§ 2 Technische Grundlagen

I. Internet

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

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

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

---

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

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

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

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

II. Zugangsdaten

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

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

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

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

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

1. Identität

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. *Identifikationsfunktion von Accounts im Internet*

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

---

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

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

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

a) Internetzugang – IP-Adresse

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

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

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

51 Nach *IETF*, RFC 791.

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

53 Standardisiert durch *IETF*, RFC 2460.

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

aa) Internetanschluss

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

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

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

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

bb) WLAN

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

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

cc) IP-Adresse

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

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

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

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

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

---

68 *Sieber*, in: *Hoeren/Sieber/Holznagel*, Kap. 1 Rn. 54, 63 f.
69 Ebd., Kap. 1 Rn. 55.
70 Mit einer Whois-Abfrage können die gespeicherten Bestandsdaten zu einer IP-Adresse oder Domain bei der zuständigen Registrierungsstelle abgefragt werden.
71 *M. Köhntopp/K. Köhntopp*, CR 2000, 248; *Grosskopf*, CR 2007, 122, 123.
72 *Alsbih*, DuD 2011, 482; *Grosskopf*, CR 2007, 122, 123; *Gietl/Mantz*, CR 2008, 810, 814 f.; *Hannemann/Solmecke*, MMR 2011, 398, 400.
73 *Brunst*, Anonymität im Internet, S. 130; *Dennis Werner*, Verkehrspflichten, S. 38; *Jandach*, in: FS Kilian, 443, 446.
74 *Brunst*, Anonymität im Internet, S. 133; *Gaycken*, S. 236.
75 *Brunst*, Anonymität im Internet, S. 133; *Jandach*, in: FS Kilian, 443, 446.

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

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

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

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

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

b) E-Mail-Adresse

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

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

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

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

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

85 Definiert durch *IETF*, RFC 2822.

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

87 *Borges*, Verträge, S. 23.

88 Nach dem Standard *IETF*, RFC 5321.

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

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

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

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

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

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

---

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

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

93 Standardisiert durch *IETF*, RFC 1939.

94 Nach *IETF*, RFC 3501.

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

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

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

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

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

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

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

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

100 Ebd., S. 87.

101 *J. Meyer*, Identität, S. 37.

102 *S. Münch*, S. 154.

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

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

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

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

c) Passwortgeschützte Benutzerkonten auf Internetseiten

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

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

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

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

aa) Informationsportale

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

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

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

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

bb) eCommerce-Seiten, Online-Shops

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

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

sätzlich eine Identifikationsfunktion bezüglich einer numerischen Identität zukommen.

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

cc) Internet-Auktionsplattformen mit Reputationssystem

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

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

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

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

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

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

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

131 *ULD*, S. 171.

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

133 *ULD*, S. 170.

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

135 *ULD*, S. 169.

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

137 Dazu ausführlich unten Rn. 620.

d) Online-Banking

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

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

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

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

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

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

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

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

143 *Schwintowski*[3], § 5 Rn. 56.

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

145 *Schwintowski*[3], § 5 Rn. 52.

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

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

e) Online-Bezahldienste

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

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

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

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

f) Elektronische Signatur

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

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

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

aa) Formen der elektronischen Signatur

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

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

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

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

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

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

bb) Asymmetrische Verschlüsselung

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

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

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

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

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

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

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

cc) Der Zertifizierungsdiensteanbieter als Trusted Authority

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

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

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

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

dd) Die Akzeptanz der elektronischen Signatur

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

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

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

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

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

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

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

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

ee) Exkurs: Ausblick

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

87

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

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

g) Elektronischer Identitätsnachweis im neuen Personalausweis (nPA)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

h) De-Mail

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

i) Zwischenergebnis zu den staatlichen Maßnahmen

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

3. Authentisierung, Authentifizierung und Autorisierung

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

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

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

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

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

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

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

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

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

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

a) Authentisierungsmittel

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

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

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

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

283 Oben Rn. 105.

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

aa) Wissen

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

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

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

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

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

bb) Besitz

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

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

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

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

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

cc) Sein

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

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

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

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

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

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

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

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

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

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

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

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

b) Zwei- und Mehr-Faktor-Authentisierung

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

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

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

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

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

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

4. Besondere Merkmale von Zugangsdaten im Internet

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

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

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

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

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

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

III. Missbrauch

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

1. Missbrauch nach bewusster Weitergabe der Zugangsdaten

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

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

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

2. *Missbrauch ohne bewusste Weitergabe der Zugangsdaten*

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

---

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

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

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

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

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

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

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

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

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

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

a) Wege, um an die Zugangsdaten zu gelangen

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

aa) Physikalischer Zugriff auf die Zugangsdaten

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

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

354 *Spindler*, CR 2003, 534.

