

Rechtliche Aspekte der Internetportale für Heilberufe

– Zugang, Beweis, Datensicherung –

Stellungnahme zum Stand und zur Entwicklung der Rechtslage

im Auftrag des TeleTrust Deutschland e.V. (TeleTrust)

von Prof. Dr. Georg Borges
Ruhr-Universität Bochum

INHALTSÜBERSICHT

A.	Einführung	S. 7
B.	Sachverhalt	S. 9
C.	Sicherer Zugang von Nachrichten in Internetportalen	S. 20
D.	Nachweis von Handlungen am Account des Teilnehmers	S. 42
E.	Anforderungen an Datensicherheit bei Internetportalen	S. 63
F.	Zusammenfassung der Ergebnisse	S. 82

INHALT

A.	Einführung	S. 7
B.	Sachverhalt	S. 9
I.	Internetportale für Heilberufe	S. 9
II.	Die Online-Abrechnung	S. 10
1.	Die Abrechnung zwischen Arzt und Kassenärztlicher Vereinigung	S. 10
2.	Die bisherige elektronische Abrechnung	S. 11
3.	Neue Verfahren der elektronischen Abrechnung	S. 11
4.	Die Online-Abrechnung im Internetportal für Heilberufe	S. 12
III.	Zugangssicherung von Internetportalen und internet- basierte Angriffe	S. 12
1.	Missbrauchsrisiken	S. 13
2.	Phishing und andere internetbasierte Angriffe	S. 14
IV.	Authentisierungsverfahren bei Internetportalen für Heilberufe	S. 16
1.	Authentisierungsverfahren	S. 16
a)	Passwort	S. 16
b)	Passwort und Softzertifikat	S. 17
c)	Chipkarte und PIN	S. 17
2.	Die zur Authentisierung verwendeten Chipkarten	S. 18
a)	Technische Eigenschaften	S. 19
b)	Das Ausgabeverfahren	S. 19
C.	Sicherer Zugang von Nachrichten in Internetportalen	S. 20
I.	Die rechtliche Bedeutung des Zugangs von Nachrichten	S. 20
II.	Grundsätze des Zugangs bei elektronischer Übermitt- lung von Erklärungen	S. 21
1.	Zugangsvarianten bei elektronischer Übermittlung von Erklärungen	S. 21

2.	Zugang durch Speicherung	S. 22
3.	Zugang durch Kenntnisnahme	S. 24
4.	Zugangsstörungen und Übermittlungsrisiko	S. 25
5.	Zugangsvereitelung und Obliegenheiten des Empfängers	S. 26
a)	Zugangsvereitelung	S. 27
b)	Obliegenheits- und Pflichtverletzungen	S. 28
aa)	Obliegenheitsverletzungen und Zugang	S. 28
bb)	Zugangsbezogene Pflichten bei elektro- nischer Übermittlung	S. 29
c)	Zugang und Spam-Filter	S. 30
6.	Der Zeitpunkt des Zugangs	S. 31
III.	Zugang bei Internetportalen für Heilberufe	S. 32
1.	Zugang durch Einstellen ins Postfach	S. 33
a)	Die materiellrechtlichen Voraussetzungen des Zugangs	S. 33
b)	Der Zeitpunkt des Zugangs	S. 34
2.	Wirksamwerden durch Kenntnisnahme	S. 35
3.	Zugang durch Bereitstellung zum Abruf	S. 36
a)	Bereitstellung und Zugangserfordernis	S. 36
b)	Mitwirkungspflichten	S. 36
4.	Zugang und Eingriffe Dritter	S. 37
5.	Die Bedeutung von Lesebestätigungen	S. 39
6.	Beweis des Zugangs	S. 40
a)	Beweis des Zugangs durch Speicherung	S. 40
b)	Beweis des Zugangs durch Kenntnisnahme	S. 41
D.	Nachweis von Handlungen am Account des Teilnehmers	S. 42
I.	Die Relevanz des Beweises der Urheberschaft von Handlungen	S. 42
II.	Der Beweis der Urheberschaft im gerichtlichen Verfahren	S. 43
1.	Die maßgebliche Regelung des Beweises	S. 43
2.	Der Nachweis der Urheberschaft	S. 44

3.	Die Anforderungen an den Beweis der Urheberschaft	S. 45
III.	Der Anscheinsbeweis der Urheberschaft	S. 46
1.	Allgemeine Grundsätze des Anscheinsbeweises	S. 46
2.	Der Anscheinsbeweis für die Urheberschaft einer elektronisch übermittelten Erklärung	S. 49
IV.	Anscheinsbeweis der Urheberschaft bei Internetportalen für Heilberufe	S. 49
1.	Anscheinsbeweis bei einfachem Passwortschutz	S. 50
a)	Bestehen eines Anscheins	S. 50
b)	Erschütterung des Anscheins	S. 51
c)	Ergebnis	S. 53
2.	Anscheinsbeweis bei Softzertifikat	S. 53
3.	Anscheinsbeweis bei Chipkarte	S. 54
a)	Anscheinsbeweis bei Verwendung von ec-Karte und PIN	S. 55
b)	Der Anscheinsbeweis bei qualifizierter elektronischer Signatur nach § 371a ZPO	S. 58
c)	Anscheinsbeweis bei Internetportalen mit Chipkartenschutz	S. 58
d)	Erschütterung	S. 60
aa)	Unbefugte Verwendung der Chipkarte durch Dritte	S. 60
bb)	Erschütterung durch Phishing-Angriffe	S. 61
V.	Ergebnis	S. 62
E.	Anforderungen an die Datensicherheit bei Internetportalen	S. 63
I.	Die gesetzlichen Anforderungen an die Datensicherheit	S. 63
1.	Datensicherheit im SGB X und den allgemeinen Datenschutzgesetzen	S. 63
2.	Die Anforderungen an die Datensicherheit	S. 65
3.	Datensicherheit und Haftung	S. 68
II.	Anforderungen an Authentisierungssysteme bei Internetportalen	S. 70

