zu liefern plant, und damit einen mittleren fünfstelligen Betrag einnimmt und verschwindet.[676]

Andererseits muss die Rolle des Vertrauens ebenfalls berücksichtigt werden. Dieses muss über einen langen Zeitraum erarbeitet werden und kann schnell verloren gehen. Die Reputation eines Anbieters ist eine entscheidende Komponente für den Onlinehandel.[677] Beim Onlinehandel ist die Sanktionsmöglichkeit gegenüber dem Anbieter bedeutend höher als beim Einzelhandel, weil es dem Kunden einfacher fällt, den Anbieter zu wechseln. Während beim Einzelhandel ein Kunde längere Wege in Kauf nehmen müsste, wenn er zu einem Konkurrenten wechseln möchte, sind beim Onlinehandel alle Anbieter unabhängig von ihrer geographischen Lage für den Kunden gleich gut erreichbar. Er kann mittels Mausklicks bestellen und erhält die Ware zur Haustür geliefert. Ein Onlinehändler kann zwar jederzeit einen neuen Account anlegen oder sogar Onlineshop eröffnen, um eine schlechte Reputation los zu werden. Und neue Teilnehmer im Markt des Onlinehandels werden von Kunden akzeptiert. Gleichwohl spielt das Vertrauen in einen Geschäftspartner sowie dessen Reputation im Onlinehandel eine große Rolle.[678] Viele Geschäftspartner wählen, wenn möglich, bekannte Anbieter. Die Vertrauensprämie ist bei online geschlossenen Rechtsgeschäften somit höher als die Opportunismusprämie, sodass die vierte Voraussetzung nicht gegeben ist. 653

(5) Zwischenergebnis

Von den vier rechtsökonomischen Voraussetzungen für eine Vertrauenshaftung liegt die Hälfte nicht vor. Aus rechtsökonomischer Sicht ist eine rechtsgeschäftliche Haftung für den Missbrauch von Zugangsdaten dem Grunde nach nicht notwendig. 654

bbb) Die Ausgestaltung einer Haftung aus rechtsökonomischer Sicht

Obwohl die Haftung rechtsökonomisch dem Grunde nach nicht erforderlich ist, soll dennoch auf eine rechtsökonomische Betrachtung der Ausgestal- 655

676 Wie bei *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08.
677 *Jehle*, S. 70.
678 Ebd., S. 51 ff.

tung einer möglichen Haftung eingegangen werden. Ist die wie bei § 172 Abs. 1 BGB gesetzlich vorgegeben oder ist das Vertrauen des Erklärungsempfänger wegen der Stärke des Rechtsscheins wie beispielsweise bei elektronischen Signaturen schutzwürdig, stellt sich die Frage nach der Ausgestaltung der Haftung auf Rechtsfolgenseite.

656 Bei einer Haftung für die willentliche Duldung eines *falsus procutrators* gibt es ökonomisch einen Zielkonflikt.[679] Die Haftung auf das negative Interesse kann nur eine optimale Abschreckung und dadurch einen optimalen Kontrollaufwand garantieren.[680] Die Haftung auf das positive Interesse hingegen leistet dies nicht, verhindert jedoch, dass Ressourcen fehlgeleitet und Schäden hochgetrieben werden.[681] Bei der Haftung für ein fahrlässiges Ermöglichen des Auftretens ohne Vertretungsmacht kann sowohl eine ex-ante- als auch ex-post-Effizienz durch die Haftung auf das negative Interesse hergestellt werden.[682]

cc) Alternative Möglichkeiten der Absicherung gegen Missbrauch

657 Bisher wurde betrachtet, wie sicher Authentisierungsmethoden sind und was Account-Inhaber sowie gegebenenfalls Plattformbetreiber zur Verhinderung des Missbrauchs unternehmen. Für die angemessene Verteilung der Risiken beim Missbrauch von Zugangsdaten im Internet ist jedoch entscheidend, was der Erklärungsempfänger als Absicherung gegen den Missbrauch tun kann. Er hat zwar keine Möglichkeiten einen Missbrauch zu verhindern, er kann sich jedoch durch verschiedene Maßnahmen dagegen absichern, dass er auf eine missbräuchlich abgegebene Willenserklärung vertraut. Dabei sind zwei Arten von Maßnahmen zu unterscheiden. Der Geschäftsgegner kann sowohl vor Empfang einer Willenserklärung als auch nach dem Empfang Maßnahmen ergreifen.

658 Vor dem Empfang der Willenserklärung kann der Geschäftsgegner bereits Kontakt mit dem späteren Vertragspartner haben. Solcher Kontakt kann zum einen durch ein Kennenlernen in der Offline-Welt bestehen sowie durch vorherige Erfahrungen bei Online-Geschäften. Wenn sich jemand beispielsweise telefonisch bei einem Vertragspartner nach einem Angebot

679 *Kötz/Schäfer*, S. 237.
680 Ebd., S. 237.
681 Ebd., S. 237.
682 Ebd., S. 238 ff.

erkundigt, der Vertragsschluss dann anschließend per mittels E-Mail ausgetauschten Willenserklärungen stattfindet, wie es bei geschäftlich handelnden Personen häufig vorkommt,[683] ist trotz der einfachen Manipulationsmöglichkeiten bei E-Mails[684] ein Missbrauch kaum möglich. Selbst wenn sich die Vertragspartner vorher nicht aus der analogen Welt kennen, sondern stets nur online kommuniziert haben, hat der Erklärungsempfänger anhand charakteristischer Merkmale der Erklärung Indizien dafür, ob sie vom Account-Inhaber stammt oder nicht. Wortwahl, Zeichensetzung, typische Ausdrücke oder spezifisches Wissen können dem Erklärungsempfänger Rückschlüsse auf den Urheber der Erklärung geben. Durch das Kontrahieren mit bekannten Vertragspartnern kann jeder Teilnehmer des Rechtsverkehrs Möglichkeiten eines Missbrauchs reduzieren.

659 Ob die Kommunikation zwischen sich bekannten Personen überwiegt oder im Internet anonyme Massenkommunikation vorherrscht,[685] ist nicht entscheidend. Auch bei einer anonymen Massenkommunikation hat der Erklärungsempfänger Möglichkeiten sich gegen Missbrauch abzusichern. Jedem Teilnehmer am Rechtsverkehr steht es frei, für jedes Rechtsgeschäft eine Authentisierungsmethode zu wählen, die seinen Sicherheitsvorstellungen entspricht.[686] Bei der Wahl kann der Teilnehmer die Bedeutung und den Wert des Rechtsgeschäfts und eine unsichere, günstige oder eine sicherere, kostenaufwendigere Authentisierungsmethode wählen. Die sehr kostengünstige und leicht zu fälschende E-Mail steht am Anfang, gefolgt von der leicht sichereren Stufe der passwortgeschützten Erklärung. Darüber hinaus stehen mit der aufwendigeren und tendenziell kostspieligen elektronischen Signatur, die in vier unterschiedlich sicheren Formen existiert,[687] verschiedene Abstufungen an Sicherheit und Kostenaufwand zur Verfügung, auf deren qualifizierten Formen der Erklärungsempfänger ein schützenswertes Vertrauen hat.[688] Der Teilnehmer am Rechtsverkehr kann daher vor Anbahnung eines Vertrags die Wahl treffen, wie sicher die Authentisierungsmethode sein soll, und für den konkreten Zweck zu unsichere Authentisierungsmethoden ausschließen.

---

683 Vgl. *Hoeren*, CR 2002, 295, 296.
684 Dazu oben Rn. 212.
685 Letzteres behauptet *Bösing*, S. 43.
686 So auch *Borges*, NJW 2011, 2400, 2402; *Roßnagel*, MMR 2003, 164, 170.
687 Zu den Formen der elektronischen Signatur oben Rn. 74.
688 Oben Rn. 578 ff.

660 Ferner kann der Teilnehmer am Rechtsverkehr sich vorab über die Reputation des späteren Vertragspartners informieren. Im und außerhalb des Internets bestehen zahlreiche Möglichkeiten sich über die Reputation eines Geschäftspartners zu informieren wie Testberichte, Meinungen von Bekannten oder Kundenforen.[689] Bei Internet-Auktionsplattformen gibt es regelmäßig ein institutionalisiertes Reputationssystem, das mittels zweier Zahlen, der Anzahl an positiven Bewertungen sowie der Prozentzahl an positiven Bewertungen gemessen an den gesamten Bewertungen, die Vertrauenswürdigkeit eines Vertragspartners einschätzbar zu machen versucht.[690]

661 Ist dem Handelnden die Reputation eines potentiellen Vertragspartners nicht ausreichend genug, hat er die Möglichkeit auf einer Identitätsüberprüfung zu bestehen. Diese kann er beispielsweise mittels des elektronischen Identitätsnachweises[691] oder des PostIdent-Verfahrens[692] machen. Ebenso kann sich der Handelnde Auskünfte über die Solvenz des potentiellen Vertragspartners beispielsweise über Banken oder die Schufa besorgen.

662 Der Empfänger einer Willenserklärung kann stets rückfragen, ob die Willenserklärung vom Account-Inhaber selbst oder von einem Dritten mit dessen Einverständnis abgegeben wurde. Stellt der Empfänger der Willenserklärung diese Rückfrage auf demselben Kommunikationsweg, auf dem er die Erklärung erhalten hat, schützt er sich nur minimal gegen Missbrauch. Bricht er jedoch das Medium und stellt die Rückfrage telefonisch oder postalisch, besteht eine große Chance einen möglichen Missbrauch aufzudecken.[693] Der Medienbruch stellt dabei zwar ein Hemmnis dar,[694] das das online abgewickelte Geschäft verlangsamt. Er bietet jedoch eine effektive und kostengünstige Methode, Schäden durch den Missbrauch von Zugangsdaten zu reduzieren. Der Behauptung, dass im elektronischen Rechtsverkehr vielfach eine solche Möglichkeit fehle,[695] kann nicht zugestimmt werden. Fehlen dem Erklärungsempfänger tatsächlich solche Möglichkeiten und möchte er sich stets durch Rückfragen absichern, muss er in letzter Konsequenz von einem konkreten Rechtsgeschäft Abstand nehmen.

---

689 *Jehle*, S. 69 f.
690 Oben Rn. 64.
691 Dazu oben Rn. 88.
692 Siehe oben Rn. 613.
693 Siehe *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 729. Dies geschah beispielsweise bei *LG Frankfurt*, Urteil v. 15. 12. 2004, 3-13 O 28/04 (nicht veröffentlicht).
694 *Bösing*, S. 43; *Knopp/Wilke/Hornung/Laue*, MMR 2008, 723, 725.
695 *Herresthal*, K&R 2008, 705, 707; *ders.*, in: *Taeger/Wiebe*, 21, 31.

