist zwar davon auszugehen, dass bei einem Internetanschluss die Identität des Anschlussinhabers vor Vertragsschluss zuverlässig überprüft wird,[3] was eine der Voraussetzungen für die Anerkennung des Rechtsscheintatbestandes ist.[4] Ein Rechtsschein dafür, dass der Account-Inhaber gehandelt hat, kann aufgrund einer Verbindung, bei der der Rechner sich mit seiner IP-Adresse ausgewiesen hat, jedoch aus zwei Gründen nicht erfolgen. Zum einen kann an der korrekten Zuordnung von IP-Adresse zum Anschluss gezweifelt werden,[5] sodass die Sicherheit der Authentisierungsmethode[6] den zuverlässigen Rückschluss auf den Account-Inhaber nicht zulässt. Ferner werden Internetanschlüsse regelmäßig von mehreren Benutzer verwendet, sodass selbst bei einer zuverlässigen Zuordnung von einer IP-Adresse zum Anschluss kein Rückschluss auf die handelnde Person möglich ist.[7] Eine Rechtsscheinhaftung für den missbräuchlichen Abschluss von Verträgen über einen Internetanschluss scheidet somit aus. Für einen Missbrauch, der **831**

1 Oben Rn. 489 ff.
2 Oben Rn. 772 ff.
3 Oben Rn. 39.
4 Oben Rn. 595 ff.
5 Oben Rn. 45.
6 Oben Rn. 534 ff.
7 Oben Rn. 47.

Verbindungsentgelte zur Folge hat, haftet der Anschlussinhaber jedoch nach § 45i Abs. 4 S. 1 TKG.[8]

2. *Beweiserleichterungen*

832 Beim Internetanschluss[9] stellt sich die Frage, ob anhand einer IP-Adresse mit anschließend ermitteltem Anschlussinhaber eine Beweiserleichterung in Betracht kommt. Eine Beweislastumkehr[10] kommt nicht in Betracht, weil der Geschäftsgegner zahlreiche andere Möglichkeiten hat, eine mögliche Beweisnot zu vermeiden.[11] Tatsächliche Vermutung[12] und Anscheinsbeweis[13] scheiden aus, weil es der Lebenserfahrung widerspricht, dass der Anschlussinhaber alleiniger Verwender eines häuslichen Internetanschlusses ist. Die Beweiserleichterungen beim Bildschirmtext[14] lassen sich nicht auf Internetanschlüsse übertragen, weil Bildschirmtext einen viel stärkeren Fokus auf den Abschluss von Rechtsgeschäften hatte, wohingegen das Internet primär ein allgemeines Informations- und Teilnahmebedürfnis befriedigt.

833 Die Beweiserleichterungen bei deliktischen Ansprüchen zeigen, dass solche auch bei der rechtsgeschäftlichen Haftung in Betracht kommen. Bei Urheberrechtsverletzungen besteht eine tatsächliche Vermutung dafür, dass der Anschlussinhaber verantwortlich ist.[15] Die tatsächliche Vermutung wird – anders als hier[16] – zur Begründung einer sekundären Darlegungslast[17] ver-

---

8 Ausführlich oben Rn. 521.
9 Oben Rn. 39.
10 Oben Rn. 776.
11 Oben Rn. 657 ff.
12 Oben Rn. 781.
13 Oben Rn. 785.
14 Oben Rn. 808.
15 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 12; Urteil v. 15. 11. 2012, I ZR 74/12 (Morpheus) – NJW 2013, 1441, Rn. 33; Urteil v. 8. 1. 2014, I ZR 169/12 (BearShare), Rn. 15; *OLG Hamm*, Urteil v. 27. 10. 2011, 22 W 82/11 – MMR 2012, 40, 40 f.; *OLG Köln*, Urteil v. 11. 9. 2009, 6 W 95/09 – MMR 2010, 44, 45; Urteil v. 23. 12. 2009, 6 U 101/09 – MMR 2010, 281; Beschluss v. 24. 3. 2011, 6 W 42/11 – MMR 2011, 396, 397; *LG Düsseldorf*, Urteil v. 21. 3. 2012, 12 O 579/10 – NJW 2012, 3663, 3663 f.
16 Oben Rn. 781.
17 Oben Rn. 792.

wendet.[18] Der Gedanke, der hinter dieser Beweiserleichterung steht, lässt sich übertragen. Der Internetanschluss befindet sich in der räumlichen Sphäre des Anschlussinhabers, sodass er den Zugang zu diesem kontrollieren kann. Eine sekundäre Darlegungslast kommt somit in Betracht. In deren Rahmen hat der Anschlussinhaber darzulegen, dass er nicht der Einzige ist, der den Internetanschluss benutzt. Bei einem Mehrpersonenhaushalt reicht dafür bereits die Tatsache, dass der Anschlussinhaber nicht alleine in dem Haushalt wohnt. Ferner kann der Anschlussinhaber durch Ortsabwesenheit zur fraglichen Zeit eventuell sogar den vollen Negativbeweis erbringen, dass er eine gewisse Handlung mit einem Rechner nicht vorgenommen hat.

II. E-Mails

1. Rechtsscheinhaftung

Bei dem Versand von E-Mails[19] fehlt es an beiden Voraussetzungen für die Anerkennung eines Rechtsscheintatbestandes. Die notwendige Sicherheit des Authentisierungsverfahrens[20] ist nicht gegeben. Zum einen kann eine E-Mail auch ohne Authentisierung beim SMTP-Server versendet werden.[21] Zum anderen ist die Absender-Angabe einer E-Mail nur eine Header-Information, die beliebig gesetzt werden kann.[22] Ebenso wie auf einen Brief ein beliebiger Absender geschrieben werden kann, kann der Versender einer Mail frei gewählt werden. Eine zuverlässige Überprüfung der Identität des Account-Inhabers findet nicht statt,[23] sodass die zweite Voraussetzung des Rechtsscheintatbestandes, eine zuverlässige Identifikationsfunktion,[24] nicht erfüllt ist. Der Empfang einer E-Mail begründet daher keinen Rechtsschein dafür, dass der Inhaber des E-Mail-Accounts gehandelt hat.[25] **834**

18 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 12.
19 Oben Rn. 48.
20 Oben Rn. 534 ff.
21 Oben Rn. 49.
22 Zu diesem sog. Mail-Spoofing oben Rn. 212.
23 Oben Rn. 51 ff.
24 Oben Rn. 595 ff.
25 Im Ergebnis ebenso *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257; *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 34; *Reese*, S. 52; *Ultsch*, DZWir 1997, 466, 470.

2. Beweiserleichterungen

835 Bei der Frage, ob bei E-Mails[26] eine Beweiserleichterung in Betracht kommt, soll zunächst die in der Literatur diskutierte Frage des Anscheinsbeweises aufgegriffen werden.[27] Ob ein Beweis des ersten Anscheins[28] dafür spricht, dass eine E-Mail tatsächlich vom angegebenen Absender versendet wurde,[29] ist umstritten. Teilweise wird dieser Anscheinsbeweis hauptsächlich unter Berufung auf rechtsökonomische Erwägungen bejaht.[30] Herrschend wird hingegen angenommen, dass ein solcher Anscheinsbeweis nicht besteht und der Anspruchsteller die Urheberschaft der E-Mail voll beweisen muss.[31]

836 Für einen Anscheinsbeweis wird die rechtsökonomische Erwägung herangezogen, dass ansonsten der Absender der Erklärung ein „Widerrufsrecht kraft Beweislastverteilung" habe.[32] Dem Rechtsverkehr solle nicht zugemutet werden, dass er in einer Papierwirtschaft mit Rückbestätigungen per E-Mail geschlossener Verträge operiert.[33] Die effektive Durchsetzung von Ansprüchen solcher Verträge würde ohne den Anscheinsbeweis erheblich beeinträchtigt werden.[34] Dagegen ist jedoch einzuwenden, dass das reine Vertrauen auf ein unsicheres Medium nicht deren rechtliche Schutzbedürftigkeit begründet. Wenn sich Vertragspartner einen einfachen, kostengünstigen, aber unsicheren Kommunikationskanal aussuchen, was ihnen mög-

---

26 Oben Rn. 48.

27 Zum Beweiswert von E-Mails siehe *Sander*, CR 2014, 292, 293 ff.

28 Oben Rn. 785.

29 Zur Frage der Beweiserleichterungen für den Zugang von E-Mails *Willems*, MMR 2013, 551.

30 *Mankowski*, NJW 2002, 2822; *ders.*, CR 2003, 44; *ders.*, MMR 2004, 181; *Winter*, JurPC Web-Dok., 71/2002, Rn. 14; wohl auch *Haug*[2], Rn. 726; ohne Begründung *AG Hannover*, Urteil v. 20. 12. 1999, 518 C 13916/99 – WuM 2000, 412.

31 *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814; *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; *AG Bonn*, Urteil v. 25. 10. 2001, 3 C 193/01 – CR 2002, 301; *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002, 127, 128; *Bergfelder*, S. 346; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 309 f.; *Ernst*, Vertragsgestaltung, Rn. 24; *ders.*, MDR 2003, 1091, 1092; *Jandach*, in: FS Kilian, 443, 451; *Kitz*, in: *Hoeren*/*Sieber*/*Holznagel*, Kap. 13.1 Rn. 69; *F. A. Koch*, Internet-Recht[2], S. 116; *Redeker*, IT-Recht[5], Rn. 906; *Roßnagel*, K&R 2003, 84, 85; *Roßnagel*/*Pfitzmann*, NJW 2003, 1209; *Wiebe*, MMR 2002, 128; *ders.*, MMR 2002, 257, 258.

32 *Mankowski*, CR 2003, 44; *ders.*, MMR 2004, 181.

33 *Mankowski*, MMR 2004, 181, 182.

34 Ebd.

lich bleiben muss,[35] verzichten sie bewusst auf den erhöhten Schutz durch die Rechtsordnung. Sie müssen ihrem Vertragspartner ein entsprechendes Vertrauen entgegenbringen oder sich über alternative Möglichkeiten,[36] wie eine Vorleistungspflicht der Gegenseite, absichern. Ferner wird argumentiert, dass die Verneinung eines Anscheinsbeweises eine Beweislastumkehr zu seinen Lasten darstelle,[37] weil der Empfänger keine Möglichkeit hat, das Absenden der E-Mail zu beweisen. Dies verkennt die grundsätzliche Beweislastverteilung.[38] Mit dem Anscheinsbeweis muss vielmehr eine von dem Normalfall abweichende Beweiserleichterung gerechtfertigt werden.

Dogmatisch wird der Anscheinsbeweis mit einem aus der Lebenserfahrung stammenden Erfahrungssatz begründet, dass E-Mails regelmäßig vom behaupteten Aussteller stammen.[39] Diese Erfahrung stammt aus der eigenen Wahrnehmung von *Mankowski*,[40] was jedoch wegen der Vielseitigkeit des Einsatzes von E-Mails nicht als ausreichende Erfahrungsgrundlage angesehen werden kann.[41] Selbst der empirische Nachweis, dass die Mehrzahl von E-Mails vom behaupteten Empfänger stammen,[42] begründet nur eine überwiegende Wahrscheinlichkeit, keine Typizität. Eine kausale Verbindung zwischen der Vermutungsbasis und der vermuteten Tatsache lässt sich daraus nicht herleiten.[43] Zu einem solchen Erfahrungssatz führt nur die selektive Wahrnehmung der zugestellten E-Mails. Bei Berücksichtigung der zahlreichen Spam- und Phishing-Mails, die häufig von entsprechenden Filtern aussortiert werden und nicht in den Posteingang des E-Mail-Kontos gelangen, lässt sich sogar an der empirischen Grundlage zweifeln.[44] Bei diesen Mails ist es üblich, dass falsche Absender verwendet werden, um den dadurch getäuschten Nutzer zu einer Interaktion zu motivieren. **837**

Für das Vorliegen des Erfahrungssatzes, der behauptete Absender stimme mit dem tatsächlichen Verfasser überein, wird ferner vorgebracht, dass **838**

35 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1214.
36 Dazu oben Rn. 657 ff.
37 *Haug*[2], Rn. 726.
38 Oben Rn. 772.
39 *Mankowski*, CR 2003, 44, 45.
40 *Mankowski*, NJW 2002, 2822, 2824.
41 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211.
42 Siehe *Ernst*, MDR 2003, 1091, 1092.
43 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211 f.; *Roßnagel*, K&R 2003, 84, 85.
44 *F. A. Koch*, Internet-Recht[2], S. 116, was ohne den daraus folgenden Schluss erkannt wird von *Mankowski*, NJW 2002, 2822, 2823.

die Wahrscheinlichkeit von Eingriffen gering sei.[45] Der bloße Verweis auf die Unsicherheit des Internets reiche nicht aus.[46] Eine Manipulation stelle eine absolute Ausnahme dar.[47] Die vielfältigen Möglichkeiten E-Mails zu fälschen sprechen bereits dagegen, dass Verfälschungen eine Ausnahme seien.[48] Die Behauptung, dass es an einer einfach umzusetzenden technischen Möglichkeit der Verfälschung von E-Mails fehle,[49] kann leicht widerlegt werden. Der Absender einer E-Mail ist eine Header-Information, die beliebig gewählt werden kann.[50] Ein Dritter kann daher problemlos über einen fremden Namen E-Mails über einen beliebigen SMTP-Server verschicken. Diese Möglichkeit solle dem Anscheinsbeweis nicht entgegen stehen, weil dieser Maskerade-Angriff durch den Zustellungsweg im Mail-Header, der nicht vom üblichen SMTP-Server initiiert ist, nachvollziehbar sei. Ein Maskerade-Angriff, der nicht aufdeckbar ist, sei nur schwer zu bewerkstelligen.[51] Dagegen ist jedoch einzuwenden, dass durch die mangelnde Authentisierung bei SMTP-Servern häufig auch das Senden über den vom Account-Inhaber benutzten SMTP-Server möglich ist.[52] Darüber hinaus kann es durchaus vorkommen, dass der Dritte eigene Zugangsdaten zum SMTP-Server besitzt, mit denen er sich authentisieren kann. Ein Mitarbeiter kann beispielsweise eine scheinbar von seinem Arbeitskollegen stammende E-Mail absetzen oder der Kunde eines Freemail-Anbieters kann E-Mails mit der Absenderangabe anderer Kunden verschicken. Ferner kann der Dritte die Zugangsdaten des Account-Inhabers zum E-Mail-Konto ausspähen[53] oder ein E-Mail-Konto unter fremdem Namen anlegen.[54] Wegen der weltweiten Nutzbarkeit der E-Mail lässt sich kein Rückschluss auf eine Person oder einen Personenkreis herleiten, von dem die E-Mail stammen könnte.[55] Der Blick auf anerkannte Beweiserleichterungen hat gezeigt, dass ein so unsicheres System wie der E-Mail-Versand keine hinreichende Grundlage

45 *Mankowski*, CR 2003, 44, 45.
46 *Winter*, JurPC Web-Dok., 71/2002, Rn. 17.
47 *Mankowski*, NJW 2002, 2822, 2824.
48 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211.
49 *Mankowski*, CR 2003, 44, 45.
50 Oben Rn. 212.
51 *Sosnitza/Gey*, K&R 2004, 465, 468; *Mankowski*, NJW 2002, 2822, 2823.
52 *Roßnagel*, K&R 2003, 84; *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211.
53 Oben Rn. 124 ff.
54 Oben Rn. 210.
55 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.

für einen Anscheinsbeweis ist.[56] Beim Absenden einer E-Mail ist daher der Schluss auf den Account-Inhaber nicht möglich.[57]

Hinzu kommt, dass die Manipulation nicht beim Versenden der E-Mail er- **839**
folgen muss. E-Mails sind lediglich Text-Dateien, deren Schriftzeichen wie bei jeder anderen Datei verändert werden können. Bei jeder Station, die eine E-Mail vom Absender zum Empfänger macht, kann ihr Inhalt verändert werden.[58] Der Empfänger kann den Mail-Header nachträglich ändern,[59] oder den Inhalt der E-Mail auf eine für ihn bessere Version ändern. Sämtliche nachträgliche Veränderungen der E-Mail sind nicht nachweisbar.[60] Eine E-Mail hat daher noch nicht einmal den Beweiswert einer nicht unterzeichneten mit Bleistift in Druckbuchstaben geschriebenen Postkarte.[61] Diese Möglichkeit die E-Mail nachträglich zu verändern, schließt die Anerkennung eines Anscheinsbeweises aus.[62]

Für den Anscheinsbeweis solle sprechen, dass es an Motiven und Anrei- **840**
zen fehle, E-Mails unter fremdem Namen zu versenden.[63] Dagegen spricht zunächst, dass sich in der Rechtsprechung Fälle finden lassen, bei denen scheinbar grundlos die Zugangsdaten eines Account-Inhabers missbraucht wurden.[64] Ferner zeigen die zahlreichen Phishing-Mails, dass Kriminelle sich materielle Vorteile davon versprechen, E-Mails unter falscher Absenderangabe zu versenden. Darüber hinaus gibt es durchaus zahlreiche Anwendungsbeispiele, bei denen ein rational nachvollziehbares Motiv für eine gefälschte Absender-Adresse vorhanden ist. Ein Angreifer bei einem Social-Engineering-Angriff[65] kann beispielsweise vor seinem Anruf als vermeintlicher technischer Ansprechpartner eine E-Mail, die scheinbar vom Vorgesetzten des Opfers stammt, in der er den Anruf ankündigt und um Zusammenarbeit bittet, verschicken.

---

56 Oben Rn. 826.
57 *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814; *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.
58 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1210.
59 Ebd., 1210.
60 *Ernst*, MDR 2003, 1091, 1092.
61 *Roßnagel*, K&R 2003, 84.
62 *AG Bonn*, Urteil v. 25. 10. 2001, 3 C 193/01 – CR 2002, 301; *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1210.
63 *Mankowski*, CR 2003, 44, 45; *ders.*, MMR 2004, 181, 182.
64 Oben Rn. 634.
65 Dazu oben Rn. 162.

841 Darüber hinaus sollen die strafrechtlichen Konsequenzen eines Missbrauchs, der nachträglichen Veränderung oder eines Prozess-Betruges ausreichend vor diesen schützen.[66] Strafrechtliche Konsequenzen schrecken jedoch insbesondere nur ab, wenn die Möglichkeit der Aufdeckung besteht. Da nachträgliche Veränderungen nicht bewiesen werden können und es zahlreiche Wege gibt, wie eine E-Mail ohne Absenden durch den behaupteten Absender zum Empfänger gelangen kann, ist dem möglichen Straftäter die Straftat nur schwer nachzuweisen. Ferner kommen Täuschungshandlungen wie der Prozessbetrug häufig vor.[67] Die strafrechtlichen Konsequenzen halten die im Zivilprozess streitenden Parteien anscheinend nicht davon ab, die Unwahrheit zu behaupten. Wer behauptet, dass die strafrechtlichen Konsequenzen eines Prozessbetrugs einen Anscheinsbeweis für die Echtheit einer E-Mail begründen, muss sich fragen lassen, ob mit diesem Argument, nicht auch ein Anscheinsbeweis dahingehend besteht, dass alles, was Prozessparteien vortragen, der Wahrheit entspricht. Die Absurdität eines solchen Anscheinsbeweises zeigt, dass das Argument der drohenden Strafbarkeit nicht für einen Anscheinsbeweis der Echtheit von E-Mails spricht.

842 Ferner solle die Erschütterung des Anscheinsbeweises, beispielsweise durch Zeugenbeweis, einfach möglich sein, sodass der Anscheinsbeweis den Absender nicht übermäßig belaste.[68] Der Absender könne beispielsweise Einblicke in sein System gewähren, um zu zeigen, dass die E-Mail sich nicht in seinem Postausgang oder Papierkorb befinde.[69] Diese Behauptung verkennt jedoch zwei entscheidende Merkmale. Zum einen können E-Mails so gelöscht werden, dass keine Spuren mehr von ihnen auf dem eigenen Mail-Server zu finden sind. Ebenso wie einen normalen Papierkorb kann man auch die elektronischen Papierkörbe leeren.[70] Zum anderen könnte das Fehlen der E-Mail im System des Account-Inhabers zahlreiche Gründe haben. Die E-Mail könnte von einem anderen Rechner versendet worden sein, sodass sie im Postausgang des einen Rechners nicht auftaucht, wenn sie nicht auf allen Endgeräten per IMAP synchron gehalten werden. Zum anderen ist der Beweis der negativen Tatsache, dass der Account-Inhaber die E-Mail nicht versendet hat, nur schwer zu führen. Dem Account-Inhaber wird

66 *Mankowski*, NJW 2002, 2822, 2825; *ders.*, MMR 2004, 181, 182; *Winter*, JurPC Web-Dok., 71/2002, Rn. 14.
67 Siehe *Krell*, JR 2012, 102.
68 *Mankowski*, MMR 2004, 181, 182 f.
69 *Mankowski*, CR 2003, 44, 49.
70 Was ebd., 49 anscheinend verkennt.

es schwer fallen, die Vermutungsbasis zu erschüttern.[71] Es wird behauptet, dass der Anspruchsteller die Urheberschaft der E-Mail nur beweisen müsse, wenn sich der Missbrauch aufdränge.[72] Dies verkennt die zahlreichen Möglichkeiten, die zur Verfälschung eines E-Mail-Absenders oder einer E-Mail bestehen. Häufig ist unaufklärbar, wie ein Dritter den Missbrauch bewerkstelligt hat. Der Account-Inhaber würde damit durch die allgemeine Systemrisiken belastet, die er ebenso wenig wie der Erklärungsempfänger kontrollieren kann. Dies wäre unbillig.

Für den Anscheinsbeweis soll darüber hinaus sprechen, dass E-Mail-Adressen auf einer einmaligen, exklusiven Zuordnung zu einem Inhaber beruhen.[73] Dies verkennt jedoch, dass zahlreiche E-Mail-Adressen nicht einem Inhaber in Form einer natürlich Person zugeordnet sind, sondern eine Gruppe von Empfängern oder eine funktionale Einheit erreicht.[74] E-Mail-Adressen wie info@firma.de, no-reply@newsletter-versender.de oder vorstand@verein.de sind gerade nicht einem Inhaber zugeordnet. **843**

Darüber hinaus sprechen systematische Argumente gegen die Anerkennung des Anscheinsbeweises. Im Umkehrschluss zu § 371a Abs. 1 S. 2 ZPO, der Nachfolgeregelung zu § 292a ZPO,[75] soll ein Anscheinsbeweis bei E-Mails gerade nicht bestehen.[76] Der Wortlaut des § 371a Abs. 1 S. 2 ZPO sperrt keine anderweitigen Anscheinsbeweise.[77] Ferner zeigt der Vergleich mit den Schrifturkunden, dass die Anerkennung eines Anscheinsbeweises in systematischem Widerspruch zu der Wertung des § 440 Abs. 1 ZPO steht. Weil bei diesen der sich auf die Urkunde Berufende deren Echtheit zu beweisen hat, muss dies erst recht für die Echtheit von E-Mails gelten.[78] Der Blick auf anerkannte Beweiserleichterungen in vergleichbaren Situationen hat gezeigt, dass für den Anscheinsbeweis eine hinreichend sichere Authentisierungsmethode sowie eine zuverlässige Identifizierung des Account-Inhabers beim Anlegen des Accounts erforderlich ist.[79] Beides fehlt bei der **844**

---

71 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1213.
72 *Winter*, JurPC Web-Dok., 71/2002, Rn. 17.
73 *Mankowski*, MMR 2004, 181, 183.
74 Oben Rn. 57.
75 Dazu oben Rn. 801 ff.
76 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1213; *Roßnagel*, K&R 2003, 84, 86; *Wiebe*, MMR 2002, 257, 258.
77 *Mankowski*, NJW 2002, 2822, 2827; *ders.*, CR 2003, 44, 47; *Sosnitza/Gey*, K&R 2004, 465, 466; *Winter*, JurPC Web-Dok., 71/2002, Rn. 12.
78 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1212; *Roßnagel*, K&R 2003, 84, 85.
79 Oben Rn. 826.

E-Mail, sodass die Annahme eines Anscheinsbeweises gängigen Wertungen widersprechen würde.

845 Ferner würde die Anerkennung eines Anscheinsbeweises falsche Anreize setzen.[80] Die Behauptung, dass eine missbräuchliche Berufung auf den Anscheinsbeweis kaum vorstellbar sei,[81] kann leicht widerlegt werden. Wenn einfach zu fälschende E-Mails als rechtssicherer Beweis anerkannt werden, könnte ein Krimineller in betrügerischer Absicht, eine E-Mail von jeder Person fälschen, deren E-Mail-Adresse und ladungsfähige Anschrift er kennt, und diese mit Zahlungsansprüchen konfrontieren. Durch die Anerkennung eines Anscheinsbeweises würde ein starker Anreiz zur Fälschung von E-Mails geschaffen werden.[82] Ein Anscheinsbeweis für E-Mails ist somit abzulehnen.

846 Eine tatsächliche Vermutung[83] dafür, dass eine E-Mail vom Account-Inhaber stammt scheidet somit erst recht aus. Eine sekundäre Darlegungslast[84] sowie eine Umkehr der Beweislast[85] scheitern daran, dass einige Missbrauchsmöglichkeiten, wie das Mail-Spoofing,[86] außerhalb der Sphäre des Account-Inhabers stammen.

III. Benutzerkonten auf Internetseiten

1. Rechtsscheinhaftung

a) Informationsportale und Online-Shops

847 Bei Benutzerkonten auf Internetseiten muss bezüglich der Rechtsscheinhaftung wegen der Vielfalt der unterschiedlichen Arten differenziert werden. Bei einem Account auf einem Informationsportal, bei dem Personendaten zur Registrierung nicht erforderlich sind,[87] scheitert der Rechtsscheintatbestand bereits an einer irgendwie gearteten Identifikationsfunktion.[88] Selbst

80 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1213.
81 *Mankowski*, CR 2003, 44, 48.
82 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1213.
83 Oben Rn. 781.
84 Oben Rn. 792.
85 Oben Rn. 776.
86 Oben Rn. 212.
87 Siehe dazu oben Rn. 60.
88 Oben Rn. 595 ff.

bei Online-Shops, die mutmaßlich ein starkes Interesse an der Solvenz ihrer Vertragspartner haben, ist keine hinreichend zuverlässige Identifikationsfunktion vorhanden.[89] Ein Rechtsscheintatbestand scheidet bei diesen Accounts somit regelmäßig aus.

b) Internet-Auktionsplattformen

Benutzerkonten auf Internetseiten mit Reputationssystem hingegen wird häufig eine Identifikationsfunktion bezüglich einer numerischen Identität zugesprochen.[90] Diese wird häufig pauschal behauptet,[91] wobei die Ausführungen darauf hindeuten, dass der Account den Account-Inhaber identifizieren soll. Zur Begründung der Identifikationsfunktion werden zwei Argumente genannt: die Geheimhaltungspflicht des Passworts sowie die Überprüfung der Angaben bei der Registrierung. **848**

Die Geheimhaltungspflicht des Passworts kann eine Identifikationsfunktion bezüglich des Account-Inhabers nicht überzeugend begründen.[92] Zum einen erfolgt die Begründung von Identifikationsfunktion und Geheimhaltungspflicht häufig zirkulär.[93] Zum anderen betrifft die Geheimhaltungspflicht lediglich die Sicherheit der verwendeten Authentisierungsmethode.[94] Die Identifikationsfunktion sowie deren Zuverlässigkeit muss jedoch durch die Art des Accounts sowie die Überprüfung der angegebenen Personendaten bei der Registrierung erfolgen.[95] **849**

Die Angabe der Daten bei der Registrierung und deren Plausibilitätskontrolle durch die Internet-Auktionsplattform kann keine Identifikationsfunktion bezüglich des Account-Inhabers überzeugend begründen. Zwar muss **850**

89 Oben Rn. 62.

90 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18; Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18; *Genius*, jurisPR-BGHZivilR 12/2011, Anm. 1, C; *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 34; *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 174; *Klein*, MMR 2011, 450; *Mankowski*, CR 2007, 606; *Stöber*, JR 2012, 225, 228.

91 Vgl. etwa *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18.

92 So aber *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18; *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 34.