1.	Authentisierungssystem und Missbrauchsgefahren	S. 70
2.	Eignung zur Abwehr „konventioneller“ Angriffe	S. 71
3.	Eignung zur Abwehr internetbasierter Angriffe	S. 72
	a) Authentisierung durch Passwort	S. 72
	b) Softzertifikate	S. 73
	c) Chipkarte und PIN	S. 73
	d) Zwischenergebnis	S. 74
III.	Erforderlichkeit von Schutzmaßnahmen	S. 75
	1. Die maßgeblichen Kosten der Authentisierungssysteme	S. 75
	2. Schutzwürdigkeit der Daten	S. 76
	3. Abwägung	S. 77
	a) Bisherige Anforderungen an Sicherung von Patientendaten	S. 77
	b) Verhältnismäßigkeit hochwertiger Authentisierungssysteme	S. 79
IV.	Ergebnis	S. 80
F.	Zusammenfassung der Ergebnisse	S. 82
	I. Sicherer Zugang von Nachrichten in Internetportalen	S. 82
	II. Nachweis von Handlungen am Account des Teilnehmers	S. 83
	III. Anforderungen an die Datensicherheit bei Internetportalen für Heilberufe	S. 84

A. Einführung. Rechtsfragen zu Internetportalen für Heilberufe

Internetportale für Heilberufe sind derzeit in der Diskussion. Zahlreiche Kassenärztliche und Kassenzahnärztliche Vereinigungen erwägen die Einführung derartiger Portale, die für die Vereinigungen und ihre Angehörigen zahlreiche Vorteile bieten, vor allem dann, wenn die Online-Abrechnung in die Portale integriert ist. Derartige Internetportale werfen zahlreiche Rechtsfragen auf. Zu den wesentlichen Aspekten gehören Fragen der Rechtssicherheit sowie der Haftung, insbesondere im Zusammenhang mit Patientendaten, die im Rahmen der Online-Abrechnung verwendet werden.

Fragen der tatsächlichen und rechtlichen Sicherheit von Internetportalen haben durch aktuelle Bedrohungen wie Phishing und ähnliche Angriffe stark an Bedeutung gewonnen. Das Phänomen des Phishing macht mit großem Nachdruck deutlich, dass internetbasierte Angriffe gegen Internetportale, die über die Accounts der Teilnehmer geführt werden, eine ernstzunehmende Bedrohung für Portale mit geschlossenen Teilnehmerbereichen und eine Herausforderung an die Gestaltung der Portale sind.

TeleTrust ist ein gemeinnütziger Verein, der es sich zur Aufgabe gemacht hat; die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik in einer offenen Systemumgebung zu fördern. Dies gilt in besonderer Weise für das Ziel einer vertrauenswürdigen IT in Medizin und Gesundheitsverwaltung sowie im elektronischen Rechtsverkehr. TeleTrust bittet um Stellungnahme zur Rechtslage und ggf. Ausblicken auf die künftige Rechtsentwicklung zu folgenden Aspekten:

(1) Zugang von Erklärungen

Im Rahmen von Internetportalen für Heilberufe ist es für den Betreiber von Bedeutung, den Teilnehmern zugangsbedürftige Erklärungen rechtswirksam über das Portal übermitteln und den Zugang nachweisen zu können.

TeleTrust fragt daher, ob und unter welchen Voraussetzungen der Zugang von Erklärungen über das Portal rechtlich wirksam erfolgt und nachweisbar ist.

(2) Beweis der Urheberschaft der Erklärungen von Teilnehmern

Die Teilnehmer an Internet-Portalen für Heilberufe nehmen vielfach Handlungen an ihrem Account vor, die für das Verhältnis zwischen Teilnehmer und Portalbetreiber rechtlich relevant sind. So werden Erklärungen an den Portalbetreiber übermittelt oder relevante tatsächliche Handlungen vorgenommen, etwa das Herunterladen des Honorarbescheids.

Es ist daher von Interesse, dass in einem etwaigen Rechtsstreit bewiesen werden kann, dass die betreffende Erklärung vom Teilnehmer abgegeben und eine tatsächliche Handlung von ihm und nicht etwa von einem Dritten vorgenommen wurde.

TeleTrust fragt daher, wie und unter welchen Voraussetzungen der Nachweis geführt werden kann, dass die betreffende Erklärung oder eine bestimmte Handlung am Account des Teilnehmers vom Teilnehmer und nicht von einem Dritten vorgenommen wurde.

(3) Anforderungen an die Authentisierung der Teilnehmer nach Datenschutzrecht

Das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutzgesetze enthalten unter anderem Anforderungen an die Datensicherheit, die den Schutz von Daten vor Missbrauch durch Dritte einschließt. Eine Verletzung dieser Anforderungen kann eine Haftung des Portalbetreibers auslösen. Ein wesentliches Element der Datensicherung ist die sichere Authentisierung der Nutzer. Angesichts aktueller Angriffe wie Phishing und ähnlicher Formen der Internetkriminalität kommt der Datensicherung, insbesondere der Authentisierung, besondere Bedeutung zu. TeleTrust fragt daher, welche Anforderungen sich aus Datenschutzrecht an die Authentisierungsverfahren ergeben.