Eine weitere Möglichkeit für den Vertragspartner besteht darin, auf der Vorleistung des Geschäftsgegners zu bestehen. Bei Online-Auktionen sichert sich der Verkäufer regelmäßig dadurch ab, dass der Käufer in Vorleistung treten muss. Verkäufer begegnen dadurch der Problematik von Spaßbietern, sodass sie höchstens den Schaden in Höhe des negativen Interesses, also den Aufwand das Angebot einzustellen, tragen müssen. 663

Letztlich hat der Teilnehmer am Rechtsverkehr noch die Möglichkeit, die Identität des Geschäftspartners außer Acht zu lassen und sich gegen einen Missbrauch zu versichern. Solange der Teilnehmer seine Leistung sicher erhält oder wenigstens seine Gegenleistung behält, kann ihm die Identität des Gegenübers oder die Berechtigung eines Dritten in seinem Namen zu handeln egal sein.[696] Der Verkäufer kann beispielsweise das Delkredererisiko auf einen Zahlungsdiensteanbieter verlagern. Online-Händler verlagern das Delkredererisiko häufig auf Kreditkarten-Acquiring-Unternehmen, die dieses Risiko aufgrund des Gesetzes der großen Zahlen zu tragen haben.[697] Selbst Privatpersonen haben Möglichkeiten, das Delkredererisiko abzusichern. PayPal bietet Verkäufern beispielsweise an, unter bestimmten Voraussetzungen das Delkredererisiko für über das System empfangene Zahlungen zu übernehmen.[698] Ebenso haben Käufer die Möglichkeit sich von PayPal gegen das Risiko abzusichern, dass der Verkäufer trotz Zahlungseingang die Ware nicht liefert.[699] Das Risiko die Gegenleistung nicht zu erhalten, können die Vertragsparteien auch durch die Einschaltung eines Treuhänders absichern. 664

Viele der Möglichkeiten der Absicherung gegen den Missbrauch haben gemeinsam, dass sie den elektronischen Geschäftsverkehr, der sich durch seine Geschwindigkeit und ständige Verfügbarkeit auszeichnet, verlangsamen. Möchte ein Teilnehmer am Rechtsverkehr von den Chancen der Geschwindigkeit des Online-Rechtsverkehrs profitieren, so muss er auch das damit einhergehende Missbrauchsrisiko tragen. 665

696 Vgl. *M. Köhler/Arndt/Fetzer*[7], Rn. 172.

697 *BGH*, Urteil v. 16. 4. 2002, XI ZR 375/00 – BGHZ 150, 286, 297 ff. sowie oben Rn. 342.

698 Vgl. *PayPal*, Verkäuferschutzrichtlinie.

699 Vgl. *PayPal*, Käuferschutzrichtlinie.

dd) Zwischenergebnis

666 Der Verkehrsschutz gebietet hier weder aus teleologischen noch aus rechtsökonomischen Erwägungen eine Rechtsscheinhaftung zu etablieren, wenn deren Voraussetzungen eigentlich nicht vorliegen.

e) Widerspruch zur herrschenden Ansicht bei Weitergabe der Zugangsdaten

667 Bei Ablehnung eines Rechtsscheintatbestandes kann bei Weitergabe[700] der Zugangsdaten eine Haftung des Account-Inhabers nicht begründet werden. Im Ergebnis wird jedoch herrschend angenommen, dass der Account-Inhaber nach Weitergabe der Zugangsdaten für einen Missbrauch hafte.[701] Dieses Ergebnis wird zum Teil über die Duldungsvollmacht[702] zum Teil über eine analoge Anwendung des § 172 Abs. 1 BGB[703] begründet. Beide Lösungen zur Begründung der Haftung setzen voraus, dass ein Rechtsscheintatbestand dahingehend besteht, dass der Account-Inhaber oder ein Dritter mit seinem Einverständnis eine Erklärung über den Account abgegeben hat. Dieser Rechtsscheintatbestand existiert jedoch weder bei der hier vertretenen Anwendung der allgemeinen Rechtsscheinhaftung noch nach herrschender Meinung bei Anwendung der Anscheinsvollmacht.[704] Die Konstellationen mit und ohne Weitergabe unterscheiden sich nicht im vom Geschäftsgegner wahrnehmbaren Rechtsschein. Er erhält in beiden Fällen eine Erklärung, die aussieht, als habe sie der Account-Inhaber abgegeben. Der Erklärung kann der Empfänger jedoch nicht ansehen, wer sie tatsächlich abgegeben hat. Nur im für den Erklärungsempfänger nicht erkennbaren Verhalten des Account-Inhabers besteht bei den Konstellationen ein Unterschied. Dieses Verhalten des Account-Inhabers ist Anknüpfungspunkt für eine unterschiedliche Beurteilung der Zurechnung in den beiden Konstellationen. Der Rechtsscheintatbestand ist mit und ohne Weitergabe der Zugangsdaten der Gleiche. Die beiden herrschenden Ansichten zur Haftung bei Weitergabe und ohne Weitergabe widersprechen sich daher.

700 Zum Begriff der Weitergabe oben Rn. 295.
701 Oben Rn. 293.
702 Oben Rn. 297 ff.
703 Oben Rn. 303 ff.
704 Oben Rn. 371 ff.

Vor diesem Hintergrund ist zu überlegen, in welche Richtung dieser Widerspruch aufzulösen ist. Teilweise wird gefordert, man müsse in beiden Konstellationen den Rechtsschein anerkennen, weil ansonsten die Haftung bei bewusster Weitergabe nicht begründet werden kann.[705] Die bewusste Schaffung der Möglichkeit einer Identitätstäuschung rechtfertige die Haftung des Account-Inhabers.[706] Weder aus rechtlichen noch aus rechtsökonomischen Gründen ist diese angestrebte Risikoverteilung jedoch zu rechtfertigen.[707] Für eine Anerkennung des Rechtsscheintatbestandes in beiden Konstellationen spreche ferner, dass ohne eine Haftung bei Weitergabe ansonsten eine Anreizstruktur fehle, die Weitergabe von Passwörtern zu unterlassen.[708] Dagegen spricht jedoch, dass der Account-Inhaber auch ohne eine Rechtsscheinhaftung Anreize hat seine Zugangsdaten geheim zu halten. Beispielsweise hat er ein Interesse daran, dass kein Dritter seine E-Mails lesen kann oder die Reputation seines eBay-Accounts durch nicht ernst gemeinte Angebote oder nicht ernst gemeintes Mitbieten zerstört. **668**

Überzeugend ist hingegen, den Widerspruch dahin gehend aufzulösen, dass ein Rechtsscheintatbestand sowohl in der Konstellation ohne Weitergabe als auch mit Weitergabe der Zugangsdaten gleichermaßen abgelehnt wird. Bei einer rein wissensbasierten Authentisierungsmethode besteht ein Rechtsscheintatbestand somit in beiden Konstellationen nicht.[709] Diesen Rechtsscheintatbestand bei Weitergabe zu bejahen, entstammt Billigkeitserwägungen, die sich dogmatisch nicht rechtfertigen lassen. Nur die Zurechnung lässt sich bei der Weitergabe der Zugangsdaten überzeugend begründen. Durch die Annahme einer Haftung des Account-Inhabers schafft die herrschende Meinung dadurch bei Weitergabe der Zugangsdaten eine Rechtsscheinhaftung ohne Rechtsschein.[710] Die herrschende Meinung bezüglich der Haftung bei Weitergabe der Zugangsdaten[711] ist daher abzulehnen. Mangels eines Rechtsscheintatbestandes haftet der Account-Inhaber dem Geschäftsgegner auch bei Weitergabe der Zugangsdaten zu einem Ac- **669**

705 *Borges*, NJW 2011, 2400, 2402.
706 Ebd., 2402.
707 Oben Rn. 625 ff.
708 *Borges*, NJW 2011, 2400, 2402.
709 Oben Rn. 544 ff.
710 Dies ist den Ansichten, die eine Haftung bei rein wissensbasierter Authentisierung bejahen vorzuwerfen oben Rn. 365, 380.
711 Oben Rn. 293.

count nicht, wenn der Account eine rein wissensbasierte Authentisierungsmethode verwendet.

f) Zwischenergebnis

670 Ein Rechtsscheintatbestand besteht beim Missbrauch von Zugangsdaten im Internet nur, wenn eine sichere Authentisierungsmethode gewählt wurde und der Account-Inhaber bei Erstellen des Accounts zuverlässig überprüft wurde. Eine ausreichend sichere Authentisierungsmethode stellt die Zwei-Faktor-Authentisierung dar.[712] Eine rein wissensbasierte Authentisierung bietet hingegen keine hinreichende Gewähr dafür, dass der Account-Inhaber gehandelt hat.[713] Die Zuordnung zwischen virtueller Identität des Accounts und dem Namensträger muss zuverlässig durch die Überprüfung seiner Identität vorgenommen werden.[714] Dafür reicht eine Plausibilitätskontrolle,[715] der Abgleich der Daten mit der Schufa[716] oder die Zusendung eines Briefes nicht aus.[717] Die Anerkennung eines Rechtsscheintatbestandes für rein wissensbasierte Authentisierungsmethoden ist auch nicht aus rechtsökonomischen Erwägungen[718] oder zur angemessenen Verteilung der Risiken erforderlich.[719]

3. Zurechenbarkeit

671 Der Rechtsscheintatbestand muss dem Account-Inhaber auch zurechenbar sein. Objektiv ist dafür erforderlich, dass er eine Möglichkeit hat, diesen zu zerstören. Subjektiv muss ihm der Rechtsschein je nach vertretener Ansicht nach dem Verschuldens- oder Risikoprinzip zurechenbar sein.[720]

712 Oben Rn. 534 ff.
713 Oben Rn. 544 ff.
714 Oben Rn. 595 ff.
715 Oben Rn. 607 ff.
716 Oben Rn. 608.
717 Oben Rn. 617.
718 Oben Rn. 635 ff.
719 Oben Rn. 625 ff.
720 Oben Rn. 233 ff.

a) Möglichkeit den Rechtsschein zu zerstören

Ein Rechtsscheintatbestand kann nur dann zurechenbar sein, wenn derjenige, der den Rechtsscheintatbestand geschaffen hat, eine Möglichkeit hat, den Rechtsschein zu beseitigen.[721] Der Namensträger muss beim Missbrauch von Zugangsdaten im Internet die Möglichkeit haben, den Rechtsscheintatbestand zu zerstören, also zu verhindern, dass ein Dritter mit seinem Account handelt. Diese Anforderungen kann beispielsweise durch eine Sperrmöglichkeit des Accounts erfüllt werden.[722] Diese Sperrmöglichkeiten sichern auch das Authentisierungsverfahren ab, denn sie dienen ähnlich wie die Sicherung der Zugangsdaten dafür, dass nur der Account-Inhaber mit dem Account handeln kann.[723] Nur wenn der Account dem Account-Inhaber zu jeder Zeit die Möglichkeit bietet, den Account zu sperren oder wieder alleinige Kontrolle über ihn zu übernehmen, kommt die Zurechnung eines möglichen Rechtsscheintatbestand in Frage. Die Zerstörung des Rechtsscheins im digitalen Verkehr ist nicht immer möglich, so kann beispielsweise das Revidieren einer digital signierten Willenserklärung nicht sicher durch ihr Löschen erfolgen.[724] 672

Aus dem Grund, dass der Account-Inhaber eine Möglichkeit haben muss, einen vorhanden Rechtsschein zu zerstören, kommt die Zurechnung nicht in Betracht, wenn es Angreifern durch Schwachstellen beim Authentisierungsnehmer möglich ist, ohne die Zugangsdaten sich in den Account des Inhabers einzuloggen.[725] Sollte das Authentifizierungssystem des Authentisierungsnehmers durch Schwachstellen der Server-Infrastruktur oder SQL-Injections, durch Cross-Site-Scripting (XSS) kompromittierbar sein, scheidet somit eine Zurechnung zum Account-Inhaber aus. Ebenso scheidet eine Zurechnung zu ihm aus, wenn ein Angreifer ohne Zutun des Account-Inhabers an die Zugangsdaten gelangt ist. Das kann zum einen durch Brute-Force-Attacken[726] oder durch die unauthorisierte Weitergabe der Zugangsdaten durch den Authentisierungsnehmer[727] erfolgen. 673

721 Siehe oben Rn. 246.
722 *Redeker*, IT-Recht[5], Rn. 877.
723 Die Sperrmöglichkeiten bei verschiedenen Authentisierungsmethoden wurden daher schon im Rahmen deren Sicherheit behandelt, vgl. oben Rn. 534 ff.
724 *provet/GMD*, S. 132.
725 Zu diesen Schwachstellen oben Rn. 215 ff.
726 Dazu oben Rn. 181.
727 Dazu oben Rn. 221.

b) Beschränkung auf grobe Fahrlässigkeit?