93 Oben Rn. 558.

94 Dazu allgemein oben Rn. 534 ff.

95 Oben Rn. 595 ff.

ein Nutzer seinen Namen und seine Adresse bei der Registrierung angeben.[96] Einer Person können diese Daten jedoch nur zuverlässig zugeordnet werden, wenn diese Daten auch überprüft werden. Die Überprüfung der E-Mail-Adresse reicht zur Identifizierung des Account-Inhabers nicht aus.[97] Die E-Mail-Adresse hat keinerlei Identifikationsfunktion bezüglich einer numerischen Identität einer Person,[98] sodass aus ihrer Überprüfung keine Identifikationsfunktion für einen Account abgeleitet werden kann. Auch die Plausibilitätskontrolle der Daten durch einen Abgleich mit der Schufa kann keine Identifikationsfunktion bezüglich der numerischen Identität des Namensträgers begründen.[99]

851 Als Zwischenergebnis lässt sich festhalten, dass die Registrierung bei einer Internet-Auktionsplattform keine Identifikationsfunktion bezüglich der numerischen Identität des Account-Inhabers herstellt. Ein Account bei einer Internet-Auktionsplattform mit Reputationssystem identifiziert daher nur die virtuelle Identität des Erstellers und nicht die numerische Identität des Account-Inhabers. Die überwiegende Zahl der Accounts bei solchen Plattformen sind vom jeweiligen Account-Inhaber erstellt. Wegen der zahlreichen Möglichkeiten einen Account unter falschem Namen zu eröffnen und erfolgreich zu betreiben, kann jedoch keine zuverlässige Identifikationsfunktion angenommen werden. Darüber hinaus kann angenommen werden, dass zahlreiche Accounts unter falschem Namen angelegt wurden, wenn sich ein betroffener Namensträger sogar durch den gesamten Instanzenzug klagen muss, um sich gegen falsche Accounts auf seinen Namen zu wehren.[100]

852 Man kann jedoch überlegen, ob eine zuverlässige Identifizierung des Account-Inhabers später durch das Reputationssystem[101] geschaffen wird. Doch selbst ein Reputationssystem begründet keine hinreichend zuverlässige Überprüfung der Zuordnung des Accounts zum Account-Inhaber.[102] Die Voraussetzung der zuverlässigen Identifikation[103] zur Anerkennung eines

96 *Gurmann*, S. 18 f.; *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 174.
97 *Gurmann*, S. 19; **a.A.** *Stöber*, JR 2012, 225, 228. Dazu bereits oben Rn. 598.
98 Oben Rn. 48. Für die E-Mail-Adresse erkennt *Stöber*, dass ohne Identitätsüberprüfung keine Identifikationsfunktion bestehen kann, ebd., 229.
99 Oben Rn. 608.
100 Vgl. *BGH*, Urteil v. 10. 4. 2008, I ZR 227/05 (Namensklau im Internet) – NJW 2008, 3714.
101 Wie beispielsweise eBay es betreibt, dazu oben Rn. 66.
102 Oben Rn. 620.
103 Oben Rn. 595 ff.

Rechtsscheintatbestandes ist somit bei Benutzerkonten auf Internetseiten regelmäßig nicht gegeben. Die in der Regel anzutreffende rein wissensbasierte Authentisierung bietet darüber hinaus keine hinreichende Gewähr dafür, dass der Account-Inhaber handelt, sodass die Anerkennung des Rechtsscheintatbestandes auch daran scheitert.[104] Ein Rechtsscheintatbestand dafür, dass der Account-Inhaber eines passwortgeschützten Benutzerkontos auf einer Internetseite selbst gehandelt hat, besteht somit nicht.[105]

c) Accounts mit Zwei-Faktor-Authentisierung

Setzen Benutzerkonten im Internet eine Zwei-Faktor-Authentisierung[106] ein, verwenden sie eine hinreichend sichere Authentisierungsmethode für die Anerkennung eines Rechtsscheintatbestandes.[107] Zahlreiche Anbieter setzen mittlerweile zur Absicherung eine Zwei-Faktor-Authentisierung ein.[108] Eine Rechtsscheinhaftung bei Missbrauch dieser Accounts kommt jedoch nur in Betracht, wenn der Account-Inhaber bei der Registrierung oder später zuverlässig identifiziert wurde,[109] was bei den genannten Beispielen nicht gegeben ist. Eine Rechtsscheinhaftung kann bei diesen Beispielen somit nur in Einzelfällen in Betracht kommen, wenn der Account-Inhaber gegenüber dem Geschäftsgegner das Zutreffen der Identitätsbehauptung des Accounts bestätigt hat.[110] **853**

2. Beweiserleichterungen

Bei Benutzerkonten auf Internetseiten werden unterschiedliche Formen der Beweiserleichterung diskutiert. Zunächst soll untersucht werden, ob ein An- **854**

104 Zur Unsicherheit der rein wissensbasierten Authentisierung oben Rn. 544 ff.

105 Im Ergebnis auch *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18; *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 10; *Wiebe/Neubauer*, in: *Hoeren/Sieber/Holznagel*, Kap. 15 Rn. 57; *M. Wolf/Neuner*[10], § 50 Rn. 108; **a.A.** *Borges*, NJW 2011, 2400, 2402; *Herresthal*, K&R 2008, 705, 708 f.; *ders.*, in: *Taeger/Wiebe*, 21, 34 f.; *Stöber*, JR 2012, 225, 229 f.

106 Dazu oben Rn. 117 ff.

107 Oben Rn. 578 ff.

108 Beispielsweise bieten Google und Facebook dies an, dazu *J. Schmidt*, heise online v. 11. 2. 2011; *ders.*, heise online v. 13. 5. 2011.

109 Oben Rn. 595 ff.

110 Oben Rn. 623.

scheinsbeweis bei Benutzerkonten auf Internet-Auktionsplattformen in Betracht kommt und anschließend, ob für sämtliche Formen der Benutzerkonten auf Internetseiten eine sekundäre Darlegungslast des Account-Inhabers begründet ist.

a) Anscheinsbeweis

855 Die Frage, ob ein Anscheinsbeweis[111] dafür spricht, dass der Account-Inhaber eine vorliegende Erklärung über den Account abgegeben hat, ist umstritten. Dies wird zum Teil aus rechtsökonomischen Erwägungen und wegen der zahlreichen problemlos verlaufenden Fälle angenommen.[112] Überwiegend wird ein Anscheinsbeweis jedoch unter Verweis auf den Sicherheitsstandard im Internet abgelehnt.[113]

856 Für den Anscheinsbeweis wird insbesondere die teleologische Erwägung angeführt, dass der Account-Inhaber nicht die Möglichkeit haben darf, sich von einem ungewollten Vertrag zu lösen.[114] Das Vertrauen in den elektroni-

111 Oben Rn. 785.

112 *Ernst*, Vertragsgestaltung, Rn. 26 ff.; *ders.*, MDR 2003, 1091, 1093; *Härting/Golz*, ITRB 2005, 137, 138; *Härting*[4], Rn. 584; *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 42 ff.; *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 183; *M. Köhler/Arndt/Fetzer*[7], Rn. 324; *Mankowski*, EWiR 2001, 1123, 1124; *ders.*, CR 2007, 606; *ders.*, CR 2011, 458.

113 *OLG Bremen*, Beschluss v. 21. 6. 2012, 3 U 1/12 – MMR 2012, 593, 594; *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06 – NJW 2007, 611; Urteil v. 20. 7. 2009, 2 U 50/09, I-2 U 50/09, Rn. 24; *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814; Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676; *OLG Naumburg*, Urteil v. 2. 3. 2004, 9 U 145/03 – OLG-NL 2005, 51; *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180; *LG Köln*, Urteil v. 27. 10. 2005, 8 O 15/05 – BeckRS 2006, 07259; *LG Konstanz*, Urteil v. 19. 4. 2002, 2 O 141/01 A – CR 2002, 609; *LG Magdeburg*, Urteil v. 21. 10. 2003, 6 O 1721/03 (321) – CR 2005, 466, 467; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15; *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002, 127, 128; *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 519; *Biallaß*, ZUM 2007, 397; *Borges*, in: Internet-Auktion, 214, 223; *Borges/Schwenk/Stuckenberg/Wegener*, S. 311; *Hanau*, Handeln unter fremder Nummer, S. 215; *Kitz*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.1 Rn. 67; *F. A. Koch*, Internet-Recht[2], S. 115; *Noack/Kremer*, AnwBl 2004, 602, 604; *Oechsler*, AcP 208 (2008), 565, 578; *ders.*, MMR 2011, 631, 632; *Schramm*, in: MüKo-BGB[6], § 164 Rn. 45b; *Wiebe*, Elektronische Willenserklärung, S. 435; *Wiebe/Neubauer*, in: *Hoeren/Sieber/Holznagel*, Kap. 15 Rn. 58; *Dennis Werner*, K&R 2011, 499, 500.

114 *Mankowski*, CR 2011, 458; *Winter*, CR 2004, 219, 221.

schen Handel solle gestärkt werden, damit er nicht zum Erliegen komme.[115] Dieses Vertrauen stützte sich bei der rein wissensbasierten Authentisierung sogar auf drei vertrauensbegründende Momente: den Benutzernamen, das Passwort sowie deren Zusammenpassen.[116] Dagegen lässt sich jedoch einwenden, dass eine rein wissensbasierte Authentisierung unter den Nachteilen leidet, dass die Information des Geheimnisses unendlich teilbar ist und eine Kontrolle über die Verbreitung des Wissens nicht stattfinden kann.[117] Häufig beträgt die Kombination aus Benutzername und Passwort um die dreißig Zeichen,[118] wovon nur das Passwort geheim ist. Die Vertrauensbasis ist daher recht gering.

Die Lebenserfahrung hat ferner gezeigt, dass auch ohne einen starken **857**
rechtlichen Schutz dieses Vertrauens, der Handel über Internetplattformen unverändert fortbesteht.[119] Häufig liegen der Annahme des Anscheinsbeweises leicht zu widerlegende Grundannahmen bezüglich passwortgeschützter Accounts zu Grunde. Der Behauptung, dass Passwörter die Antwort auf die unsichere E-Mail seien,[120] ist zu widersprechen. Passwortgeschützte Accounts dienen dem Nutzer primär dazu, eine virtuelle Identität bei einem Authentisierungsnehmer zu erstellen. Daraus entstehen dem Nutzer beispielsweise die Vorteile, dass er auf der Seite wiedererkannt wird und Einblick in seine vorangegangen Aktionen, wie Bestellungen, nehmen kann oder seine Daten oder Präferenzen wegen der gespeicherten Informationen nicht erneut eingeben muss. Aus dem gleichen Grund ist der Behauptung, dass Passwörter zur Vermeidung von Kaufreue dienen sollen,[121] zu widersprechen. Mit diesen Behauptungen wird versucht, den passwortgeschützten Accounts eine nicht vorhandene Bedeutung zuzusprechen, die den Anscheinsbeweis mit der nicht vorhandenen Zweckrichtung rechtfertige. Vielmehr ist jedoch darauf einzugehen, ob die sich auf zahlreichen praktischen Vorteilen entwickelten Accounts die rechtlichen Anforderungen an den Anscheinsbeweis erfüllen.

---

115 *Mankowski*, EWiR 2001, 1123.
116 *Mankowski*, CR 2007, 606, 607; *ders.*, CR 2011, 458.
117 Oben Rn. 111.
118 Der Benutzername „max.mustermann@web.de“ sowie ein acht Zeichen langes Passwort ergeben zusammen 29 Zeichen.
119 Oben Rn. 385.
120 *Mankowski*, CR 2007, 606, 607; *ders.*, CR 2011, 458.
121 *Ernst*, MDR 2003, 1091, 1093.

858 Die angemessene Verteilung der Risiken beim Online-Handel solle ebenfalls einen Anscheinsbeweis rechtfertigen. Der Anspruchsteller solle eine reelle Chance haben, den Anspruch durchzusetzen.[122] Das Risiko des Missbrauchs dürfe nicht allein dem Erklärungsempfänger auferlegt werden,[123] weil sich beide Parteien diesem Risiko gleichermaßen aussetzen.[124] Dagegen ist jedoch einzuwenden, dass demjenigen, der sich auf ein Rechtsgeschäft einlässt, ohne sich durch unterschiedliche Möglichkeiten abzusichern[125] oder ohne sichere Beweismittel zu schaffen, das Risiko billigerweise aufgebürdet werden kann.[126] Im Offline-Bereich ist anerkannt, dass der Anbieter das Risiko missbräuchlicher Bestellung zu tragen hat.[127] Ein unberechtigtes Vertrauen in einen Vertragspartner muss nicht durch die Rechtsordnung geschützt werden. Der mündliche Vertragsschluss beispielsweise ist auch schwer zu beweisen, zum Beispiel unter Vertragspartnern, die sich kennen und vertrauen, jedoch auch ohne Schutz durch die Rechtsordnung üblich. Eine angemessene Risikoverteilung muss daher nicht zu einem Anerkennen des Anscheinsbeweises führen.

859 Sodann soll überprüft werden, ob die Voraussetzung des Anscheinsbeweises, dass ein Erfahrungssatz nach der allgemeinen Lebenserfahrung gegeben sein muss, vorliegt. Vielfach wird für den Anscheinsbeweis ins Felde geführt, dass die große Anzahl an problemlos verlaufenden Transaktionen sowie der prozentual geringe Anteil an Missbrauchsfällen einen für einen Anscheinsbeweis tauglichen Erfahrungssatz begründen.[128] Eine behauptete Seltenheit der Angriffe[129] sowie die unzutreffend[130] behauptete geringe Wahrscheinlichkeit einer Manipulation[131] sollen einen Anscheinsbeweis rechtfertigen. Die zahlreichen korrekt abgewickelten Geschäfte können den

122 *Winter*, CR 2004, 219, 221.
123 *Ernst*, MDR 2003, 1091, 1093.
124 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180; *Biallaß*, ZUM 2007, 397.
125 Zu den Möglichkeiten oben Rn. 657.
126 *Kuhn*, S. 257.
127 *F. A. Koch*, Internet-Recht[2], S. 115.
128 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 44; *Wiebe/Neubauer*, in: *Hoeren/Sieber/Holznagel*, Kap. 15 Rn. 58; *M. Köhler/Arndt/Fetzer*[7], Rn. 324; *Winter*, CR 2004, 219, 221.
129 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 184.
130 Oben Rn. 127.
131 *Mankowski*, EWiR 2001, 1123, 1124.

Anscheinsbeweis nicht begründen.[132] Eine empirische Statistik reicht nicht aus, weil diese nur eine Aussage bezüglich der statistischen Masse, nicht bezüglich des Einzelfalls trifft.[133]

Es ist daher entscheidend, ob ein Erfahrungssatz nach der Lebenserfahrung vorliegt, dass über einen Account abgegebene Erklärungen vom Account-Inhaber stammen. Dafür ist entscheidend, wie die Zugangsdaten missbraucht werden können und wie wahrscheinlich dies ist. Der Anscheinsbeweis verlangt dafür keine absolute Sicherheit,[134] sondern nur eine Typizität. Ein Erfahrungssatz lässt sich wegen der Missbrauchsmöglichkeiten nur schwer annehmen.[135] Ferner liegen kaum Erkenntnisse darüber vor, wie wahrscheinlich verschiedene Geschehensabläufe sind. Neben dem Handeln des Account-Inhabers selbst, kann er die Zugangsdaten einem Dritten weitergeben,[136] der sie befugt oder unbefugt nutzt. Der Account-Inhaber könnte die Zugangsdaten jedoch auch notiert oder in der Schlüsselbund-Verwaltung gespeichert haben.[137] Beobachtungen dazu entstehen nur durch singuläre Betrachtungen, aus denen sich kein Erfahrungssatz ableiten lässt.[138] Die erforderliche Typizität lässt sich aus der Lebenserfahrung daher nicht feststellen.[139] **860**

Ein Anscheinsbeweis kann daher nur als „Anscheinsbeweis ohne ersten Anschein“[140] über den Ausschluss alternativer Geschehensabläufe begründet werden.[141] Es kommt daher auf die Wahrscheinlichkeit der verschiedenen Geschehensabläufe an. Der Geschehensablauf, dass der Account-Inhaber mit seinen Zugangsdaten die Erklärung abgibt, muss zur Anerkennung des Anscheinsbeweises hoch wahrscheinlich sein. Für diese Wahrscheinlichkeit muss die rein wissensbasierte Authentisierung einen gewissen Si- **861**

132 *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15.

133 Oben Rn. 787 sowie *BGH*, Urteil v. 27. 5. 1957, II ZR 132/56 (Einschreibbrief) – BGHZ 24, 308, 312.

134 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 44.

135 *Oechsler*, AcP 208 (2008), 565, 578; *ders.*, MMR 2011, 631, 632.

136 Zur Weitergabe oben Rn. 125.

137 Oben Rn. 132 ff.

138 *BGH*, Urteil v. 4. 7. 1989, VI ZR 309/88 – NJW 1989, 2947. Dies ist bei der ec-Karte ähnlich *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 345.

139 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; *LG Köln*, Urteil v. 27. 10. 2005, 8 O 15/05 – BeckRS 2006, 07259.

140 *Jungmann*, ZZP 120 (2007), 459.

141 Dazu oben Rn. 788.

cherheitsstandard aufweisen. Brute-Force-Attacken[142] müssen vom Authentisierungsnehmer erschwert werden und der Authentisierungsnehmer muss durch Vorgaben wie eine Mindestpasswortlänge sichere Passwörter erzwingen.[143] Dabei sind die Sicherungsmaßnahmen des Authentisierungsnehmers im Einzelfall zu untersuchen, weil es keinen gesetzlichen Standard für Passwörter gibt.[144]

862 Dabei besteht ferner das Problem, dass zur abschließenden Beurteilung der Wahrscheinlichkeit die Sicherheitsinfrastruktur des Authentisierungsnehmers detailliert bewertet werden muss. Denn wenn diese Schwachstellen aufweist, ist ein Missbrauch auch ohne Zutun des Account-Inhabers möglich.[145] Beim Missbrauch einer ec-Karte besteht dieses Problem in ähnlicher, aber schwächerer Form.[146] Der Authentisierungsnehmer wird regelmäßig keinen Einblick in seine Sicherheitsinfrastruktur geben, weil er die Sicherheit dadurch gefährden könnte.[147] Bei Zwei-Personen-Konstellationen, wie sie auch bei ec-Karten vorhanden sind, besteht die prozessuale Möglichkeit den Authentisierungsnehmer durch eine sekundäre Darlegungslast[148] im Rahmen des Zumutbaren zur Preisgabe der Informationen zu bewegen.[149] Da die Preisgabe von Informationen über die Sicherheitsinfrastruktur des Authentisierungsnehmers die Sicherheit gefährdet, ist ihm eine vollständige Offenlegung jedoch nicht zumutbar. Bei einer Drei-Personen-Konstellation, wie sie bei Internetauktions-Plattformen besteht, ist der Authentisierungsnehmer jedoch nicht Prozesspartei, sodass es im Prozess keine prozessuale Möglichkeit gibt, ihn zu Angaben über die Sicherheitsinfrastruktur zu bewegen. Ob die Sicherheit bei einem gewissen Authentisierungsnehmer eine hinreichende Wahrscheinlichkeit begründet, lässt sich daher mangels notwendiger Informationen nicht abschließend bestimmen.

863 Zwar ist zur positiven Entscheidung, ob ein Anscheinsbeweis vorliegt, die Sicherheitsinfrastruktur des jeweiligen Authentisierungsnehmers erforderlich. Die negative Entscheidung, dass er nicht gegeben ist, kann jedoch durch die Wahrscheinlichkeit alternativer Geschehensabläufe begrün-

142 Oben Rn. 181.
143 *Ernst*, Vertragsgestaltung, Rn. 30; *ders.*, MDR 2003, 1091, 1094.
144 Siehe *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.
145 Oben Rn. 215.
146 Oben Rn. 816.
147 Vgl. zur ec-Karte *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 349 f.
148 Oben Rn. 792.
149 Siehe *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 350.

det werden. Die pauschale Ablehnung des Anscheinsbeweises mit der Begründung, dass der Sicherheitsstandard nicht ausreichend sei,[150] soll folgend überprüft werden. Dazu soll untersucht werden, ob die zahlreichen Missbrauchsmöglichkeiten gegen einen Anscheinsbeweis sprechen. Einem Angreifer stehen zahlreiche Möglichkeiten offen, das Passwort auszuspähen.[151] Die große Anzahl an Zugangsdaten, die in einer Dropzone erworben werden können, deutet auf eine nicht zu vernachlässigende Wahrscheinlichkeit gestohlener Zugangsdaten hin.[152]

Neben dem Diebstahl kommt auch in Betracht, dass ein Nutzer die Zu- **864**
gangsdaten aufgeschrieben oder in der Schlüsselbund-Verwaltung verwahrt hat.[153] Die Wahrscheinlichkeit dieses Geschehensablaufs ist keinesfalls gering. Die Komplexität der Passwörter hat die paradoxe Wirkung, dass sichere Passwörter schwer zu merken sind und daher notiert werden, was die Authentisierungsmethode unsicher werden lässt.[154] Beim Online-Banking ist sogar anerkannt, dass dem Kunden die Notiz der Zugangsdaten möglich sein muss und nicht per AGB ausgeschlossen werden kann.[155] Es ist daher wahrscheinlich, dass ein Account-Inhaber die Zugangsdaten aufgeschrieben hat und nicht unwahrscheinlich, dass er diese Notiz oder Speicherung nicht sorgfältig schützt. Ferner wäre es dem Account-Inhaber in der Praxis unmöglich, die Behauptung, er habe seine Zugangsdaten aufgeschrieben, zu widerlegen. Diese alternativen Geschehensabläufe verhindern die Anerkennung eines Anscheinsbeweises.[156]

Gegen die Wahrscheinlichkeit dieser alternativen Geschehensabläufe **865**
wird häufig eingewendet, dass Dritten bei vielen Accounts eine Motivation fehle, die Zugangsdaten zu missbrauchen.[157] Selbst wenn es an einem rationalen Grund fehlen sollte, lassen sich Fälle finden, bei denen anschei-

150 *OLG Bremen*, Beschluss v. 21. 6. 2012, 3 U 1/12 – MMR 2012, 593, 594; *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06 – NJW 2007, 611; *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180.

151 Oben Rn. 126 ff.

152 *BSI*, Lagebericht 2011, S. 22: Im Jahr 2010 standen Zugangsdaten zu über 350.00 Accounts auf Handelsplattformen und Online-Shops in Dropzones zum Verkauf.

153 Oben Rn. 132 ff.

154 Oben Rn. 562.

155 Oben Rn. 563.

156 So ausdrücklich auch *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814.

157 *M. Köhler/Arndt/Fetzer*[7], Rn. 324.

nend grundlos die Zugangsdaten missbraucht wurden.[158] Ein mangelndes rationales Interesse eines Dritten an einem Missbrauch der Zugangsdaten spricht somit nicht für einen Anscheinsbeweis.[159] Die Strafbarkeit des Dritten beim Missbrauch der Zugangsdaten[160] spricht wegen der geringen Wahrscheinlichkeit der Aufdeckung ebenso wie bei der E-Mail[161] nicht für den Anscheinsbeweis.

866 Die erste Voraussetzung, die sich aus der Analyse von Anscheinsbeweisen in vergleichbaren Konstellationen ergeben hat,[162] dass eine sichere Authentisierungsmethode mit hoher Wahrscheinlichkeit dafür spricht, dass der Account-Inhaber gehandelt hat, liegt nicht vor. Die zweite Voraussetzung der zuverlässigen Identifizierung des Account-Inhabers ist ebenfalls nicht gegeben. Bei Accounts zu Informationsportalen oder Online-Shops ist diese Voraussetzung mangels Überprüfung der Identitätsbehauptung nicht gegeben.[163] Auch bei Benutzerkonten, bei denen eine Plausibilitätskontrolle stattfindet und ein Reputationssystem vorhanden ist, besteht keine zuverlässige Identifikationsfunktion.[164] Accounts werden häufig unter fremden oder falschen Namen angelegt.[165] Ein Anscheinsbeweis kommt daher für die Echtheit des Kontos nicht in Betracht. Diese Echtheit, also das Zutreffen der Identitätsbehauptung, ist stets voll zu beweisen.[166]

867 Die dritte Voraussetzung zur Anerkennung des Anscheinsbeweises ist die Wahrscheinlichkeit der Unverfälschtheit der Erklärung. Da die Erklärungen, die über einen Account abgegeben wurden, ebenso wie E-Mails[167] nur als Dateien auf einem Rechner liegen, sind sie ebenso manipulierbar und nachträglich nicht nachweisbar. Im Zwei-Personen-Verhältnis kann eine Prozesspartei durch die Manipulation der Erklärung einen Vorteil erlangen. Sie hat damit einen rationalen Grund die Erklärung nachträglich zu verfälschen, was gegen die Wahrscheinlichkeit der Unverfälschtheit spricht. Im Drei-Personen-Verhältnis, wie bei einer Internet-Auktionsplattform, hat der

158 Oben Rn. 634.
159 *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15.
160 Dazu *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 44.
161 Oben Rn. 841.
162 Oben Rn. 826.
163 Oben Rn. 847.
164 Oben Rn. 848 ff.
165 *F. A. Koch*, Internet-Recht[2], S. 201.
166 *Kitz*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.1 Rn. 67.
167 Zur nachträglichen Manipulierbarkeit von E-Mails oben Rn. 839.

Authentisierungsnehmer die Erklärungen entgegen genommen und gespeichert. Zwar kann eine Prozesspartei ihre Belege der Erklärungen, wie die Benachrichtigungs-E-Mails oder Kopien von der Bestätigungsseite, manipulieren. Durch eine Rückfrage bei der Handelsplattform, deren Geschäftsmodell in dem Abschluss der Rechtsgeschäfte liegt, wodurch eine Herausgabe der Informationen zu erwarten ist, lassen sich solche Manipulationen jedoch aufdecken. Die nachträgliche Manipulation beim Dritten ist zwar ebenso möglich, jedoch wegen des mangelnden Eigeninteresses an der Manipulation und dem hohen Eigeninteresse an der Unverfälschtheit der Daten, unwahrscheinlich.[168]

Die aus anerkannten Beweiserleichterungen herausgearbeiteten Voraus- **868**
setzungen sprechen somit gegen einen Anscheinsbeweis. Folgend soll kurz auf Versuche eingegangen werden, einzelne anerkannte Beweiserleichterungen auf Benutzerkonten im Internet zu übertragen. Zwar entfaltet der gesetzlich kodifizierte Anscheinsbeweis bei der elektronischen Signatur in § 371a Abs. 1 S. 2 ZPO[169] systematisch betrachtet keine Sperrwirkung für andere Anscheinsbeweise.[170] Die Vorschrift spreche somit nicht gegen die Anerkennung eines Anscheinsbeweises.[171] Dagegen lässt sich jedoch einwenden, dass sich aus der Wertung des § 371a Abs. 1 ZPO entnehmen lässt, dass eine vergleichbar sichere Authentisierungsmethode gewählt werden muss. Im Umkehrschluss dazu ergibt sich, dass ein Anscheinsbeweis bei einer rein wissensbasierten Authentisierungsmethode nicht in Betracht kommt.[172] Die Beweiserleichterung beim Bildschirmtext[173] lässt sich nicht übertragen, weil der Missbrauch dort nur in der räumlichen Sphäre des Account-Inhabers stattfinden kann.[174] Die rein wissensbasierte Authentisierung ist durch die allerorts mögliche Authentisierung größeren Gefahren ausgesetzt.[175] Ebenso kann einer Übertragung des Anscheinsbeweises bei

168 Ähnlich *Borges*, Verträge, S. 485.
169 Oben Rn. 801.
170 *Biallaß*, ZUM 2007, 397, 397 f.; vgl. zur Sperrwirkung bezüglich der E-Mail oben Rn. 844.
171 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 45; *Ernst*, MDR 2003, 1091, 1093.
172 *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15.
173 Oben Rn. 808.
174 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15.
175 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.

der ec-Karte[176] nicht zugestimmt werden. Durch die Besitz-Komponente ist auch sie geringeren Angriffsmöglichkeiten ausgesetzt.[177]

869 Teilweise wird versucht mit der Möglichkeit des Erschütterns[178] den Anscheinsbeweis dennoch zu rechtfertigen. Der Anscheinsbeweis sei anzuerkennen, weil der Anscheinsbeweis leicht zu erschüttern sei.[179] Dem kann nicht zugestimmt werden. Das Erschüttern kann dem Account-Inhaber erhebliche Probleme bereiten.[180] Einzelne Gerichte behaupten, ein Phishing-Angriff beispielsweise sei mittels der Verlaufsprotokolle und des Caches eines Internetbrowsers „noch relativ lange" nachweisbar, weil anhand dessen die besuchten Internetseiten nachvollziehbar sind.[181] Zwar speichert beispielsweise der Browser Firefox das Verlaufsprotokoll in den Standardeinstellungen ohne zeitliche Beschränkungen. Der Browser Safari löscht standardmäßig alle Einträge aus diesem Verlauf, die älter als zwei Wochen sind. Selbst bei Nutzern, die mit den Standardeinstellungen surfen, ist der Verlauf somit eher nur eine kurze Zeit lang gespeichert. Darüber hinaus kann der Nutzer im Browser den Verlauf jederzeit manuell löschen. Ein Nutzer, dem Datenschutz wichtig ist, konfiguriert seinen Browser ohnehin so, dass der Verlauf gar nicht erst aufgezeichnet oder nach dem Schließen des Browsers gelöscht wird. Der Browser-Cache liefert ebenfalls keine hinreichende Grundlage für einen Beweis über längere Zeit hinweg. Er wird bei entsprechender Einstellungen des Nutzers nach dem Schließen des Browsers gelöscht, sodass er auch keine über längere Zeit zuverlässige Quelle von Beweisen ist. Ferner existieren Missbrauchsmöglichkeiten, die sich nicht in der Sphäre des Account-Inhabers abspielen, sodass der Account-Inhaber den Anscheinsbeweis nicht durch die konkrete Möglichkeit eines solchen Missbrauchs erschüttern kann. Deswegen sollte auch der Anscheinsbeweis nicht wegen Anreizfunktion für den Account-Inhaber, den handelnden Dritten zu offenbaren,[182] anerkannt werden. Dies setzt voraus, dass der Dritte stets bekannt ist, was jedoch nicht der Fall ist.