Die Erörterung dieser Aspekte bezieht sich spezifisch auf Internetportale für Heilberufe. Die Untersuchung ist daher nicht uneingeschränkt auf andere Bereiche übertragbar.

B. Sachverhalt

I. Internetportale für Heilberufe

Angehörige von Heilberufen nutzen zunehmend das Internet. Das Internet wird vor allem für Informationszwecke genutzt, aber auch für die Übermittlung von Daten im Rahmen der Online-Abrechnung mit den Kassenärztlichen Vereinigungen etc. sowie für die Übermittlung von Nachrichten per E-Mail.

Ein neuer Trend der Internetnutzung ist die Einrichtung von Internetportalen für Heilberufe, die oft auf bestimmte Heilberufe zugeschnitten sind. Derartige Portale werden für den Bereich der Zahnärzte durch das Projekt „Zahnärzte Online Deutschland“ (ZOD) der Kassenzahnärztlichen Bundesvereinigung (KZBV) vorbereitet.¹

Besondere Bedeutung haben die von den Berufsorganisationen, etwa den Kassenärztlichen Vereinigungen, betriebenen Portale. Nutzer dieser Portale sind regelmäßig vor allem Angehörige des jeweiligen Heilberufs (z.B. Zahnärzte), bei den Kassenärztlichen Vereinigungen jeweils die jeweiligen Mitglieder. Die Portale bieten eine Reihe von Leistungen an, etwa Informationsdienstleistungen. Besonders wichtig ist die Online-Abrechnung zwischen den Angehörigen der Heilberufe und den jeweiligen Kassen- bzw. Kassenzahnärztlichen Vereinigungen. Die Einführung derartiger Portale unter Einbeziehung der Online-Abrechnung wird derzeit in zahlreichen Kassenärztlichen Vereinigungen und Kassenzahnärztlichen Vereinigungen geplant oder zumindest erwogen. Die Kassenzahnärztliche Vereinigung Nordrhein² und die Kassenzahnärztliche Vereinigung Westfalen-Lippe³ betreiben bereits mit Erfolg entsprechende Portale, die ihren Nutzern unter anderem eine Online-Abrechnung bieten.

Die Portale stellen regelmäßig eine Reihe verschiedener Dienste zur Verfügung und differenzieren zwischen einem frei zugänglichen und einem

¹ Siehe die Informationswebsite „www.zahnaerzte-online.de“.

² Vgl. www.mykzv.de.

³ Vgl. www.zahnaerzte-wl.de.

geschützten Bereich, der nur für zugelassene Teilnehmer, im wesentlichen Mitglieder der jeweiligen KV bzw. KZV, zugänglich ist. Im frei zugänglichen Bereich werden verschiedene Informationen für Ärzte bzw. Zahnärzte bereitgestellt. Die wichtigeren Dienste sind jedoch nur im Teilnehmerbereich zugänglich. Der Zugang zum Teilnehmerbereich erfordert jeweils eine Authentisierung des Teilnehmers (dazu unten 3.). Zu den Diensten des Teilnehmerbereichs gehört typischerweise ein Postfach des Vertragsarztes⁴, die Möglichkeit, Einblick in das Finanzbuchhaltungskonto der Praxis zu nehmen, die Anforderung von Sofortauszahlungen des Honorars und weitere Serviceangebote. Außerdem wird die Einsicht in verschiedene Dokumente ermöglicht. Dazu gehören etwa der Rechnungsabschluss zwischen der KV bzw. KZV und dem Vertragsarzt, Korrekturbelege, Nachrichten der KV bzw. KZV an ihre Mitglieder, sowie sonstige Belege und Bescheide.

II. Die Online-Abrechnung

1. Die Abrechnung zwischen Arzt und Kassenärztlicher Vereinigung

Die von Vertragsärzten für Kassenpatienten erbrachten Leistungen werden über die zuständige Kassenärztliche Vereinigung vergütet. Die Abrechnung erfolgt durch die Vereinigung auf der Grundlage von Abrechnungsdaten, die beim Arzt durch die Praxissoftware erstellt werden. Die Abrechnungsdaten enthalten unter anderem den Namen des Patienten sowie Abrechnungskennziffern, aus denen sich die Art der Behandlung ergibt. Daneben wird im Regelfall auch die Diagnose des Arztes dokumentiert.

Die Kassenärztliche Vereinigung berechnet jeweils quartalsweise in der Abrechnung die endgültige Vergütung für jeden Arzt. Die Abrechnung, die sehr umfangreich sein kann, wird dem Arzt übermittelt. Traditionell wird die Abrechnung auf Papier ausgedruckt und auf dem Postweg an den Arzt versandt.

⁴ Der Begriff „Vertragsarzt“ bedeutet im folgenden Vertragsärzte sowie Vertragszahnärzte.

2. Die bisherige elektronische Abrechnung

Praxissoftware und Patientendaten werden bisher aus Sicherheitsgründen regelmäßig auf Rechnern des Arztes gespeichert, die keine Verbindung zum Internet haben. Der Versand der Abrechnungsdaten vom Arzt an die Kassenärztliche Vereinigung konnte bisher auf Papier oder in elektronischer Form erfolgen. Künftig ist nur noch der Versand in elektronischer Form zulässig. Beim Versand der Daten in elektronischer Form erfolgt der Versand entweder über Diskette auf dem Postweg oder über ein Extranet. Die Abrechnung wird auch in diesem Verfahren als Ausdruck an den Arzt verschickt.