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

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

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

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

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

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

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

bb) Zugriff zu gespeicherten Zugangsdaten

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

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

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

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

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

cc) Phishing

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

aaa) Klassisches Phishing

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

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

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

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

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

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

378 *Knupfer*, MMR 2004, 641.

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

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

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

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

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

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

---

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

bbb) Pharming

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

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

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

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

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

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

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

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

403 Zu den Infektionswegen unten Rn. 182 ff.

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

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

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

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

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

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

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

409 *Popp*, MMR 2006, 84.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ccc) Zweite Phase: die Internetseite des Angreifers

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

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

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

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

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

dd) Social Engineering

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

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

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

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

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

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

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

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

ee) Keylogger

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

gg) Sniffing: Mitlesen des Datenverkehrs

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

b) Infektionswege

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

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

aa) Sicherheitslücken in Programmen, Zero-Day-Exploits

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

513 *Schwenk/Gajek*, in: Internet-Auktion, 180, 183; *Gaycken*, S. 238; *Schneier*, S. 151; *Dennis Werner*, Verkehrspflichten, S. 57. Vgl. auch die Legaldefinition von Schadprogrammen in § 2 Abs. 5 BSIG.
514 *BKA*, S. 9; *Gaycken*, S. 238.
515 *Ernst*, CR 2006, 590, 591; *Frank*, in: Informationsstrafrecht, 23, 24.
516 *Ernst*, CR 2006, 590, 591; *Mantz*, offene Netze, S. 39; *Dennis Werner*, Verkehrspflichten, S. 58.
517 *BSI*, Lagebericht 2011, S. 25.
518 Ebd., S. 25; *Höhmann*, heise online v. 9. 7. 2012.
519 *BSI*, Lagebericht 2011, S. 25.
520 Unten Rn. 202.
521 *BSI*, Lagebericht 2011, S. 26.
522 *Graf*, in: MüKo-StGB^2, § 202a Rn. 66. Allgemein zu Programmierfehlern *Taeger*, S. 47 ff.

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

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

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

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

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

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

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

bb) Computervirus

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

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

cc) Computerwurm

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

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

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

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

dd) Trojanisches Pferd, Trojaner

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

545 *Erfurth*, WM 2006, 2198, 2199; *Sodtalbers*, Rn. 123; *Dennis Werner*, Verkehrspflichten, S. 60; *Pierrot*, in: *Ernst*, Rn. 109.
546 *Mantz*, offene Netze, S. 38; *Dennis Werner*, Verkehrspflichten, S. 61; *Wien*[3], S. 195.
547 *Henning*, in: *U. Schneider/Dieter Werner*[7], 11.7.1; *Dennis Werner*, Verkehrspflichten, S. 61. So der ILOVEYOU-Wurm, dazu *Eckert*[8], S. 70; *Frank*, in: Informationsstrafrecht, 23.
548 *Dennis Werner*, Verkehrspflichten, S. 61.
549 Dazu oben Rn. 185.
550 *Eckert*[8], S. 68.
551 *BSI*, Lagebericht 2011, S. 23.
552 *Eckert*[8], S. 73; *Holznagel*, § 3 Rn. 13; *Schneier*, S. 155.
553 *BSI*, IT-Grundschutz-Kataloge, G 5.21; *Frank*, in: Informationsstrafrecht, 23, 26; *Gaycken*, S. 241; *Sodtalbers*, Rn. 127; *Dennis Werner*, Verkehrspflichten, S. 62; *Graf*, in: MüKo-StGB[2], § 202a Rn. 64; *Schneier*, S. 155; *Schwenk*[3], S. 243.

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

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

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

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

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

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

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

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

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

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

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

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

ee) Rootkits

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

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

ff) Drive-By-Infection

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

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

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

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

c) Schutz gegen Infektionen des Rechners

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

aa) Antiviren-Programm

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

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

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

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

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

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

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

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

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

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

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

bb) Firewall

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

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

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

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

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

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

3. Missbrauch durch Erstellen eines Accounts unter falschem Namen

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

4. Missbrauch ohne Erlangen der Zugangsdaten vom Account-Inhaber

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

a) Mail-Spoofing

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

---

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

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

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

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

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

b) Schwachstellen beim Authentisierungsnehmer

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

aa) SQL-Injection

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

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

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

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

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

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

bb) Cross-Site-Scripting (XSS)

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

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

cc) Schwachstellen in der IT-Infrastruktur

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

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

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

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

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

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

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

650 *Fox*, DuD 2012, 840.

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

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

dd) Unbefugte Weitergabe der Zugangsdaten

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

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

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

653 Dazu oben Rn. 181.

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

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

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

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

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