---

176 Dafür *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 44; *Härting*[4], Rn. 584.

177 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002, 127, 128.

178 Oben Rn. 790.

179 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 45; *Winter*, CR 2004, 219, 221.

180 *Ernst*, MDR 2003, 1091, 1093.

181 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261.

182 So *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 185.

Wird entgegen der hier vertretenen Meinung der Anscheinsbeweis anerkannt, muss er durch eine konkrete und nicht nur abstrakte Möglichkeit eines abweichenden Geschehensablaufs erschüttert werden.[183] Die pauschale Behauptung der Unsicherheit reiche dafür nicht aus.[184] Eine zeitnahe Sperrung des Legitimationszeichens erfülle diese Anforderungen hingegen.[185] Eine Betrachtung der Gesamtumstände kann ebenfalls den Anscheinsbeweis erschüttern, beispielsweise beim Kauf eines Luxusgutes, was sich der Account-Inhaber nicht leisten kann.[186] Ein Befall des Rechners mit einem Trojaner[187] reicht ebenfalls aus, um einen möglichen Anscheinsbeweis zu erschüttern. Dieser ist stets als konkrete Möglichkeit in Betracht zu ziehen.[188] 870

Ein Anscheinsbeweis dafür, dass eine Erklärung über einen Account von dessen Inhaber abgegeben wurde, besteht somit nicht. Teilweise wird für einen Sonderfall ein Anscheinsbeweis angenommen. Wenn der Account-Inhaber einen Missbrauch durch eine Person behauptet, die nicht in der Lage ist, die Zugangsdaten professionell auszuspähen, spreche ein Anscheinsbeweis für die Weitergabe.[189] Gegen diesen Anscheinsbeweis lässt sich einwenden, dass er nicht notwendig ist, um eine Beweisnot zu überwinden. Der Richter kann über die freie Beweiswürdigung (§ 286 Abs. 1 S. 1 ZPO) bei solchen konkreten Vorträgen Schutzbehauptungen erkennen.[190] Ein Bedürfnis für den Anscheinsbeweis besteht daher nicht. 871

Eine tatsächliche Vermutung[191] kommt wegen der fehlenden Voraussetzungen für einen Anscheinsbeweis erst recht nicht in Betracht. Der Missbrauch liegt häufig, aber nicht immer in der Sphäre des Account-Inhabers, sodass dieser ihn nicht unbedingt beweisen kann.[192] Eine Beweislastumkehr ohne tatsächliche Vermutung[193] kommt daher auch nicht in Betracht. 872

183 *Mankowski*, CR 2011, 458.
184 *Winter*, MMR 2002, 836, 17.
185 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 45.
186 *Ernst*, MDR 2003, 1091, 1093.
187 Oben Rn. 193.
188 Unten Rn. 903.
189 *Sonnentag*, WM 2012, 1614, 1618; *Oechsler*, MMR 2011, 631, 632; *ders.*, AcP 208 (2008), 565, 580.
190 Oben Rn. 795.
191 Oben Rn. 781.
192 *Kuhn*, S. 255.
193 Oben Rn. 776.

b) Sekundäre Darlegungslast

873 Nach der Ablehnung der Beweiserleichterung über den Anscheinsbeweis stellt sich die Frage, ob den Account-Inhaber eine sekundäre Darlegungslast[194] beim Missbrauch eines seiner Benutzerkonten auf einer Internetseite trifft. Teilweise wird diese sekundäre Darlegungslast angenommen, weil es sich um Vorgänge in der Sphäre des Account-Inhabers handele.[195] Durch diese Beweiserleichterung werde die als „Widerrufsrecht kraft Beweislastverteilung“[196] bezeichnete Situation verhindert.[197] Ein Missbrauch, etwa mittels eines Trojaners,[198] sei stets mit konkreten Anhaltspunkten im Einzelfall zu belegen.[199]

874 Gegen diese Beweiserleichterung in Form der sekundären Darlegungslast wird eingewandt, dass die Voraussetzungen einer sekundären Darlegungslast nicht vorlägen.[200] Zunächst muss die beweisbelastete Partei die Informationen haben oder sie müssten leicht zu beschaffen sein.[201] Dies sei nicht der Fall, wenn beispielsweise nach einem Trojaner-Angriff, bei dem die Zugangsdaten ausgespäht wurden, dieser sich nicht mehr nachweisen lässt, weil der Computer neu formatiert wurde.[202] Dabei wird jedoch die Natur der sekundären Darlegungslast verkannt. In deren Rahmen muss der Belastete nur die Tatsachen substantiiert darlegen, nicht beweisen.[203] Der Account-Inhaber muss daher nur aus seiner eigenen Kenntnis darlegen, dass er Opfer eines Angriffs wurde, bei dem sein Computer infiziert wurde und er ihn deswegen formatiert hat. Der Geschäftsgegner muss dann anhand dieser substantiierten Darlegung beweisen, dass dies nicht der Fall war. Dieser Einwand spricht somit nicht gegen die sekundäre Darlegungslast.

---

194 Oben Rn. 792.

195 *Ellenberger*, in: *Palandt*[73], § 172 BGB Rn. 18; *Kremer*, in: NK-BGB[2], Anh zu § 156 Rn. 29; *Noack*/*Kremer*, AnwBl 2004, 602, 604; *Schramm*, in: MüKo-BGB[6], § 164 Rn. 45b; wohl auch *Teuber*/*Melber*, MDR 2004, 185, 186; *Wenn*, CR 2006, 137, 138; **a.A.** *Biallaß*, ZUM 2007, 397, 398.

196 *Mankowski*, CR 2003, 44; *ders.*, MMR 2004, 181; dazu oben Rn. 773.

197 *Kremer*, in: NK-BGB[2], Anh zu § 156 Rn. 29.

198 Zu Trojanern oben Rn. 193.

199 *Teuber*/*Melber*, MDR 2004, 185, 186.

200 *Biallaß*, ZUM 2007, 397, 398.

201 Oben Rn. 793.

202 *Biallaß*, ZUM 2007, 397, 398.

203 Oben Rn. 794 sowie *Leipold*, in: *Stein*/*Jonas*[22], § 138 ZPO Rn. 38.

Gegen die sekundäre Darlegungslast lässt sich jedoch einwenden, dass dem Account-Inhaber die Substantiierung teilweise nicht möglich sein wird. Ein intelligent programmierter Trojaner wird sich nach einer gezielten Manipulation selbst löschen,[204] um die Spuren zu verwischen. Teilweise werden auch bei der Aktualisierung des Virenschutzes Schadprogramme vernichtet, ohne dass dessen Funktionsweise protokolliert wurde.[205] Es sind daher Angriffsszenarien möglich, bei denen der Account-Inhaber keine Informationen über den Angriff hat und diese auch nicht leicht beschaffen kann. Somit liegen die Voraussetzungen der sekundären Darlegungslast bezüglich Informationen aus der Sphäre des Account-Inhabers nicht vor. Ferner muss berücksichtigt werden, dass es zahlreiche Möglichkeiten des Missbrauchs gibt, die sich außerhalb der Sphäre des Account-Inhabers abspielen. Das Ausprobieren der Zugangsdaten mittels Brute-Force-Attacke[206] oder Schwachstellen beim Authentisierungsnehmer[207] spielen sich außerhalb der Sphäre des Account-Inhabers ab. Die Grundvoraussetzungen, dass der Account-Inhaber somit wegen seiner Sachnähe zu seiner eigenen Sphäre die Darlegung zugemutet wird, liegt somit nicht vor. **875**

Es kann zwar vom Account-Inhaber verlangt werden, dass er substantiierte Behauptungen zu den Tatsachen aus seiner Sphäre macht. Reichen diese jedoch nicht aus, um einen Missbrauch plausibel erscheinen zu lassen, kann ihm daraus kein Nachteil entstehen. Unterlässt der Account-Inhaber solche Behauptungen ist nach der Lebenserfahrung davon auszugehen, dass ihm solche Darlegungen nicht möglich oder zumutbar sind.[208] Bei Benutzerkonten auf Internetseiten müssen somit Schutzbehauptungen durch die freie richterliche Beweiswürdigung (§ 286 Abs. 1 S. 1 ZPO)[209] verhindert werden. **876**

IV. Online-Banking

Beim Online-Banking kommt eine Rechtsscheinhaftung nur in Betracht, wenn der Ansicht gefolgt wird, dass diese nicht durch § 675u S. 1 BGB **877**

204 *Armgardt/Spalka*, K&R 2007, 26, 31 f.
205 *Borges*, Elektronischer Identitätsnachweis, S. 252.
206 Oben Rn. 181.
207 Oben Rn. 215.
208 Vgl. *Musielak*, Grundkurs[11], Rn. 403.
209 Oben Rn. 795.

ausgeschlossen ist.[210] Bei einem einfachen TAN-Verfahren[211] sowie beim iTAN-Verfahren[212], die eine rein wissensbasierte Authentisierungsmethode verwenden,[213] kommt wegen der Unsicherheit der Authentisierungsmethode eine Rechtsscheinhaftung nicht in Betracht.[214]

878 Das mTAN-Verfahren hingegen setzt auf eine Zwei-Faktor-Authentisierung[215] und bietet somit grundsätzlich eine ausreichende Grundlage für die Anerkennung eines Rechtsscheintatbestandes. Die Identität des Bank-Kunden wird vor Abschluss des Vertrags ausreichend sicher überprüft.[216] Der Bankkunde ist zur Geheimhaltung der Zugangsdaten ebenso verpflichtet (§ 675l S. 1 BGB) wie die Bank (§ 675m Abs. 1 S. 1 BGB). Die Bank muss eine Sperrmöglichkeit zur Verfügung stellen (§ 675m Abs. 1 S. 1 Nr. 3 BGB), der Kunde sie nutzen (§ 675l S. 2 BGB).[217] Das mTAN-Verfahren ist somit ausreichend sicher für die Anerkennung eines Rechtsscheintatbestandes.

879 Bezüglich der Beweiserleichterungen beim Online-Banking ist auf die Wiedergabe der ausführlichen Diskussion in der Literatur zu verweisen.[218]

V. Online-Bezahldienste

880 Bei einem anonymen Online-Bezahldienst[219] kommt ein Rechtsscheintatbestand mangels Identifikationsfunktion nicht in Betracht. Bei einem Bezahldienst, der mittels einer Überprüfung von Bankkonto oder Kreditkarte an der Identitätsüberprüfung während der Kontoeröffnung partizipiert, ist zwar die Zuverlässigkeit der Identifikationsfunktion[220] gewährleistet. Setzt ein Online-Bezahldienst wie PayPal jedoch auf eine rein wissensbasierte Au-

---

210 Dazu oben Rn. 512.
211 Dazu *van Look*, in: *Claussen*[4], § 4 Rn. 41; *Schwintowski*[3], § 9 Rn. 34 ff.
212 Dazu *Hansen*, S. 9.
213 Oben Rn. 545.
214 Oben Rn. 544 ff.
215 Oben Rn. 118.
216 Dazu oben Rn. 67.
217 Dazu *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 50.
218 Oben Rn. 819.
219 Zu Online-Bezahldiensten oben Rn. 71.
220 Zu der Notwendigkeit oben Rn. 595 ff.

thentisierung scheitert die Anerkennung des Rechtsscheintatbestandes daran.[221]

Bei nicht-anonymen Online-Bezahldiensten ergeben sich bei den Beweiserleichterungen beim Einsatz einer rein wissensbasierten Authentisierungsmethode keine Unterschiede zu Benutzerkonten auf Internetseiten. Wie bei den Benutzerkonten[222] kommt somit keine Beweiserleichterung in Betracht, weder in Form von Beweislastumkehr mit oder ohne tatsächlicher Vermutung, noch in Form von Anscheinsbeweis oder sekundärer Darlegungslast.[223] 881

VI. Elektronische Signatur

1. Rechtsscheinhaftung

Für die unterschiedlichen Formen der elektronischen Signatur soll im Folgenden überprüft werden, ob sie die Voraussetzungen für die Anerkennung eines Rechtsscheintatbestandes erfüllen. 882

a) Sicherheit der Authentisierungsmethode

Zunächst müsste die elektronische Signatur eine hinreichend sichere Authentisierungemethode verwenden.[224] Die einfache elektronische Signatur (§ 2 Nr. 1 SigG)[225] verwendet keine Authentisierungsmethode. Bei der fortgeschrittenen elektronischen Signatur (§ 2 Nr. 2 SigG) beschränkt sich die Authentisierung auf das Wissen des geheimen Schlüssels, sodass diese rein wissensbasierte Authentisierung keine hinreichende Grundlage für einen Rechtsscheintatbestand ist.[226] Die qualifizierte elektronische Signatur (§ 2 Nr. 2 SigG) hingegen setzt eine Zwei-Faktor-Authentisierung ein. Der geheime Schlüssel darf nur auf der sicheren Signaturerstellungseinheit (§ 2 883

221 Oben Rn. 544 ff. Auf die Unsicherheit der Authentisierung bei PayPal weisen auch hin *Jehle*, S. 353; *Meder/Grabe*, BKR 2005, 467, 474.
222 Oben Rn. 854.
223 Zu den Formen der Beweiserleichterung oben Rn. 774 ff.
224 Dazu oben Rn. 534 ff.
225 Zu den Formen der elektronischen Signatur oben Rn. 74.
226 Oben Rn. 544 ff.

Nr. 10 SigG) gespeichert werden (§ 5 Abs. 4 S. 3 SigG).[227] Dadurch wird eine Besitzkomponente für die Authentisierung verwendet. Auf den darauf gespeicherten geheimen Schlüssel darf nur nach der Abfrage einer PIN[228] zugegriffen werden (vgl. § 15 Abs. 1 S. 1 SigV). Für die qualifizierte elektronische Signatur ist die Verwendung einer sicheren Signaturerstellungseinheit (§ 2 Nr. 10 SigG) erforderlich,[229] was die Sicherheit der Authentisierungsmethode erhöht. Die verwendete Zwei-Faktor-Authentisierung bei der qualifizierten elektronischen Signatur bietet grundsätzlich hinreichende Sicherheit für die Anerkennung eines Rechtsscheintatbestandes.[230]

884 Die Sicherheit der Authentisierungsmethode muss jedoch nicht nur technisch angelegt sein, sondern auch durch den Account-Inhaber unterstützt werden.[231] Bei der qualifizierten elektronischen Signatur betrifft dies insbesondere die Geheimhaltung der PIN sowie die sichere Verwahrung der Chip-Karte. Die Geheimhaltung der PIN ist dem Signaturschlüssel-Inhaber nicht gesetzlich auferlegt. Durch die Pflicht der Zertifizierungsdiensteanbieter die Geheimhaltung des privaten Schlüssels sicherzustellen (§ 5 Abs. 4 S. 2 SigG), haben diese den Signaturschlüssel-Inhaber über die Geheimhaltung der PIN im Rahmen der Belehrung nach § 6 Abs. 1 SigG zu informieren (§ 6 S. 1 Nr. 2 SigG).[232] Darüber hinaus kann angenommen werden, dass die Zertifizierungsdiensteanbieter den Signaturschlüssel-Inhabern eine Geheimhaltungspflicht vertraglich auferlegen.[233] Seitens des Accounts-Inhabers kann somit die notwendige Sorgfalt mit dem Umgang der Zugangsdaten erwartet werden

885 Der Zertifizierungsdiensteanbieter muss ebenfalls dafür sorgen, dass der Authentisierungsvorgang sicher ist.[234] Gesetzlich werden ihm zahlreiche Vorgaben bezüglich der Sicherheit gemacht, beispielsweise § 5 Abs. 5 SigG. Er muss die Sicherheit jedoch nicht nur technisch gewährleisten, sondern auch eine Möglichkeit bieten, die Zugangsdaten zu sperren. Dies muss der Zertifizierungsdiensteanbieter bei qualifizierten elektronischen Signaturen nach § 8 Abs. 1 S. 1 SigG ermöglichen. Die qualifizierte elektronische Si-

227 Dazu *Sanner*, S. 22.
228 Zum Erfordernis der PIN *F. A. Koch*, Internet-Recht[2], S. 145; *Sanner*, S. 22.
229 Dazu im Einzelnen *Bergfelder*, S. 199.
230 Oben Rn. 117 ff.
231 Oben Rn. 586.
232 Dazu *Gramlich*, in: *Spindler/F. Schuster*[2], § 6 SigG Rn. 5; *B. E. Brisch/K. M. Brisch*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.3 Rn. 167.
233 Vgl. *Reese*, S. 26.
234 Oben Rn. 588.

gnatur verwendet also eine hinreichend sichere Authentisierungsmethode.

b) Zuverlässigkeit der Identifikationsfunktion

Ferner muss die Verwendung einer elektronischen Signatur den Account-Inhaber zuverlässig identifizieren.[235] Bei der einfachen und der fortgeschrittenen elektronischen Signatur wird die Identität des Account-Inhabers nicht überprüft, sodass ein Rechtsscheintatbestand an der Unzuverlässigkeit der Identifikationsfunktion scheitert. Bei der qualifizierten elektronischen Signatur hingegen wird die Zuverlässigkeit der Identifikationsfunktion durch die Überprüfung der Identität des Signaturschlüssel-Inhabers (§ 5 Abs. 1 S. 1 SigG) sichergestellt. Die Identifizierung muss mittels Personalausweis oder Reisepass oder eines anderen hoheitlichen Ausweispapiers erfolgen.[236] Die Überprüfung hoheitlicher Ausweisdokumente bietet eine hinreichende Sicherheit zur Identifizierung des Account-Inhabers.[237] 886

Diese strengen Anforderungen wurden durch das 1. SigÄndG[238] deutlich abgeschwächt. Nach § 5 Abs. 1 S. 2 SigG n.F. kann nunmehr die Identifizierung anhand vorhandener personenbezogener Daten erfolgen. Ferner ist durch die Neuregelung ein persönlicher Kontakt zwischen Zertifizierungsdiensteanbieter und Signaturschlüssel-Inhaber nicht mehr erforderlich. Nach § 5 Abs. 2 SigV 2001 musste die Signaturkarte persönlich übergeben werden und nach § 6 Abs. 3 S. 1 SigG 2001 war die schriftliche Belehrung über Rechts- und Sicherheitsfragen schriftlich zu bestätigen. Diese beiden Regelungen stellten einen persönlichen Kontakt sicher.[239] Die Zuverlässigkeit der Identifikationsfunktion ist durch die Änderungen des 1. SigÄndG empfindlich betroffen. Ein Ehemann kurz vor der Trennung oder der Pfleger einer älteren Dame kann nun – wenn er Zugang zum Online-Banking- und E-Mail-Account hat – mit ein paar Mausklicks eine qualifizierte elektronische Signatur über das Online-Banking beantragen, den privaten Schlüssel auf die Bank-Karte laden, den Brief mit der PIN abfangen und notwendige 887

235 Oben Rn. 595 ff.
236 *Gramlich*, in: *Spindler/F. Schuster*[2], § 5 SigG Rn. 5.
237 Siehe oben Rn. 612.
238 Erstes Gesetz zur Änderung des Signaturgesetzes vom 4. 1. 2005, BGBl I, S. 2. Siehe dazu Begr. 1. SigÄndG, BT-Drucks. 15/3417; *Roßnagel*, NJW 2005, 385.
239 *Roßnagel*, NJW 2005, 385, 386.

Erklärungen mit dem fremden E-Mail-Account bestätigen.[240] Es gibt daher nach der neuen Fassung des SigG Wege sich ein qualifiziertes Zertifikat auf einen fremden Namen auszustellen. Durch die Übersendung der Zugangsdaten mittels eines Medienbruchs besteht wenigstens ein geringes Maß an Überprüfung der Identität.[241] Diese Absenkung der Sicherheitsanforderungen durch den Gesetzgeber führen jedoch nicht dazu, dass der Rechtsschein nicht mehr besteht.[242] Eine Zurechnung des Rechtsscheins scheidet jedoch aus, wo die elektronische Signatur nicht vom Signaturschlüssel-Inhaber beantragt wurde.[243]

888 Die Zuverlässigkeit der Identifikationsfunktion kommt jedoch nur in Betracht, wenn ein Account einmalig ist. Bei der elektronischen Signatur bedeutet dies, dass der geheime Schlüssel nur eimal vergeben werden darf.[244] Gesetzlich ist dies nach § 2 Nr. 2 lit. b SigG vorgeschrieben, sodass die Identifizierung des Signaturschlüssel-Inhabers ermöglicht wird.[245] Der Gesetzgeber schätzt die Zuverlässigkeit der Identitätsfeststellung bei der elektronischen Signatur als sicher ein, dass andere Dienste auf diese vertrauen dürfen, wenn sie die Identität eines Nutzers überprüfen wollen. Nach § 3 Abs. 3 S. 1 Nr. 1 a.E. DeMailG darf die Identität bei Erstellung eines De-Mail-Kontos mittels qualifizierter elektronischer Signatur überprüft werden. Die qualifizierte elektronische Signatur besitzt somit eine zuverlässige Identifikationsfunktion. Ein Rechtsscheintatbestand, dass der Account-Inhaber der qualifizierten elektronischen Signatur gehandelt hat, besteht somit.[246]

c) Zwischenergebnis

889 Bei der qualifizierten Signatur besteht somit ein Rechtsscheintatbestand dahin gehend, dass der Schlüssel-Inhaber die Erklärung verfasst hat.[247] Bei

240 Die Beispiele stammen von *Roßnagel*, NJW 2005, 385, 386.
241 Zur Überprüfung mittels Medienbruch oben Rn. 617.
242 *Spiegelhalder*, S. 137.
243 Zum Erstellen von Accounts durch Dritte oben Rn. 718.
244 *Borges*, Verträge, S. 51.
245 *Bösing*, S. 24.
246 Im Ergebnis auch *Rieder*, S. 261 ff.; *Reese*, S. 51 ff.; *Spiegelhalder*, S. 126 ff.; *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 10; *Sonnentag*, WM 2012, 1614, 1616; *Ultsch*, DZWir 1997, 466, 473; *M. Wolf/Neuner*[10], § 50 Rn. 108.
247 So auch *Ultsch*, in: Vernetzte Welt – gloables Recht, 127, 136 f.; *ders.*, DZWir 1997, 466, 473; *Rieder*, S. 281; *Spiegelhalder*, S. 162; *Reese*, S. 123; *Dörner*, AcP 202

der Zurechnung ergeben sich keine Unterschiede zu anderen Accounts.[248] Der Account-Inhaber haftet jedenfalls bei Weitergabe auf das positive Interesse des Geschäftsgegners.

2. *Beweiserleichterungen*

Bei der qualifizierten elektronischen Signatur (§ 2 Nr. 3 SigG)[249] existiert mit § 371a Abs. 1 S. 2 ZPO ein gesetzlich normierter Anscheinsbeweis,[250] sodass die Frage der Beweiserleichterungen gesetzlich vorgegeben ist. Bei den schwächeren Formen der elektronischen Signatur stellt sich jedoch die Frage, inwiefern Beweiserleichterungen in Betracht kommen. Eine einfache elektronische Signatur (§ 2 Nr. 1 SigG) verwendet keine Authentisierungsmethode. Sie kann einfach kopiert und nachgeahmt werden. Vom Sicherheitsniveau ist sie damit deutlich unterhalb der E-Mail angesiedelt, bei der keine Beweiserleichterungen in Betracht kommen.[251] Somit kommt bei der einfachen elektronischen Signatur erst recht keine Beweiserleichterung in Betracht. **890**

Bei der fortgeschrittenen elektronischen Signatur (§ 2 Nr. 2 SigG) ist technisch ein breites Spektrum an Sicherheit möglich. Je nach konkreter Ausgestaltung kann eine Beweiserleichterung in Betracht kommen.[252] Eine fortgeschrittene elektronische Signatur, die mit der Software Pretty Good Privacy (PGP) erstellt wurde, basiert auf einer rein wissensbasierten Authentisierung. Insofern lassen sich die Ergebnisse zu Benutzerkonten im Internet[253] übertragen, sodass eine Beweiserleichterung nicht in Betracht kommt. Nähert sich eine fortgeschrittene elektronische Signatur dem Sicherheitsstandard der qualifizierten elektronischen Signatur, können jedoch Beweiserleichterungen im Einzelfall begründet sein. **891**

(2002), 363, 388; *Redeker*, IT-Recht[5], Rn. 878; *M. Köhler/Arndt/Fetzer*[7], Rn. 227; einschränkend *Schnell*, S. 267.

248 Zur Zurechnung oben Rn. 671 ff.

249 Zu den Formen der elektronischen Signatur oben Rn. 74.

250 Oben Rn. 801.

251 Oben Rn. 835.

252 *Ernst*, MDR 2003, 1091, 1092.

253 Oben Rn. 854.

VII. Elektronischer Identitätsnachweis

1. Rechtsscheinhaftung

892 Beim elektronischen Identitätsnachweis[254] soll ebenfalls untersucht werden, ob dessen Einsatz hinreichende Grundlage für eine Rechtsscheinhaftung ist. Dazu müsste neben dem Einsatz einer ausreichend sicheren Authentisierungsmethode, die Zuordnung des Accounts zur numerischen Identität des Inhabers zuverlässig erfolgen.

a) Sicherheit der Authentisierungsmethode

893 Zunächst müsste der neue Personalausweis (nPA) eine hinreichend sichere Authentisierungemethode verwenden.[255] Der elektronische Identitätsnachweis im neuen Personalausweis setzt auf eine Authentisierung mittels Besitz und Wissen.[256] Der Zugriff auf den Token in der Chip-Karte des neuen Personalausweises ist durch eine sechsstellige PIN geschützt.[257] Bei der Eingabe der PIN besteht je nach Einsatz des Kartenlesegeräts eine Schwachstelle. Werden Kartenleser der Klasse 1[258] verwendet, der lediglich die Karte lesen kann und bei dem die PIN über die Tastatur des Rechners eingegeben wird, kann die PIN auf einem infizierten Rechner durch einen Trojaner[259] ausgespäht werden.[260] Der Grund für den Einsatz von Klasse-1-Kartenleser ist der günstigere Preis im Vergleich zu Klasse-2- und Klasse-3-Kartenlesern, was eine weite Verbreitung hindern könnte.[261] Ist die PIN einem Dritten bekannt, würde die Authentisierung mittels Wissen und Besitz, praktisch auf eine reine Authentisierung des Besitzes zurückgefahren werden.[262] Um die

254 Dazu oben Rn. 88.
255 Dazu oben Rn. 534 ff.
256 *Borges*, NJW 2010, 3334, 3336; *ders.*, Elektronischer Identitätsnachweis, S. 30; *Engel*, DuD 2006, 207, 209; *W. Müller/Redlich/Jeschke*, DuD 2011, 465, 466; *Roßnagel/Hornung/Schnabel*, DuD 2008, 168, 169.
257 *Borges*, NJW 2010, 3334, 3336; *Roßnagel/Hornung/Schnabel*, DuD 2008, 168; *Bender/Kügler/Margraf/Naumann*, DuD 2008, 173; *Eckert*[8], S. 580.
258 Zur Einteilung der Kartenleser in Klassen *Eckert*[8], S. 592 f.; *Borges/Schwenk/Stuckenberg/Wegener*, S. 157 f.
259 Dazu oben Rn. 193.
260 *Borges*, NJW 2010, 3334, 3337; *Eckert*[8], S. 593, 599.
261 *Borges*, NJW 2010, 3334, 3338.
262 *Borges/Schwenk/Stuckenberg/Wegener*, S. 161.