3. Neue Verfahren der elektronischen Abrechnung

Es besteht ein zunehmendes Bedürfnis der Angehörigen von Heilberufen und der Kassenärztlichen Vereinigungen nach einer Ablösung der traditionellen Abrechnung durch eine Online-Abrechnung. Die Online-Abrechnung führt zu erheblichen Vereinfachungen beim Versand der Abrechnungsdaten, da die Übermittlung auf Papierausdruck oder Diskette entfällt. Vielmehr können die Abrechnungen unmittelbar von den Rechnern, auf denen die Praxissoftware betrieben wird, elektronisch an die Kassenärztliche Vereinigung übersandt werden. Die Online-Abrechnung erspart weiterhin die Übersendung der Abrechnung in Papierform an den Arzt. Stattdessen wird die Abrechnung in elektronischer Form auf dem Server der Kassenärztlichen Vereinigung hinterlegt und kann vom Arzt eingesehen, heruntergeladen und ggf. ausgedruckt werden.

Die Online-Abrechnung kann in weitere Dienste integriert werden. So bieten einige Kassenärztliche und Kassenzahnärztliche Vereinigungen über ihr Portal eine Probeabrechnung an, die es dem Vertragsarzt während des laufenden Quartals ermöglicht, die zu übermittelnden Abrechnungsdaten auf syntaktische und inhaltliche Fehlerfreiheit zu überprüfen. Die Online-Abrechnung wird besonders komfortabel, wenn sie in das Internetportal der Kassenärztlichen Vereinigung integriert ist.

4. Die Online-Abrechnung im Internetportal für Heilberufe

Wenn das Portal für seine Teilnehmer eine Online-Abrechnung anbietet, wie es etwa im Portal mykzv der KZV Nordrhein der Fall ist, wird die Übermittlung der Abrechnungsdaten an die Kassenärztliche bzw. Kassenzahnärztliche Vereinigung regelmäßig in das Portal integriert. Zur Übermittlung der Daten ist eine Anmeldung im Teilnehmerbereich erforderlich. Im Teilnehmerbereich kann die Übertragung über ein spezifisches Formular ausgelöst werden.

Wenn der Honorarbescheid erstellt wurde, wird er nebst Anlagen auf dem Server bereitgestellt und der Vertragsarzt elektronisch darüber benachrichtigt, dass der Bescheid zur Verfügung steht. Der Vertragsarzt kann sodann den Bescheid einsehen, herunterladen und ggf. ausdrucken. Zur Sicherheit wird der Honorarbescheid – ohne Anlagen – meist per Post an den Vertragsarzt geschickt.

Da die fristgemäße Zustellung des Honorarbescheids an den Vertragsarzt für die Kassenärztliche bzw. Kassenzahnärztliche Vereinigung wichtig ist, werden meist besondere Vorkehrungen zur Sicherung der Zustellungsfrist getroffen. Da der Bescheid aus Sicherheitsgründen nicht an den Vertragsarzt verschickt wird, sondern auf dem Server der Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigung verbleibt und vom Vertragsarzt dort eingesehen wird, wird gleichzeitig mit der Bereitstellung des Honorarbescheids eine Benachrichtigung in das Postfach des Vertragsarztes eingestellt. Das Öffnen dieser Benachrichtigung durch den Vertragsarzt wird mit Datum und Uhrzeit protokolliert. Wenn die Authentisierung durch Verwendung einer Chipkarte erfolgt, kann gleichzeitig protokolliert werden, über welche Chipkarte die Verbindung aufgebaut wurde, innerhalb derer die Nachricht geöffnet wurde. Damit wird der Inhaber der jeweiligen Chipkarte als Öffnender identifiziert.

III. Zugangssicherung von Internetportalen und internetbasierte Angriffe

Die Authentisierung der Teilnehmer beim Zugriff auf den Teilnehmerbereich von Internetportalen ist in mehrfacher Hinsicht von herausragender Bedeutung. Zum einen sichert sie die über das Portal

einsehbaren Daten vor dem Zugriff durch Unbefugte und zum anderen identifiziert sie die Person, die über das Portal rechtserhebliche Handlungen vornimmt, etwa Erklärungen abgibt oder entgegennimmt.

1. Missbrauchsrisiken

Die Anforderungen an die Authentisierung der Teilnehmer an Internetportalen für Heilberufe richten sich maßgeblich nach den Missbrauchsrisiken. Dabei sind unter dem Gesichtspunkt der Authentisierung solche Missbräuche durch unbefugte Dritte relevant, die aufgrund des Zugangs zum Teilnehmerbereich des Portals ermöglicht werden. Bei Portalen für Heilberufe erscheinen verschiedene Missbräuche denkbar: So könnten falsche Abrechnungsdaten durch Dritte eingestellt werden, Zahlungen veranlasst werden, es könnten Nachrichten, die für den Teilnehmer bestimmt sind, gelöscht, verändert oder als gelesen markiert werden, die Finanzdaten des Teilnehmers könnten eingesehen werden und ähnliches. Die Missbrauchsmöglichkeiten hängen im Einzelnen stark von der Ausgestaltung des Portals ab. So sind die Postfächer einzelner Portalbetreiber so konfiguriert, dass Nachrichten, die ins Postfach des Vertragsarztes eingestellt wurden, weder vom Vertragsarzt noch von Dritten gelöscht werden können. Bei anderen Portalen hat der Vertragsarzt die Möglichkeit, eingegangene Nachrichten zu löschen.

Vor allem aber könnte der Dritte während der Übertragung Einsicht in die Patientendaten nehmen, die zum Zwecke der Abrechnung auf dem Server des Portalbetreibers gespeichert sind. Dies gilt aber nur, soweit der Portalbetreiber im Teilnehmerbereich den Zugriff auf diese Daten einräumt. Dies ist teilweise lediglich bei Daten mit Änderungen der Fall. Andere Anbieter sind hier aber großzügiger und erlauben Einsicht in alle Abrechnungsdaten.

