§ 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 hinaus, 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- 373

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 Berührung 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] 410

Die Geheimhaltungspflicht solle primär dem Schutz Dritter dienen,[128] 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. 411

Ferner ist fraglich, ob Geschäftsgegner bestimmungsgemäß in gleicher 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 412

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, **419**
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.

Mit der Annahme eines Schuldverhältnisses mit Schutzwirkungen zu **420**
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.

e) Schutzbedürftigkeit des Dritten

Die vierte Voraussetzung, auch als Subsidiarität des Schuldverhältnisses mit **421**
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]

Ein eigener vertraglicher Anspruch gegen den Account-Inhaber hat der **422**
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

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 **426**
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).

g) Zwischenergebnis

Die Haftung für den Missbrauch von Zugangsdaten kann nicht über den **427**
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]

III. Lösung über die culpa in contrahendo

Ein weiterer diskutierter Lösungsweg ist die Anwendung der *culpa in con-* **428**
trahendo (c.i.c.). Demnach hätte der Geschäftsgegner einen Schadensersatz-

---

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 In- 498
ternets, 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.

Der Anschlussinhaber konnte sich mit Anschlusskennung, die hardware- 499
seitig 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]

aa) Rechtsscheintatbestand

Beim Bildschirmtext stellen sich die gleichen Rechtsfragen des Miss- 500
brauchs 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

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

509 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.

aa) Fehlerhafte Überweisungen

510 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,

---

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]

524 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]

525 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]

526 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-

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.

538 Zusammenfassend lässt sich feststellen, dass für die Anerkennung eines 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]

539 Die Sicherheit der verwendeten Authentisierungsmethode muss das Ziel 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]

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. 553

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. 554

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

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. 574

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- 575

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 re- **599**
gelmäßig 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.

Einige Stimmen in Rechtsprechung und Literatur meinen, es bedürfe ei- **600**
ner 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]

Ferner könnte ein Vergleich zu § 172 Abs. 1 BGB gegen die Notwendig- **601**
keit der Überprüfung der Identität bei der Erstellung des Accounts sprechen. Nach § 172 Abs. 1 BGB ist eine unterschriebene Vollmachtsurkunde ein

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.

615 Fraglich ist dabei, ob dieses Verfahren noch ausreichend sicher ist. Die 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.

630 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]

aa) Die vermeintliche Notwendigkeit Schutzbehauptungen zu verhindern

631 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]

---

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 te- 635
leologisch 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.

Eine bedeutende Figur im Rahmen der ökonomischen Analyse des 636
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 *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.