Identität des Ausweisinhabers zu missbrauchen, müsste der Dritte in diesem Fall noch in den Besitz des Ausweises gelangen[263] und der Ausweis dürfte noch nicht gesperrt sein.

Ein Man-in-the-Middle-Angriff,[264] der den Datenverkehr durch eine Manipulation von DNS-Einträgen auf den Angreifer umleitet, kann durch das Zurückweisen eines vertrauensunwürdigen SSL-Zertifikats durch die Ausweis-App verhindert werden.[265] Man-in-the-Middle-Angriffe, die hingegen darauf setzen, mittels Echtzeitveränderungen eine Diskrepanz zwischen den übermittelten Daten und der Anzeige beim Account-Inhaber herzustellen, indem die übermittelnden Daten durch einen Trojaner[266] verändert werden, sind jedoch möglich.[267] Diese Zwei-Faktor-Methode bietet trotz der Angriffsmöglichkeiten grundsätzlich eine hinreichende Sicherheit für die Anerkennung als Rechtsscheintatbestand.[268] 894

Auf Seiten des Account-Inhabers, der ausgebenden Stelle sowie des Authentisierungsnehmers werden zahlreiche Vorkehrungen getroffen, den Authentisierungsvorgang abzusichern. Der Authentisierungsvorgang kann nur durchgeführt werden, wenn der Authentisierungsnehmer ein Berechtigungszertifikat besitzt (§ 18 Abs. 4 S. 1 PAuswG). Dieses Prinzip der doppelten Authentisierung,[269] dass sich nicht nur der Account-Inhaber, sondern auch der Authentisierungsnehmer authentisieren muss, schützt vor Phishing.[270] 895

Bereits bei der Ausgabe des Personalausweises und der Übermittelung der geheimen PIN werden auf Seiten der ausgebenden Behörde Sicherheitsvorkehrungen getroffen. Die PIN wird gemeinsam mit der Aufforderung den Personalausweis abzuholen vom Ausweishersteller an den Namensträger per Post verschickt (§ 13 PAuswG).[271] Der Namensträger muss sich den Ausweis anschließend persönlich bei der Behörde abholen.[272] In der Authentisierungsinfrastruktur ist eine Sperrmöglichkeit vorgesehen (vgl. § 24 Abs. 2 S. 1 PAuswV). 896

263 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 191.
264 Dazu oben Rn. 168.
265 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 174.
266 Dazu oben Rn. 193.
267 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 192.
268 Oben Rn. 117 ff.
269 *Borges*, Elektronischer Identitätsnachweis, S. 30.
270 *Roßnagel*/*Hornung*/*Schnabel*, DuD 2008, 168, 170.
271 Dazu ebd., 169.
272 *Borges*, NJW 2010, 3334, 3337; *ders.*, Elektronischer Identitätsnachweis, S. 38.

897 Die Mitwirkung des Ausweisinhabers, die zur Sicherheit des Authentisierungsvorgangs notwendig ist,[273] ist ebenfalls gesetzlich verlangt. Sobald der Ausweisinhaber die Authentisierungsmittel erhalten hat, treffen ihn Pflichten zur Sicherung der Zuverlässigkeit des Authentisierungsvorgangs. Er hat zum einen die PIN geheim zu halten und darf sie nicht notieren (§ 27 Abs. 2 PAuswG). Zum anderen muss er durch technische und organisatorische Maßnahmen den Rechner, den er zum Authentisierungsvorgang nutzt, ausreichend sichern (§ 27 Abs. 3 PAuswG). Die Besitzkomponente des Authentisierungsvorgangs, der Personalausweis selbst, kann abhandenkommen oder gestohlen werden. In diesen Fall kann er gesperrt werden,[274] sodass ein Missbrauch nur zwischen Abhandenkommen und Sperranzeige möglich ist. Der Ausweisinhaber ist sogar zur Sperrung verpflichtet (§ 27 Abs. 1 Nr. 3 PAuswG).[275] Der Authentisierungsvorgang ist somit für die Anerkennung als Rechtsscheingrundlage ausreichend sicher.

b) Zuverlässigkeit der Identifikationsfunktion

898 Ferner muss der Ausweisinhaber bei Ausstellung des Ausweises zuverlässig identifiziert werden.[276] Rechtlich stellt sich jedoch die Frage, wie zuverlässig und nachvollziehbar diese Identifikationsfunktion erfüllt wird. Zuverlässig ist die Identifikationsfunktion des Personalausweises, wenn bei der Ausstellung des Ausweises die Angaben des Antragstellers überprüft werden. Die Angaben zur Person entnimmt die ausstellende Behörde entweder dem Melderegister oder der Antragsteller hat sie mit Nachweisen zu belegen (§ 9 Abs. 3 S. 3 PAuswG). Die Zuverlässigkeit der Zuordnung wird ferner dadurch sichergestellt, dass der Ausweis regelmäßig persönlich beantragt werden muss (§ 9 Abs. 1 S. 6 PAuswG) und bei Zweifeln seine Identität überprüft wird (§ 9 Abs. 4 PAuswG). Es gibt jedoch ein „Ungewissheitsdelta“, das die Identitätswahrscheinlichkeit und deren Zweifelsfreiheit ausdrückt.[277] Trotz verbleibender Unsicherheiten ist der Personalausweis das „klassische und universelle Authentisierungsmedium.“[278] Einige gesetz-

273 Oben Rn. 586.
274 *Polenz*, MMR 2010, 671, 675; *Eckert*[8], S. 580.
275 Dazu *Borges*, Elektronischer Identitätsnachweis, S. 39.
276 Oben Rn. 595 ff.
277 *Bohrer*, MittBayNot 2005, 460, 461.
278 *Borges*, Elektronischer Identitätsnachweis, S. 29.

liche Regelungen, die erlauben, dass mittels des neuen Personalausweises eine Identitätsüberprüfung online ebenso möglich ist wie bei Inaugenscheinnahme des Ausweisdokuments, zeigen, dass der Gesetzgeber die Identifikationsfunktion als ausreichend zuverlässig wertet. Bei Erstellen eines De-Mail-Kontos (§ 3 Abs. 3 S. 1 Nr. 1 a.E. DeMailG), eines Bank-Kontos (§ 6 Abs. 2 Nr. 2 lit. c GwG) sowie eines qualifizierten Zertifikats für eine elektronische Signatur (§ 3 Abs. 1 S. 2 SigG) darf der elektronische Identitätsnachweis im neuen Personalausweis zur Überprüfung der Identität des Account-Inhabers verwendet werden. Die Identität des Ausweisinhabers bei Ausstellung des Ausweises wird somit ausreichend sicher überprüft. Die Verwendung des neuen Personalausweises setzt somit einen Rechtsschein bezüglich des Handelns des Ausweisinhabers.[279] Bezüglich der Zurechnung[280] ergeben sich keine Besonderheiten bei der elektronischen Signatur.

2. Beweiserleichterungen

Bei den Beweiserleichterungen für die Verwendung des elektronischen Iden- **899**
titätsnachweises[281] soll zunächst auf die diskutierte Möglichkeit eines Anscheinsbeweises[282] eingegangen werden. Beim Anscheinsbeweis ist zwischen der Authentisierung und der Urheberschaft einer Erklärung zu unterscheiden.[283] Für einen Anscheinsbeweis, dass der Ausweisinhaber die Authentisierung vorgenommen hat, fehlt es zunächst mangels praktischer Erfahrungen an einem Erfahrungssatz.[284] Nach der Ausschlussmethode kann jedoch ein Anscheinsbeweis ohne ersten Anschein[285] durch die Unwahrscheinlichkeit alternativer Möglichkeiten begründet werden. Die Voraussetzung, dass die Identität des Ausweisinhabers zuverlässig überprüft wird,[286]

---

279 Im Ergebnis auch *Borges*, NJW 2010, 3334, 3338; *ders.*, Elektronischer Identitätsnachweis, S. 134 f.
280 Oben Rn. 671 ff.
281 Oben Rn. 88.
282 Oben Rn. 785.
283 *Borges*, Elektronischer Identitätsnachweis, S. 242; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 314.
284 *Borges*, Elektronischer Identitätsnachweis, S. 243; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 313.
285 Oben Rn. 788.
286 Oben Rn. 826.

liegt beim elektronischen Identitätsnachweis vor.[287] Wenn die Ergebnisse der Autorisierung bei einem unabhängigen Dritten gespeichert werden, ist auch die nachträgliche Manipulation der Daten unwahrscheinlich, sodass die dritte Voraussetzungen auch vorliegt. Die eingesetzte Zwei-Faktor-Authentisierung[288] im elektronischen Identitätsnachweis bietet eine hohe Sicherheit.[289] Diese wird in vergleichbaren Konstellationen als ausreichend zur Anerkennung und erste Voraussetzung eines Anscheinsbeweises anerkannt.[290] Ein Angriff durch einen Trojaner[291] als alternativer Geschehensablauf ist bei unsicheren Kartenlesegeräten[292] jedoch möglich. Ein Anscheinsbeweis für die Authentisierung durch den Erklärenden komme daher nur in Betracht, wenn ein Trojaner-Angriff ausgeschlossen werden kann.[293] Das bedeutet, dass ein Anscheinsbeweis für die Authentisierung des Ausweisinhabers in Betracht kommt, wenn dieser ein sicheres Lesegerät der Klasse 2 oder aufwärts verwendet hat.

900 Teilweise wird behauptet, dass der Anscheinsbeweis der ec-Karte[294] zu übertragen sei.[295] Diese Begründung überzeugt nicht. Zwar lässt sich aus dem Anscheinsbeweis bei der ec-Karte entnehmen, dass die Zwei-Faktor-Authentisierung eine hinreichende Grundlage für einen Anscheinsbeweis darstellt. Der Anscheinsbeweis bei der ec-Karte ist jedoch aus zwei Gründen ungeeignet für eine Übertragung auf den elektronischen Identitätsnachweis. Zum einen ist das Beweisobjekt bei der ec-Karte ein anderes. Der Anscheinsbeweis bezieht sich bei der ec-Karte zunächst auf das Handeln des Bankkunden. Steht wie häufig der Fall fest, dass dieser nicht gehandelt hat, bezieht sich der Anscheinsbeweis auf das Vorliegen einer haftungsbegründenden Pflichtverletzung.[296] In dieser zweiten Ausformung der Pflichtverletzung hat der Anscheinsbeweis seine hauptsächliche praktische Bedeutung. Beim Einsatz des elektronischen Identitätsnachweises geht es jedoch

287 Oben Rn. 898.
288 Oben Rn. 117.
289 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 314.
290 Oben Rn. 826.
291 Oben Rn. 193.
292 Oben Rn. 893.
293 *Borges*, Elektronischer Identitätsnachweis, S. 243 f.; *ders.*, NJW 2010, 3334, 3338; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 314.
294 Oben Rn. 812.
295 *Roßnagel*/*Hornung*, DÖV 2009, 301, 305; *Borges*, Elektronischer Identitätsnachweis, S. 244; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 314.
296 Oben Rn. 813.

primär darum, einen Anscheinsbeweis dafür zu begründen, dass der Ausweisinhaber selbst gehandelt hat. Wegen dieser unterschiedlichen Beweisobjekte eignet sich der Anscheinsbeweis der ec-Karte schlecht zur Übertragung auf den elektronischen Identitätsnachweis. Zum anderen existiert ein sachnäherer Anscheinsbeweis, der sich zur Übertragung anbietet. Wenn jedoch ein Anscheinsbeweis im Wege eines Einzelvergleichs übertragen werden soll, ist die elektronische Signatur aus zwei Gründen zu wählen. Zum einen handelt es sich bei der Regelung des § 371a Abs. 1 S. 2 ZPO um eine gesetzlich ausgeformte Beweiserleichterung, der eine größere demokratische Legitimation als einem sich stetig fortentwickelnden Richterrecht zuzusprechen ist. Zum anderen ist die elektronische Signatur dem elektronischen Identitätsnachweis deutlich sachnäher, weil es sich bei beiden um Zugangsdaten im Internet handelt, die über ein Karten-Lesegerät in Verbindung mit einem eigenen Rechner zum Einsatz kommen.

Ob von dem Anschein, dass der Account-Inhaber die Authentisierung **901**
vorgenommen hat, auch auf einen Anschein seiner Urheberschaft einer später abgegebenen Erklärung geschlossen werden kann, ist beim derzeitigen Kenntnisstand schwer zu beurteilen.[297] Mangels eines vorhandenen Erfahrungssatzes ist somit nach der Ausschlussmethode ein Anscheinsbeweis ohne ersten Anschein[298] zu erwägen. Ein Man-in-the-Browser-Angriff[299] auf eine Plattform mit der Folge, dass eine Erklärung nach Authentisierung gefälscht werden kann, erscheint möglich.[300] Ein Anscheinsbeweis für die Urheberschaft einer anschließenden Erklärung kommt jedoch nicht erst in Betracht, wenn Angriffe nicht plausibel erscheinen.[301] Er ist grundsätzlich anzuerkennen. Wenn ein Angriff jedoch plausibel erscheint, ist das Erschüttern des Anscheinsbeweises möglich.

Erschüttern[302] kann der Ausweisinhaber den Anscheinsbeweis beispiels- **902**
weise durch den Nachweis der Weitergabe des Ausweises oder dessen Abhandenkommen.[303] Dann spricht jedoch wie bei der ec-Karte ein weiterer Anscheinsbeweis dafür, dass der Ausweisinhaber Karte und PIN pflichtwid-

297 *Borges*, Elektronischer Identitätsnachweis, S. 248.
298 Oben Rn. 788.
299 Oben Rn. 172.
300 *Borges*, Elektronischer Identitätsnachweis, S. 249.
301 So ebd., S. 250.
302 Oben Rn. 790.
303 *Borges*, Elektronischer Identitätsnachweis, S. 244, 251.

rig zusammen verwahrt hat.[304] Ein Angriff mittels eines Trojaners[305] kann den Anscheinsbeweis erschüttern. Fraglich ist, wie hohe Anforderungen an das Erschüttern zu stellen sind. Eine strenge Anforderung wäre, dass der Account-Inhaber darlegen muss, dass sein Rechner mittels eines Trojaners befallen war und dass dieser konkrete Trojaner zu Missbräuchen der Art des Einzelfalls fähig ist.[306] Weniger streng wäre die Anforderung, dass der Account-Inhaber nur darlegen muss, dass sein Rechner infiziert war.[307]

903 Sehr leicht wäre der Anscheinsbeweis zu erschüttern, wenn der Befall des Rechners des Account-Inhabers mit einem Trojaner stets als konkrete Möglichkeit in Betracht kommt.[308] Antiviren-Programme bieten keinen Schutz gegen neuartige Bedrohungen, weil sie hauptsächlich über die Wiederkennung bekannter Schadsoftware funktionieren.[309] Ferner haben sie erhebliche Probleme, Trojaner zu erkennen. Antiviren-Programme mindern zwar das Infektionsrisiko, schließen es aber nicht aus.[310] Auch eine Firewall verhindert die Infektion des Rechners mit Malware nicht.[311] Erschwerend kommt hinzu, dass Antiviren-Programme teilweise Schadprogramme vernichten, ohne deren genaue Funktionsweise zu protokollieren.[312] Es ist daher dem Ausweisinhaber eventuell trotz erfolgtem Missbrauch über einen Trojaner nicht möglich, substantiiert zur Infektion vorzutragen. Dem Ausweisinhaber kann somit nicht zugemutet werden, genaue Angaben zur Infektion seines Rechners zu machen. Der Ausweisinhaber kann mithin den Anscheinsbeweis stets dadurch erschüttern, dass er die Infektion seines Rechners mit Malware vorträgt.

904 Gelingt dem Account-Inhaber die Erschütterung des Anscheinsbeweises, kommt je nach konkretem Vortrag zum Erschüttern eine Rechtsscheinhaf-

304 *Borges*, Elektronischer Identitätsnachweis, S. 246; *Borges/Schwenk/Stuckenberg/Wegener*, S. 315.
305 Oben Rn. 193.
306 Dagegen *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08 – MMR 2008, 626, 627. Dazu auch *Borges*, Elektronischer Identitätsnachweis, S. 251 m.w.N.
307 In diese Richtung *Teuber/Melber*, MDR 2004, 185, 186.
308 So *Borges*, Elektronischer Identitätsnachweis, S. 251; in die gleiche Richtung *Armgardt/Spalka*, K&R 2007, 26, 31 f.
309 Oben Rn. 203.
310 Oben Rn. 206.
311 Oben Rn. 209.
312 *Borges*, Elektronischer Identitätsnachweis, S. 251.

tung des Ausweisinhabers[313] in Betracht. Wegen der Anerkennung des Anscheinsbeweises bedarf es keiner weiteren Beweiserleichterungen.

VIII. De-Mail

1. Rechtsscheinhaftung

Bei der De-Mail[314] stellt sich bezüglich der Rechtsscheinhaftung ebenso die Frage, ob die verwendete Authentisierungsmethode ausreichend sicher ist.[315] Im Regelfall erfolgt eine sichere Anmeldung, ausnahmsweise kann auch eine einfache Anmeldung erfolgen (§ 4 Abs. 1 S. 1 DeMailG).[316] Als sichere Authentisierungsmethode wird dabei die Zwei-Faktor-Authentisierung vorgesehen (§ 4 Abs. 1 S. 2 DeMailG).[317] Die einfache, unsicherere Authentisierung ist eine, die lediglich auf einer Wissenskomponente basiert (§ 4 Abs. 1 S. 3 DeMailG).[318] Grund für die Wahl der Zwei-Faktor-Authentisierung ist die Rechtsprechung, die bei einer rein wissensbasierten Authentisierung einen Anscheinsbeweis verneint.[319] Diese Zwei-Faktor-Authentisierung kann nur mittels eines aktiven und in Echtzeit arbeitenden Man-in-the-Middle-Angriffs[320] überwunden werden.[321] Nach § 10 Abs. 1 S. 1 Nr. 1 DeMailG besteht für den Nutzer die Möglichkeit ein Konto zu sperren, sodass der Nutzer die Möglichkeit hat, zur Sicherheit des Authentisierungsvorgangs beizutragen, wenn die Zugangsdaten abhandengekommen sind. Mit der Zwei-Faktor-Authentisierung setzt die De-Mail eine ausreichend sichere Authentisierungsmethode ein[322] und erfüllt somit die erste Voraussetzung zur Anerkennung eines Rechtsscheintatbestandes. **905**

313 Oben Rn. 892 ff.
314 Dazu oben Rn. 92.
315 Zu den Anforderungen daran oben Rn. 534 ff.
316 Dazu *Roßnagel*, NJW 2011, 1473, 1475; *Spindler*, CR 2011, 309, 312.
317 Dazu *Roßnagel*, NJW 2011, 1473, 1475; *ders.*, CR 2011, 23, 26; *Spindler*, CR 2011, 309, 312; *Rose*, K&R 2011, 439, 442.
318 Dazu *Roßnagel*, CR 2011, 23, 26.
319 Begr. DeMailG, BT-Drucks. 17/3630, S. 27 f.; Begr. BPG, BT-Drucks. 16/12598, S. 21.
320 Dazu oben Rn. 168.
321 *Dennis Werner/Wegener*, CR 2009, 310, 311.
322 Oben Rn. 117 ff.

906 Ferner muss der Account-Inhaber bei Erstellung des Accounts zuverlässig identifiziert werden.[323] Kritisch wurde im Gesetzgebungsvorgang insbesondere vom Bundesrat betrachtet, dass den Nutzer keine Pflicht trifft, dem Diensteanbieter Änderungen seiner persönlichen Daten wie der Anschrift mitzuteilen.[324] Abgelehnt wurde diese Forderung des Bundesrates von der Bundesregierung mit der Begründung, dass das DeMailG nur Pflichten für Diensteanbieter statuiere und eine Pflicht für Nutzer somit nicht in das Konzept des Gesetzes passe.[325] Die Diensteanbieter können jedoch durch eine entsprechende Klausel in ihren AGB eine Pflicht zur Mitteilung von Änderungen dem Nutzer auferlegen.[326] Für die zuverlässige Identifizierung des Account-Inhabers bei Registrierung des Accounts spielt eine nachträgliche Adressänderung jedoch keine Rolle. Zwar hat der Geschäftsgegner dadurch womöglich ohne weitere Recherchen keine ladungsfähige Adresse des Account-Inhabers. Dieses Problem unterliegt jedoch dem allgemeinen Geschäftsrisiko.

907 Die Zuverlässigkeit der Identifikation des Account-Inhabers stellt das DeMailG dadurch sicher, dass bei der Anmeldung dessen Identität zuverlässig überprüft werden muss (§ 3 Abs. 2 DeMailG).[327] Bei natürlichen Personen wird dafür z.B. ein amtlicher Ausweis kontrolliert (§ 3 Abs. 3 DeMailG). Die Überprüfung erfolgt über das PostIdent-Verfahren, den neuen Personalausweis[328] oder einen Besuch in einer Geschäftsstelle.[329] Diese Überprüfung ist zentral für die Nutzung von De-Mail,[330] eine Nutzung des Accounts darf der Anbieter vorher nicht zulassen (§ 3 Abs. 4 DeMailG). Die Identität des Account-Inhabers wird somit bei Registrierung des Accounts ausreichend sicher überprüft. Bei Verwendung von De-Mail besteht somit ein Rechtsschein dahingehend, dass der Account-Inhaber die Mail verschickt hat. Für die Zurechnung des Rechtsscheintatbestandes kann auf

323 Oben Rn. 595 ff.
324 BT-Drucks. 17/4145, S. 4.
325 Ebd., S. 10.
326 *Spindler*, CR 2011, 309, 312; *Rose*, K&R 2011, 439, 440.
327 Dazu *Roßnagel*, NJW 2011, 1473, 1474; *ders.*, CR 2011, 23, 26; *Spindler*, CR 2011, 309, 311 f.; *Rose*, K&R 2011, 439, 441.
328 *Dennis Werner/Wegener*, CR 2009, 310, 312; *J. Dietrich/Keller-Herder*, DuD 2010, 299, 300.
329 *Stach*, DuD 2008, 184, 185.
330 Begr. DeMailG, BT-Drucks. 17/3630, S. 27.

die allgemeinen Ausführungen verwiesen werden, weil diese sich nicht von den anderen Accounts unterscheidet.[331]

2. *Beweiserleichterungen*

Bei der De-Mail[332] soll zunächst auf die diskutierte Beweiserleichterung des Anscheinsbeweises eingegangen werden. Bei ihr liegen zwar mangels praktischer Verbreitung keine Erfahrungssätze vor, die einen Anscheinsbeweis begründen können. Dafür kann jedoch wiederum die Figur des Anscheinsbeweises ohne ersten Anschein durch Ausschluss alternativer Geschehensabläufe bemüht werden.[333] Wegen der Sicherheit der Zwei-Faktor-Authentisierung[334] sind Geschehensabläufe, bei denen nicht der Account-Inhaber oder ein Berechtigter gehandelt hat, unwahrscheinlich.[335] Die Grundsätze zum Anscheinsbeweis der ec-Karte[336] zu übertragen,[337] überzeugt jedoch ebenso wenig wie beim elektronischen Identitätsnachweis.[338] Bei einer Einzelübertragung ist vielmehr der sachnähere § 371a Abs. 1 S. 1 ZPO heranzuziehen. Am überzeugendsten lässt sich der Anscheinsbeweis jedoch durch die Analyse anerkannter Beweiserleichterungen in vergleichbaren Situationen begründen. Die Analyse anerkannter Beweiserleichterungen hat ergeben, dass eine Zwei-Faktor-Authentisierung eine ausreichende Grundlage zur Anerkennung des Anscheinsbeweises ist. Neben der sicheren Zwei-Faktor-Authentisierung findet bei der De-Mail eine zuverlässige Identitätsüberprüfung statt[339] und durch die Lagerung der Daten bei einem Dritten ist die nachträgliche Manipulation unwahrscheinlich. **908**

331 Dazu oben Rn. 671 ff.
332 Oben Rn. 92.
333 Oben Rn. 788.
334 Oben Rn. 117.
335 Oben Rn. 826. So auch *Roßnagel*, NJW 2011, 1473, 1477.
336 Oben Rn. 812.
337 So *Roßnagel*, NJW 2011, 1473, 1477.
338 Oben Rn. 900.
339 Oben Rn. 906.

909 Bei der Verwendung der De-Mail spricht daher ein Anscheinsbeweis dafür, dass die Mail vom Account-Inhaber abgesendet wurde.[340] Diese betrifft jedoch nur die Identität des Handelnden, nicht den Inhalt der Nachricht.[341] Erschüttern[342] kann der Account-Inhaber den Anscheinsbeweis dadurch, dass er beispielsweise die Weitergabe der Zugangsdaten oder das Abhandenkommen der Chip-Karte darlegt. Eine Infektion des Rechners des Account-Inhabers mit einem Trojaner[343] ist bei Privatpersonen stets als konkrete Möglichkeit anzusehen,[344] sodass dadurch der Anscheinsbeweis leicht erschüttert werden kann. Ist der Anscheinsbeweis erschüttert, kommt eine Haftung nach Rechtsscheingrundsätzen[345] in Betracht. Wegen der Anerkennung des Anscheinsbeweises kommt es auf weitere Beweiserleichterungen nicht an.

340 Begr. DeMailG, BT-Drucks. 17/3630, S. 19; Begr. BPG, BT-Drucks. 16/12598, S. 21; *Roßnagel*, NJW 2011, 1473, 1477; *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 733. Wohl auch *Fechner*[14], Kap. 12 Rn. 190; *Wien*[3], S. 99. Offen gelassen von *Redeker*, IT-Recht[5], Rn. 906.

341 *Spindler*, CR 2011, 309, 315; *Roßnagel*, NJW 2011, 1473, 1477.

342 Oben Rn. 790.

343 Oben Rn. 193.

344 Oben Rn. 903. Vgl. auch *Armgardt/Spalka*, K&R 2007, 26, 31 f.; *Borges*, Elektronischer Identitätsnachweis, S. 251.

345 Oben Rn. 905.

§ 12 Zusammenfassung der Ergebnisse

Für die Beurteilung der juristischen Frage der Haftung für den Missbrauch von Zugangsdaten spielen die technischen Grundlagen eine bedeutende Rolle. Es gibt zahlreiche Möglichkeiten, wie ein Angreifer die Zugangsdaten vom Account-Inhaber ausspähen kann[1] oder ohne dessen Zutun an die Zugangsdaten gelangen kann.[2] 910

Bei der Frage nach der materiellen Haftung bejaht eine unwidersprochene, herrschende Meinung im Ergebnis eine Haftung des Account-Inhabers, wenn dieser die Zugangsdaten weitergegeben hat.[3] Die beiden Ansätze, die über die Duldungsvollmacht[4] und über die analoge Anwendung des § 172 Abs. 1 BGB[5] zu diesem Ergebnis gelangen, überzeugen weder in ihrer dogmatischen Herleitung[6] noch im Ergebnis.[7] 911

Die Haftung des Account-Inhabers ohne Weitergabe der Zugangsdaten kann dogmatisch überzeugend nicht über die Anscheinsvollmacht, die *culpa in contrahendo*, das Schuldverhältnis mit Schutzwirkungen zu Gunsten Dritter, die analoge Anwendung von § 122 BGB sowie über das Deliktsrecht gelöst werden.[8] Ein dogmatisch überzeugender Lösungsweg besteht vielmehr für die Frage der Haftung ohne Weitergabe der Zugangsdaten als auch in den Konstellationen der Weitergabe und des Erstellens des Accounts durch einen Dritten, in der Anwendung der allgemeinen Rechtsscheinhaftung.[9] 912

Bei der Anwendung der allgemeinen Rechtsscheinhaftung liegt ein Rechtsscheintatbestand nur vor, wenn der Authentisierungsnehmer eine hinreichend sichere Authentisierungsmethode einsetzt[10] und die Identität des Account-Inhabers ausreichend überprüft wurde.[11] Eine sichere Authen- 913

1 Oben Rn. 124 ff.
2 Oben Rn. 215 ff.
3 Oben Rn. 293 ff.
4 Oben Rn. 297 ff.
5 Oben Rn. 303.
6 Oben Rn. 366.
7 Oben Rn. 717.
8 Oben Rn. 716.
9 Oben Rn. 489 ff.
10 Oben Rn. 534 ff.
11 Oben Rn. 595 ff.

tisierungsmethode stellt insbesondere eine Zwei-Faktor-Authentisierung mit den Komponenten Besitz und Wissen dar.[12] Eine rein wissensbasierte Authentisierungsmethode begründet hingegen keinen Rechtsscheintatbestand.[13] Der Widerspruch der jeweils herrschenden Ansichten zur Haftung des Account-Inhabers mit und ohne Weitergabe der Zugangsdaten[14] ist somit dahingehend aufzulösen, dass der bei Weitergabe angenommene Rechtsscheintatbestand für Accounts mit rein wissensbasierter Authentisierungsmethoden nicht besteht.[15] Eine Zurechnung kommt nur in Betracht, wenn der Account-Inhaber die Zugangsdaten weitergegeben hat.[16]

914 Die Frage, ob Beweiserleichterungen für den Geschäftsgegner zum Nachweis, dass der Account-Inhaber eine Handlung über den Account vorgenommen hat, in Betracht kommen, ist entsprechend zur Frage des Rechtsscheintatbestandes zu lösen. Beweiserleichterungen können in Form von Beweislastumkehr, tatsächlicher Vermutung, Anscheinsbeweis oder sekundärer Darlegungslast bestehen.[17] Beweiserleichterungen kommen nur dann in Betracht, wenn eine ausreichend sichere Authentisierungsmethode verwendet wurde und die Identifikationsfunktion des Accounts hinreichend zuverlässig ist.[18] Soll nicht nur bewiesen werden, dass der Account-Inhaber mit dem Account gehandelt hat, sondern auch, dass er eine Erklärung eines gewissen Inhalts abgegeben hat, muss die Erklärung gegen eine nachträgliche Verfälschung gesichert sein.[19]

915 Bei Internetanschluss, E-Mails und Benutzerkonten auf Internetseiten kommen somit weder eine Rechtsscheinhaftung noch Beweiserleichterungen in Betracht.[20] Bei der qualifizierten elektronischen Signatur, dem elektronischen Identitätsnachweis sowie der De-Mail bestehen hingegen sowohl eine Rechtsscheinhaftung des Account-Inhabers als auch Beweiserleichterungen zu Gunsten des Geschäftsgegners.[21]

---

12 Oben Rn. 578 ff.
13 Oben Rn. 544 ff.
14 Oben Rn. 391.
15 Oben Rn. 717.
16 Oben Rn. 679 ff.
17 Oben Rn. 774 ff.
18 Oben Rn. 826 ff.
19 Oben Rn. 828.
20 Oben Rn. 831 ff.
21 Oben Rn. 882 ff.