Derartige Missbräuche an Internetportalen für Heilberufe sind möglich, wenn unbefugte Personen die Zugangssperre überwinden, etwa weil sie sich die Möglichkeit verschaffen, die Authentisierungsmedien des Teilnehmers zu verwenden. Besondere Bedeutung haben in jüngster Zeit internetbasierte Angriffe wie Phishing und Trojaner-Angriffe, die die Rechtssicherheit im elektronischen Geschäftsverkehr gefährden.

2. Phishing und andere internetbasierte Angriffe

Die Problematik des Phishing und ähnlicher Angriffe wird aufgrund der seit 2004 in den USA, seit 2005 auch in Deutschland und anderen europäischen Staaten zahlreich auftretenden Phishing-Angriffe zunehmend als eine Gefahr für den elektronischen Geschäftsverkehr wahrgenommen. Seit 2004 hat der Umfang an Phishing-Angriffen und das Ausmaß der dadurch verursachten Schäden dramatisch zugenommen.⁵ Am stärksten betroffen sind bisher das Onlinebanking, danach mit großem Abstand das Auktionshaus eBay.

Diese Formen der Internetkriminalität erfolgen meist in der Weise, dass die Täter, die überwiegend vom Ausland aus agieren, geheime Daten, wie Passwörter, PIN und TAN der Kunden erbeuten und damit Transaktionen vornehmen, etwa eine Überweisung im Onlinebanking veranlassen, oder betrügerische Angebote in fremde eBay-Accounts einstellen.⁶

Es sind verschiedene Formen von internetbasierten Angriffen auf Zugangsdaten bekannt. Beim Phishing im engeren Sinne sendet der Täter dem Opfer eine E-Mail, die wie die eines Geschäftspartners, etwa der Bank, erscheint und ihn auffordert, sich über einen mitgesandten Link bei der Bank anzumelden. Der Link führt aber zu einer gefälschten – oft täuschend echt aussehenden – Website der Täter, die zur Eingabe der Authentisierungsdaten (Passwort, PIN und TAN) auffordert.⁷

Beim Pharming oder DNS-Spoofing wird die Zuordnung von IP-Adressen zu Websites gefälscht.⁸ In der Praxis erfolgt dies bisher fast ausschließlich durch eine Manipulation der lokalen Zuordnungstabelle, der sogenannten

⁵ Laut dem Dezember-Bericht der Anti Phishing Working Group (APWG) wurde im Oktober 2006 ein neuer Höchststand an Phishing-Websites erreicht (insgesamt 37.444). Im Dezember 2006 lag die Zahl mit 28.531 immerhin noch rund 4 mal so hoch wie im Dezember 2005. Der Bericht ist abrufbar unter http://www.antiphishing.org/reports/apwg_report_december_2006.pdf:

⁶ *Borges*, NJW 2005, 3313.

⁷ *Borges*, NJW 2005, 3313 f.

⁸ Zu den unterschiedlichen Methoden eines Pharming-Angriffs s. auch *Atkins/Austein*, Threat Analysis of the Domain Name System, RFC 3833, August 2004, abrufbar unter <http://www.rfc-archive.org/getrfc.php?rfc=3833>.

hosts-Datei, auf dem Rechner des Teilnehmers.⁹ Diese Manipulation wird durch Trojaner verursacht, die der Täter per Internet auf den Rechner des Teilnehmers schleust.¹⁰

Die meisten Schäden werden derzeit durch Trojaner-Angriffe verursacht.¹¹ Zum Erschleichen von Passwörtern werden oft Keylogger verwendet, die die Eingabe des Passworts über die Tastatur protokollieren und die aufgezeichneten Daten per Internet an den Täter senden. Bei Angriffen im Onlinebanking wird nicht nur die Eingabe der PIN bei der Authentisierung auf der Website der Bank, sondern auch die Eingabe der TAN protokolliert und sodann der Abbruch der Internet-Verbindung veranlasst. Daneben sind freilich deutlich aufwendigere Trojaner bekannt, die in der Lage sind, auch komplexere Authentisierungssysteme zu überwinden.¹²

Die Bedrohung des elektronischen Geschäftsverkehrs durch Phishing und ähnliche Angriffe, die an der Authentisierung ansetzen und auf diese Weise Zugang zu Portalen und Webseiten erhalten, ist erst seit kurzem ins Bewusstsein der Öffentlichkeit getreten. Aufgrund der aktuellen Entwicklung besteht aber kein Zweifel daran, dass derartige Angriffe ein generelles, für alle Branchen bestehendes Risiko für vertrauliche Prozesse per Internet sind und dass diese Gefährdung des elektronischen Geschäftsverkehrs voraussichtlich dauerhaft bestehen wird. Dies bedeutet, dass die Authentisierung von Teilnehmern an Portalen und Websites, die Zugang zu schutzbedürftigen Inhalten vermitteln, eine zentrale Herausforderung für die Sicherheit von Internetportalen darstellen.

⁹ Pharming durch Manipulation eines DNS-Servers ist indes, kein rein theoretisches Phänomen, dies bewies eine große Attacke im April 2005, die eine Schwäche im DNS-Cache von Symantec-Firewalls ausnutzte.
(<http://www.heise.de/security/result.xhtml?url=/security/artikel/58275/>).

¹⁰ *Gajek/Schwenk/Wegener*, DuD 2005, 639, 641.