674 Mit unterschiedlichen Anknüpfungspunkten kann erwogen werden, dass der Account-Inhaber nur bei Vorliegen von grober Fahrlässigkeit beim Missbrauch der Zugangsdaten haften muss. Diese Erwägungen setzen zunächst voraus, dass die Zurechnung nach dem Verschuldensprinzip[728] erfolgt, weil ansonsten kein Raum für einen Verschuldensmaßstab vorhanden ist. Zunächst ist die Erwägung aufzugreifen, dass sich eine Rechtsscheinhaftung im Bürgerlichen Recht nur bei Vorliegen von grober Fahrlässigkeit rechtfertigt.[729] Die scharfe Rechtsfolge der Erfüllungshaftung rechtfertige sich im Bürgerlichen Recht im Gegensatz zum Handelsrecht nur bei Erfüllung dieser strengen Voraussetzung. Liege diese nicht vor, komme nur eine Haftung aus *culpa in contrahendo* in Betracht.[730] Es mag zwar dem Rechtsempfinden entsprechen, die scharfe Rechtsfolge der Erfüllungshaftung nur bei Vorliegen der strengeren Voraussetzung der groben Fahrlässigkeit zu gewähren. Dogmatisch lässt sich diese Ansicht jedoch kaum begründen. Die gesetzlichen Rechtsscheintatbestände setzen eine willentliche Schaffung voraus.[731] Wenn mit einer *BGH*-Entscheidung begründet wird, dass dort die Erfüllungshaftung wegen einfacher Fahrlässigkeit verneint wurde,[732] begründet dies nicht eine Haftung auf das positive Interesse bei grober Fahrlässigkeit. In der Entscheidung wird klargestellt, dass § 172 Abs. 1 BGB mit dem „Aushändigen" die willentliche Schaffung eines Rechtsscheintatbestandes voraussetzt und unterhalb dieser Voraussetzungen nur eine Haftung nach den „Grundsätzen, wie sie zu der Haftung auf das negative Interesse entwickelt worden sind" in Betracht komme.[733]

675 Andere Überlegungen dagegen wollen den Haftungsmaßstab der groben Fahrlässigkeit anwenden. Wenn mangels Vorsatzes die Haftung auf das positive Interesse scheitert solle im Rahmen einer Haftung aus *culpa in contrahendo* der Verschuldensmaßstab auf grobe Fahrlässigkeit beschränkt werden.[734] Systematisch solle dabei vorsichtig der § 675v Abs. 2 BGB her-

728 Dazu oben Rn. 237.
729 *Hübner*[2], Rn. 1289.
730 Ebd., Rn. 1289.
731 Dazu oben Rn. 249.
732 *Hübner*[2], Rn. 1289; unter Verweis auf *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13.
733 *BGH*, Urteil v. 30. 5. 1975, V ZR 206/73 – BGHZ 65, 13, 14 f.
734 *Oechsler*, MMR 2011, 631, 633, ihm folgend *Linardatos*, Jura 2012, 53, 55; *Sonnentag*, WM 2012, 1614, 1619 f.

angezogen werden.[735] Dieser finde beim Missbrauch von Kreditkarten im Mail-Order-Verfahren Anwendung, was mit Zugangsdaten im Internet vergleichbar sei.[736] Viele Accounts im Internet haben mit dem Mail-Order-Verfahren gemeinsam, dass eine rein wissensbasierte Authentisierungsmethode verwendet wird. Wenn zur Begründung darauf auf die hohe Missbrauchsanfälligkeit sowie die komplexen technischen Rahmenbedingungen abgestellt wird,[737] kann dem nur eingeschränkt zugestimmt werden. Zugangsdaten im Internet funktionieren über einen komplexen technischen Ablauf, das Mail-Order-Verfahren jedoch nicht. Zwar wird mit Verweis auf die Intention des Gesetzgebers[738] verneint, dass Kreditkarten im Mail-Order-Verfahren ein Zahlungsauthentifizierungsinstrument im Sinne des § 1 Abs. 5 ZAG, wie von § 675v BGB vorausgesetzt, seien.[739] Im Ergebnis besteht jedoch Einigkeit darin, dass § 675v BGB auch bei Kreditkarten im Mail-Order-Verfahren angewendet wird.[740] Insbesondere ist jedoch § 675v BGB auf den Missbrauch beim Online-Banking anwendbar.[741] Beim Online-Banking handelt es sich sogar um Zugangsdaten im Internet, sodass der Rechtsgedanke des § 675v BGB überzeugend zur Lösung des Missbrauchs von anderen Zugangsdaten im Internet herangezogen werden kann.

676 Folgend soll daher geprüft werden, ob die Voraussetzungen einer Analogie, eine planwidrige Gesetzeslücke sowie eine vergleichbare Interessenlage,[742] vorliegen. Die planwidrige Gesetzeslücke liegt in Form einer nachträglichen Regelungslücke vor.[743] Fraglich erscheint jedoch, ob die Interessenlage vergleichbar ist. Dafür spricht zunächst, dass beim Online-Banking ebenso wie bei anderen Accounts im Internet Zugangsdaten verwendet werden. Man könnte somit einen Erst-Recht-Schluss ziehen. § 675u Abs. 1 BGB schließt einen Aufwendungsersatzanspruch der Bank gegen ihren Kunden aus. Die Banken verwenden teilweise AGB, die den Kunden bei fahrlässigem Umgang mit den Zugangsdaten in die Haftung nehmen.[744] § 675v Abs. 2 BGB gebietet eine Beschränkung der Haftung auf Fälle von

735 *Oechsler*, MMR 2011, 631, 633.
736 Ebd., 633.
737 So ebd., 633.
738 Begr. ZAG, BT-Drucks. 14/11613, S. 36.
739 *Casper*/*Pfeifle*, WM 2009, 2343, 2347; dagegen *Oechsler*, WM 2010, 1381, 1382.
740 *Casper*/*Pfeifle*, WM 2009, 2343, 2345 f.; *Oechsler*, WM 2010, 1381, 1328 f.
741 Dazu ausführlich *Maihold*, in: *Schimansky*/*Bunte*/*Lwowski*[4], § 55 Rn. 92 ff.
742 Oben Rn. 329 ff.
743 Dazu oben Rn. 330.
744 *Casper*, in: MüKo-BGB[6], § 675v Rn. 6.

grober Fahrlässigkeit. Daraus könnte geschlossen werden, dass wenn schon privatautonom der Account-Inhaber sich nicht verpflichten kann für den leicht fahrlässigen Umgang mit Zugangsdaten zu haften, dies erst recht im Rahmen der Rechtsscheinhaftung gelten müsse.

677 Gegen die vergleichbare Interessenlage spricht, dass § 675v BGB auf die Besonderheiten der Interessen der Beteiligten beim Einsatz von Zahlungsauthentisierungsinstrumenten zugeschnitten ist und sich nicht übertragen lässt. Erstens wirkt die Beschränkung der Haftung auf grobe Fahrlässigkeit nach § 675u Abs. 2 BGB für sämtliche Authentisierungsmethoden, also sowohl für rein wissensbasierte als auch für Zwei-Faktor-Methoden. Während bei rein wissensbasierten Authentisierungsmethoden ein Rechtsschein nicht vorliegt,[745] sodass dieser auch bei grober Fahrlässigkeit nicht zugerechnet werden kann, besteht beim Einsatz der Zwei-Faktor-Authentisierung ein Rechtsscheintatbestand, bei dem eine Beschränkung auf grobe Fahrlässigkeit den Account-Inhaber entlastet. Zweitens sind die Zahlungsauthentisierungsinstrumente ein häufiges Ziel von Angreifern. Bei ihnen handelt es sich um ein Massengeschäft und sie werden häufig missbraucht. § 675v BGB trifft für diese besondere Konstellation eine Regelung, die die Interessen von beiden Seiten berücksichtigt und Rechtssicherheit schafft. Diese Interessenlage weicht von Zugangsdaten für andere Accounts im Internet ab.

678 Drittens und entscheidend schafft § 675v BGB eine ausdifferenzierte Lösung, die als Gesamtkonzept zu verstehen ist. Zwar wird der Bankkunde durch die Beschränkung der unbegrenzten Haftung auf grobe Fahrlässigkeit (§ 675v Abs. 2 BGB) entlastet. Im Gegenzug wird er beim Verlust von Besitz-Authentisierungsmitteln auf einen begrenzten Geldbetrag mit einer verschuldensunabhängigen Haftung belastet (§ 675v Abs. 1 S. 1 BGB). Dieses Gesamtkonzept lässt sich jedoch nicht übertragen. Eine verschuldensunabhängige Haftung für den Missbrauch von Zugangsdaten im Internet lässt sich nicht begründen. Die mit der verschuldensunabhängigen begrenzten Haftung einhergehende Beschränkung auf grobe Fahrlässigkeit für die unbegrenzte Haftung lässt sich wertungsstimmig nicht isolieren. Eine vergleichbare Interessenlage liegt somit nicht vor. § 675 Abs. 2 BGB lässt sich somit nicht auf Zugangsdaten zu anderen Accounts im Internet übertragen.[746]

---

745 Oben Rn. 544 ff.

746 So auch *Borges*, NJW 2012, 2385, 2387; *Borges/Schwenk/Stuckenberg/Wegener*, S. 294; **a.A.** *Hossenfelder*, Pflichten von Internetnutzern, S. 255.

c) Maßstab der Zurechnung

Die willentliche Schaffung eines Rechtsscheintatbestandes begründet stets dessen Zurechenbarkeit.[747] Dies zeigt sich unter anderem in der Wertung des § 172 Abs. 1 BGB,[748] der ein Aushändigen der Vollmachtsurkunde erfordert.[749] Die Weitergabe der Zugangsdaten begründet daher die Zurechenbarkeit eines etwa vorhandenen Rechtsscheintatbestandes.[750] 679

Sodann stellt sich die Frage, ob eine Zurechnung auch ohne willentliche Weitergabe der Zugangsdaten erfolgen werden kann.[751] Dafür spräche, dass jeder Teilnehmer am Rechtsverkehr für das aus seiner Risikosphäre stammende zurechenbare Verhalten Dritter einzustehen habe.[752] 680

Andererseits könnte die Zurechnung des Rechtsscheintatbestandes auf die willentliche Weitergabe der Zugangsdaten beschränkt sein.[753] Erstens spricht dafür, dass die gesetzlichen Rechtsscheinvollmachten in §§ 170 ff. BGB stets eine willentliche Schaffung des Rechtsscheintatbestandes voraussetzen.[754] Zweitens ist eine Rückkopplung der konkreten Willenserklärung an den Account-Inhaber schwierig. Bei abhandengekommenen Willenserklärungen[755] sowie dem fehlenden Erklärungsbewusstsein[756] hat der Geschäftsherr den Großteil der Erklärung selbst geschaffen. Der Rechts- 681

747 Oben Rn. 249.

748 Darauf begründen einige ihre Meinung zur Haftung für den Missbrauch von Zugangsdaten im Internet, dazu oben Rn. 303 ff.