Entscheidungsverzeichnis

Literaturverzeichnis

Adams, *Michael*, Ökonomische Theorie des Rechts, 2. Aufl., Frankfurt am Main 2004.

Adolphsen, *Jens*, Zivilprozessrecht, 4. Aufl., Baden-Baden 2014.

Ahrens, *Hans-Jürgen*, 21 Thesen zur Störerhaftung im UWG und im Recht des Geistigen Eigentums, WRP 2007, S. 1281-1290.

Akerlof, *George*, The Market for „Lemons": Quality Uncertanty And The Market Mechanism, Quarterly Journal of Economics 84 (1970), S. 488-500.

Albrecht, *Astrid*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Baden-Baden 2003, Zugl.: Frankfurt am Main, Univ., Diss., 2003.

Allner, *Uwe*, Die tatsächliche Vermutung mit besonderer Berücksichtigung der GEMA-Vermutung, Pfaffenweiler 1993, Zugl.: Göttingen, Univ., Diss., 1992.

Alsbih, *Amir*, Der reale Wert einer IP-Adresse, DuD 2011, S. 482-488.

Amazon, Amazon.de Allgemeine Geschäftsbedingungen*, abrufbar unter*: http://www.amazon.de/gp/help/customer/display.html?nodeId=505048 (zuletzt abgerufen am 14. 6. 2014).

Anti-Phishing Working Group (*APWG*), Origins of the Word „Phishing"*, abrufbar unter*: http://docs.apwg.org/word_phish.html (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *APWG*.

Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland / Zweite Deutsche Fernsehen (*ARD / ZDF*), Online-Studie 2013, Medienausstattung / -nutzung*, abrufbar unter*: http://www.ard-zdf-onlinestudie.de/index.php?id=398 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *ARD / ZDF*, Online-Studie 2013, Medienausstattung / -nutzung.

– (*ARD / ZDF*), Online-Studie 2013, Onlinenutzung*, abrufbar unter*: http://www.ard-zdf-onlinestudie.de/index.php?id=394 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *ARD / ZDF*, Online-Studie 2013, Onlinenutzung.

Armgardt, *Matthias / Spalka*, *Adrian*, Der Anscheinsbeweis gemäß § 371 a Abs. 1 S. 2 ZPO vor dem Hintergrund der bestehenden Sicherheitslücken bei digitalen Signaturen, K&R 2007, S. 26-32.

Auerbach, *Andreas*, Bestellvorgänge mittels Bildschirmtext, CR 1988, S. 18-23.

Bachfeld, *Daniel*, Risiken beim Online-Banking, c't 22/2005, S. 148-153.

Baier, *Tobias*, Persönliches digitales Identitätsmanagement – Untersuchung und Entwicklung von Konzepten und Systemarchitekturen für die kontrollierte Selbstdarstellung in digitalen Netzen, Hamburg 2005, Zugl.: Hamburg, Univ., Diss., 2005.

Bamberger, *Georg / Roth*, *Herbert (Hrsg.)*, Kommentar zum Bürgerlichen Gesetzbuch, Bd. 1, §§ 1-610, CISG, 3. Aufl., München 2012, *zitiert als: Bearbeiter,* in: *Bamberger/H. Roth*[3].

Bartels, *Florian*, Zur bereicherungsrechtlichen Rückabwicklung von Überweisungen nach Umsetzung der Zahlungsdiensterichtlinie, WM 2010, S. 1828-1833.

Baumbach, *Adolf* / *Hopt*, *Klaus J. (Hrsg.)*, Beck'scher Kurzkommentar: Handelsgesetzbuch, 35. Aufl., München 2012, *zitiert als: Bearbeiter,* in: *Baumbach/Hopt*[35].

Baumgärtel, *Gottfried*, „Tatsächliche Vermutung" im Zivilprozess, in: *Gottwald*, *Peter* / *Prütting*, *Hanns* (Hrsg.), Festschrift für Karl Heinz Schwab zum 70. Geburtstag, München 1990, S. 43-51, *zitiert als*: *Baumgärtel*, in: FS Schwab.

– *(Begr.)* / *Laumen*, *Hans-Willi* / *Prütting*, *Hanns* (Hrsg.), Handbuch der Beweislast, Bd. 1, Grundlagen, 2. Aufl., Köln 2009, *zitiert als: Bearbeiter,* in: *Baumgärtel*[2].

Belling, *Detlev W.* / *Belling*, *Johannes*, Zahlungsdiensterecht und Bereicherungsausgleich bei nicht autoristierten Zahlungsvorgängen, JZ 2010, S. 708-711.

Bender, *Jens*, Aktuelle Entwicklungen der Haftung bei Phishing, WM 2008, S. 2049-2059.

Bender, *Jens* / *Kügler*, *Dennis* / *Margraf*, *Marian* / *Naumann*, *Ingo*, Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis – Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen, DuD 2008, S. 173-177.

Bergfelder, *Martin*, Der Beweis im elektronischen Rechtsverkehr, Hamburg 2006, Zugl.: Freiburg i. Br., Univ., Diss., 2006.

Berlit, *Uwe*, Staatliche Infrastrukturverantwortung für rechtssichere Kommunikation im Netz – rechtliche Rahmenbedingungen und Probleme, JurPC Web-Dok., 39/2011.

Beseler, *Dora von* / *Jacobs-Wüstefeld*, *Barbara*, Law Dictionary – Technical dictionary of the Anglo-American legal terminology including commercial and political terms, 4. Aufl., Bd. Englisch-Deutsch, Berlin 1986.

Beyerlein, *Thorsten*, Anmerkung zu *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband), EWiR 2009, S. 453-454.

Biallaß, *Isabelle Désirée*, Anmerkung zu *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06, ZUM 2007, S. 397-399.

– Zivilrechtliche Aspekte des Phishing, in: *Borges*, *Georg* (Hrsg.), Rechtsfragen der Internet-Auktion, Baden-Baden 2007, S. 11-25, *zitiert als*: *Biallaß*, in: Internet-Auktion.

Biallaß, *Isabelle Désirée* / *Borges*, *Georg* / *Dienstbach*, *Paul* / *Gajek*, *Sebastian* / *Meyer*, *Julia* / *Schwenk*, *Jörg* / *Wegener*, *Christoph* / *Werner*, *Dennis*, Aktuele Gefahren im Onlinebanking: Technische und juristische Hintergründe, in: *Bundesamt für Sicherheit in der Informationstechnik* (Hrsg.), Innovationsmotor IT-Sicherheit – Tagungsband zum 10 Deutschen IT-Sicherheitskongress, Gau-Algesheim 2007, S. 495-511, *zitiert als*: *Biallaß/Borges/Dienstbach/Gajek/J. Meyer/Schwenk/Wegener/Dennis Werner*, in: Innovationsmotor IT-Sicherheit.

Binder, *Jens-Hinrich*, Gesetzliche Form, Formnichtigkeit und Blankett im bürgerlichen Recht, AcP 207 (2007), S. 155-197.

Bohrer, *Michael*, Identität und Identifikation, MittBayNot 2005, S. 460-464.

Borges, *Georg*, Verträge im elektronischen Geschäftsverkehr, München 2003, Zugl.: Köln, Univ., Habil.-Schr., 2002, *zitiert als*: *Borges*, Verträge.

– Rechtsfragen des Phishing – ein Überblick, NJW 2005, S. 3313-3317.

– Anmerkung zu *OLG Hamburg*, Beschluß v. 07.07.2006, 1 U 75/06, ZIP 2006, S. 1983-1986.

– Zivilrechtliche Aspekte des Phishing, in: *Borges*, *Georg* (Hrsg.), Rechtsfragen der Internet-Auktion, Baden-Baden 2007, S. 214-224, *zitiert als*: *Borges*, in: Internet-Auktion.

– Anmerkung zu *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07, MMR 2008, S. 262-265.

Borges, *Georg*, Anmerkung zu *LG Mannheim*, Urteil v. 16. 5. 2008, 1 S 189/07, BKR 2009, S. 85-87.
– Der neue Personalausweis und der elektronische Identitätsnachweis, NJW 2010, S. 3334-3339.
– Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, Baden-Baden 2011, *zitiert als*: *Borges*, Elektronischer Identitätsnachweis.
– Rechtsscheinhaftung im Internet, NJW 2011, S. 2400-2404.
– Haftung für Identitätsmissbrauch im Online-Banking, NJW 2012, S. 2385-2389.
Borges, *Georg* / *Meyer*, *Julia*, Anmerkung zu *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05, EWiR 2006, S. 419-420.
Borges, *Georg* / *Schwenk*, *Jörg* / *Stuckenberg*, *Carl-Friedrich* / *Wegener*, *Christoph*, Identitätsdiebstahl und Identitätsmissbrauch im Internet – Rechtliche und technische Aspekte, Heidelberg 2011.
Bork, *Reinhard*, Allgemeiner Teil des Bürgerlichen Gesetzbuches, 3. Aufl., Tübingen 2011.
Börner, *Christian*, Untervollmacht und Rechtsscheinsvollmacht – Grundlagen und Anwendbarkeit der Rechtsscheinsgrundsätze auf die Untervollmacht, Bonn 2008, Zugl.: Bonn, Univ., Diss., 2008.
Borsum, *Wolfgang* / *Hoffmeister*, *Uwe*, Bildschirmtext und Bankgeschäfte, BB 1983, S. 1441-1446.
– Rechtsgeschäftliches Handeln unberechtigter Personen mittels Bildschirmtext, NJW 1985, S. 1205-1207.
Bösing, *Sebastian*, Authentifizierung und Autorisierung im elektronischen Rechtsverkehr – qualifizierte Signaturschlüssel- und Attributszertifikate als gesetzliche Instrumente digitaler Identität, Baden-Baden 2005, Zugl.: Kassel, Univ., Diss., 2005.
Bous, *Ulrich*, Zum Nachweis bestehender Vertretungsmacht gegenüber dem Grundbuchamt unter besonderer Berücksichtigung des § 172 Abs. 1 BGB, RPfleger 2006, S. 357-364.
Braun, *Frank* / *Roggenkamp*, *Jan Dirk*, 0zapftis - (Un)Zulässigkeit von „Staatstrojanern", K&R 2011, S. 681-686.
Briegleb, *Volker*, 145 Millionen Kunden von eBay-Hack betroffen, in: heise online v. 22. 5. 2014*, abrufbar unter*: http://www.heise.de/security/meldung/145-Millionen-Kunden-von-eBay-Hack-betroffen-2195974.html?wt_mc=rss.security.beitrag.atom (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Briegleb*, heise online v. 22. 5. 2014.
Brinkmann, *Werner*, Vertragsrechtliche Probleme bei Warenbestellungen über Bildschirmtext, BB 1981, S. 1183-1190.
Brockhaus – Die Enzyklopädie, 21. Aufl., Leipzig 2006.
Brox, *Hans*, Die Einschränkung der Irrtumsanfechtung, Karlsruhe 1960, Zugl.: Münster (Westf.), Univ., Habil.-Schr., 1958-1959.
Brox, *Hans* / *Walker*, *Wolf-Dietrich*, Allgemeiner Teil des BGB, 37. Aufl., München 2013, *zitiert als*: *Brox*/*Walker*, BGB AT[37].
– Allgemeines Schuldrecht, 37. Aufl., München 2013, *zitiert als*: *Brox*/*Walker*, Schuldrecht AT[37].
Brückner, *Dirk*, Online-Banking - Sphärenhaftung, Rechtsscheinhaftung, Verschuldenshaftung, Berlin 2002, Zugl.: München, Univ., Diss., 1999-2000.
Bruns, *Rudolf*, Zivilprozeßrecht, 2. Aufl., München 1979.

Brunst, *Phillip W.*, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, Berlin 2009, Zugl.: Erlangen-Nürnberg, Univ., Diss., 2008/09, *zitiert als*: *Brunst*, Anonymität im Internet.
– Staatlicher Zugang zur digitalen Identität – Erosion der Anonymität im Internet, DuD 2011, S. 618-623.
Bundesamt für Sicherheit in der Informationstechnik (*BSI*), IT-Grundschutz-Kataloge – 13. Ergänzungslieferung – 2013, *abrufbar unter*: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-Grundschutz-Kataloge_2013_EL13_DE.pdf?__blob=publicationFile (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *BSI*, IT-Grundschutz-Kataloge.
– Authentisierung im E-Government, Bonn 2005, Stand 18.4.2005, *zitiert als*: *BSI*, E-Government-Handbuch.
– Die Lage der IT-Sicherheit in Deutschland 2011, Bonn 2011, *zitiert als*: *BSI*, Lagebericht 2011.
Bundeskriminalamt (*BKA*), Cybercrime, Bundeslagebild 2011, *abrufbar unter*: http://www.bka.de/nn_205994/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2011,templateId=raw,property=publicationFile.pdf/cybercrimeBundeslagebild2011.pdf (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *BKA*.
Bunte, *Hermann-Josef*, AGB-Banken und Sonderbedinungen, 3. Aufl., München 2011.
Burgard, *Ulrich*, Online-Marktordnung und Inhaltskontrolle, WM 2001, S. 2102-2113.
Bydlinski, *Franz*, Privatautonomie und objektive Grundlagen des verpflichtenden Rechtsgeschäftes, Wien 1967, *zitiert als*: *Bydlinski*, Privatautonomie.
– Erklärungsbewußtsein und Rechtsgeschäft, JZ 1975, S. 1-6.

Calabresi, *Guido*, The costs of accidents – a legal and economic analysis, London 1975.
Canaris, *Claus-Wilhelm*, Die Vertrauenshaftung im deutschen Privatrecht, München 1971, zugl.: München, Univ., Habil.-Schr., 1967 u.d.T.: Die Rechtsscheinhaftung im deutschen Privatrecht, *zitiert als*: *Canaris*, Vertrauenshaftung.
– Der Bereicherungsausgleich im Dreipersonenverhältnis, in: *Paulus*, *Gotthard* / *Diedrichsen*, *Uwe* / *Canaris*, *Claus-Wilhelm* (Hrsg.), Festschrift für Karl Larenz zum 70. Geburtstag, München 1973, S. 799-865, *zitiert als*: *Canaris*, in: FS Larenz[1973].
– Anmerkung zu *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73, JZ 1976, S. 132-134.
– Die Feststellung von Lücken im Gesetz – eine methodologische Studie über Voraussetzungen und Grenzen der richterlichen Rechtsfortbildung praeter legem, 2. Aufl., Berlin 1983, Zugl.: München, Univ., Diss., 1965, *zitiert als*: *Canaris*, Lücken im Gesetz[2].
– Anmerkung zu Urteil v., 7. 6. 1984, IX ZR 66/83, NJW 1984, S. 2281-2282.
– Die Vertrauenshaftung im Lichte der Rechtsprechung des Bundesgerichtshofes, in: *Canaris*, *Claus-Wilhelm* (Hrsg.), 50 Jahre Bundesgerichtshof – Festgabe aus der Wissenschaft, Bd. 1, 2000, S. 129-197, *zitiert als*: *Canaris*, in: FG 50 Jahre BGH, Bd. 1.
– Die Reform des Rechts der Leistungsstörungen, JZ 2001, S. 499-524.
– Grundlagen und Rechtsfolgen der Haftung für anfängliche Unmöglichkeit nach § 311a Abs. 2 BGB, in: *Lorenz*, *Stephan* / *Trunk*, *Alexander* / *Eidenmüller*, *Horst* / *Wendehorst*, *Christiane* / *Adolff*, *Johannes* (Hrsg.), Festschrift für Andreas Heldrich zum 70. Geburtstag, München 2005, S. 11-38, *zitiert als*: *Canaris*, in: FS Heldrich.

Canaris, *Claus-Wilhelm*, Bankvertragsrecht, in: *Staub*, *Hermann* (Hrsg.), Handelsgesetzbuch Großkommentar, 4. Aufl., Bd. 5, 2005, *zitiert als*: *Canaris*, in: Bankvertragsrecht[4], Bd. 5.

– Handelsrecht, 24. Aufl., München 2006, *zitiert als*: *Canaris*, Handelsrecht[24].

Casper, *Matthias* / *Pfeifle*, *Theresa*, Missbrauch der Kreditkarte im Präsenz- und Mail-Order-Verfahren nach neuem Recht, WM 2009, S. 2343-2350.

Claussen, *Carsten Peter*, Recht des Bankkontos, in: *Claussen*, *Carsten Peter* (Hrsg.), Bank- und Börsenrecht, 4. Aufl., München 2008, *zitiert als*: *Claussen*, in: *Claussen*[4].

Clemens, *Rudolf*, Die elektronische Willenserklärung – Chancen und Gefahren, NJW 1985, S. 1998-2005.

Coase, *Ronald Harry*, The Problem Of Social Cost, The Journal of Law & Economics 3 (1960), S. 1-44.

Conrad, *Christian*, Die Vollmacht als Willenserklärung – Rechtsschein und Verkehrsschutz im Recht der gewillkürten Stellvertretung, Hamburg 2012, Zugl.: Bonn, Rheinische Friedrich-Wilhelms-Univ., Diss., 2012.

Cooter, *Robert* / *Ulen*, *Thomas*, Law & economics, 6. Aufl., Boston 2012.

Craushaar, *Götz von*, Die Bedeutung der Rechtsgeschäftslehre für die Problematik der Scheinvollmacht, AcP 174 (1974), S. 2-25.

Czeguhn, *Ignacio*, Beweiswert und Beweiskraft digitaler Dokumente im Zivilprozess, JuS 2004, S. 124-126.

Damker, *Herber* / *Federrath*, *Hannes* / *Schneider*, *Michael J.*, Maskerade-Angriffe im Internet – Eine Demonstration von Unsicherheit, DuD 1996, S. 286-294.

Damker, *Herber* / *Müller*, *Günter*, Verbraucherschutz im Internet, DuD 1997, S. 24-29.

Dästner, *Christian*, Neue Formvorschriften im Prozessrecht, NJW 2001, S. 3469-3471.

Dauner-Lieb, *Barbara* / *Heidel*, *Thomas* / *Ring*, *Gerhard (Hrsg.)*, NomosKommentar BGB, Bd. 2/1, Schuldrecht, §§ 241-610, 2. Aufl., Baden-Baden 2011, *zitiert als: Bearbeiter,* in: NK-BGB[2].

– *(Hrsg.)*, NomosKommentar BGB, Bd. 1, Allgemeiner Teil, EGBGB, 2. Aufl., Baden-Baden 2012, *zitiert als: Bearbeiter,* in: NK-BGB[2].

Deutsch, *Andreas*, Vertragsschluss bei Internetauktionen – Probleme und Streitstände, MMR 2004, S. 586-589.

Deutsches Network Information Center EG (*Denic*), DENIC-Domainbedingungen*, abrufbar unter*: http://www.denic.de/domainbedingungen.html (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Denic*.

Dienstbach, *Paul* / *Mühlenbrock*, *Tobias*, Haftungsfragen bei Phishing-Angriffen, K&R 2008, S. 151-155.

Dietrich, *Jens* / *Keller-Herder*, *Jutta*, De-Mail — verschlüsselt, authentisch, nachweisbar, DuD 2010, S. 299-301.

Dietrich, *Ralf*, Rechtliche Bewältigung von netzbasiertem Datenaustausch und Verteidigungsstrategien – 20000 Verfahren gegen Filesharingnutzer, NJW 2006, S. 809-811.

Dolle, *Wilhelm* / *Wegener*, *Christoph*, Windows Rootkits – eine aktuelle Bedrohung, DuD 2006, S. 471-475.

Dörner, *Heinrich*, Rechtsgeschäfte im Internet, AcP 202 (2002), S. 363-396.

Dreier, *Thomas* / *Schulze*, *Gernot (Hrsg.)*, Urheberrechtsgesetz Kommentar, 4. Aufl., München 2013, *zitiert als: Bearbeiter,* in: *Dreier/Schulze*[4].

Duden, Das große Wörterbuch der deutschen Sprache, 3. Aufl., Mannheim 1999.

eBay, Allgemeine Geschäftsbedingungen für die Nutzung der deutschsprachigen eBay-Websites, gültig seit 2. Januar 2007*, abrufbar unter*: http://pages.ebay.de/help/community/png-user-old.html (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *eBay*, AGB.
– Angebot an unterlegenen Bieter*, abrufbar unter*: http://pages.ebay.de/help/sell/second_chance_offer.html (zuletzt abgerufen am 14. 6. 2014).
– So funktioniert das Bewertungssystem*, abrufbar unter*: http://pages.ebay.de/help/feedback/howitworks.html (zuletzt abgerufen am 14. 6. 2014).
– Über eBay – Das Unternehmen*, abrufbar unter*: http://pages.ebay.de/aboutebay/thecompany/companyoverview.html (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *eBay*, Das Unternehmen.
– Überprüfung durch die Schufa*, abrufbar unter*: http://pages.ebay.de/help/account/schufa-help.html (zuletzt abgerufen am 14. 6. 2014).
– Von Käufern zu erfüllende Bedingungen auswählen*, abrufbar unter*: http://pages.ebay.de/help/sell/buyer-requirements.html (zuletzt abgerufen am 14. 6. 2014).
– Werden Sie „Geprüftes Mitglied“*, abrufbar unter*: http://pages.ebay.de/help/account/id-verify.html (zuletzt abgerufen am 14. 6. 2014).

Ebenroth, *Thomas* / *Boujong*, *Karlheinz* / *Joost*, *Detlev* / *Strohn*, *Lutz (Hrsg.)*, Handelsgesetzbuch, Bd. 2, §§ 343-475h, Transportrecht, Bank- und Börsenrecht, 2. Aufl., München 2009, *zitiert als: Bearbeiter,* in: *Ebenroth/Boujong/Joost/Strohn*[2].

Eckert, *Claudia*, IT-Sicherheit — Konzepte – Verfahren – Protokolle, 8. Aufl., München 2013.

Eickenberg, *Ronald*, Googles Zwei-Faktor-Authentifizierung ausgetrickst, in: heise online v. 26. 2. 2013*, abrufbar unter*: http://heise.de/-1811237 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Eickenberg*, heise online v. 26. 2. 2013.

Einsele, *Dorothee*, Bank- und Kapitalmarktrecht – nationale und internationale Bankgeschäfte, 2. Aufl., Tübingen 2010.

Engel, *Christian*, Auf dem Weg zum elektronischen Personalausweis – Der elektronische Personalausweis (ePA) als universelles Identifikationsdokument, DuD 2006, S. 207-210.

Enneccerus, *Ludwig* / *Lehmann*, *Heinrich*, Recht der Schuldverhältnisse, 15. Aufl., Tübingen 1958.

Enneccerus, *Ludwig* / *Nipperdey*, *Hans Carl*, Allgemeiner Teil des Bürgerlichen Rechts, 15. Aufl., Bd. I, 2, Tübingen 1960.

Erfurth, *René*, Haftung für Missbrauch von Legitimationsdaten durch Dritte beim Online-Banking, WM 2006, S. 2198-2207.

Erman, *Walter (Begr.)* / *Westermann*, *Harm Peter* (Hrsg.), Bürgerliches Gesetzbuch, Handkommentar, Bd. 1, 13. Aufl., Köln 2011, *zitiert als: Bearbeiter,* in: *Erman*[13].

Ernst, *Stefan*, Internet-Auktionsvertrag, in: *Redeker*, *Helmut* (Hrsg.), Handbuch der IT-Verträge, Köln, Losebl., Stand: Mai 2012, *zitiert als*: *Ernst*, in: IT-Verträge.
– Die Online-Versteigerung, CR 2000, S. 304-312.
– Anmerkung zu *OLG Hamm*, Urteil v. 14. 12. 2000, 2 U 58/00, CR 2001, S. 121-122.

Ernst, *Stefan*, Beweisprobleme bei E-Mail und anderen Online-Willenserklärungen, MDR 2003, S. 1091-1094.
– Vertragsgestaltung im Internet, München 2003, *zitiert als*: *Ernst*, Vertragsgestaltung.
– Trojanische Pferde und die Telefonrechnung, CR 2006, S. 590-594.
Europäischen Union, *Statistisches Amt der* (*Eurostat*), Personen die das Internet zum Senden/Empfangen von E-Mails genutzt haben*, abrufbar unter*: http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do?tab=table&plugin=1&pcode=tin00094&language=de (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Eurostat*.

Faust, *Florian*, Nutzung eines fremden eBay-Mitgliedskontos, JuS 2011, S. 1027-1030.
– Bürgerliches Gesetzbuch, Allgemeiner Teil, 3. Aufl., Baden-Baden 2013, *zitiert als*: *Faust*, BGB AT[3].
Fechner, *Frank*, Medienrecht – Lehrbuch des gesamten Medienrechts unter besonderer Berücksichtigung von Presse, Rundfunk und Multimedia, 14. Aufl., Tübingen 2013.
Federrath, *Hannes* / *Pfitzmann*, *Andreas*, Datenschutz und Datensicherheit, in: *Schneider*, *Uwe* / *Werner*, *Dieter* (Hrsg.), Taschenbuch der Informatik, 7. Aufl., München 2012, *zitiert als*: *Federrath*/*Pfitzmann*, in: *U. Schneider*/*Dieter Werner*[7].
Feldmann, *Karl*, Haftung und Anfechtung bei mißbräuchlich ausgefüllten Blankourkunden des bürgerlichen Rechts, Frankfurt am Main 1955, Zugl.: Frankfurt, Univ., Diss., 1955.
Fezer, *Karl-Heinz (Hrsg.)*, Beck'scher Kurzkommentar – Markenrecht, 4. Aufl., München 2009, *zitiert als: Bearbeiter,* in: MarkenR[4].
– *(Hrsg.)*, Lauterkeitsrecht – Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG), Bd. 2, §§ 5-20 UWG, 2. Aufl., München 2010, *zitiert als: Bearbeiter,* in: *Fezer*[2].
Fiege, *Carsten*, Anonymer Zahlungsverkehr mit elektronischem Geld, CR 1998, S. 41-47.
Fischer, *Gerfried*, Die Blanketterklärung – eine typologische Untersuchung, Göttingen 1975, Zugl.: Göttingen, Univ., Diss., 1973.
Fischer, *Peter*, Die dogmatische Stellung der Blanketterklärung, Bonn 1969, Zugl.: Bonn, Univ., Diss., 1969.
Fischer, *Thomas (Hrsg.)*, Beck'scher Kurzkommentar – Strafgesetzbuch, 60. Aufl., München 2013, *zitiert als: Bearbeiter,* in: StGB-Kommentar[60].
Fleischer, *Holger*, Informationsasymmetrie im Vertragsrecht – eine rechtsvergleichende und interdisziplinäre Abhandlung zu Reichweite und Grenzen vertragsschlußbezogener Aufklärungspflichten, München 2001, Zugl.: Köln, Univ., Habil.-Schr., 1998-1999.
Flume, *Werner*, Allgemeiner Teil des Bürgerlichen Rechts, Zweiter Band: Das Rechtsgeschäft, 4. Aufl., Bd. 2, Heidelberg 1992.
Foerster, *Max*, Nicht autorisierte Zahlungsvorgänge und Ausschlussfrist des § 676b Abs. 2 BGB — Ausgleich in Anweisungsfällen, AcP 213 (2013), S. 405-442.
Fornasier, Der Bereicherungsausgleich bei Fehlüberweisungen und das eruopäische Recht der Zahlungsdienste, AcP 212 (2012), S. 411-452.
Förschler, *Peter* / *Steinle*, *Hermann*, Der Zivilprozess – Ein Lehrbuch für die Praxis, 7. Aufl., Stuttgart 2010.
Fox, *Dirk*, Schlüsseldienst, c't 9/1995, S. 184.
– Missglückte Auferstehung, DuD 2009, S. 387.
– Cross Site Scripting (XSS), DuD 2012, S. 840.