¹¹ Laut Bericht der APWG von Dezember 2006 ist die Anzahl von Phishing-Trojanern (Keyloggern) im Vergleich zum Dezember 2005 von 180 auf 340 gestiegen. Damit ist ein neuer Höchststand erreicht. Der Bericht ist abrufbar unter http://www.antiphishing.org/reports/apwg_report_december_2006.pdf:

¹² *Biallaß/Borges/Dienstbach/Gajek/Meyer/Schwenk/Wegener/Werner*, Aktuelle Gefahren im Onlinebanking: Technische und juristische Hintergründe, 2007, S. 4, angenommen zum 10. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Mai 2007.

IV. Authentisierungsverfahren bei Internetportalen für Heilberufe

Beim Zugriff auf den Teilnehmerbereich von Portalen für Heilberufe ist eine sichere Authentisierung der Nutzer unerlässlich. Die Portale verwenden das Verfahren der einmaligen Authentisierung beim Zugang zum Teilnehmerbereich. Nach dem Login ist für die einzelnen Transaktionen, etwa das Einsehen von Daten oder die Übermittlung von Erklärungen, keine zusätzliche Authentisierung erforderlich.

1. Authentisierungsverfahren

Für die Authentisierung von Teilnehmern an Internetportalen stehen ganz unterschiedliche Verfahren zur Verfügung. Nachfolgend werden drei Verfahren vorgestellt, die der rechtlichen Untersuchung zugrundegelegt werden: die Authentisierung durch Passwort, die Authentisierung durch Passwort und Softzertifikat und die Authentisierung durch Chipkarte mit PKI-Infrastruktur und Passwort.

a) Passwort

Das traditionelle, im elektronischen Geschäftsverkehr weit verbreitete Authentisierungsverfahren sieht die Authentisierung durch Nutzernamen und Passwort vor. In diesen Fällen muss der Nutzer beim Log-In seinen Nutzernamen und ein Passwort oder eine PIN eingeben.

Dieses Authentisierungsverfahren kann in zahlreichen Varianten mit unterschiedlichem Sicherheitsniveau verwendet werden. Von Bedeutung ist etwa, welche Anforderungen das System an die Auswahl des Nutzernamens, vor allem des Passworts stellt, und nicht zuletzt, ob ein Fehlerzähler verwendet wird, der den Zugang nach einer bestimmten Anzahl von Fehlversuchen sperrt. Das zentrale Authentifizierungsmerkmal ist hier das Wissen des geheimen Passworts.

Diese Methode der Zugangssicherung wurde traditionell auch im Bereich des Gesundheitswesens verwendet. Derzeit sehen noch fast alle Portale der Körperschaften im Gesundheitswesen die Authentisierung durch Nutzernamen und Passwort vor.

b) Passwort und Softzertifikat

In den Überlegungen zu Internetportalen für Heilberufe wird nicht selten das Konzept der Authentisierung durch Nutzernamen, Passwort und Softzertifikat genannt.

Softzertifikate oder Softwarezertifikate sind Zertifikate, die etwa eine bestimmte Person als nutzungsberechtigten Teilnehmer ausweisen. Sie können dieselben Angaben enthalten wie auf Chipkarten gespeicherte Zertifikate und verwenden eine Technologie der asymmetrischen Verschlüsselung. Der zentrale Unterschied zwischen beiden Authentisierungsmitteln liegt darin, dass Softzertifikate als reine Dateien vom Speichermedium unabhängig sind und wie andere Dateien dupliziert werden können, wogegen der auf einer hinreichend gesicherten Chipkarte gespeicherte Schlüssel an die Karte gebunden ist und nicht vervielfältigt werden kann.

Bei der Verwendung von Softzertifikaten erfolgt die Authentisierung entscheidend durch das Wissen des geheimen Passworts und die Herrschaft über das Softzertifikat, das dieser Person zugeordnet und übergeben wurde. Derartige Softzertifikate werden in der Praxis nicht selten für die Sicherung von Online-Portalen eingesetzt. So vertraut etwa das ELSTER-Projekt (ELEktronische STEuerERklärung) im sogenannten ELSTER-Basischutz auf den Schutz durch ein Softzertifikat, das dem Steuerbürger im Rahmen des Registrierungsprozesses zur Verfügung gestellt wird.

c) Chipkarte und PIN

Als Authentifizierungsmedium wird nicht selten eine Chipkarte mit einem Schlüsselpaar zur asymmetrischen Verschlüsselung gewählt. Die Verwendung der Chipkarte wird zusätzlich gegen Missbrauch gesichert, bisher regelmäßig durch eine PIN. Chipkarte und zugehörige PIN werden einer bestimmten Person persönlich und ausschließlich zugeordnet.

Die Authentisierung der Teilnehmer beim Zugang zum Teilnehmerbereich erfolgt durch Verwendung einer Chipkarte mit Authentisierungsschlüssel sowie durch Eingabe einer PIN. Die Authentisierung erfolgt also durch eine Kombination durch Besitz (der Chipkarte) und Wissen (der geheimen PIN).

Dieses Verfahren verwenden z.B. die Internetportale der Kassenzahnärztlichen Vereinigung Nordrhein und der Kassenzahnärztlichen Vereinigung Westfalen-Lippe. Wegen der hohen Sicherheitsanforderungen lassen die Portale für die Authentisierung nur Chipkarten zu, die im ZOD-Projekt zugelassen sind und damit die Rahmenvorgaben der Kassenzahnärztlichen Bundesvereinigung erfüllen und den technischen Spezifikationen der ZOD entsprechen (dazu unten 2.).