749 Oben Rn. 314.

750 Vgl. nur *Oechsler*, MMR 2011, 631, 632; *Reese*, S. 76; *Sonnentag*, WM 2012, 1614, 1617; *Ultsch*, DZWir 1997, 466, 473.

751 So *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 518 f.; *Herresthal*, K&R 2008, 705, 708 f.; *ders.*, in: *Taeger/Wiebe*, 21, 37; *Kuhn*, S. 230 ff.; *Stöber*, EWiR 2011, 521, 552; *ders.*, JR 2012, 225, 229; *Verse/Gaschler*, Jura 2009, 213, 215. Für die elektronische Signatur *Bergfelder*, S. 390; *Dörner*, AcP 202 (2002), 363, 392 f.; *M. Köhler/Arndt/Fetzer*[7], Rn. 227; *Reese*, S. 133 ff.; *Rieder*, S. 284 ff.; *Spiegelhalder*, S. 160 ff.

752 *Herresthal*, K&R 2008, 705, 708 f.; *ders.*, in: *Taeger/Wiebe*, 21, 37.

753 So *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 181; *Faust*, BGB AT[3], § 26 Rn. 41; *M. Köhler/Arndt/Fetzer*[7], Rn. 324; *Langenbucher*, S. 146; *Linardatos*, Jura 2012, 53, 55; *Redeker*, IT-Recht[5], Rn. 875; *Rieder*, S. 315; *Ultsch*, DZWir 1997, 466, 473. Für die Zurechnung nur nach einem erweitertem Weitergabebegriff *Borges*, Elektronischer Identitätsnachweis, S. 136; *ders.*, NJW 2011, 2400, 2403; *Sonnentag*, WM 2012, 1614, 1618.

754 Für § 172 Abs. 1 BGB oben Rn. 314.

755 Oben Rn. 476.

756 Oben Rn. 472.

verkehr bekommt seine Handlungen oder deren Ergebnisse unmittelbar mit, sodass ein schutzwürdiges Vertrauen darin besteht. Dies ist bei Zugangsdaten im Internet nicht der Fall. Die Weitergabe oder das Ausspähen der Zugangsdaten ist für den Rechtsverkehr nicht einsehbar und bei ihm fehlt es am rechtsgeschäftlichen Bezug. Ferner zeigen die Wertungen aus den sog. Überweisungsfällen bei Bankgeschäften, dass es an der notwendigen Rückkopplung fehlt. Führt eine Bank eine Überweisung doppelt aus, fehlt es an einem Verhalten des Bankkunden mit Bezug auf das konkrete Rechtsgeschäft, an das angeknüpft werden kann.[757] Ebenso fehlt dieses Verhalten des Account-Inhabers beim Missbrauch der Zugangsdaten.

682 Drittens zeigt die Wertung des § 935 BGB, dass das fahrlässige Abhandenkommen von Sachen nur bei überragendem Verkehrsschutz eine Zurechnung begründet. Regelmäßig muss der Eigentümer einer Sache diese willentlich aus der Hand geben, damit ein gutgläubiger Erwerb aufgrund des Rechtsscheins des Besitzes möglich ist (vgl. § 935 Abs. 1 S. 1 BGB). Nur bei Wertpapieren bedarf es dieser Zurechnung zum Eigentümer nicht, sodass diese auch bei Abhandenkommen gutgläubig erworben werden können (§ 935 Abs. 2 BGB). Ein den Wertpapieren entsprechendes Verkehrsschutzbedürfnis besteht bei Vollmachtsurkunden[758] und Blanketten nicht.[759] Diese Erwägungen treffen ebenso auf Zugangsdaten im Internet zu, sodass die Wertung des § 935 BGB für eine Beschränkung der Zurechnung auf die Weitergabe der Zugangsdaten spricht.

683 Viertens lässt die Beschränkung der Zurechnung auf die willentliche Schaffung durch einen Erst-Recht-Schluss zu § 172 Abs. 1 BGB begründen. Der Rechtsschein des § 172 Abs. 1 BGB ist je nach verwendeter Authentisierungsmethode leicht bis erheblich stärker als ein solcher bei Zugangsdaten im Internet.[760] Bei diesem starken Rechtsscheintatbestand ist die Zurechnung nach herrschender Ansicht nur bei willentlicher Übergabe der Vollmachtsurkunde möglich.[761] Wenn die Zurechnung beim stärkeren Rechtsscheintatbestand schon auf die willentliche Schaffung begrenzt ist, muss dies erst recht für den schwächeren Rechtsscheintatbestand der Zugangsdaten im Internet gelten. Die Zurechnung ist somit begrenzt auf die willentliche Schaffung des Rechtsscheintatbestandes. Eine Zurechnung

757 Oben Rn. 511.
758 Oben Rn. 317.
759 Oben Rn. 327.
760 Oben Rn. 345 ff.
761 Dazu und zur Gegenauffassung oben Rn. 315.

kommt somit nur in Betracht, wenn der Account-Inhaber die Zugangsdaten weitergeben hat.

d) Fälle der Zurechnung

Für das Risiko- und Verschuldensprinzip soll untersucht werden, wie unterschiedliche Fallkonstellationen zu beurteilen sind. Bei dieser Untersuchung wird unterstellt, dass nicht nur die willentliche Weitergabe der Zugangsdaten eine Zurechnung begründet,[762] weil ansonsten bei keiner der folgenden Konstellationen eine Zurechnung zu bejahen wäre. Ebenso soll mit untersucht werden, ob ein Verhalten grob fahrlässig ist, worauf die Zurechnung nach einer hier abgelehnten Meinung beschränkt ist.[763] **684**

Nach dem Risikoprinzip[764] hat der Account-Inhaber für alle Risiken einzustehen, die er eher beherrschen kann als der andere Teil.[765] Nach dem Verschuldensprinzip[766] kommt eine Zurechnung bei Abhandenkommen in Betracht, wenn der Account-Inhaber schuldhaft, also fahrlässig im Sinne des § 276 Abs. 2 BGB, umgegangen ist. Bestehen gesetzliche Regelungen über den Umgang mit den Zugangsdaten, wie die Obliegenheit der Geheimhaltung bei der elektronischen Signatur (vgl. § 5 Abs. 4 S. 2 SigG), richtet sich der Sorgfaltsmaßstab nach diesen. Bestehen keine gesetzlichen oder vertraglichen Regeln zur Aufbewahrung der Zugangsdaten, richtet sich das Verschulden nach einem „Verschulden gegen sich selbst".[767] Einschränkend ist nach dem Verschuldensprinzip zu fordern, dass der Account-Inhaber mit einem Missbrauch gerechnet hat oder bei pflichtgemäßem Verhalten hätte rechnen müssen.[768] **685**

Für eine Zurechnung reicht noch nicht die Einrichtung des Accounts.[769] Damit wird lediglich die Möglichkeit zur Kommunikation geschaffen. Für **686**

762 Entgegen der hier vertretenen Auffassung, oben Rn. 679 ff.
763 Oben Rn. 674.
764 Dazu oben Rn. 243.
765 Im Rahmen des Missbrauchs von Zugangsdaten vertreten von *Spiegelhalder*, S. 153; *Reese*, S. 133 ff.; *Rieder*, S. 230 ff.
766 Dazu oben Rn. 237.
767 Siehe oben Rn. 238.
768 *Borges*, NJW 2011, 2400, 2403; *Herresthal*, K&R 2008, 705, 709; *ders.*, in: *Taeger/Wiebe*, 21, 38; *Stöber*, EWiR 2011, 521, 552; *ders.*, JR 2012, 225, 229.
769 *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676, 1677; *Borges*, in: Internet-Auktion, 214, 216.

eine Zurechnung ausreichend ist hingegen, wenn der Account-Inhaber nach Kenntnis vom Missbrauch der Zugangsdaten nichts gegen einen weiteren Missbrauch unternimmt.[770]

aa) Sorgfalts- und Verkehrspflichten des Account-Inhabers

687 Bevor Einzelfälle der Zurechnung für die unterschiedlichen Möglichkeiten, die Zugangsdaten zu missbrauchen,[771] untersucht werden, sollen allgemeine Sorgfaltspflichten des Account-Inhabers bezüglich der Absicherung seines Rechners betrachtet werden, weil sie für eine Zurechnung nach dem Verschuldensprinzip[772] relevant sind. Insgesamt ist der Umfang der Sorgfaltspflichten bezüglich der IT-Sicherheit noch nicht genau herausgearbeitet.[773] Nachfolgend werden daher Anforderungen an die Account-Inhaber betrachtet, die diesen aus unterschiedlichen Gründen auferlegt werden. Sowohl deliktische Verkehrspflichten als auch Sorgfaltspflichten innerhalb von Vertragsbeziehungen werden herangezogen.

688 Grundsätzlich stellt sich die Frage, wie hoch die Anforderungen an einen Account-Inhaber sind. Fachspezifisches IT-Hintergrundwissen kann von ihm nicht verlangt werden. Vielmehr ist auf einen durchschnittlichen Nutzer abzustellen, der über solches Wissen nicht verfügt.[774] Insgesamt darf der Sorgfaltsmaßstab nicht all zu hoch angesetzt werden, weil die elektronischen Prozesse der Datenverarbeitung nur mit besonderem Fachwissen verstanden werden können. Im Gegensatz zu anderen Bereichen wie dem Straßenverkehr finden die Datenverarbeitungsprozesse innerhalb des Rechners unzugänglich für die Wahrnehmung durch Sinnesorgane statt.[775] Ein Nutzer kann somit nicht durch Beobachtung des Rechners erkennen, welche Rechenoperationen dieser gerade durchführt. Die Tendenz an diejenigen, die IT-Systeme für private Zwecke nutzen, keine zu hohen Anforderungen zu stellen, lässt sich auch in der höchstrichterlichen Rechtsprechung wiederfinden. Die höchstrichterlichen Anforderungen an den technischen

770 *Borges*, in: Internet-Auktion, 214, 216; *ders.*, NJW 2011, 2400, 2403.
771 Dazu oben Rn. 124.
772 Dazu oben Rn. 237.
773 *Spindler*, MMR 2008, 7, 13.
774 *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08 – MMR 2008, 626, 628; *Erfurth*, WM 2006, 2198, 2201.
775 *Erfurth*, WM 2006, 2198, 2201.

Sachverstand bei der Bestimmung der im Verkehr erforderlichen Sorgfalt sind nicht sehr hoch. Bei der Sicherung eines Routers muss dieser beispielsweise auf dem Stand der Sicherungstechnik beim Kauf sein.[776] Bezüglich Trojanern muss der durchschnittliche Nutzer nicht damit rechnen, dass sich Schadprogramme in harmlos erscheinenden Dateien befinden.[777]

689 Für die Anerkennung einer Verkehrs- oder Sorgfaltspflicht ist der Bekanntheitsgrad der Gefahr entscheidend.[778] Die Account-Inhaber müssen die Gefahren, die von ihren Rechnern und Accounts ausgehen, nur durch Sorgfaltsmaßnahmen abwenden, soweit diese Gefahren allgemein bekannt sind. Die Nutzer müssen sich über aktuelle Gefahren nicht in Fachzeitschriften oder Fachseiten im Internet informieren. Das Verfolgen von aktuellen Meldungen in allgemeinen und klassischen Medien reicht aus.[779] Darüber hinaus müssen Account-Inhaber die Warnungen des jeweiligen Authentisierungsnehmers zur Kenntnis nehmen.[780]

690 Bei der Konfiguration seines Rechners können vom Account-Inhaber keine spezifischen Fachkenntnisse verlangt werden. Die sichere Konfiguration seiner Umgebung ist ihm nur insoweit zumutbar, als dass die Einstellmöglichkeiten in einer für den Nutzer verständlichen Sprache erklärt sind.[781] Anderenfalls ist ihm die sichere Konfiguration technisch nicht zumutbar. Insbesondere kann von ihm nicht erwartet werden, dass er bestehende System- oder Netzwerkeinstellungen bewertet.[782] Sicherheitsrelevante Einstellungen im Betriebssystem und Browser können von einem privaten IT-Nutzer nicht erwartet werden.[783] Wirtschaftlich sind ihm nur Maßnahmen zumutbar, die er ohne fremde Hilfe realisieren kann.[784] Die Kosten für einen

776 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 23.