Fox, *Dirk*, Social Engineering, DuD 2013, S. 5.

Franck, *Jens-Uwe* / *Massari*, *Philipp*, Die Zahlungsdiensterichtlinie: Günstigere und schnellere Zahlungen durch besseres Vertragsrecht?, WM 2009, S. 1117-1128.

Frank, *Thomas*, 20 Jahre Computervirus und 132 Jahre StGB, in: *Hilgendorf*, *Eric* (Hrsg.), Informationsstrafrecht und Rechtsinformatik, Berlin 2004, S. 23-55, *zitiert als*: *Frank*, in: Informationsstrafrecht.

Freitag, *Robert*, Die Abwicklung von Zahlungen im Zuge von Internetauktionen, in: *Leible*, *Stefan* / *Sosnitza*, *Olaf* (Hrsg.), Versteigerungen im Internet, Heidelberg 2004, *zitiert als*: *Freitag*, in: *Leible*/*Sosnitza*.

Freund, *Bernhard* / *Schnabel*, *Christoph*, Bedeutet IPv6 das Ende der Anonymität im Internet? Technische Grundlagen und rechtliche Beurteilung des neuen Internet-Protokolls, MMR 2011, S. 495-499.

Friedmann, *Stefan*, Bildschirmtext und Rechtsgeschäftslehre, Köln 1986, Zugl.: Köln, Univ., Diss., 1986.

Fritsch, *Jörg* / *Gundel*, *Steffen*, Firewalls im Unternehmenseinsatz, 2. Aufl., Heidelberg 2005.

Frotz, *Gerhard*, Verkehrsschutz im Vertretungsrecht, Tübingen 1972, Zugl.: Tübingen, Univ., Habil.-Schr., 1966.

Fuchs, *Maximilian* / *Pauker*, *Werner*, Delikts- und Schadensersatzrecht, 8. Aufl., Heidelberg 2012.

Fuhrberg, *Kai*, Technische Sicherheit im Internet, K&R 1999, S. 20-24.

Gassen, *Dominik*, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, Köln 2003, Zugl: Köln, Univ., Diss., 2002.

Gaycken, *Sandro*, Cyberwar – das Internet als Kriegsschauplatz, München 2011.

Gelzhäuser, *Sven*, Erfolgreiches De-Mail Pilotprojekt: Teilnehmer ziehen Bilanz, DuD 2010, S. 646-648.

Genius, *Barbara*, Vertragliche Haftung des Kontoinhabers bei unbefugter Nutzung eines eBay-Mitgliedskontos?, jurisPR-BGHZivilR 12/2011, Anm. 1.

Geppert, *Martin* / *Piepenbrock*, *Hermann-Josef* / *Schütz*, *Raimund* / *Schuster*, *Fabian (Hrsg.)*, Beck'scher TKG-Kommentar, 4. Aufl., München 2013, *zitiert als: Bearbeiter,* in: Beck'scher TKG-Kommentar[4].

Gercke, *Marco*, Die Strafbarkeit von „Phishing" und Identitätsdiebstahl – Eine Analyse der Reichweite des geltenden Strafrechts, CR 2005, S. 606-612.

Gietl, *Andreas* / *Mantz*, *Reto*, Die IP-Adresse als Beweismittel im Zivilprozess – Beweiserlangung, Beweiswert und Beweisverbote, CR 2008, S. 810-816.

Glatt, *Christoph*, Vertragsschluss im Internet – Unter besonderer Berücksichtigung der Rechtsentwicklung in der Europäischen Union und des internationalen Verbrauchervertrages, Baden-Baden 2002, Zugl.: Freiburg, Univ., Diss., 2001.

Gooren, *Paul*, Anmerkung zu *BGH*, Urteil v. 28. 3. 2012, VIII ZR 244/10, MMR 2012, S. 453-454.

Gössmann, *Wolfgang* / *Sönke*, *Bredenkamp*, Phishing, Vishing, Spoofing, Pharming oder Sniffing, in: *Habersack*, *Mathias* / *Joeres*, *Hans-Ulrich* / *Krämer*, *Achim* (Hrsg.), Entwicklungslinien im Bank- und Kapitalmarktrecht – Festschrift für Gerd Nobbe, Köln 2009, S. 93-118, *zitiert als*: *Gössmann*/*Sönke*, in: FS Nobbe.

Gotthardt, *Peter Jürgen*, Der Vertrauensschutz bei der Anscheinsvollmacht im deutschen und im französischen Recht, Karlsruhe 1970, Zugl.: Freiburg i.Br., Univ., Diss., 1969.
Gräbig, *Johannes*, Aktuelle Entwicklungen bei Haftung für mittelbare Rechtsverletzungen, MMR 2011, S. 504-509.
Grapentin, *Sabine*, Vertragsschluss bei Internet-Auktionen, GRUR 2001, S. 713-716.
Grosskopf, *Lambert*, Anmerkung zu *LG Hamburg*, Beschluss v. 21. 4. 2006, 308 O 139/06, CR 2007, S. 122-124.
Grundmann, *Stefan*, Das neue Recht des Zahlungsverkehrs – Teil 1, WM 2009, S. 1109-1117.
– Das neue Recht des Zahlungsverkehrs – Teil 2, WM 2009, S. 1157-1164.
Grunewald, *Barbara*, Gesellschaftsrecht, 8. Aufl., Tübingen 2011.
Günther, *Thomas*, Beweiserschütterung und -verteilung beim Bankkarten-Anscheinsbeweis, WM 2013, S. 496-503.
Gurmann, *Stefan*, Internet-Auktionen – Gewerberecht, Zivilrecht, Strafrecht, Wien 2005, Zugl.: Graz, Univ., Diss., 2003.

Hanau, *Max Ulrich*, Handeln unter fremder Nummer, Köln 2004, Zugl.: Köln, Univ., Diss., 2004, *zitiert als*: *Hanau*, Handeln unter fremder Nummer.
– Handeln unter fremder Nummer, VersR 2005, S. 1215-1220.
Handelsverband Deutschland (*HDE*), E-Commerce-Umsatz in Deutschland 1999 bis 2012 und Prognose für 2013 (in Milliarden Euro), zitiert nach de.statista.com *abrufbar unter*: http://de.statista.com/statistik/daten/studie/3979/umfrage/e-commerce-umsatz-in-deutschland-seit-1999/ (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *HDE*.
Hannemann, *Jennifer* / *Solmecke*, *Christian*, OLG Köln: Unerlaubtes Anbieten eines Computerspiels über Tauschbörsen im Internet, MMR 2011, S. 398-400.
Hansen, *David*, Strafbarkeit des Phishing nach Internetbanking-Legitimationsdaten, Hamburg 2007, Zugl.: Passau, Univ., Diss., 2007.
Harte-Bavendamm, *Henning* / *Henning-Bodewig*, *Frauke (Hrsg.)*, Gesetz gegen den unlateren Wettbewerb (UWG) – Kommentar, 3. Aufl., München 2013, *zitiert als: Bearbeiter,* in: *Harte-Bavendamm/Henning-Bodewig*[3].
Härting, *Niko*, Internetrecht, 4. Aufl., 2010.
Härting, *Niko* / *Golz*, *Robert*, Rechtsfragen des eBay-Handels, ITRB 2005, S. 137-140.
Härting, *Niko* / *Strubel*, *Michael*, Anmerkung zu *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband), BB 2011, S. 2188-2189.
Hartmann, *Alexander*, Unterlassungsansprüche im Internet, München 2009, Zugl.: Potsdam, Univ., Diss., 2009.
Hauck, *Ronny*, Handeln unter fremdem Namen, JuS 2011, S. 967-970.
Haug, *Volker*, Internetrecht – Erläuterungen mit Urteilsauszügen, Schaubildern und Übersichten, 2. Aufl., Stuttgart 2010.
Hauschka, *Christoph E. (Hrsg.)*, Corporate Compliance, 2. Aufl., München 2010, *zitiert als: Bearbeiter,* in: *Hauschka*[2].
Hayek, *Friedrich August von*, The Use of Knowledge in Society, American Economic Review 35 (1945), S. 519-530.
Hecht, *Florian*, Verantwortlichkeit für Benutzerkonten im Internet, K&R 2009, S. 462-464.

Hecker, *Manfred R.*, Das Handschriftengutachten als Sachbeweis, NStZ 1990, S. 463-469.
– Forensische Handschriftenuntersuchung, Heidelberg 1993, *zitiert als*: *Hecker*, Forensische Handschriftenuntersuchung.
Heckmann, *Dirk*, Editorial, JurisPR-ITR 3/2009, Anm. 1.
Heibey, *Hanns-Wilhelm* / *Quiring-Kock*, *Gisela*, Biometrische Authentisierung – Möglichkeiten und Grenzen, DuD 2010, S. 332-333.
Henning, *Peter A.*, Internet und Intranet, in: *Schneider*, *Uwe* / *Werner*, *Dieter* (Hrsg.), Taschenbuch der Informatik, 7. Aufl., München 2012, *zitiert als*: *Henning*, in: *U. Schneider/Dieter Werner*[7].
Herresthal, *Carsten*, Die Haftung bei Account-Überlassung und Account-Missbrauch im Bürgerlichen Recht, in: *Taeger*, *Jürgen* / *Wiebe*, *Andreas* (Hrsg.), Von AdWords bis Social Networks – Neue Entwicklungen im Informationsrecht, 2008, S. 21-46, *zitiert als*: *Herresthal*, in: *Taeger/Wiebe*.
– Haftung bei Account-Überlassung und Account-Missbrauch im Bürgerlichen Recht, K&R 2008, S. 705-711.
– Benutzung eines eBay-Mitgliedskontos durch einen Dritten, JZ 2011, S. 1171-174.
Hildebrandt, *Heinz*, Erklärungshaftung – ein Beitrag zum System des bürgerlichen Rechtes, Berlin 1931.
Hilgendorf, *Eric* / *Valerius*, *Brian*, Computer- und Internetstrafrecht, 2. Aufl., Berlin 2012.
Hirshleifer, *Jack*, The Private and Social Value of Information and the Reward to Inventive Activity, American Economic Review 61 (1971), S. 561-574.
Hoenike, *Mark* / *Szodruch*, *Alexander*, Rechtsrahmen innovativer Zahlungssysteme für Multimediadienste, MMR 2006, S. 519-526.
Hoeren, *Thomas*, Internet und Recht — Neue Paradigmen des Informationsrechts, NJW 1998, S. 2849-2854.
– Beweislast für Vertragsschluss bei Online-Auktion, Anmerkung zu *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00, CR 2002, S. 295-296.
– Grundzüge des Internetrechts – E-Commerce, Domains, Urheberrecht, 2. Aufl., München 2002, *zitiert als*: *Hoeren*, Internetrecht[2].
– Bewertungen bei eBay – Eine kritische Rechtsprechungsübersicht zur Suche nach angemessenen rechtlichen Bewertungen, CR 2005, S. 498-502.
– Das Pferd frisst keinen Gurkensalat — Überlegungen zur Internet Governance, NJW 2008, S. 2615-2619.
– Anmerkung zu *BGH*, Urteil v. 28. 3. 2012, VIII ZR 244/10, EWiR 2012, S. 471-472.
– Verbraucherschutz im Bereich der Versorgungsdienstleistungen, in: *Tamm*, *Marina* / *Tonner*, *Klaus* (Hrsg.), Verbraucherrecht, Baden-Baden 2012, *zitiert als*: *Hoeren*, in: Verbraucherrecht.
Hoeren, *Thomas* / *Sieber*, *Ulrich* / *Holznagel*, *Bernd (Hrsg.)*, Handbuch Multimedia-Recht, München 2013, Losebl., 35. Ergänzungslieferung, Stand: Juli 2013, *zitiert als: Bearbeiter,* in: *Hoeren/Sieber/Holznagel*.
Höffe, *Otfried*, Identitäten im Zeitalter der Digitalisierung*, abrufbar unter*: http://www.privacy-security.ch/sps2003/deutsch/anmeldung/pdf/07_Hoeffe_text.pdf (zuletzt abgerufen am 14. 6. 2014).
Hoffmann, *Jochen*, Vertrags- und Haftungsrecht, in: *Leible*, *Stefan* / *Sosnitza*, *Olaf* (Hrsg.), Versteigerungen im Internet, Heidelberg 2004, *zitiert als*: *J. Hoffmann*, in: *Leible/Sosnitza*.

Hoffmann, *Mario*, Willenserklärungen im Internet – Rechtssicherheit durch elektronische Signaturen sowie Anpassung der Formvorschriften und des Beweisrechts, Hamburg 2003, Zugl.: Dresden, Univ., Diss., 2002-2003.

Hoffmann-Riem, *Wolfgang*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009-1022.

Höhmann, *Ingmar*, Die neuen Waffen der Phisher, in: heise online v. 9. 7. 2012*, abrufbar unter*: http://heise.de/-1629704 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Höhmann*, heise online v. 9. 7. 2012.

Hollenders, *Anna-Sophie*, Mittelbare Verantwortlichkeit von Intermediären im Netz, Baden-Baden 2012, Münster (Westf.), Univ., Diss., 2011.

Holznagel, *Bernd*, Recht der IT-Sicherheit, München 2003.

Honan, *Mat*, How Apple and Amazon Security Flaws Led to My Epic Hacking, in: Wired v. 8. 6. 2012*, abrufbar unter*: http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/ (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Honan*, Wired v. 8. 6. 2012.

Hoppen, *Peter*, Datenarchivierung – DV-technische Aspekte bei der Erfüllung rechtlicher Aufbewahrungspflichten, CR 2008, S. 674-680.

Hornung, *Gerrit*, Die digitale Identität, Baden-Baden 2005, Zugl.: Kassel, Univ., Diss., 2005, *zitiert als*: *Hornung*, Die digitale Identität.

– Brüsseler Angriff auf den neuen Personalausweis?, MMR 2012, S. 633-634.

Hossenfelder, *Martin*, Onlinebanking und Haftung – Zu den Sorgfaltspflichten des Bankkunden im Lichte des neuen Zahlungsdiensterechts, CR 2009, S. 790-794.

– Pflichten von Internetnutzern zur Abwehr von Malware und Phishing in Sonderverbindungen, Baden-Baden 2013, Zugl.: Bochum, Univ., Diss., 2011/12, *zitiert als*: *Hossenfelder*, Pflichten von Internetnutzern.

Hubmann, *Heinrich*, Grundsätze der Interessenabwägung, AcP 155 (1956), S. 85-134.

Hübner, *Heinz*, AT des Bürgerlichen Gesetzbuches, 2. Aufl., Berlin 1996.

Hupka, *Josef*, Die Vollmacht, eine civilistische Untersuchung mit besonderer Berücksichtigung des Deutschen Bürgerlichen Gesetzbuchs, Leizip 1990.

Ikas, *Klaus*, Zum Recht der elektornischen Zahlung mit Debitkarten in bargeldlosen Kassensystemen (EFTPOS), Berlin 1992, Zugl.: Tübingen, Univ., Diss., 1990.

Ingerl, *Reinhard* / *Rohnke*, *Christian (Hrsg.)*, Markengesetz Kommentar, 3. Aufl., München 2010, *zitiert als: Bearbeiter,* in: MarkenG[3].

Internet Engineering Task Force (*IETF*), Request for Comments 1939 – Post Office Protocol, Version 3*, abrufbar unter*: http://tools.ietf.org/html/rfc1939 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *IETF*, RFC 1939.

– (*IETF*), Request for Comments 2460 – Internet Protocol, Version 6 (IPv6) – Specification*, abrufbar unter*: http://tools.ietf.org/html/rfc2460 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *IETF*, RFC 2460.

– (*IETF*), Request for Comments 2616 – Hypertext Transfer Protocol – HTTP/1.1, *abrufbar unter*: http://tools.ietf.org/html/rfc2616 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *IETF*, RFC 2616.

– (*IETF*), Request for Comments 2822 – Internet Message Format*, abrufbar unter*: http://tools.ietf.org/html/rfc2822 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *IETF*, RFC 2822.

Internet Engineering Task Force (*IETF*), Request for Comments 2828 – Internet Security Glossary*, abrufbar unter*: http://tools.ietf.org/html/rfc2822 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *IETF*, RFC 2828.

– (*IETF*), Request for Comments 3501 – Internet Message Access Protocol – Version 4rev1*, abrufbar unter*: http://tools.ietf.org/html/rfc3501 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *IETF*, RFC 3501.

– (*IETF*), Request for Comments 5321 – Simple Mail Transfer Protocol*, abrufbar unter*: http://tools.ietf.org/html/rfc5321 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *IETF*, RFC 5321.

– (*IETF*), Request for Comments 791 – Internet Protocol, Darpa Internet Program Protocol Specification*, abrufbar unter*: http://tools.ietf.org/html/rfc791 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *IETF*, RFC 791.

Isay, *Hermann*, Die Geschäftsführung nach dem Bürgerlichen Gesetzbuche für das Deutsche Reich, Jena 1900.

Jacobi, *Ernst*, Die Haftung des Kommanditisten und die Eintragung der Haftung ins Handelsregister, JherJB 70 (1921), S. 300-335.

Jandach, *Thomas*, Identität und Anonymität bei der elektronischen Kommunikations, in: *Taeger*, *Jürgen* / *Wiebe*, *Andreas* (Hrsg.), Informatik – Wirtschaft – Recht, Regulierung in der Wissensgesellschaft, Festschrift für Wolfgang Kilian zum 65. Geburtstag, Tübingen 2004, S. 443-461, *zitiert als*: *Jandach*, in: FS Kilian.

Jandt, *Silke*, Die Mitwirkung Dritter bei der Signaturerzeugung, K&R 2009, S. 548-555.

Jauernig, *Othmar (Hrsg.)*, Bürgerliches Gesetzbuch mit Allgemeinem Gleichbehandlungsgesetz, 15. Aufl., München 2014, *zitiert als: Bearbeiter,* in: *Jauernig*[15].

Jauernig, *Othmar* / *Hess*, *Burkhard*, Zivilprozessrecht, 30. Aufl., München 2011.

Jehle, *Stefanie*, Vertrauen und Recht im Internet, Hamburg 2010, Zugl.: Chemnitz, Univ., Diss., 2010.

Jhering, *Rudolf von*, Schadensersatz bei nichtigen oder nicht zur Perfection gelangten Verträgen, JherJB 4 (1861), S. 1-112.

Joecks, *Wolfgang* / *Wiebach*, *Klaus (Hrsg.)*, Münchener Kommentar zum Strafgesetzbuch, Bd. 4, §§ 185-262 StGB, 2. Aufl., München 2012, *zitiert als: Bearbeiter,* in: MüKo-StGB[2].

Jötten, *Herbert Kai*, Logout: Zivilrechtliche Haftung im Rahmen ausgewählter Internetdienstleistungen, Hamburg 2010, Zugl.: Köln, Univ., Diss., 2009.

Jung, *Peter*, Handelsrecht, 9. Aufl., München 2012.

Jungmann, *Carsten*, Missbrauch von ec-Karten bei PIN-basierten Transaktionen – Rechtfertigung, Grenzen und Zukunft des von der Rechtsprechung entwickelten Beweises des ersten Anscheins, in: *Zetzsche*, *Dirk* / *Neef*, *Andreas* / *Makoski*, *Bernadette* / *Beurskens*, *Michael* (Hrsg.), Jahrbuch Junger Zivilrechtswissenschaftlicher 2007 – Recht und Wirtschaft, Stuttgart 2007, S. 329-358, *zitiert als*: *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007.

– Der „Anscheinsbweis ohne ersten Anschein“, ZZP 120 (2007), S. 459-473.

Juretzek, *Peter*, Anmerkung zu *BGH*, Urteil v. 28. 3. 2012, VIII ZR 244/10, CR 2012, S. 462-464.

Kalabis, *Lukas* / *Kunz*, *Thomas* / *Wolf*, *Ruben*, Sichere Nutzung von Cloud-Speicherdiensten – Wie Trennung von Identity-, Access- und Key-Management für mehr Sicherheit und Flexibilität sorgt, DuD 2013, S. 512-516.

Karper, *Irene*, Sorgfaltspflichten beim Online-Banking – Der Bankkunde als Netzwerkprofil?, DuD 2006, S. 215-219.

Kaspersky, *Eugene*, Malware – von Viren, Würmern, Hackern und Trojanern und wie man sich vor ihnen schützt, München 2008.

Kent, *Stephen T.* / *Millet*, *Lynette I.*, Who Goes There? – Authentication through the Lens of Privacy, Washington 2003.

Kiehnle, *Arndt*, Anmerkung zu Urteil v. 1. 6. 2010, XI ZR 389/09, EWiR 2010, S. 485-486.

– Fehlüberweisungen und Bereicherungsausgleich nach der Zahlungsdiensterichtlinie, Jura 2012, S. 895-901.

Kind, *Michael* / *Werner*, *Dennis*, Rechte und Pflichten im Umgang mit PIN und TAN, CR 2006, S. 353-360.

Kindl, *Johann*, Rechtsscheintatbestände und ihre rückwirkende Beseitigung, Berlin 1999, Zugl.: Augsburg, Univ., Habil.-Schr., 1998.

Klees, *Andreas*, Rechtsscheinhaftung im digitalen Rechtsverkehr, MDR 2007, S. 185-188.

Klees, *Andreas* / *Keisenberg*, *Johanna*, Vertragsschluss bei eBay – „3. . . 2(. . . 1). . . meins“?, MDR 2011, S. 1214-1218.

Kleier, *Ulrich*, Bildschirmtext – Wirtschaftliche und rechtliche Auswirkungen, WRP 1983, S. 534-540.

Klein, *Winfried*, Anmerkung zu Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung), MMR 2011, S. 450-451.

Knopp, *Michael* / *Wilke*, *Daniel* / *Hornung*, *Gerrit* / *Laue*, *Philip*, Grunddienste für die Rechtssicherheit elektronischer Kommunikation – Rechtlicher Bedarf für eine gewährleistete Sicherheit, MMR 2008, S. 723-728.

Knupfer, *Jörg*, Phishing for Money, MMR 2004, S. 641-642.

Koch, *Frank A.*, Internet-Recht, 2. Aufl., München 2005, *zitiert als*: *F. A. Koch*, Internet-Recht[2].

– Updating von Sicherheitssoftware – Haftung und Beweislast, Eine Problemskizze zur Verkehrssicherungspflicht zum Einsatz von Antivirenprogrammen, CR 2009, S. 485-491.

Koch, *Philip*, Technisches Lexikon, in: *Kilian*, *Wolfgang* / *Heussen*, *Benno* (Hrsg.), Computerrechts-Handbuch, 2012, Kap. 24, Losebl., 31. Ergänzungslieferung, Stand: Mai 2012, *zitiert als*: *P. Koch*, in: Computerrechts-Handbuch.

Koch, *Robert*, Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, S. 801-807.

– Geltungsbereich von Internet-Auktionsbedingungen – Inwieweit begründen Internet-Auktionsbedingungen Rechte und Pflichten zwischen den Teilnehmern?, CR 2005, S. 502-510.

Köhler, *Helmut*, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen, AcP 182 (1982), S. 126-171.

– BGB – Allgemeiner Teil, 37. Aufl., München 2013, *zitiert als*: *H. Köhler*, BGB AT[37].

Köhler, *Helmut* / *Bornkamm*, *Joachim (Hrsg.)*, Beck'scher Kurzkommentar – Gesetz gegen den unlauteren Wettbewerb, 31. Aufl., München 2013, *zitiert als: Bearbeiter,* in: *H. Köhler/Bornkamm*[31].

Köhler, *Markus* / *Arndt*, *Hans-Wolfgang* / *Fetzer*, *Thomas*, Recht des Internet, 7. Aufl., Heidelberg 2011.

Köhntopp, *Marit* / *Köhntopp*, *Kristian*, Datenspuren im Internet, CR 2000, S. 248-257.

Koller, *Ingo*, Fälschung und Verfälung von Wertpapieren, WM 1981, S. 210-220.

Koller, *Ingo* / *Roth*, *Wulf-Henning* / *Morck*, *Winfried (Hrsg.)*, Handelsgesetzbuch Kommentar, 7. Aufl., München 2011, *zitiert als: Bearbeiter,* in: *Koller/W. Roth/Morck*[7].

Kollhosser, *Helmut*, Anscheinsbeweis und freie richterliche Beweiswürdigung, AcP 165 (1965), S. 46-83.

Kollrus, *Harald*, Missbräuchliche Abhebung von Bargeld an Geldautomaten, MDR 2012, S. 377-380.

Kommission der Europäischen Gemeinschaft (*EG-Kommission*), Eine allgemeine Politik zur Bekämpfung der Internetkriminalität – KOM (2007) 267 endg., *abrufbar unter*: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:DE:PDF (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *EG-Kommission*.

Köndgen, *Johannes*, Selbstbindung ohne Vertrag – zur Haftung aus geschäftsbezogenem Handeln, Tübingen 1981, Teilw. zugl.: Tübingen, Univ., Habil.-Schr., 1979-1980.

Konrath, *Christoph*, Recht und Identität – Einführende Überlegungen, London 2003, Zugl.: Wien, Univ., Diss., 2003.

Kossel, *Axel* / *Kötter*, *Markus*, Wenn Schadprogramme den PC kapern, c't 2/2007, S. 76-77.

Kötz, *Hein*, Vertragliche Aufklärungspflichten – Eine rechtökonomische Studie, in: *Basedow*, *Jürgen* / *Hopt*, *Klaus J.* / *Kötz*, *Hein* (Hrsg.), Festschrift für Ulrich Drobnig zum siebzigsten Geburtstag, Tübingen 1998, S. 563-577, *zitiert als*: *Kötz*, in: FS Drobnig.

Kötz, *Hein* / *Schäfer*, *Hans-Bernd*, Judex oeconomicus – 12 höchstrichterliche Entscheidungen kommentiert aus ökonomischer Sicht, Tübingen 2003.

Krell, *Paul*, Probleme des Prozessbetrugs, JR 2012, S. 102-109.

Kuhn, *Matthias*, Rechtshandlungen mittels EDV und Telekommunikation – Zurechenbarkeit und Haftung, München 1991, Zugl.: Regensburg, Univ., Diss., 1990.

Kühnhauser, *Winfried E.*, Root Kits, DuD 2003, S. 218-222.

Lachmann, *Jens-Peter*, Ausgewählte Probleme aus dem Recht des Bildschirmtextes, NJW 1984, S. 405-408.

Lackner, *Karl* / *Kühl*, *Kristian (Hrsg.)*, Strafgesetzbuch, Kommentar, 27. Aufl., München 2011, *zitiert als: Bearbeiter,* in: *Lackner/Kühl*[27].

Lange, *Heinrich* / *Kuchinke*, *Kurt*, Erbrecht – ein Lehrbuch, 5. Aufl., München 2001.

Langenbucher, *Katja*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, München 2001, Zugl.: München, Univ., Habil., 2001.

Langenbucher, *Katja* / *Bliesener*, *Dirk* / *Spindler*, *Gerald (Hrsg.)*, Bankrechts-Kommentar, München 2013, *zitiert als: Bearbeiter,* in: *Langenbucher/Bliesener/Spindler*.

Lapp, *Thomas*, Brauchen wir De-Mail und Bürgerportale? – Überflüssige Anwendung mit Geburtsfehlern, DuD 2009, S. 651-655.

Lardschneider, *Michael*, Social Engineering – Eine ungewöhnliche aber höchst effiziente Security Awareness Maßnahme, DuD 2008, S. 574-578.

Larenz, *Karl*, Verpflichtungsgeschäfte „unter" fremdem Namen, in: *Nipperdey*, *Hans Carl* (Hrsg.), Festschrift für Heinrich Lehmann zum 80. Geburtstag, Bd. 1, Tübingen 1956, S. 234-252, *zitiert als*: *Larenz*, in: FS Lehmann, Bd. 1.