Als weiteres Sicherheitsmerkmal kann eine „authentische“ Datenverbindung verwendet werden, bei der die Chipkarte für die gesamte Übermittlung erforderlich ist. Dies beruht darauf, dass der für SSL maßgebliche Schlüssel aus Daten des geheimen Schlüssels gebildet wird. Dies erfolgt nicht nur einmal; vielmehr wird bei jedem Übertragungsvorgang erneut der geheime Schlüssel abgefragt. Wenn die Karte während einer Sitzung entfernt wird, wird die Datenverbindung abgebrochen.

2. Die zur Authentisierung verwendeten Chipkarten

Soweit die Authentisierung der Teilnehmer von Internetportalen für Heilberufe durch Chipkarte und PIN erfolgt, kommt der Ausgestaltung der Chipkarte und des Ausgabeverfahrens entscheidende Bedeutung für die Sicherheit des Systems zu. Die Nutzung zur Authentisierung verlangt Chipkarten mit hohen Sicherheitsmerkmalen. Die Kassenzahnärztliche Bundesvereinigung hat im Rahmen ihres Projektes „Zahnärzte Online Deutschland“ (ZOD) Rahmenvorgaben für die Anforderungen an sichere Chipkartensysteme sowie technische Anforderungsprofile aufgestellt. Sie hat außerdem ein Zulassungsmodell entwickelt, das es Anbietern ermöglicht, für ihre Produkte die Zulassung zur Verwendung innerhalb des ZOD-Projekts zu beantragen. Derzeit sind die Karten der Medisign GmbH und der DGN Service GmbH für das ZOD-Projekt zugelassen, weitere werden voraussichtlich demnächst hinzutreten.

Die Chipkarten der Medisign GmbH und der DGN Service GmbH haben folgende Eigenschaften:

a) Technische Eigenschaften

Die Chipkarten sind sog. 3-Schlüssel-Karten mit drei asymmetrischen Schlüsselpaaren. Jede Schlüsseleinheit enthält den geheimen und den öffentlichen Schlüssel sowie das vom Aussteller (z.B. Medisign GmbH) ausgestellte Zertifikat, das die Zuordnung des öffentlichen Schlüssels zu einer bestimmten Person (Karteninhaber) bestätigt. Der Chip der Karte erfüllt alle Anforderungen für qualifizierte Signaturen. Für die Authentisierung wird das dritte Schlüsselpaar verwendet. Da die drei Schlüssel auf der Karte technisch gleichartig sind, erfüllen alle Schlüssel die Anforderungen des Signaturgesetzes.

Die Verwendung des Schlüssels ist durch eine PIN gesichert. Die Karte der Medisign GmbH verwendet eine 6-stellige PIN. Die Karte wird nach 10 Fehlversuchen gesperrt.

b) Das Ausgabeverfahren

Das Verfahren der Kartenausgabe verläuft nach einer ZOD-Richtlinie in mehreren Stufen. Auf der ersten Stufe erfolgt nach Antragstellung eine Identifizierung des Teilnehmers. Danach erfolgt eine Übermittlung der Antragsdaten an die Kassenärztliche bzw. Kassenzahnärztliche Vereinigung, die diese und die Approbation prüft. Die Karte wird persönlich übergeben, nachdem der Teilnehmer nochmals identifiziert wurde. Erst danach wird die PIN auf dem Postweg an den Teilnehmer verschickt.

C. Sicherer Zugang von Nachrichten in Internetportalen

I. Die rechtliche Bedeutung des Zugangs von Nachrichten

Die Internetportale der Berufsvereinigungen von Angehörigen von Heilberufen dienen nicht zuletzt der Übermittlung von Erklärungen und sonstigen Nachrichten und Daten zwischen der Vereinigung und ihren Mitgliedern. Zur Gewährleistung der Rechtssicherheit in diesem Verhältnis ist es daher von Bedeutung, dass das Übermittlungsverfahren des jeweiligen Portals den Zugang von Erklärungen tatsächlich und rechtlich zuverlässig bewirkt.

Für den Zugang von Erklärungen der Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigungen gelten unterschiedliche Regeln je nach der Art der Erklärung. Verwaltungsakte sind gemäß § 37 Abs. 1 Sozialgesetzbuch, 10. Buch (SGB X) dem Vertragsarzt bekannt zu geben. Die Kassenärztliche bzw. Kassenzahnärztliche Vereinigung erlassen Verwaltungsakte vor allem im Zusammenhang mit der Honorarabrechnung. So wird das Honorar des Vertragsarztes gemäß § 85 Abs. 4 Sozialgesetzbuch, 5. Buch (SGB V) durch einen Honorarbescheid festgesetzt, der rechtlich als Verwaltungsakt zu qualifizieren ist. Die Bekanntgabe eines schriftlichen oder eines elektronisch übermittelten Verwaltungsaktes setzt den Zugang beim Adressaten voraus, wie sich aus § 37 Abs. 2 SGB X ergibt. Der Begriff des Zugangs wird im SGB allerdings nicht definiert. Vielmehr ist der allgemeine Begriff des Zugangs maßgeblich, auf den auch § 130 des Bürgerlichen Gesetzbuchs (BGB) verweist.¹³

Für alle anderen Erklärungen, die nicht als Verwaltungsakt zu qualifizieren sind, gilt § 37 SGB X wohl nicht. Ebenso wie § 41 Verwaltungsverfahrensgesetz, dem § 37 SGB X nachgebildet ist, gilt § 37 SGB X nur für Verwaltungsakte, nicht aber für sonstige Erklärungen einer

¹³ Vgl. BSG, NJW 2005, 1303, 1304; Hess. LSG, Urt. v. 9.3.2005, L 6 AL 1276/03, info also 2005, 260; Hauck/Noftz-*Recht*, Sozialgesetzbuch X (Losebl., Stand 06/2006), § 37 Rz. 5; *Waschull*, in Diering/Timme/ Waschull (Hrsg.), Sozialgesetzbuch X, 2004 (i.F. LPK-SGB X), § 37 Rz. 4.