777 *BGH*, Urteil v. 4. 3. 2004, III ZR 96/03 (Dialer) – BGHZ 158, 201, 209.

778 *Mantz*, K&R 2007, 566, 568; *Spindler*, BSI-Studie, Rn. 286.

779 *Bender*, WM 2008, 2049, 2054; *Spindler*, BSI-Studie, Rn. 288; *Dennis Werner*, Verkehrspflichten, S. 174.

780 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261.

781 *Dennis Werner*, Verkehrspflichten, S. 153.

782 Ebd., S. 153.

783 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261; *Spindler*, BSI-Studie, Rn. 307 f.; *Dennis Werner*, Verkehrspflichten, S. 166 ff.; **a.A.** *Bender*, WM 2008, 2049, 2054.

784 *Spindler*, BSI-Studie, Rn. 292; *Dennis Werner*, Verkehrspflichten, S. 154.

IT-Fachmann, die unverhältnismäßig hoch sein können, muss er zur Sicherung seines Rechners nicht aufwenden.[785]

691 Viele Möglichkeiten die Zugangsdaten des Account-Inhabers auszuspähen basieren auf einer Infektion des Rechners mit Malware.[786] Er kann die Risiken einer solchen Infektion seines Rechners durch die Verwendung eines Antiviren-Programms verringern.[787] Antiviren-Programme setzten bei der Installation keine Fachkenntnisse voraus und sie sind kostengünstig oder kostenlos verfügbar.[788] Die Kenntnis, dass mit Antiviren-Programmen der Rechner geschützt werden kann, ist weit verbreitet.[789] Vom Account-Inhaber kann daher erwartet werden, dass er einen ständig aktualisierten Antiviren-Schutz verwendet.[790] Die Details der Pflicht zum Einsatz einer Antiviren-Software bei Windows sind nicht abschließend geklärt. Beim Signaturerkennungsverfahren, das die wichtigste Komponente von Antiviren-Software ist,[791] besteht ein Schutz nur, soweit die jeweilige Malware in der Datenbank des Antiviren-Herstellers erfasst ist. Die Datenbank aktualisiert der Hersteller regelmäßig, um seine Kunden vor aktuellen Bedrohungen zu schützen. Einige Stimmen in der Literatur betrachteten eine wöchentliche Aktualisierung zur Erfüllung der Pflicht eines ständig aktualisierten Antiviren-Programms als ausreichend.[792] Andere Vertreten erwarten vom Nutzer, dass dieser seinen Antiviren-Schutz täglich aktualisiert.[793] Die Verwen-

785 *Mantz*, K&R 2007, 566, 570; *Spindler*, BSI-Studie, Rn. 292; *Dennis Werner*, Verkehrspflichten, S. 154; **a.A.** *LG Hamburg*, Beschluss v. 21. 4. 2006, 308 O 139/06 – MMR 2007, 131, 132.

786 Oben Rn. 182.

787 Oben Rn. 202.

788 *Hossenfelder*, Pflichten von Internetnutzern, S. 127.

789 *Dennis Werner*, Verkehrspflichten, S. 156.

790 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261; *Bender*, WM 2008, 2049, 2054; *Borges*, MMR 2008, 262, 264 f.; *Borges/Schwenk/Stuckenberg/Wegener*, S. 273 f., 284; *B. Lorenz*, DuD 2013, 220, 225; *Herresthal*, in: *Langenbucher/Bliesener/Spindler*, Kap. 5 § 675l BGB Rn. 11; *Hossenfelder*, Pflichten von Internetnutzern, S. 180, 202, 231, 244; *ders.*, CR 2009, 790, 793; *R. Koch*, NJW 2004, 801, 804; *F. A. Koch*, CR 2009, 485, 488; *Libertus*, MMR 2005, 507, 510; *Mantz*, K&R 2007, 566, 570; *Redeker*, IT-Recht[5], Rn. 1063; *Spindler*, BSI-Studie, Rn. 295 ff.; *Dennis Werner*, Verkehrspflichten, S. 155 ff.; **a.A.** *Kind/Dennis Werner*, CR 2006, 353, 355.

791 Oben Rn. 203.

792 *Dienstbach/Mühlenbrock*, K&R 2008, 151, 154 f.; *Libertus*, MMR 2005, 507, 510; *Spindler*, BSI-Studie, Rn. 296; *Dennis Werner*, Verkehrspflichten, S. 157.

793 *Bender*, WM 2008, 2049, 2054; *Borges/Schwenk/Stuckenberg/Wegener*, S. 274, 284; *F. A. Koch*, CR 2009, 485, 489 f.; *B. Lorenz*, DuD 2013, 220, 225.

dung eines kostenfreien Antiviren-Programms ist zur Erfüllung der Sorgfaltspflicht ausreichend.[794] Verwendet ein Nutzer kein Antiviren-Programm handelt er grob fahrlässig.[795]

692 Diese Pflicht zum Einsatz eines Antiviren-Programms bezieht sich – auch wenn dies in der Diskussion nicht explizit zum Ausdruck kommt – auf das Absichern des Betriebssystems Windows mit einem Virenschutz. Ob auch ein Nutzer von Linux oder Mac OS X[796] seinen Rechner absichern muss, ist ungeklärt. Diese Betriebssysteme gelten wegen ihrer von Windows abweichenden Systemarchitektur als sicherer. Angriffe mit Malware sind in der Vergangenheit nur vereinzelt aufgetreten, durch Sicherheitsupdates jedoch zügig unterbunden worden. Ferner ist die Auswahl an Antiviren-Programmen gering. Ob eine Pflicht für Nutzer von Linux und Mac OS X besteht, ihren Rechner mit einem Antiviren-Programm zu schützen, ist zu bezweifeln.

693 Der Einsatz einer Firewall[797] ist zwar ein wichtiger Bestandteil der Absicherung von IT-Systemen. Firewalls besitzen jedoch nur in sehr begrenztem Maße die Fähigkeit, eine Infektion der hinter der Firewall befindlichen Rechner mit Malware zu verhindern.[798] Diese ambivalenten Eigenschaften der Firewall spiegeln sich auch in den Ansichten zur Pflicht des Account-Inhabers eine Firewall einzusetzen nieder. Teilweise wird vertreten, dass der Einsatz einer Firewall zumutbar und daher zu erwarten ist.[799] Zahlreiche Stimmen der Literatur lehnen jedoch eine Pflicht zur Einsatz einer Firewall ab.[800] Zum einen sei die Möglichkeit sich mit einer Firewall zu schützen noch zu wenig bekannt.[801] Zum anderen ist sichere Konfiguration nur mit Spezialkenntnissen möglich, wodurch es privaten Anwendern technisch

794 *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08 – MMR 2008, 626, 629; *Mühlenbrock/Dienstbach*, MMR 2008, 630, 631.

795 *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 134; differenzierend nach der Art des Accounts *Hossenfelder*, Pflichten von Internetnutzern, S. 203, 232.

796 14,4 % der Nutzer verwenden diese Betriebssysteme, *Schnarz/Seeger*, DuD 2012, 253, 254.

797 Oben Rn. 207.

798 Oben Rn. 209.

799 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261; *Hossenfelder*, Pflichten von Internetnutzern, S. 180; *ders.*, CR 2009, 790, 793; *F. A. Koch*, CR 2009, 485, 488.

800 *Borges/Schwenk/Stuckenberg/Wegener*, S. 274; *Spindler*, BSI-Studie, Rn. 298 ff.; *Dennis Werner*, Verkehrspflichten, S. 161 ff..

801 *Spindler*, BSI-Studie, Rn. 301; *Dennis Werner*, Verkehrspflichten, S. 162.

nicht zumutbar sei, eine Firewall einzusetzen.[802] Eine auf dem Betriebssystem vorinstallierte Firewall darf jedoch nicht deaktiviert werden.[803]

694 Sicherheitslücken in dem verwendetem Betriebssystem sowie den eingesetzten Programmen können ebenfalls eine Infektion des Rechners mit Malware ermöglichen.[804] Regelmäßige Updates von Betriebssystemen und den Anwendungen können dieses Risiko verringern.[805] In welchem Maße die Installation von Updates Nutzern zumutbar ist, ist nicht abschließend geklärt. Manche Stimmen der Literatur sehen den Nutzer nur dann als zur Installation von Updates verpflichtet an, wenn diese sich automatisch oder halb-automatisch installieren.[806] Teilweise wird eine Pflicht zur Aktualisierung ohne diese Einschränkung angenommen.[807] Bei der Zumutbarkeit lässt sich ebenfalls bezüglich des Aufwands der Updates differenzieren. Einzelne Stimmen in der Literatur verneinen die Pflicht zum Herunterladen von Updates mit einem großen Datenvolumen.[808] Andererseits wird den Nutzern zugemutet auch große Datenmengen an Updates herunter zu laden, das Warten oder das Umstellen auf eine schnellere Internet-Verbindung sei zumutbar.[809]

695 Zusammenfassend lässt sich festhalten, dass der Umfang der Sorgfalts- und Verkehrspflichten an den Nutzer eines Rechners noch nicht ausreichend konkretisiert ist. Es lässt sich jedoch die Tendenz feststellen, dass private Nutzer nicht allzu hohe Anforderungen erfüllen müssen. Sie müssen sich jedoch jedenfalls vor Gefahren schützen, die allgemein bekannt sind, weil beispielsweise die klassischen Medien über sie berichten. Der Einsatz eines Antiviren-Programms kann jedenfalls von Windows-Nutzern erwartet werden.

802 *Spindler*, BSI-Studie, Rn. 300; *Dennis Werner*, Verkehrspflichten, S. 162.

803 *Mühlenbrock/Dienstbach*, MMR 2008, 630, 631; *Dennis Werner*, Verkehrspflichten, S. 162.

804 Oben Rn. 184.

805 Oben Rn. 201.

806 *Spindler*, BSI-Studie, Rn. 302 ff.; *Dennis Werner*, Verkehrspflichten, S. 164 ff. Zwei Drittel der Nutzer verlassen sich auf diese automatischen Updates, *Schnarz/Seeger*, DuD 2012, 253, 255.

807 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261; *Hossenfelder*, Pflichten von Internetnutzern, S. 204, 244.

808 *Dennis Werner*, Verkehrspflichten, S. 165.