– Lehrbuch des Schuldrechts, 14. Aufl., Bd. 1, München 1987, *zitiert als*: *Larenz*, Schuldrecht[14].

Larenz, *Karl* / *Canaris*, *Claus-Wilhelm*, Methodenlehre der Rechtswissenschaft, 3. Aufl., Berlin 1995.

Larenz, *Karl* / *Wolf*, *Manfred*, Allgemeiner Teil des Bürgerlichen Rechts, 9. Aufl., München 2004.

Laumen, *Hans-Willi*, Die „Beweiserleichterung bis zur Beweislastumkehr" – Ein beweisrechtliches Phänomen, NJW 2002, S. 3739-3746.

Lechtenbörger, *Jens*, Zur Sicherheit von De-Mail, DuD 2011, S. 268-269.

Lehmann, *Michael* / *Giedke*, *Anna*, Cloud Computing – technische Hintergründe für die territorial gebundene rechtliche Analyse, CR 2013, S. 608-616.

Lehner, *Marcel* / *Hermann*, *Eckehard*, Auffinden von verschleierter Malware, DuD 2006, S. 768-772.

Leible, *Stefan* / *Sosnitza*, *Olaf*, Sniper-Software und Wettbewerbsrecht, Zur vertrags- und lauterkeitsrechtlichen Beurteilung automatisierter Gebote bei Internet-Auktionen, CR 2003, S. 344-349.

Leipold, *Dieter*, BGB I: Einführung und Allgemeiner Teil, 7. Aufl., Tübingen 2013, *zitiert als*: *Leipold*, BGB I: Einführung und Allgemeiner Teil[7].

Leistner, *Matthias*, Störerhaftung und mittelbare Schutzrechtsverletzung, GRUR-Beil. 2010, S. 1-32.

Leistner, *Matthias* / *Stang*, *Felix*, Die Neuerung der wettbewerbsrechtlichen Verkehrspflichten – Ein Siegeszug der Prüfungspflichten?, WRP 2008, S. 533-555.

– Anmerkung zu *BGH*; Urteil v. 17.09.2009, Xa ZR 2/08 (MP3-Player-Import), LMK 2010, 297473.

Lettl, *Tobias*, Handelsrecht, 2. Aufl., München 2011.

Leupold, *Andreas* / *Glossner*, *Silke (Hrsg.)*, Münchener Anwaltshandbuch IT-Recht, 2. Aufl., München 2011, *zitiert als: Bearbeiter,* in: Handbuch IT-Recht[2].

Libertus, *Michael*, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, S. 507-512.

Lieb, *Manfred*, Zum Handeln unter fremdem Namen, JuS 1967, S. 107-113.

Lilja, *Anna-Julka*, Anmerkung zu *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung), NJ 2011, S. 427-428.

Linardatos, *Dimitrios*, Handeln unter fremdem Namen und Rechtsscheinhaftung bei Nutzung eines fremden eBay-Accounts, Jura 2012, S. 53-55.

Lipski, *Marcus*, Social Engineering – der Mensch als Sicherheitsrisiko in der IT, Hamburg 2009, Zugl.: Darmstadt, Private FernFachhochsch., Diplomarbeit, 2009.

Lobinger, *Thomas*, Rechtsgeschäftliche Verpflichtung und autonome Bindung – zu den Entstehungsgründen vermögensaufstockender Leistungspflichten im Bürgerlichen Recht, Tübingen 1999, Zugl.: Tübingen, Univ., Diss., 1999, *zitiert als*: *Lobinger*, Rechtsgeschäftliche Verpflichtung.

– Anmerkung zu Urteil v., 16. 3. 2006, III ZR 152/05 (R-Gespräch), JZ 2006, S. 1076-1080.

Löffler, *Helmut*, Datenkommunikation, in: *Schneider*, *Uwe* / *Werner*, *Dieter* (Hrsg.), Taschenbuch der Informatik, 7. Aufl., München 2012, *zitiert als*: *Löffler*, in: *U. Schneider*/*Dieter Werner*[7].

Looschelders, *Dirk*, Schuldrecht – Allgemeiner Teil, 11. Aufl., München 2013, *zitiert als*: *Looschelders*, Schuldrecht AT[11].

– Schuldrecht – Besonderer Teil, 8. Aufl., München 2013, *zitiert als*: *Looschelders*, Schuldrecht BT[8].

Lorenz, *Bernd*, Sorgfaltspflichten im Umgang mit Passwörter, DuD 2013, S. 220-226.

Lorenz, *Stephan*, Der Schutz vor dem unerwünschten Vertrag – eine Untersuchung von Möglichkeiten und Grenzen der Abschlußkontrolle im geltenden Recht, München 1997, Zugl.: München, Univ., Habil.-Schr., 1996-1997.

Lorenz, *Stephan* / *Riehm*, *Thomas*, Lehrbuch zum neuen Schuldrecht, München 2002.

Lüke, *Wolfgang*, Zivilprozessrecht, 10. Aufl., München 2011.

Mankowski, *Peter*, Anmerkung zu *AG Erfurt*, Urteil vom 14.9.2001 – 28 C 2534/00, EWiR 2001, S. 1123-1124.

– Wie problematisch ist die Identität des Erklärenden bei E-Mails wirklich?, NJW 2002, S. 2822-2827.

– Für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mails, CR 2003, S. 44-50.

– Anmerkung zu *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03, MMR 2004, S. 181-183.

– Anmerkung zu *BGH*, Urteil v. 16. 3. 2006, III ZR 152/05 (R-Gespräch), MMR 2006, S. 458-461.

– Anmerkung zu *LG Aachen*, Urteil v. 15. 12. 2006, 5 S 184/06, CR 2007, S. 606-607.

– Anmerkung zu *AG Mitte*, Urteil v. 07.08.2009, 15 C 423/08, MMR 2009, S. 784-785.

– Wegfall der Vergütungspflicht – Die begrenzte Reichweite des § 51i Abs. 4 TKG, MMR 2009, S. 808-813.

– BGH: Keine Anscheinsvollmacht aufgrund mangelnder Sicherung von eBay-Zugangsdaten, CR 2011, S. 458-459.

Mantz, *Reto*, Haftung für kompromittierte Computersysteme – § 823 Abs. 1 BGB und Gefahren aus dem Internet, K&R 2007, S. 566-572.

– Rechtsfragen offener Netze, Karlsruhe 2008, Zugl.: Freiburg (Breisgau), Univ., Diss., 2008, *zitiert als*: *Mantz*, offene Netze.

Marberth-Kubicki, *Annette*, Computer- und Internetstrafrecht, 2. Aufl., München 2010.

Meder, *Stephan*, Die Kreditkartenzahlung im Internet und Mail-Order-Verfahren, WM 2002, S. 1993-1998.

Meder, *Stephan* / *Grabe*, *Olaf*, PayPal – Die „Internet-Währung" der Zukunft?, BKR 2005, S. 467-477.

Medicus, *Dieter*, Allgemeiner Teil des BGB, 10. Aufl., Heidelberg 2010.

Medicus, *Dieter* / *Lorenz*, *Stephan*, Schuldrecht I – Allgemeiner Teil, 20. Aufl., München 2012.

Meyer, *Herbert*, Handelsregistererklärungen und Widerruf der Prokura, ZHR 81 (1918), S. 365-425.

Meyer, *Julia*, Einbeziehung und Geltungsbereich von AGB, in: *Borges*, *Georg* (Hrsg.), Rechtsfragen der Internet-Auktion, Baden-Baden 2007, S. 26-45, *zitiert als*: *J. Meyer*, in: Internet-Auktion.

Meyer, *Julia*, Identität und virtuelle Identität natürlicher Personen im Internet, Baden-Baden 2011, Zugl.: Bochum, Univ., Diss., 2009, *zitiert als*: *J. Meyer*, Identität.

Möller, *Mirko*, Rechtsfragen im Zusammenhang mit dem Postident-Verfahren, NJW 2005, S. 1601-1604.

Moore, *Gordon E.*, Cramming more components onto integrated circuits, Electronics 8/38 (1965), S. 114-117.

Moritz, *Hans-Werner* / *Dreier*, *Thomas (Hrsg.)*, Rechts-Handbuch zum E-Commerce, 2. Aufl., Köln 2005, *zitiert als: Bearbeiter,* in: *Moritz/Dreier*[2].

Motive zu dem Entwurfe eines Bürgerlichen Gesetzbuchs, Bd. 1, Berlin 1888.

Mugdan, *Benno*, Die gesammten Materialien zum Bürgerlichen Gesetzbuch für das Deutsche Reich – Einführungsgesetz und Allgemeiner Theil, Bd. 1, Berlin 1899.

Mühlenbrock, *Tobias* / *Dienstbach*, *Paul*, Anmerkung zu *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08, MMR 2008, S. 630-631.

Mülbert, *Peter O.*, Was Kreditinstitute für erforderlich halten dürfen – Risikoverteilung zwischen Kreditinstitut und Kunde bei Zahlungen an betrügerische Dritte, in: *Heldrich*, *Andreas* / *Prölss*, *Jürgen* / *Koler*, *Ingo* (Hrsg.), Festschrift für Claus-Wilhelm Canaris zum 70. Geburtstag, Bd. 2, München 2007, S. 271-297, *zitiert als*: *Mülbert*, in: FS Canaris, Bd. 2.

Müller, *Gerd*, Zu den Grenzen der analogen Anwendbarkeit des § 172 BGB in den Fällen des Blankettmißbrauchs und den sich daraus ergebenden Rechtsfolgen, AcP 181 (1981), S. 515-544.

Müller, *Wolf* / *Redlich*, *Jens-Peter* / *Jeschke*, *Mathias*, Auth[2](nPA) – Starke Authentifizierung mit nPA für jedermann, DuD 2011, S. 465-470.

Münch, *Joachim*, Rechtliche Probleme bei Electronic Banking, NJW-CoR 4/1989, S. 7-10.

Münch, *Stefan*, Der Schutz vor Verletzungen der Persönlichkeitsrechte in den neuen Medien, Frankfurt am Main 2004, Zugl.: Tübingen, Univ., Diss., 2004.

Musielak, *Hans-Joachim*, Die Grundlagen der Beweislast im Zivilprozeß, Berlin 1975, Zugl.: Köln, Univ., Habil.-Schr., 1972, *zitiert als*: *Musielak*, Grundlagen.

– Hilfen bei Beweisschwierigkeiten im Zivilprozeß, in: *Schmidt*, *Karsten* (Hrsg.), 50 Jahre Bundesgerichtshof – Festgabe aus der Wissenschaft, Bd. 3, 2000, S. 193-225, *zitiert als*: *Musielak*, in: FG 50 Jahre BGH, Bd. 3.
– Bürgerliches Recht: Probleme der Rechtsscheinhaftung, JuS 2004, S. 1081-1084.
– Zur Sachverhaltsklärung im Zivilprozess – unter besonderer Berücksichtigung der in jüngerer Zeit geschaffenen gesetzlichen Regelungen, in: *Greger*, *Reinhard* / *Gleussner*, *Irmgard* / *Heinemann*, *Jörn* (Hrsg.), Neue Wege zum Recht – Festgabe für Max Vollkommer, Köln 2006, S. 237-255, *zitiert als*: *Musielak*, in: FG Vollkommer.
– Die sog. tatsächliche Vermutung, JA 2010, S. 561-566.
– Grundkurs ZPO, 11. Aufl., München 2012, *zitiert als*: *Musielak*, Grundkurs[11].
– *(Hrsg.)*, Kommentar zur Zivilprozessordnung: ZPO Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz, 10. Aufl., München 2013, *zitiert als: Bearbeiter,* in: *Musielak*[10].

Neuner, *Jörg*, Der Redlichkeitsschutz bei abhandengekommenen Sachen, JuS 2007, S. 401-411.

Noack, *Ulrich* / *Kremer*, *Sascha*, Online-Auktionen: „eBay-Recht" als Herausforderung für den Anwalt?, AnwBl 2004, S. 602-606.

Oechsler, *Jürgen*, Die Bedeutung des § 172 Abs. 1 BGB beim Handeln unter fremdem Namen im Internet, AcP 208 (2008), S. 565-583.
– Die Haftung nach § 675v BGB im kreditkartengestützten Mailorderverfahren, WM 2010, S. 1381-1387.
– Haftung beim Missbrauch eines eBay-Mitgliedskontos, MMR 2011, S. 631-633.
Oertmann, *Paul*, Grundsätzliches zur Lehre vom Rechtsschein, ZHR 95 (1930), S. 443-485.
Olshausen, *Eberhard von*, Der Rechtsschein im Dreipersonenverhältnis, in: *Wackerbarth*, *Ulrich* / *Vormbaum*, *Thomas* / *Marutschke*, *Hans-Peter* (Hrsg.), Festschrift für Ulrich Eisenhardt zum 70. Geburtstag, München 2007, S. 277-299, *zitiert als*: *v. Olshausen*, in: FS Eisenhardt.
Ott, *Claus*, Vorvertragliche Aufklärungspflichten im Recht des Güter- und Leistungsaustausches, in: *Schäfer*, *Hans-Bernd* / *Ott*, *Claus* (Hrsg.), Ökonomische Probleme des Zivilrechts – Beiträge zum 2. Travemünder Symposium zur ökonomischen Analyse des Rechts, Berlin 1991, S. 142-162, *zitiert als*: *C. Ott*, in: Ökonomische Probleme.
Ott, *Stephan*, Urheber- und wettbewerbsrechtliche Probleme von Linking und Framing, Stuttgart 2004, Zugl.: Bayreuth, Univ., Diss., 2003.

Paefgen, *Christian*, Bildschrimtext aus zivilrechtlicher Sicht – Die elektronische Anbahnung und Abwicklung von Verträgen, Weinheim 1988, *zitiert als*: *Paefgen*, Bildschrimtext.
– Rechtsscheinhaftung im Btx-Dienst, CR 1993, S. 559-563.
Palandt, *Otto (Begr.)*, Beck'scher Kurzkommentar: Bürgerliches Gesetzbuch, 73. Aufl., München 2014, *zitiert als: Bearbeiter,* in: *Palandt*[73].
Paulus, *Christoph G.*, Zivilprozessrecht, 4. Aufl., Berlin 2010.
Pawlowski, *Hans-Martin*, Anmerkung zu *BGH*, Urteil v. 29. 2. 1996, IX ZR 153/95, JZ 1997, S. 309-312.
– Methodenlehre für Juristen, 3. Aufl., Heidelberg 1999, *zitiert als*: *Pawlowski*, Methodenlehre[3].
– Allgemeiner Teil des BGB, 7. Aufl., Heidelberg 2003, *zitiert als*: *Pawlowski*, BGB AT[7].
PayPal, PayPal-Datenschutzgrundsätze*, abrufbar unter*: https://cms.paypal.com/cms_content/DE/de_DE/files/ua/DE_Privacy_012412.pdf (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *PayPal*, Datenschutzgrundsätze.
– PayPal-Käuferschutzrichtlinie*, abrufbar unter*: https://cms.paypal.com/cms_content/DE/de_DE/files/ua/buyerprotection.pdf (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *PayPal*, Käuferschutzrichtlinie.
– PayPal-Nutzungsbedingungen*, abrufbar unter*: https://cms.paypal.com/cms_content/DE/de_DE/files/ua/ua.pdf (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *PayPal*, Nutzungsbedingungen.

PayPal, PayPal-Verkäuferschutzrichtlinie, *abrufbar unter*: https://cms.paypal.com/cms_content/DE/de_DE/files/ua/sellerprotection.pdf (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *PayPal*, Verkäuferschutzrichtlinie.

Peters, *Frank*, Zur Geltungsgrundlage der Anscheinsvollmacht, AcP 179 (1979), S. 214-244.

Pfeiffer, *Gerd (Hrsg.)*, Strafprozessordnung, 5. Aufl., München 2005, *zitiert als: Bearbeiter,* in: *Pfeiffer*[5].

Pierrot, *Oliver*, Hacker, Computerviren, in: *Ernst*, *Stefan* (Hrsg.), Hacker, Cracker & Computerviren, Köln 2004, *zitiert als*: *Pierrot*, in: *Ernst*.

Piper, *Henning* / *Ohly*, *Ansgar* / *Sosnitza*, *Olaf (Hrsg.)*, Gesetz gegen den unlateren Wettbewerb – Kommentar, 5. Aufl., München 2010, *zitiert als: Bearbeiter,* in: *Piper/Ohly/Sosnitza*[5].

Pohlmann, *Norbert*, Bedrohungen und Herausforderungen des E-Mail-Dienstes, DuD 2010, S. 607-613.

Polenz, *Sven*, Der neue elektronische Personalausweis E-Government im Scheckkartenformat, MMR 2010, S. 671-676.

Popp, *Andreas*, Von „Datendieben" und „Betrügern" – Zur Strafbarkeit des so genannten „phishing", NJW 2004, S. 3517-3518.

– „Phishing", „Pharming" und das Strafrecht, MMR 2006, S. 84-86.

– Die „Staatstrojaner"-Affäre: (Auch) ein Thema für den Datenschutz Kurzer Überblick aus strafprozessualer und datenschutzrechtlicher Sicht, ZD 2012, S. 51-55.

Posner, *Richard A.*, Economic analysis of law, 8. Aufl., Austin 2011.

Probandt, *Wolfgang jr.*, Zivilrechtliche Probleme des Bildschirmtextes, UFITA 98 (1984), S. 9-29.

Projektgruppe verfassungsverträgliche Technikgestaltung (provet) / *Gesellschaft für Mathematik und Datenverarbeitung mbH, mittlerweile GMD-Forschungszentrum Informationstechnik GmbH (GMD)*, Die Simulationsstudie Rechtspflege – eine neue Methode zur Technikgestaltung für Telekooperation, Berlin 1994.

Prütting, *Hanns*, Gegenwartsprobleme der Beweislast – eine Untersuchung moderner Beweislasttheorien und ihrer Anwendung insbesondere im Arbeitsrecht, München 1983, Zugl.: Erlangen-Nürnberg, Univ., Habil.-Schr., 1981, *zitiert als*: *Prütting*, Gegenwartsprobleme.

Prütting, *Hanns* / *Gehrlein*, *Markus (Hrsg.)*, ZPO Kommentar, 5. Aufl., Köln 2013, *zitiert als: Bearbeiter,* in: *Prütting/Gehrlein*[5].

Prütting, *Hanns* / *Wegen*, *Gerhard* / *Weinreich*, *Gerd (Hrsg.)*, BGB Kommentar, 8. Aufl., Köln 2013, *zitiert als: Bearbeiter,* in: *Prütting/Wegen/Weinreich*[8].

Quiring-Kock, *Gisela*, Entwurf EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, DuD 2013, S. 20-24.

Rademacher, *Lukas*, § 675u BGB: Einschränkung des Verkehrsschutzes im Überweisungsrecht?, NJW 2011, S. 2169-2172.

Rauscher, *Thomas* / *Wax*, *Peter* / *Wenzel*, *Joachim (Hrsg.)*, Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen, Bd. 2, §§ 355-1024, 4. Aufl., München 2012, *zitiert als: Bearbeiter,* in: MüKo-ZPO[4].

Rauscher, *Thomas* / *Wax*, *Peter* / *Wenzel*, *Joachim (Hrsg.)*, Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen, Bd. 1, §§ 1 354, 4. Aufl., München 2013, *zitiert als: Bearbeiter,* in: MüKo-ZPO[4].

Recknagel, *Einar*, Vertrag und Haftung beim Internet-Banking, München 2005, Zugl.: Göttingen, Univ., Diss., 2004.

Redeker, *Helmut*, Geschäftsabwicklung mit externen Rechnern im Bildschirmtextdienst, NJW 1984, S. 2390-2394.

– IT-Recht, 5. Aufl., München 2012, *zitiert als*: *Redeker*, IT-Recht[5].

Reese, *Nicole*, Vertrauenshaftung und Risikoverteilung bei qualifizierten elektronischen Signaturen, Köln 2006, Zugl.: Osnabrück, Univ., Diss., 2006.

Reichsgerichtsräte-Kommentar (Hrsg.), Das Bürgerliche Gesetzbuch mit besonderer Berücksichtigung der Rechtsprechung des Reichsgerichts und des Bundesgerichtshofes, Bd. 1, §§ 1-240, 12. Aufl., Berlin 1982, *zitiert als: Bearbeiter,* in: RGRK[12].

Reinicke, *Dietrich* / *Tiedtke*, *Klaus*, Die Haftung des Blankettgebers aus dem abredewidrig ausgefüllten Blankett im bürgerlichen Recht, JZ 1984, S. 550-554.

Reisen, *Andreas*, Digitale Identität im Scheckkartenformat – Datenschutzvorkehrungen für den elektronischen Personalausweis, DuD 2008, S. 164-167.

Rieder, *Markus S.*, Die Rechtsscheinhaftung im elektronischen Geschäftsverkehr, Berlin 2004, Zugl.: München, Univ., Diss., 2003.

Riehm, *Thomas*, Abwägungsentscheidungen in der praktischen Rechtsanwendung, München 2006, Zugl.: München, Univ., Diss., 2006, *zitiert als*: *Riehm*, Abwägungsentscheidungen.

– Die überschießende Umsetzung vollharmonisierender EG-Richtlinien im Privatrecht, JZ 2006, S. 1035-1045.

– Pflichtverletzung und Vertretenmüssen – Zur Dogmatik der §§ 280ff. BGB, in: *Heldrich*, *Andreas* / *Prölss*, *Jürgen* / *Koler*, *Ingo* (Hrsg.), Festschrift für Claus-Wilhelm Canaris zum 70. Geburtstag, Bd. 1, München 2007, S. 1079-1103, *zitiert als*: *Riehm*, in: FS Canaris, Bd. 1.

– Gesetzliche Schuldverhältnisse, in: *Langenbucher*, *Katja* (Hrsg.), Europäisches Privat- und Wirtschaftsrecht, 3. Aufl., Baden-Baden 2013, *zitiert als*: *Riehm*, in: Europäisches Privatrecht[3].

Ries, *Uli*, Account-Klau bei Skype leichtgemacht, in: heise online v. 14. 11. 2012*, abrufbar unter*: http://heise.de/-1749875 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Ries*, heise online v. 14. 11. 2012.

Riesenhuber, *Karl*, Die Rechtsbeziehungen zwischen Nebenparteien – dargestellt anhand der Rechtsbeziehungen zwischen Mietnachbarn und zwischen Arbeitskollegen, Berlin 1997, Zugl.: Potsdam, Univ., Diss., 1997, *zitiert als*: *Riesenhuber*, Nebenparteien.

– Die Rechtsbeziehungen zwischen Arbeitnehmern, JZ 1999, S. 711-718.

Rojas, *Raúl*, Mathematische Notbeatmung für das Mooresche Gesetz, in: Telepolis v. 4. 6. 2012*, abrufbar unter*: http://www.heise.de/tp/artikel/36/36996/1.html (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Rojas*, Telepolis v. 4. 6. 2012.

Romain, *Alfred* / *Bader*, *Hans Anton* / *Byrd*, *B. Sharon*, Wörterbuch der Rechts- und Wirtschaftssprache, 5. Aufl., Bd. 1, München 2000.

Rose, *Edgar*, De-Mail-Gesetz in Kraft: Sicherheitsgewinn in der elektronischen Kommunikation, K&R 2011, S. 439-445.

Rosenberg, *Leo*, Die Beweislast auf der Grundlage des Bürgerlichen Gesetzbuchs und der Zivilprozessordnung, 5. Aufl., München 1965.

Rosenberg, *Leo* / *Schwab*, *Karl Heinz* / *Gottwald*, *Peter*, Zivilprozessrecht, 17. Aufl., München 2010.

Rossa, *Caroline Beatrix*, Mißbrauch beim electronic cash, CR 2007, S. 138-147.

Rössel, *Markus*, BGH: Haftung für ein eBay-Mitgliedskonto – Halzband, CR 2009, S. 453-455.

Roßnagel, *Alexander*, Die Sicherheitsvermutung des Signaturgesetzes, NJW 1998, S. 3312-3320.

– Auf dem Weg zu neuen Signaturregelungen – Drei Novellierungsentwürfe für SigG, BGB und ZPO, MMR 2000, S. 451-461.
– Rechtliche Unterschiede von Signaturverfahren, MMR 2002, S. 215-222.
– Weltweites Internet – globale Rechtsordnung?, MMR 2002, S. 67-71.
– Die fortgeschrittene elektronische Signatur, MMR 2003, S. 164-170.
– Kommentar zu OLG Köln, Urteil v. 6. September 2002 – 19 U 16/02, K&R 2003, S. 84-86.
– Qualifizierte elektronische Signatur mit Einschränkungen für das Besteuerungsverfahren, K&R 2003, S. 379-385.
– Elektronische Signaturen mit der Bankkarte? – Das Erste Gesetz zur Änderung des Signaturgesetzes, NJW 2005, S. 385-388.
– Fremdsignierung elektronischer Rechnungen: Vorsteuerabzug gefährdet, BB 2007, S. 1233-1237.
– Fremderzeugung von qualifizierten Signaturen? Ein neues Geschäftsmodell und seine Rechtsfolgen, MMR 2008, S. 22-28.
– Grundlage für mehr Rechtssicherheit im Internet, NJW 2011, S. 1473-1478.
– Rechtsregeln für einen sicheren elektronischen Rechtsverkehr – Zum Regierungsentwurf für ein De-Mail-Gesetz, CR 2011, S. 23-30.
– Rechtsetzung zu Sicherheitsdiensten: Europäisierung ja, Monopolisierung nein!, MMR 2012, S. 781-782.

Roßnagel, *Alexander* / *Fischer-Dieskau*, *Stefanie*, Automatisiert erzeugte elektronische Signaturen, MMR 2004, S. 133-139.

– Elektronische Dokumente als Beweismittel – Neufassung der Beweisregelungen durch das Justizkommunikationsgesetz, NJW 2006, S. 806-808.

Roßnagel, *Alexander* / *Hornung*, *Gerrit*, Ein Ausweis für das Internet – Der neue Personalausweis enthält einen „elektronischen Identitätsnachweis“, DÖV 2009, S. 301-306.

Roßnagel, *Alexander* / *Hornung*, *Gerrit* / *Knopp*, *Michael* / *Wilke*, *Daniel*, De-Mail und Bürgerportale – Eine Infrastruktur für Kommunikationssicherheit, DuD 2009, S. 728-734.

Roßnagel, *Alexander* / *Hornung*, *Gerrit* / *Schnabel*, *Christoph*, Die Authentisierungsfunktion des elektornischen Personalausweises aus datenschutzrechtlicher Sichet, DuD 2008, S. 168-172.

Roßnagel, *Alexander* / *Johannes*, *Paul C.*, Entwurf einer EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, ZD 2013, S. 65-72.

Roßnagel, *Alexander* / *Pfitzmann*, *Andreas*, Der Beweiswert von E-Mail, NJW 2003, S. 1209-1214.

Roßnagel, *Alexander* / *Scholz*, *Philip*, Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, S. 721-731.

Rüthers, *Bernd* / *Stadler*, *Astrid*, Allgemeiner Teil des BGB, 17. Aufl., München 2011.