809 *F. A. Koch*, CR 2009, 485, 489.

bb) Einzelfälle

Die Betrachtung vergleichbarer Konstellationen hat gezeigt, dass eine Zurechnung nur in Betracht kommt, wenn dem Account-Inhaber zumutbare Möglichkeiten zur Verfügung stehen, den Missbrauch zu verhindern.[810] Er muss keinesfalls alle erdenklichen Maßnahmen zur Verhinderung eines Missbrauchs treffen. Es reicht aus, dass er bekannte und wirtschaftlich zumutbare Sicherungsmaßnahmen trifft. 696

Ermöglicht der Account-Inhaber den physikalischen Zugang zu aufgeschriebenen Zugangsdaten,[811] ist zu erwägen, dass dies in seine Risikosphäre fällt. Nach dem Risikoprinzip muss abgegrenzt werden, ob der Diebstahl noch in die neutrale Sphäre oder schon in die Sphäre des Account-Inhabers fällt. Das grundsätzliche Diebstahlrisiko kann der Account-Inhaber ebenso wenig wie der Geschäftsgegner kontrollieren.[812] Nur wenn er die Zugangsdaten unsorgfältig aufbewahrt, schafft er dadurch ein erhöhtes Risiko, für das er einzustehen hat.[813] Nach dem Verschuldensprinzip ist im Einzelfall zu überprüfen, ob die Form der Notiz der Zugangsdaten fahrlässig ist. Es kann nicht verlangt werden, dass jeder Nutzer seine Passwörter auswendig lernt.[814] Ihm muss also grundsätzlich möglich sein, sich seine Passwörter aufzuschreiben.[815] Notiert er sie sich, muss dies an einem sicheren Ort erfolgen.[816] Ein am Monitor befindlicher Klebezettel mit den Zugangsdaten ist dabei möglicherweise sogar als grob fahrlässig anzusehen,[817] ebenso das offene Herumliegenlassen von Passwort oder Chip-Karte und PIN.[818] Hat der Account-Inhaber das Passwort jedoch ohne Zusammenhang zum Account versteckt, ist dies nicht als sorgfaltswidrig anzusehen.[819] 697

Speichert der Account-Inhaber das Passwort ungesichert auf seinem Rechner in einer Schlüsselbund-Verwaltung[820] und erlaubt er anderen Personen die Nutzung seines Computers, ist dies ein Risiko, das in seine Sphäre 698

810 Oben Rn. 527.
811 Zu dieser Konstellation oben Rn. 132.
812 *Spiegelhalder*, S. 164.
813 *Spiegelhalder*, S. 164; *Rieder*, S. 285.
814 *B. Lorenz*, DuD 2013, 220, 223.
815 Oben Rn. 132.
816 *B. Lorenz*, DuD 2013, 220, 223.
817 *Borges*, NJW 2011, 2400, 2403.
818 *Dörner*, AcP 202 (2002), 363, 393.
819 *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 181.
820 Dazu oben Rn. 135.

fällt und somit nach dem Risikoprinzip zurechenbar ist. Ebenfalls nach dem Verschuldensprinzip ist das Speichern in der Schlüsselbund-Verwaltung zuzurechnen, weil es grob fahrlässig ist, ein Passwort ungeschützt auf einem Rechner zu speichern und diesen einen Dritten nutzen zu lassen.[821] Verwendet ein Account-Inhaber einen Passwortspeicher auf seinem Rechner muss er den Zugang dazu mit einem Passwort absichern und die darin gespeicherten Passwörter verschlüsseln.[822] Nutzt der Account-Inhaber hingegen einen Cloud-Speicher[823] für seine Passwörter und werden dem Cloud-Anbieter die Zugangsdaten entwendet, kommt eine Zurechnung zum Nutzer nicht in Betracht. Den einzigen Vorwurf, dem man ihm in diesem Fall machen könnte, ist, dass er den Cloud-Anbieter nicht sorgfältig ausgewählt hat. Für den Nutzer ist jedoch kaum bis gar nicht nachvollziehbar, wie gut die Daten beim Anbieter geschützt sind.[824]

699 Gelangt ein Angreifer durch einen Phishing-Angriff an die Zugangsdaten des Account-Inhabers,[825] stellt sich ebenfalls die Frage der Zurechnung. Nach dem Risikoprinzip kann beim klassischen Phishing die Zurechnung zum Account-Inhaber bejaht werden. Es fällt in seine Risikosphäre die Zugangsdaten nicht, auch nicht unbemerkt, weiterzugeben. Durch die unbewusste Weitergabe erhöht er das Missbrauchsrisiko so erheblich, dass ihm die Folgen dieser Risikoerhöhung zuzurechnen sind. Im Rahmen des Verschuldensprinzips ist nach den Umständen des Einzelfalls zu prüfen, ob der Account-Inhaber bei Beachtung der ordnungsgemäßen Sorgfalt hätte erkennen können, dass die Phishing-Seite nicht vom Authentisierungsnehmer stammt und dass deswegen durch Eingabe der Zugangsdaten mit einem Missbrauch zu rechnen sei.

700 Zur Herausarbeitung eines Sorgfaltsmaßstabes kann auf die umfangreichen Fälle des Phishings im Rahmen des Online-Bankings zurückgegriffen werden.[826] Man könnte in Anlehnung an die zum Online-Banking vertretenen Ansichten die Zurechnung aus zwei Gründen ausschließen: dem Account-Inhaber fehlen die Möglichkeiten den Missbrauch im Voraus zu erkennen und zu verhindern und weil der Missbrauchende nicht aus dem

821 *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 519; *Oechsler*, AcP 208 (2008), 565, 582.
822 *B. Lorenz*, DuD 2013, 220, 225.
823 Dazu oben Rn. 136.
824 *Schulz/Bosesky/C. Hoffmann*, DuD 2013, 95, 99.
825 Zu den verschiedenen Formen des Phishings oben Rn. 138 ff.
826 Siehe hierzu oben Rn. 519.

Lager des Account-Inhabers stammt, sei eine Rechtsscheinhaftung nicht geboten.[827] Letzteres Argument überzeugt nicht. Die Rechtsscheinhaftung entscheidet darüber, welches Vertrauen des Rechtsverkehrs schutzwürdig ist. Bei der Zurechnung kommt es auf die Verbindung von Haftenden zum Rechtsscheintatbestand an, nicht aus welchem Lager ein möglicher Handelnder stammt. Das erste Argument, dass die Möglichkeit den Missbrauch im Voraus zu erkennen fehle, trifft häufig aber nicht immer zu. Es gibt einige Anzeichen an Phishing-Seiten, die diese als betrügerischen Versuch erkennen lassen, sodass der Account-Inhaber erkennen kann, dass damit die ausgespähten Zugangsdaten später missbraucht werden sollen. Da Banken so präsent warnen, dass bei jeder Transaktion jeweils nur eine TAN abgefragt wird, ist jedenfalls die Eingabe von mehr als einer TAN einer indizierten Liste[828] als fahrlässig einzustufen. Die Eingabe einer gesamten Liste ist als grob fahrlässig einzustufen.[829] Es ist gemeinhin bekannt, dass Zugangsdaten zum Online-Banking zur späteren Plünderung des Kontos gephisht werden, sodass bei Verdachtsmomenten ebenfalls damit gerechnet werden muss, dass die Zugangsdaten nach Eingabe missbraucht werden. Offensichtliche Betrugsversuche, beispielsweise bei Phishing-Seiten mit eklatanten Rechtschreib- und Grammatikfehlern, nicht zu erkennen, ist fahrlässig.[830] Fahrlässig handelt beispielsweise auch, wer als Bankkunde der Aufforderung in einem Pop-up-Fenster, die mit der Androhung der Sperrung des Online-Banking-Zugangs verbunden ist, einen Geldbetrag zu überweisen nachkommt und die Bank auf solche Angriffsszenarien aufmerksam gemacht hat.[831] Das Fehlen einer HTTPS-Verbindung ist jedoch nicht fahrlässig, weil auch trotz der unterschiedlichen Anzeige im Browser die Unterscheidung zwischen einer HTTP- und einer HTTPS-Verbindung von einem durchschnittlichen Nutzer nicht erwartet werden kann.[832] Nach dem Verschuldensprinzip kann es daher beim klassischen Phishing zur Zurechnung kommen.

---

827 Oben Rn. 519.

828 *BGH*, Urteil v. 24. 4. 2012, XI ZR 96/11 – NJW 2012, 2422.

829 *OLG München*, Urteil v. 23. 1. 2012, 17 U 3527/11 – MMR 2013, 163; **a.A.** *LG Landshut*, Urteil v. 14. 7. 2011, 24 O 1129/11, Rn. 26.

830 *Hossenfelder*, CR 2009, 790, 793.

831 *AG Köln*, Urteil v. 26. 6. 2013, 119 C 143/13 – BKR 2013, 482, 483.

832 *Erfurth*, WM 2006, 2198, 2203; *Hossenfelder*, Pflichten von Internetnutzern, S. 204 f.; *ders.*, CR 2009, 790, 793; *Kind/Dennis Werner*, CR 2006, 353, 356; **a.A.** *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261.

701 Beim Pharming[833] kommt eine Zurechnung nur bei gewissen Konstellationen in Betracht. Beim DNS-Poisoning sowie dem DNS-Cache-Poisoning liegt die Ursache für die Ermöglichung des Pharming-Angriffs beim Betreiber des DNS-Servers. Der Account-Inhaber hat darauf keinen Einfluss,[834] sodass eine Zurechnung bereits nach dem allgemeinen Grundsatz ausscheidet, dass der Account-Inhaber eine Möglichkeit haben muss, den Rechtsschein zu verhindern.[835] Geschieht das Pharming in Form einer Veränderung der Hosts-Datei oder als Drive-By-Pharming stammt die Ursache für die Ermöglichung des Pharmings aus der Sphäre des Account-Inhabers, sodass ihm ein späterer Missbrauch nach dem Risikoprinzip zuzurechnen ist. Bei Anwendung des Verschuldensprinzips kommt es darauf an, ob bei Beachtung der ordnungsgemäßen Sorgfalt das Ausspähen der Daten sowie der spätere Missbrauch hätte verhindert werden können. Diese beiden Formen des Pharmings funktionieren durch eine Infektion des Rechners oder des Routers des Accounts-Inhabers.[836] Fahrlässig handelt der Account-Inhaber insbesondere dann, wenn er durch Nachlässigkeit die Infektion seines Computers mit Schadsoftware verursacht hat, zum Beispiel durch einen fehlenden aktuellen Virenschutz beim Einsatz des Windows-Betriebssystems. Ein Verschulden kann in diesem Fall darüber hinaus begründet werden, dass die Phishing-Seite aufgrund ihrer Gestaltung ernsthafte Zweifel daran begründet, dass sie vom Authentisierungsnehmer stammt.[837] Eine grobe Fahrlässigkeit kommt beim Pharming nur in Betracht, wenn die Phishing-Seite aufgrund ihrer Gestaltung eindeutig als Fälschung zu identifizieren ist, beispielsweise durch Text in gebrochenem Deutsch oder offensichtlichen Layout-Fehlern. Manche Phishing-Seiten sind jedoch den Internetseiten des Authentisierungsnehmers so ähnlich, dass ein Opfer sie kaum vom Original unterscheiden kann.[838] Bei solchen Täuschungen handelt der Account-Inhaber nicht fahrlässig. Eine Zurechnung nach dem Verschuldensprinzip scheidet somit regelmäßig aus.[839]

---

833 Zu den verschiedenen Arten des Pharmings oben Rn. 147 ff.

834 Daher trifft den Nutzer auch keine Pflicht das DNS-System vor Angriffen zu schützen, *Dennis Werner*, Verkehrspflichten, S. 169 f.

835 Oben Rn. 672.

836 Zu den Infektionswegen oben Rn. 182 ff.

837 *Hossenfelder*, CR 2009, 790, 793.

838 *Hossenfelder*, Pflichten von Internetnutzern, S. 197.

839 Diese Ergebnis stimmt überein mit den Wertungen beim Online-Banking, dazu oben Rn. 519.

Späht ein Angreifer mittels eines Keyloggers die Zugangsdaten des Account-Inhabers aus,[840] stellt sich beim Risikoprinzip die Frage, aus welcher Sphäre das Risiko stammt. Handelt es sich um einen physischen Keylogger, lässt sich die Risikosphäre anhand dessen Einsatzortes bestimmen. Wurde beispielsweise ein Adapter zwischen Tastatur und Anschluss am Rechner des Account-Inhabers installiert, der die Tastatureingaben aufzeichnet, ist dies dem Account-Inhaber nach dem Risikoprinzip zurechenbar. Wurde der Keylogger jedoch als zusätzliches PIN-Eingabefeld auf dem Geldautomaten einer Bank installiert, fällt dies in den Risikobereich des Authentisierungsnehmers. Nach dem Verschuldensprinzip kommt eine Zurechnung nur in Betracht, wenn der Account-Inhaber den Keylogger bei ordnungsgemäßer Sorgfalt hätte erkennen können. Ist der Keylogger in der räumlichen Sphäre des Authentisierungsnehmers installiert, wie beispielsweise das zusätzliche PIN-Eingabefeld beim Geldautomaten, handelt der Account-Inhaber regelmäßig nicht fahrlässig, wenn er dies nicht erkennt. Er darf darauf vertrauen, dass der Authentisierungsnehmer den Authentisierungsvorgang sicher gestaltet. Nur bei sich aufdrängenden Verdachtsmomenten, beispielsweise einem schiefen PIN-Eingabefeld, kann das schützenswerte Vertrauen des Account-Inhabers beeinträchtigt sein. Bei physischen Keyloggern in der eigenen räumlichen Sphäre handelt der Account-Inhaber fahrlässig, wenn er den Keylogger bei der Beachtung der ordnungsgemäßen Sorgfalt hätte erkennen können. Handelt es sich um einen Adapter, der zwischen Tastatur und Anschluss am Rechner gesteckt ist, ist das Erkennen schwer. Regelmäßig befinden sich die Anschlüsse hinten am Rechner, der so gedreht ist, dass der Verwender des Rechners diese nicht sehen kann. Der Account-Inhaber hat zwar die Möglichkeit diesen Adapter zu erkennen, es entspricht jedoch nicht der im Verkehr erforderlichen Sorgfalt seinen Rechner regelmäßig auf Keylogger zu untersuchen. Ein fahrlässiges Handeln scheidet somit regelmäßig aus. 702

Software-Keylogger hingegen fallen in die Risikosphäre des Account-Inhabers, sodass nach dem Risikoprinzip eine Zurechnung stattfindet. Sie installieren sich durch eine Infektion des Rechners, sodass der Account-Inhaber fahrlässig handelt, sofern er seinen Rechner nicht hinreichend gegen eine Infektion gesichert hat.[841] Ferner hat der Account-Inhaber keine zumutbare Möglichkeit zu überprüfen, ob und welche Zugangsdaten proto- 703

840 Zu Keyloggern oben Rn. 166.

841 Oben Rn. 691.

kolliert werden und an wen diese gesendet werden. Einen Missbrauch kann er so bei Beachtung der im Verkehr erforderlichen Sorgfalt nicht vorhersehen. Leichte oder grobe Fahrlässigkeit ist ihm insofern regelmäßig nicht vorzuwerfen.

704 Das Erlangen der Zugangsdaten mittels Social Engineerings[842] fällt in die Risikosphäre des Account-Inhabers, sodass nach dem Risikoprinzip eine Zurechnung erfolgen kann. Nach dem Verschuldensprinzip ist im Einzelfall zu entscheiden, ob das Verhalten des Account-Inhabers bei der Weitergabe der Zugangsdaten fahrlässig war und ob er einen späteren Missbrauch hätte vorhersehen können. Wird der Account-Inhaber durch Social Engineering auf eine Phishing-Seite geleitet (Spear-Phishing), stellt sich wie beim Phishing und Pharming die Frage, ob er aufgrund der Gestaltung der Seite Verdacht schöpfen muss. Ist dies nicht der Fall, handelt der Account-Inhaber fahrlässig, wenn er die Täuschung und die böse Absicht des Angreifers hätte erkennen können. Nach den Umständen des Einzelfalls kommt eine grobe Fahrlässigkeit in Betracht, wenn der Account-Inhaber zu leichtgläubig dem Angreifer unglaubwürdige Behauptungen geglaubt hat.[843]

705 Bei einem Man-in-the-Middle-Angriff[844] kommt es auf die Angriffsmethode an, um zu bestimmen, welcher Risikosphäre der Angriff zuzuordnen ist. Bei einem Angriff mittels DNS-Spoofing auf zentrale DNS-Server fällt dies in die neutrale Sphäre. Das Zwischenschalten eines WLAN-Hotspots oder einer GSM-Basisstation als Evil Twin kann der Account-Inhaber nicht beeinflussen, sodass dies ebenfalls in die neutrale Sphäre fällt. Lediglich wenn der Angreifer beim Man-in-the-Middle-Angriff den Verkehr über seinen Rechner deswegen umleiten konnte oder lediglich dessen Inhalt verändert, fällt dies in die Risikosphäre des Account-Inhabers, weil er am besten seinen Rechner vor solchen Angriffen schützen kann. Nur in diesem Fall ist der Missbrauch mittels eines Man-in-the-Middle-Angriffs dem Account-Inhaber nach dem Risikoprinzip zuzurechnen. Nach dem Verschuldensprinzip kommt eine Zurechnung bei einem Man-in-the-Middle-Angriff regelmäßig nicht in Betracht. Wird der Angriff mittels DNS-Spoofing oder Evil Twin vollzogen, konnte der Account-Inhaber die Umleitung des Datenverkehrs nicht beeinflussen, sodass ihm daraus kein Verschuldensvorwurf gemacht werden kann. Im Gegensatz zum Phishing und Pharming werden bei einem

842 Siehe dazu oben Rn. 162.

843 Vgl. etwa *AG Hamburg-St. Georg*, Urteil v. 24. 2. 2009, 918 C 463/08, Rn. 28.

844 Dazu oben Rn. 168 ff.

Man-in-the-Middle-Angriff die Zugangsdaten entweder unbemerkt mitgehört oder direkt zum Missbrauch verwendet, häufig unter Vortäuschung des gewollten Vorgangs. Während der Account-Inhaber Auffälligkeiten bei der Phishing-Seite bemerken könnte, hat er beim Man-in-the-Middle-Angriff häufig keine Anzeichen, dass seine Daten mitgelesen oder missbraucht werden. Ein Verschuldensvorwurf ist ihm daher nicht zu machen. Sichert der Account-Inhaber seinen Rechner nicht ausreichend gegen eine Infektion ab, benutzt er beispielsweise einen Windows-Rechner ohne Antiviren-Schutz, ermöglicht er den Man-in-the-Middle-Angriff fahrlässig. Den späteren Missbrauch wird der Account-Inhaber bei der mangelnden Sicherung jedoch häufig nicht erkennen, sodass ihm diesbezüglich keine Fahrlässigkeit vorzuwerfen ist. Grobe Fahrlässigkeit wird beim Man-in-the-Middle-Angriff regelmäßig erst recht nicht vorliegen. Nach dem Verschuldensprinzip ist der Missbrauch nach einem Man-in-the-Middle-Angriff somit häufig nicht zurechenbar.

706 Beim Sniffing[845] kommt es nach dem Risikoprinzip darauf an, wer das Sniffing durch den Einsatz einer unverschlüsselten Verbindung ermöglicht hat. Die Absicherung der eigenen WLAN-Verbindung fällt in die Risikosphäre des Account-Inhabers. Setzt der Authentisierungsnehmer jedoch beim Authentisierungsvorgang eine nicht verschlüsselte Verbindung ein, ist dieser Umstand seiner Risikosphäre zuzurechnen. Wird der Mobilfunkverkehr mitgelesen, fällt dies in die neutrale Sphäre. Nach dem Risikoprinzip ist somit nur der Einsatz einer unverschlüsselten WLAN-Verbindung dem Account-Inhaber zuzurechnen. Bei Anwendung des Verschuldensprinzips ergibt sich das Gleiche. Wird der Mobilfunk-Verkehr mitgelesen oder setzt der Authentisierungsnehmer eine unverschlüsselte Verbindung ein, sind dies Umstände, die der Account-Inhaber nicht beeinflussen kann, sodass ein Verschuldensvorwurf daraus nicht erwachsen kann. Bereits seit mehreren Jahren ist es verkehrsüblich ein WLAN zu verschlüsseln,[846] sodass der Einsatz eines schlecht gesicherten WLANs gegen die im Verkehr erforderliche Sorgfalt verstößt. Während der Einsatz einer unsicheren Verschlüsselungsmethode wie WEP als fahrlässig eingestuft werden kann, ist das Fehlen einer Verschlüsselungsmethode beim Wireless LAN als

845 Siehe oben Rn. 177.

846 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 33.

grob fahrlässig anzusehen. Eine Zurechnung nach dem Verschuldensprinzip kommt in diesem Fall in Betracht.

707 Errät der Angreifer die Zugangsdaten durch das Ausprobieren bekannter Daten,[847] stellt sich nach dem Risiko die Frage, welcher Sphäre dies zuzuordnen ist. Bei dem Herausfinden durch einen Brute-Force-Angriff fällt es jedenfalls nicht in den Risikobereich des Account-Inhabers, weil dieser keine Möglichkeit hat dies zu verhindern. Durch das Verwenden des immer gleichen Passworts bei verschiedenen Authentisierungsnehmern könnte er jedoch ein erhöhtes Risiko setzen. Das Risiko, das der Account-Inhaber dadurch setzt, ist jedoch sehr gering. Die Kombination der Zugangsdaten muss erst ausgespäht werden, damit ein Angriff auf einer anderen Seite funktioniert. Man kann daher erwägen, dies der neutralen Sphäre zuzuordnen. Dagegen spricht jedoch, dass dieses minimale Risiko vom Account-Inhaber besser beherrscht werden kann. Dass das Risiko klein ist, schmälert lediglich die Wahrscheinlichkeit des Missbrauchs, hat jedoch keinen Einfluss auf die Haftung des Account-Inhabers. Begünstigt der Account-Inhaber somit durch das Verwenden der stets selben Kombination bei den Zugangsdaten ein Erraten, ist ihm dies nach dem Risikoprinzip zuzurechnen. Nach dem Verschuldensprinzip stellt sich die Frage, ob es verkehrsüblich ist, bei jedem Authentisierungsnehmer eine unterschiedliche Kombination von Zugangsdaten zu verwenden. Angesichts der Tatsache, dass die Mehrheit der Account-Inhaber nur drei oder weniger unterschiedliche Passwörter bei den zahlreichen Accounts,[848] die sie besitzt verwendet, ist bereits an der Verkehrsüblichkeit zu zweifeln. Doch nur weil eine Mehrheit sich nicht an ein Sicherheitsniveau hält, entspricht das unsichere Verhalten nicht der im Verkehr erforderlichen Sorgfalt. Nur weil sehr viele Autofahrer sich nicht an die zulässige Höchstgeschwindigkeit (vgl. § 3 Abs. 3 StVO) halten, entfällt die Fahrlässigkeit ihres Verhaltens durch die schiere Anzahl an Überschreitungen nicht. Das durch die Verwendung der gleichen Zugangsdaten bei unterschiedlichen Authentisierungsnehmern gesetzte Risiko ist jedoch nicht so hoch, dass eine Pflicht zur Verwendung unterschiedlicher Benutzernamen oder Passwörter besteht.[849] Zwar kann dem Account-Inhaber somit unter Umständen Fahrlässigkeit vorgeworfen werden, wenn er das immer gleiche Passwort bei unterschiedlichen Authentisierungsnehmern verwen-