Säcker, *Franz Jürgen* / *Rixecker*, *Roland (Hrsg.)*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 1, Allgemeiner Teil, §§ 1-240, ProstG, AGG, 6. Aufl., München 2012, *zitiert als: Bearbeiter,* in: MüKo-BGB[6].
– *(Hrsg.)*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 2, Schuldrecht – Allgemeiner Teil, §§ 241-432, 6. Aufl., München 2012, *zitiert als: Bearbeiter,* in: MüKo-BGB[6].
– *(Hrsg.)*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 4, Schuldrecht, Besonderer Teil II, §§ 611-704 – EFZG, TzBfG, KSchG, 6. Aufl., München 2012, *zitiert als: Bearbeiter,* in: MüKo-BGB[6].
– *(Hrsg.)*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 6, Sachenrecht, §§ 854-1296, WEG, ErbauRG, 6. Aufl., München 2013, *zitiert als: Bearbeiter,* in: MüKo-BGB[6].
– *(Hrsg.)*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 6, Schuldrecht, Besonderer Teil III, §§ 705-853, Partnerschaftsgesellschaftsgesetz, Produkthaftungsgesetz, 6. Aufl., München 2013, *zitiert als: Bearbeiter,* in: MüKo-BGB[6].
– *(Hrsg.)*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 9, Erbrecht, §§ 1922-2385, §§ 27-35 BeurkG, 6. Aufl., München 2013, *zitiert als: Bearbeiter,* in: MüKo-BGB[6].
Sander, *Stefan*, E-Mails und die Beweisführung im Prozess, CR 2014, S. 292-299.
Sanner, *Markus*, Die digitale Signatur, Regensburg 2001, Zugl.: Regensburg, Univ., Diss., 2001.
Schack, *Haimo*, BGB – Allgemeiner Teil, 14. Aufl., Heidelberg 2013.
Schäfer, *Hans-Bernd*, Ökonomische Analyse von Aufklärungspflichten, in: *Schäfer*, *Hans-Bernd* / *Ott*, *Claus* (Hrsg.), Ökonomische Probleme des Zivilrechts – Beiträge zum 2. Travemünder Symposium zur ökonomischen Analyse des Rechts, Berlin 1991, S. 117-141, *zitiert als*: *Schäfer*, in: Ökonomische Probleme.
Schäfer, *Hans-Bernd* / *Ott*, *Claus*, Lehrbuch der ökonomischen Analyse des Zivilrechts, 5. Aufl., Berlin 2012.
Schapiro, *Leo*, Unterlassungsansprüche gegen die Betreiber von Internet-Auktionshäusern und Internet-Meinungsforen, Tübingen 2011, Zugl.: Berlin, Freie-Univ., Diss., 2010.
Scheibengruber, *Christian*, Zur Zulässigkeit und Sinnhaftigkeit der Verlagerung des Missbrauchrisikos bei Zahlungsdiensten auf die Nutzer – Ein Beitrag zur Analyse der Umsetzung der Zahlungsdiensterichtlinie in das BGB und die AGB der Banken, BKR 2010, S. 15-23.
Schellhammer, *Kurt*, Zivilprozess, 14. Aufl., Heidelberg 2012.
Schemmann, *Till*, Die Beweiswirkung elektronischer Signaturen und die Kodifizierung des Anscheinsbeweises in § 371 a Abs. 1 Satz 2 ZPO, ZZP 118 (2005), S. 161-183.
Schepple, *Kim Lane*, Legal Secrets – Equality and Efficiency in the Common Law, Chicago 1988.
Scheurle, *Klaus-Dieter* / *Mayen*, *Thomas (Hrsg.)*, Telekommunikationsgesetz – Kommentar, 2. Aufl., München 2008, *zitiert als: Bearbeiter,* in: *Scheurle/Mayen*[2].
Schilken, *Eberhard*, Zivilprozessrecht, 6. Aufl., München 2010, *zitiert als*: *Schilken*, Zivilprozessrecht[6].
Schimansky, *Herbert* / *Bunte*, *Hermann-Josef* / *Lwowski*, *Hans-Jürgen (Hrsg.)*, Bankrechts-Handbuch, Bd. 1, Allgemeine Grundlagen, Bargeldloser Zahlungsverkehr, 4. Aufl., München 2011, *zitiert als: Bearbeiter,* in: *Schimansky/Bunte/Lwowski*[4].

Schimmer, *Klaus*, Wenn der Hacker zweimal fragt! – Wie bereite ich meine Mitarbeiter auf Social Engineering Angriffe vor, DuD 2008, S. 569-573.

Schinkels, *Boris*, Die Verteilung des Haftungsrisikos für Drittmissbrauch von Medien des bargeldlosen Zahlungsverkehrs – eine Betrachtung von Scheck, Kreditkarte, Debetkarte und Geldkarte, Berlin 2001, Zugl.: Bielefeld, Univ., Diss., 2000-2001, *zitiert als*: *Schinkels*, Bargeldloser Zahlungsverkehr.

– Rechtsscheinszurechnung des Handelns unter fremder eBay-Nutzerkennung (Account-Missbrauch), LMK 2011, 320461.

Schlegel, *Ralf Oliver*, R-Gespräche – Haftung der Eltern für Minderjährige, MDR 2006, S. 1021-1024.

Schmidt, *Jürgen*, So arbeiten moderne Schädlinge, c't 2/2007, S. 86.

– BaBaBanküberfall, c't 22/2010, S. 42.

– Facebook mit 2-Faktor-Login und weiteren Sicherheitsverbesserungen, in: heise online v. 13. 5. 2011*, abrufbar unter*: http://heise.de/-1242500 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *J. Schmidt*, heise online v. 13. 5. 2011.

– Google führt 2-Faktor-Authentifizierung ein, in: heise online v. 11. 2. 2011*, abrufbar unter*: http://heise.de/-1187971 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *J. Schmidt*, heise online v. 11. 2. 2011.

– Sicherheit: mangelhaft, c't 4/2011, S. 35.

Schmidt, *Karsten*, Handelsrecht, 5. Aufl., Köln 1999, *zitiert als*: *K. Schmidt*, Handelsrecht[5].

– Gesellschaftsrecht, 4. Aufl., Köln 2002, *zitiert als*: *K. Schmidt*, Gesellschaftsrecht[4].

Schnarz, *Pierre* / *Seeger*, *Mark M.*, Bürgerbefragung zur IT-Sicherheit im Endanwenderbereich, DuD 2012, S. 253-257.

Schneier, *Bruce*, Secrets and Lies – Digital Security in a Networked World, Indianapolis 2004.

Schnell, *Daniel*, Signaturmissbrauch und Rechtsscheinhaftung, Berlin 2007, Zugl.: München, Univ., Diss., 2006.

Scholz, *Philip*, Datenschutz beim Internet-Einkauf, Baden-Baden 2003, Zugl.: Kassel, Univ., Diss., 2002.

Schöttle, *Hendrik*, Zahlungsmittel im elektronischen Geschäftsverkehr, K&R 2007, S. 183-187.

Schricker, *Gerhard* / *Loewenheim*, *Ulrich (Hrsg.)*, Urheberrecht Kommentar, 4. Aufl., München 2010, *zitiert als: Bearbeiter,* in: *Schricker/Loewenheim*[4].

Schulte am Hülse, *Ulrich* / *Klabunde*, *Sebastian*, Abgreifen von Bankzugangsdaten im Onlinebanking, Vorgehensweise der Täter und neuezivilrechtliche Haftungsfragen des BGB, MMR 2010, S. 84-90.

Schulte am Hülse, *Ulrich* / *Welchering*, *Peter*, Der Anscheinsbeweis bei missbräuchlicher Bargeldabhebung an Geldautomaten mit Karte und Geheimzahl, NJW 2012, S. 1262-1266.

Schulz, *Sönke E.*, Der neue „E-Personalausweis" — elektronische Identitätsnachweise als Motor des E-Government, E-Commerce und des technikgestützten Identitätsmanagement?, CR 2009, S. 267-272.

– Rechtsprobleme des Identitätsmanagements, DuD 2009, S. 601-606.

Schulz, *Sönke E.* / *Bosesky*, *Pino* / *Hoffmann*, *Christian*, Datenhoheit im Cloud-Umfeld, DuD 2013, S. 95-100.

Schumacher, *Astrid*, Akkreditierung und Zertifizierung von De-Mail-Diensteanbietern, DuD 2010, S. 302-307.

Schuster, *Johannes*, Notiz-Dienst Evernote wurde gehackt, in: heise online v. 3. 3. 2013, *abrufbar unter*: http://heise.de/-1815222 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *J. Schuster*, heise online v. 3. 3. 2013.

Schwenk, *Jörg*, Sicherheit und Kryptographie im Internet – Von sicherer E-Mail bis zu IP-Verschlüsselung, 3. Aufl., Wiesbaden 2010.

Schwenk, *Jörg* / *Gajek*, *Sebastian*, Technische Probleme und Risiken der Internet-Auktion, in: *Borges*, *Georg* (Hrsg.), Rechtsfragen der Internet-Auktion, Baden-Baden 2007, S. 180-189, *zitiert als*: *Schwenk*/*Gajek*, in: Internet-Auktion.

Schwenk, *Jörg* / *Gajek*, *Sebastian* / *Wegener*, *Christoph*, Identitätsmissbrauch im Onlinebanking, DuD 2005, S. 639-642.

Schwintowski, *Hans-Peter*, Bankrecht, 3. Aufl., München 2011.

Selter, *Wolfgang*, Die Entstehung und Entwicklung des Rechtsscheinprinzips im deutschen Zivilrecht, Hamburg 2006, Zugl.: Bonn, Univ., Diss., 2005-2006.

Sester, *Peter*, Vertragsabschluss bei Internet-Auktionen, CR 2001, S. 98-108.

Sieber, *Ulrich*, Gutachten C zum 69. Deutschen Juristentag – Straftaten und Strafverfolgung im Internet, München 2012, *zitiert als*: *Sieber*, Gutachten zum 69. DJT.

Siegel, *Julius*, Die Blanketterklärung – Ihre juristische Konstruktion und ihre Behandlung nach dem materiellen Recht und dem Prozeßrecht, München 1908, Zugl.: München, Univ., Diss., 1908, *zitiert als*: *Siegel*, Blanketterklärung.

– Die privatrechtliche Funktion der Urkunde, AcP 111 (1914), S. 1-134.

Singer, *Reinhard*, Geltungsgrund und Rechtsfolgen der fehlerhaften Willenserklärung, JZ 1989, S. 1030-1035.

– Rezension zu Thomas Lobinger, Rechtsgeschäftliche Verpflichtung und autonome Bindung. AcP 201 (2001), S. 93-101.

Skistims, *Hendrik* / *Roßnagel*, *Alexander*, Rechtlicher Schutz vor Staatstrojanern? – Verfassungsrechtliche Analyse einer Regierungs-Malware, ZD 2012, S. 3-7.

Sodtalbers, *Axel*, Softwarehaftung im Internet, Frankfurt am Main 2006, Zugl.: Göttingen, Univ., Diss., 2005.

Soergel, *Hans Theodor (Begr.)*, Kohlhammer-Kommentar – Bürgerliches Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Bd. 2, Allgemeiner Teil 2, §§ 104-240, 13. Aufl., Stuttgart 1999, *zitiert als: Bearbeiter,* in: *Soergel*[13].

Sonnentag, *Michael*, Vertragliche Haftung bei Handeln unter fremdem Namen im Internet, WM 2012, S. 1614-1620.

Sosnitza, *Olaf* / *Gey*, *Michael*, Zum Beweiswert von E-Mails – Technische Hintergründe und rechtliche Konsequenzen, K&R 2004, S. 465-469.

Spiegelhalder, *Torsten*, Rechtsscheinhaftung im Stellvertretungsrecht bei der Verwendung elektronischer Signaturen, Hamburg 2007, Zugl.: Kiel, Univ., Diss., 2006.

Spindler, *Gerald*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären – Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler, Universität Göttingen*, abrufbar unter*: https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30962/Gutachten_pdf.pdf (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Spindler*, BSI-Studie.

– Vertragsschluss und Inhaltskontrolle bei Internet-Auktionen, ZIP 2001, S. 809-819.

– Authentifizierungssysteme – Datenschutz- und sicherheitsrechtliche Anforderungen sowie zivilrechtliche Auswirkungen, CR 2003, S. 534-541.

Spindler, *Gerald*, Vertragliche Haftung und Pflichten des Martkplatzbetreibers und der Marktteilnehmer, in: *Spindler*, *Gerald* / *Wiebe*, *Andreas* (Hrsg.), Internet-Auktionen und Elektronische Marktplätze, 2. Aufl., Köln 2005, S. 125-210, *zitiert als*: *Spindler*, in: Internet-Auktionen[2].

– IT-Sicherheit – Rechtliche Defizite und rechtspolitische Alternativen, MMR 2008, S. 7-13.

– Internet-Banking und Haftungsverteilung zwischen Bank und Kunden, in: *Habersack*, *Mathias* / *Joeres*, *Hans-Ulrich* / *Krämer*, *Achim* (Hrsg.), Entwicklungslinien im Bank- und Kapitalmarktrecht – Festschrift für Gerd Nobbe, Köln 2009, S. 215-235, *zitiert als*: *Spindler*, in: FS Nobbe.

– Das De-Mail-Gesetz – ein weiterer Schritt zum sicheren E-Commerce, CR 2011, S. 309-319.

– Präzisierungen der Störerhaftung im Internet – Besprechung des BGH-Urteils „Kinderhochstühle im Internet", GRUR 2011, S. 101-108.

Spindler, *Gerald* / *Rockenbauch*, *Matti*, Die elektronische Identifizierung – Kritische Analyse des EU-Verordnungsentwurfs über elektronische Identifizierung und Vertrauensdienste, MMR 2013, S. 139-148.

Spindler, *Gerald* / *Schuster*, *Fabian (Hrsg.)*, Recht der elektronischen Medien, 2. Aufl., München 2011, *zitiert als: Bearbeiter,* in: *Spindler/F. Schuster*[2].

Spindler, *Gerald* / *Volkmann*, *Christian*, Die zivilrechtliche Störerhaftung der Internet-Provider, WRP 2003, S. 1-15.

Stach, *Heike*, Mit Bürgerportalen für einfach sichere, vertrauliche und verbindliche elektronische Kommunikation, DuD 2008, S. 184-188.

Stadler, *Astrid*, Der Zivilprozeß und neue Formen der Informationstechnik, ZZP 115 (2002), S. 413-444.

Stadler, *Thomas*, Haftung für Informationen im Internet, 2. Aufl., Berlin 2005, *zitiert als*: *T. Stadler*, Haftung für Informationen[2].

– Keine vertragliche Haftung bei missbräuchliher Nutzung eines eBay-Accounts, jurisPR-ITR 14/2011, Anm. 2.

Stang, *Felix* / *Hühner*, *Sebastian*, Störerhaftung des WLAN-Inhabers, GRUR 2010, S. 636-637.

Staudinger, *Julius von (Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführhungsgesetz und Nebengesetzen, Bd. 1, Allgemeiner Teil, 11. Aufl., Berlin 1957, *zitiert als: Bearbeiter,* in: *Staudinger*[11].

– *(Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführhungsgesetz und Nebengesetzen, Buch 1, Allgemeiner Teil 5, §§ 164-240, 13. Aufl., Berlin 2009, *zitiert als: Bearbeiter,* in: *Staudinger*[13].

– *(Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführhungsgesetz und Nebengesetzen, Buch 2, Recht der Schuldverhältnisse, Einleitung zum Schuldrecht; §§ 241-243 (Treu und Glauben), 13. Aufl., Berlin 2009, *zitiert als: Bearbeiter,* in: *Staudinger*[13].

– *(Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführhungsgesetz und Nebengesetzen, Buch 2, Recht der Schuldverhältnisse, §§ 328-345 (Vertrag zugunsten Dritter, Draufgabe, Vertragsstrafe), 13. Aufl., Berlin 2009, *zitiert als: Bearbeiter,* in: *Staudinger*[13].

Staudinger, *Julius von (Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 4, Familienrecht, §§ 1589-1600d (Abstammung), 13. Aufl., Berlin 2011, *zitiert als: Bearbeiter,* in: *Staudinger*[13].
– *(Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 1, Allgemeiner Teil 3, §§ 90-124; 130-133, 13. Aufl., Berlin 2012, *zitiert als: Bearbeiter,* in: *Staudinger*[13].
– *(Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 2, Recht der Schuldverhältnisse, §§ 675c-676c (Zahlungsdiensterecht), 13. Aufl., Berlin 2012, *zitiert als: Bearbeiter,* in: *Staudinger*[13].
– *(Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 2, Recht der Schuldverhältnisse, §§ 830 838 (Unerlaubte Handlungen 3), 13. Aufl., Berlin 2012, *zitiert als: Bearbeiter,* in: *Staudinger*[13].
– *(Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 2, Recht der gesetzlichen Schuldverhältnisse, §§ 311, 311a, 312, 312a-i (Vertragsschluss), 13. Aufl., Berlin 2013, *zitiert als: Bearbeiter,* in: *Staudinger*[13].
– *(Begr.)*, Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Buch 3, Sachenrecht, §§ 985-1011 (Eigentum 3), 13. Aufl., Berlin 2013, *zitiert als: Bearbeiter,* in: *Staudinger*[13].
Steckler, *Brunhilde*, Grundzüge des IT-Rechts – das Recht der Datenverarbeitung und der Online-Dienste, 3. Aufl., München 2011.
Stein, *Friedrich* / *Jonas*, *Martin (Hrsg.)*, Kommentar zur Zivilprozessordnung, Bd. 3, §§ 128-252, 22. Aufl., Tübingen 2005, *zitiert als: Bearbeiter,* in: *Stein/Jonas*[22].
– *(Hrsg.)*, Kommentar zur Zivilprozessordnung, Bd. 5, §§ 328-510b, 22. Aufl., Tübingen 2006, *zitiert als: Bearbeiter,* in: *Stein/Jonas*[22].
– *(Hrsg.)*, Kommentar zur Zivilprozessordnung, Bd. 4, §§ 253-327, 22. Aufl., Tübingen 2008, *zitiert als: Bearbeiter,* in: *Stein/Jonas*[22].
Stigler, *George J.*, The Economics of Information, The Journal of Political Economy 3/69 (1961), S. 213-225.
Stöber, *Michael*, Anmerkung zu Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung), EWiR 2011, S. 521-522.
– Die analoge Anwendung der §§ 171, 172 BGB am Beispiel der unbefugten Benutzung fremder Internet- und Telekommunikationszugänge, JR 2012, S. 225-231.
Stoll, *Heinrich*, Haftung aus Bescheinigung, AcP 135 (1932), S. 89-116.
Striepling, *Ingo*, Verbraucherschutz bei Online-Auktionen, Berlin 2011, Zugl.: Münster, Univ., Diss., 2010.
Ströbele, *Paul* / *Hacker*, *Franz (Hrsg.)*, Markengesetz Kommentar, 10. Aufl., Köln 2012, *zitiert als: Bearbeiter,* in: *Ströbele/Hacker*[10].
Stumpf, *Frederic* / *Sacher*, *Markus* / *Roßnagel*, *Alexander* / *Eckert*, *Claudia*, Erzeugung elektronischer Signaturen mittels Trusted Platform Module, DuD 2007, S. 357-361.
Süßenberger, *Christoph*, Das Rechtsgeschäft im Internet, Frankfurt am Main 2000, Zugl.: Frankfurt (Main), Univ., Diss., 2000.

Taeger, *Jürgen*, Außervertragliche Haftung für fehlerhafte Computerprogramme, Tübingen 2005, Zugl.: Hannover, Univ., Habil.-Schr., 1994.
Tanenbaum, *Andrew S.* / *Wetherall*, *David J.*, Computernetzwerke, 5. Aufl., München 2012.

Teuber, *Hanno* / *Melber*, *Michael*, „Online-Auktionen" — Pflichten der Anbieter durch das Fernabsatzrecht, MDR 2004, S. 185-190.

Thomas, *Heinz* / *Putzo*, *Hans (Hrsg.)*, Zivilprozessordnung, 34. Aufl., München 2013, *zitiert als: Bearbeiter,* in: *Thomas/Putzo*[34].

TNS Infratest, Wie lange schauen Sie am Tag Fernsehen und wie lange surfen Sie täglich im Internet?, zitiert nach de.statista.com *abrufbar unter*: http://de.statista.com/statistik/daten/studie/269898/umfrage/umfrage-zur-taeglichen-nutzungsdauer-von-tv-und-internet/ (zuletzt abgerufen am 14. 6. 2014).

Towfigh, *Emanuel Vahid* / *Petersen*, *Niels*, Ökonomische Methoden im Recht, Tübingen 2010.

Tuhr, *Andreas von*, Der Allgemeine Teil des Deutschen Bürgerlichen Rechts, Bd. II, 1, Berlin 1957.

Ufer, *Frederic*, Die Haftung der Internet Provider nach dem Telemediengesetz, Hamburg 2007, Zugl.: Köln, Univ., Diss., 2007.

Ultsch, *Michael L.*, Zivilrechtliche Probleme elektronischer Erklärungen – dargestellt am Beispiel der Electronic Mail, DZWir 1997, S. 466-473.

– Digitale Willenserklärungen und digitale Signaturen, in: *Immenhauser*, *Martin* / *Wichtermann*, *Jürg* (Hrsg.), Vernetzte Welt – gloables Recht. Jahrbuch Junger Zivilrechtswissenschaftler, Stuttgart 1998, S. 127-152, *zitiert als*: *Ultsch*, in: Vernetzte Welt – gloables Recht.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (*ULD*), Verkettung digitaler Identitäten*, abrufbar unter*: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *ULD*.

Ungern-Sternberg, *Joachim v.*, Die Rechtsprechung des Bundesgerichtshofs zum Urheberrecht und zu den verwandten Schutzrechten in den Jahres 2008 und 2009 (Teil II), GRUR 2010, S. 386-396.

van Gelder, *Alfons*, Phisher, Pharmer & Co. In: *Habersack*, *Mathias* / *Joeres*, *Hans-Ulrich* / *Krämer*, *Achim* (Hrsg.), Entwicklungslinien im Bank- und Kapitalmarktrecht – Festschrift für Gerd Nobbe, Köln 2009, S. 55-73, *zitiert als*: *van Gelder*, in: FS Nobbe.

van Look, *Frank*, Recht des Bankkontos, in: *Claussen*, *Carsten Peter* (Hrsg.), Bank- und Börsenrecht, 4. Aufl., München 2008, *zitiert als*: *van Look*, in: *Claussen*[4].

Verse, *Dirk A.* / *Gaschler*, *Andreas*, „Download to own" – Online-Geschäfte unter fremdem Namen, Jura 2009, S. 213-220.

Vogt, *Aegidius* / *Rayermann*, *Marcus*, Die Haftung des Mobiltelefon-Anschlussinhabers nach dem TKG – Anwendbarkeit des § 45i Abs. 4 TKG auf die Abrechnung mobiler Mehrwertdienste von Drittanbietern, MMR 2012, S. 207-211.

Volkmann, *Christian*, Der Störer im Internet, München 2005, Zugl.: Göttingen, Univ., Diss., 2004, *zitiert als*: *Volkmann*, Störer im Internet.

– Aktuelle Entwicklungen in der Providerhaftung im Jahr 2009, K&R 2010, S. 368-375.

Wagner, *Tobias* / *Zenger*, *Ralph*, Vertragsschluss bei eBay und Angebotsrücknahme – Besteht ein „Loslösungsrecht" vom Vertrag contra legem?, MMR 2013, S. 343-348.
Warnecke, *Thomas*, Das Bürgerportalgesetz – Vertrauliche Kommunikation im E-Government und E-Commerce?, MMR 2010, S. 227-232.
Wassermeyer, *Heinz*, Der prima facie Beweis und die benachbarten Erscheinungen, Münster 1954.
Weck, *Andreas*, Soviel ist ein Facebook-Fan wert [Studie], in: t3n v. 18. 4. 2013*, abrufbar unter*: http://t3n.de/news/facebook-fan-marke-458603/ (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Weck*, t3n v. 18. 4. 2013.
Wefel, *Sandro*, Hardware-Crypto-Token gestütztes Single Sign-On für zertifikatsbasierte Authentifizierung, Halle (Saale) 2009, Zugl.: Halle (Salle), Univ., Diss.
Weichert, *Thilo*, Biometrie – Freund oder Feind des Datenschutzes?, CR 1997, S. 369-376.
Weinschenk, Haftung bei ungeüngender Verwahrung von Vollmachtsurkunden, LZ 1931, S. 1310-1311.
Wellspacher, *Moriz*, Vertrauen auf äußere Tatbestände im Bürgerlichen Recht, Wien 1906.
Wenn, *Matthias*, AG Bremen: Vertragsstrafe für „Spaßbieter" bei Online-Auktion, CR 2006, S. 137-138.
Werner, *Dennis*, Anmerkung zu *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08, K&R 2008, S. 554-556.
– Verkehrspflichten privater IT-Nutzer in Bezug auf die Verbreitung von Schadsoftware, Baden-Baden 2010, Zugl.: Bochum, Univ., Diss., 2008/2009, *zitiert als*: *Dennis Werner*, Verkehrspflichten.
– Kommentar zu BGHZ 189, 346, K&R 2011, S. 499-501.
Werner, *Dennis* / *Wegener*, *Christoph*, Bürgerportale – Technische und rechtliche Hintergründe von DE-Mail und Co. CR 2009, S. 310-316.
Werner, *Stefan*, Beweislastverteilung und Haftungsrisiken im elektronischen Zahlungsverkehr, MMR 1998, S. 232-235.
Weßelmann, *Bettina*, Maßnahmen gegen Social Engineering – Traninung muss Awareness-Maßnahmen ergänzen, DuD 2008, S. 601-604.
Widmaier, *Gunter (Hrsg.)*, Münchener Anwalts-Handbuch Strafverteidigung, München 2006, *zitiert als: Bearbeiter,* in: *Widmaier*.
Wiebe, *Andreas*, Vertragsschluss bei Online-Auktionen, MMR 2000, S. 323-329.
– AG Erfurt: Nachweis der Authentizität bei Internettransaktionen, MMR 2002, S. 128-129.
– Anmerkung zu *BGH*, Urteil v. 7. 11. 2001, VIII ZR 13/01 (ricardo.de), CR 2002, S. 216-217.
– Die elektronische Willenserklärung, Tübingen 2002, Zugl.: Hannover, Univ., Habil.-Schr., 2001, *zitiert als*: *Wiebe*, Elektronische Willenserklärung.
– LG Bonn: Identität eines Teilnehmers an einer Internetauktion, MMR 2002, S. 257-258.
– Vertragsschluss und Verbraucherschutz, in: *Spindler*, *Gerald* / *Wiebe*, *Andreas* (Hrsg.), Internet-Auktionen und Elektronische Marktplätze, 2. Aufl., Köln 2005, S. 53-96, *zitiert als*: *Wiebe*, in: Internet-Auktionen[2].
Wien, *Andreas*, Internetrecht, 3. Aufl., Wiesbaden 2012.

Wikipedia, Anmelden / Benutzerkonto anlegen, *abrufbar unter*: http://de.wikipedia.org/wiki/Spezial:Anmelden/signup (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Wikipedia*, Anmelden.

– Über Wikipedia, *abrufbar unter*: http://de.wikipedia.org/wiki/Wikipedia:%C3%83%C2%9Cber_Wikipedia (zuletzt abgerufen am 14. 6. 2014).

Wilke, *Daniel* / *Jandt*, *Silke* / *Löwe*, *Jutta* / *Roßnagel*, *Alexander*, Eine Beweisführung von Format — Die Transformation signierter Dokumente auf dem Prüfstand, CR 2008, S. 607-612.

Wilkens, *Andreas*, Google verkürzt Cookie-Lebensdauer, in: heise online v. 17. 7. 2007, *abrufbar unter*: http://heise.de/-151848 (zuletzt abgerufen am 14. 6. 2014), *zitiert als*: *Wilkens*, heise online v. 17. 7. 2007.

Willems, *Constantin*, Beweis und Beweislastverteilung bei Zugang einer E-Mail Fallkonstellationen unter besonderer Betrachtung elektronischer Bewerbungen, MMR 2013, S. 551-556.

Williamson, *Oliver E.*, Die ökonomischen Institutionen des Kapitalismus – Unternehmen, Märkte, Kooperationen, Tübingen 1990.

Winkelhaus, *Jan-Dirk*, Der Bereicherungsausgleich im Lichte des neuen Zahlungsdiensterechtes, BKR 2010, S. 441-449.

Winter, *Ralf*, Anmerkung zu *LG Konstanz*, Urteil v. 19. 4. 2002, 2 O 141/01 A, MMR 2002, S. 836-837.

– Anmerkungen zu *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01, JurPC Web-Dok., 71/2002.

– Anmerkung zu *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03, CR 2004, S. 219-221.

Wißner, *Bernd* / *Jäger*, *Karl-Werner*, Technisches Lexikon, in: *Kilian*, *Wolfgang* / *Heussen*, *Benno* (Hrsg.), Computerrechts-Handbuch, 2012, Kap. 300, Losebl., 31. Ergänzungslieferung, Stand: Mai 2012, *zitiert als*: *Wißner*/*Jäger*, in: Computerrechts-Handbuch.

Wolf, *Manfred* / *Neuner*, *Jörg*, Allgemeiner Teil des Bürgerlichen Rechts, 10. Aufl., München 2012.

Wurm, *Michael*, Blanketterklärung und Rechtsscheinhaftung, JA 1986, S. 577-584.

Zahedani, *Said* / *Obert*, *Thomas*, Sicherheit = Menschen, Prozesse und Technik, DuD 2006, S. 627-631.

Zimmermann, *Johannes*, Bei Anruf Zahlung? – Das Pay by Call-Verfahren zwischen Rechtsscheinhaftung und Minderjährigenschutz, MMR 2011, S. 516-520.

Zippelius, *Reinhold*, Juristische Methodenlehre, 11. Aufl., München 2012.

Zöller, *Richard (Begr.)*, Zivilprozessordnung, 30. Aufl., Köln 2013, *zitiert als: Bearbeiter,* in: *Zöller*[30].

Stichwortverzeichnis