847 Dazu oben Rn. 180.
848 Vgl. *Wefel*, S. 3.
849 *B. Lorenz*, DuD 2013, 220, 223.

det. Eine Zurechnung nach dem Verschuldensprinzip scheitert jedoch daran, dass er mit einem konkreten Missbrauch nicht rechnen braucht. Erst wenn er Kenntnis davon erlangt, dass die Zugangsdaten möglicherweise in die Hände eines Angreifers gelangt sind,[850] besteht für ihn Anlass sein Passwort zu ändern.[851]

Darüber hinaus erwägen einzelne Stimmen der Literatur weitere Anfor- **708**
derungen an den Account-Inhaber bezüglich seiner Zugangsdaten. Der Account-Inhaber sei verpflichtet, ein Passwort mit ausreichender Länge zu wählen, das nicht durch einen Wörterbuch-Angriff angreifbar ist.[852] Diese Anforderung an den Account-Inhaber überzeugt nicht. Der Authentisierungsnehmer muss durch entsprechende Vorgaben vielmehr sicherstellen, dass die Authentisierungsgeber sichere Passwörter wählen. Ferner solle eine Pflicht des Account-Inhabers bestehen, die Passwörter regelmäßig zu ändern.[853] Um diese Pflicht zu erfüllen müssen die Passwörter nicht alle drei, sondern alle ein bis zwei Jahre geändert werden.[854] Zwar kann der Account-Inhaber durch das häufige Ändern des Passworts Missbrauch durch ausgespähte Zugangsdaten verhindern. Es ist ihm jedoch nicht zumutbar, die Passwörter für alle seine Accounts jedes Jahr oder auch nur alle zwei Jahre zu ändern, weil er wahrscheinlich über so viele Accounts verfügt, dass diese Pflicht ihn zu stark belasten würde.

e) Zwischenergebnis

Der Rechtsscheintatbestand ist dem Account-Inhaber nur bei willentlicher **709**
Schaffung, also der Weitergabe der Zugangsdaten zuzurechnen.[855] Der Account-Inhaber muss im konkreten Fall die Möglichkeit gehabt haben, den Missbrauch zu verhindern.[856]

---

850 Wenn bekannt wird, dass die Authentisierungsdaten des Authentisierungsnehmers gestohlen wurden, besteht Anlass dazu. Dies passierte beispielsweise dem Notiz-Dienst Evernote Anfang 2013, dazu *J. Schuster*, heise online v. 3. 3. 2013.

851 *B. Lorenz*, DuD 2013, 220, 224.

852 Ebd., 223.

853 Ebd., 224.

854 Ebd., 224.

855 Oben Rn. 679 ff.

856 Oben Rn. 672.

4. Schutzwürdigkeit des Geschäftsgegners

710 Die allgemeine Voraussetzung der Schutzbedürftigkeit des Geschäftsgegners muss auch bei der Haftung für den Missbrauch von Zugangsdaten im Internet erfüllt sein.[857] Da die Stärke des Rechtsscheins über den Grad des schädlichen Wissens entscheidet, muss für den Missbrauch von Zugangsdaten im Internet das schädliche Wissen bestimmt werden. Zwar ist beim Missbrauch von Zugangsdaten im Internet wegen des Handelns unter fremdem Namen die Vertretungskonstellation nicht offensichtlich. Eine Nähe zu den Rechtsscheinvollmachten besteht jedoch. In Anlehnung an § 173 BGB schadet daher bereits leicht fahrlässige Unkenntnis.[858]

5. Disposition im Vertrauen auf den Rechtsschein

711 Die allgemeine Voraussetzung der Rechtsscheinhaftung, dass der Geschäftsgegner im Vertrauen auf den Rechtsschein eine Disposition getroffen hat,[859] ist bei dem Missbrauch von Zugangsdaten im Internet ebenfalls anwendbar.

6. Rechtsfolge

712 Grundsätzlich erhält der Vertrauende bei der Rechtsscheinhaftung das, was seinem Vertrauen entspricht.[860] Vertraut der Empfänger einer Willenserklärung, die über das Internet verschickt wurde, schützenswert darauf, dass diese vom Account-Inhaber stammt, ist er vom Account-Inhaber so zu stellen, als ob dies zutrifft. Dies läuft auf eine Erfüllungshaftung auf das positive Interesse hinaus.

713 Der Haftende kann seine Haftung jedoch auf das negative Interesse begrenzen, wenn die Anfechtung des Rechtsscheintatbestandes möglich wäre.[861] Auch wenn dies nicht immer mit der Anfechtungsmöglichkeit des Rechtsscheins begründet wird, lassen sich Vertreter dieser Ansicht

857 Allgemein zu dieser Voraussetzung oben Rn. 252.
858 Im Ergebnis auch *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 36; *Kuhn*, S. 226; *Reese*, S. 56 f.; *Spiegelhalder*, S. 165 f.
859 Oben Rn. 254.
860 Oben Rn. 257.
861 Dazu oben Rn. 258.

finden.[862] Wegen der Nähe zu den Rechtsscheinvollmachten, wo eine Anfechtungsmöglichkeit herrschend ausgeschlossen wird,[863] ist dies jedoch bei der Haftung für den Missbrauch von Zugangsdaten abzulehnen.[864]

714 Ebenso wie bei jeder Rechtsscheinhaftung stellt sich die Frage, ob der Geschäftsgegner ein Wahlrecht zwischen der scheinbaren und der wirklichen Lage besitzt.[865] Wegen der Nähe zu den Rechtsscheinvollmachten ist zu erwägen, die herrschende Meinung, dass bei diesen ein Wahlrecht nicht besteht,[866] zu übertragen. Dagegen spricht jedoch, dass der Geschäftsgegner, falls zweifelhaft ist, ob eine Rechtsscheinhaftung im Einzelfall gegeben ist, nicht das Prozessrisiko tragen soll, sondern sich direkt an den Handelnden wenden können soll.[867] Daher hinaus steht dem Vertrauenden bei der Rechtsscheinhaftung grundsätzlich ein Wahlrecht zwischen dem Schein und der Wirklichkeit zu.[868] Der Geschäftsgegner hat daher beim Missbrauch von Zugangsdaten im Internet die Wahl den Schein gelten zu lassen und den Account-Inhaber in Anspruch zu nehmen oder die tatsächliche Lage zu Grunde zu legen und sich an den Handelnden zu wenden.

7. Zwischenergebnis

715 Nach den Grundsätzen der allgemeinen Rechtsscheinhaftung besteht ein Rechtsscheintatbestand dafür, dass der Account-Inhaber eine Erklärung über seinen Account abgegeben hat, wenn eine sichere Authentisierungsmethode wie die Zwei-Faktor-Authentisierung verwendet und die Identität des Account-Inhabers bei Erstellung des Accounts überprüft wird.[869] Zurechenbar ist dem Account-Inhaber dieser Rechtsscheintatbestand nur, wenn er die Zugangsdaten willentlich übergeben hat.[870]

---

862 *Herresthal*, K&R 2008, 705, 709; *ders.*, in: *Taeger/Wiebe*, 21, 39; *Klees*, MDR 2007, 185, 188; *Kuhn*, S. 239; *Spiegelhalder*, S. 174.
863 Siehe oben Rn. 259.
864 So auch *Rieder*, S. 317.
865 Allgemein dazu oben Rn. 260.
866 Siehe oben Rn. 260.
867 Vgl. *Canaris*, Vertrauenshaftung, S. 519; *M. Wolf/Neuner*[10], Kap. 51 Rn. 112.
868 So *Canaris*, Vertrauenshaftung, S. 519.
869 Oben Rn. 670.
870 Oben Rn. 709.

VII. Zwischenergebnis

716 Der Missbrauch von Zugangsdaten im Internet lässt sich nicht überzeugend über die Anscheinsvollmacht lösen, weil mangels Erkennbarkeit des Dritten kein Rechtsschein bezüglich dessen Berechtigung zu handeln besteht.[871] Sofern vertragliche Beziehungen zwischen dem Account-Inhaber und dem Authentisierungsnehmer vorliegen, kann das Problem über diese vertraglichen Vereinbarungen und Pflichten gelöst werden.[872] Solche vertraglichen Vereinbarungen fehlen jedoch häufig, beispielsweise bei Drei-Personen-Konstellationen, bei denen Authentisierungsnehmer und Geschäftsgegner auseinanderfallen.[873] Für diese Konstellationen kann über eine Lösung über die *culpa in contrahendo* nachgedacht werden, die jedoch regelmäßig an einem vorvertraglichen Schuldverhältnis scheitert.[874] Der vertraglichen Beziehung zwischen Account-Inhaber und Authentisierungsnehmer Schutzwirkungen zu Gunsten des Geschäftsgegners zuzusprechen, kann in Drei-Personen-Konstellationen wegen der mangelnden Leistungsnähe des Geschäftsgegners und der fehlenden Erkennbarkeit für den Account-Inhaber das Problem nicht überzeugend lösen.[875] Eine Lösung über die analoge Anwendung des § 122 BGB scheitert an der fehlenden Vergleichbarkeit der Interessenlage.[876] Eine deliktische Lösung über § 823 Abs. 1 BGB scheitert an der fehlenden Ersatzfähigkeit fahrlässig verursachter Vermögensschäden.[877] Eine Lösung über § 823 Abs. 2 BGB scheitert an dem Vorliegen von Schutzgesetzen.[878]

717 Die Haftung für den Missbrauch von Zugangsdaten im Internet lässt sich überzeugend mit den allgemeinen Grundsätzen der Rechtsscheinhaftung lösen.[879] Ein Rechtsscheintatbestand besteht nur bei Verwendung einer hinreichend sicheren Authentisierungsmethode und bei hinreichend zuverlässiger Identifikationsfunktion des Accounts. Eine hinreichend sichere Authentisierungsmethode stellt die Zwei-Faktor-Authentisierung dar.[880] Die rein

871 Oben Rn. 370 ff.
872 Oben Rn. 397.
873 Oben Rn. 292.
874 Oben Rn. 428 ff.
875 Oben Rn. 403 ff.
876 Oben Rn. 471 ff.
877 Oben Rn. 487.
878 Oben Rn. 487.
879 Oben Rn. 489 ff.
880 Oben Rn. 578 ff.

wissensbasierte Authentisierung hingegen begründet keinen Rechtsschein für das Handeln des Account-Inhabers.[881] Eine Haftung für die Weitergabe der Zugangsdaten bei einer rein wissensbasierten Authentisierung scheidet somit entgegen der dazu vertretenen Ansichten aus. Die Lösung über die Duldungsvollmacht[882] oder über eine analoge Anwendung des § 172 Abs. 1 BGB[883] überzeugen somit weder in der Begründung des Lösungswegs noch im Ergebnis. Bei welchen Account-Typen eine Haftung des Account-Inhabers in Betracht kommt, wird noch ausführlich untersucht.[884]

881 Oben Rn. 544 ff.
882 Oben Rn. 297 ff.
883 Oben Rn. 303 ff.
884 Unten Rn. 830.