Behörde.¹⁴ Hier werden vielmehr die allgemeinen Grundsätze des Zugangs (§ 130 BGB) angewandt.¹⁵ Bedeutung hat diese Unterscheidung vor allem für den Zeitpunkt des Zugangs (dazu unten II.6.). Im Übrigen sind, da § 37 SGB X auch auf den Zugang verweist, letztlich stets die allgemeinen Grundsätze des BGB zum Zugang maßgeblich.

Nachfolgend werden zunächst die Grundsätze des Zugangs bei elektronischer Übermittlung von Erklärungen (II.) dargestellt, sodann der Zugang unter den Bedingungen der Internetportale für Heilberufe (unten III.) erörtert.

II. Grundsätze des Zugangs bei elektronischer Übermittlung von Erklärungen

1. Zugangsvarianten bei elektronischer Übermittlung von Erklärungen

Die Anforderungen an den Zugang von Erklärungen sind nicht gesetzlich geregelt. § 130 BGB besagt aber, dass eine empfangsbedürftige Willenserklärung wirksam wird, wenn sie dem Empfänger zugeht. § 312e Abs. 1 S. 2 BGB, der auf den Zugang elektronisch übermittelter Bestellungen und Empfangsbestätigungen Bezug nimmt, regelt nach herrschender Auffassung nur diesen speziellen Fall und enthält keine allgemeine Definition des Zugangs.¹⁶

Das deutsche Recht kennt unterschiedliche Möglichkeiten für das Wirksamwerden von Willenserklärungen je nach Art der Übermittlung. Eine

¹⁴ *Kopp/Ramsauer*, *Verwaltungsverfahrensgesetz*, 9. Aufl. 2005, § 41 Rz. 80; *Schwarz*, in *Fehling/Berthold/Wahrendorf* (Hrsg.), *Handkommentar Verwaltungsrecht* (zit.: *Hk-VerwR*), 2006, § 41 VwVfG Rz. 2; *P. Stelkens/U. Stelkens*, in *Stelkens/Bonk/Sachs* (Hrsg.), *Verwaltungsverfahrensgesetz*, 6. Aufl. 2001, § 41 Rz. 3a; *Wolff*, in *Wolff/Decker*, *Verwaltungsgerichtsordnung, Verwaltungsverfahrensgesetz*, 2005, § 41 VwVfG, Rz. 3.

¹⁵ *Kopp/Ramsauer* (Fn. 14), § 41 Rz. 80; *Hk-VerwR-Schwarz* (Fn. 14), § 41 VwVfG Rz. 4; *P. Stelkens/ U. Stelkens*, in *Stelkens/Bonk/Sachs* (Fn. 14), § 41 Rz. 3a; *Wolff*, in *Wolff/Decker* (Fn. 14), § 41 Rz. 4.

¹⁶ Dazu im einzelnen *Borges*, *Verträge im elektronischen Geschäftsverkehr*, 2003, S. 226 ff.

Erklärung kann durch Eingang in den Bereich des Empfängers wirksam werden. Dies wird mit dem Begriff des Zugangs beschrieben. Unabhängig davon wird eine Erklärung aber auch wirksam, wenn sie vom Empfänger zur Kenntnis genommen wird. Teilweise wird auch hier von „Zugang“ gesprochen.

Der Zugang einer Erklärung kann auch durch Übergabe einer Nachricht an eine Mittelsperson des Empfängers erfolgen.¹⁷ Teilweise werden solche Mittelspersonen (Empfangsboten) auch ausdrücklich zum „Bereich“ des Empfängers gezählt.¹⁸ Damit bleibt es bei zwei unterschiedlichen Möglichkeiten des Wirksamwerdens von Erklärungen (Wirksamwerden durch Zugang, Wirksamwerden durch Kenntnisnahme).

2. Zugang durch Speicherung

Der Zugang von Nachrichten erfolgt mit Eingang in den Bereich oder „Machtbereich“ des Empfängers derart, dass die Kenntnisnahme vom Empfänger erwartet werden kann.¹⁹ Dies setzt eine Verkörperung oder Speicherung der Nachricht im Bereich des Empfängers voraus. Der Bereich des Empfängers umfasst insbesondere die vom Empfänger zum Empfang von Nachrichten bereitgehaltenen Einrichtungen, die sog. Empfangseinrichtungen.²⁰ Klassische Empfangseinrichtungen sind etwa der Briefkasten, ein (bei der Post eingerichtetes) Postfach,²¹ ein Anrufbeantworter,²² ein Telefaxgerät.²³ Zum Bereich in diesem Sinne

¹⁷ Unstr.; siehe nur BSG, NJW 2005, 1303, 1304; Palandt-*Heinrichs*, Bürgerliches Gesetzbuch, 66. Aufl. 2007, § 130 Rz. 9; *Borges* (Fn. 16), S. 232; ausführlich *Brinkmann*, Der Zugang von Willenserklärungen, 1984, S. 108 ff.

¹⁸ So bei BGH, NJW 1951, 313.

¹⁹ So die klassische Definition; vgl. BSG, NJW 2005, 1303, 1304 m. Verweis auf die Rspr. des BGH; Hauck/Noftz-*Recht* (Fn. 13), § 37 Rz. 5; Palandt-*Heinrichs* (Fn. 17), § 130 Rz. 5; *Kopp/Ramsauer* (Fn. 14), § 41 Rz. 81.

²⁰ *Borges* (Fn. 16), S. 231 m.w.N.

²¹ Unstr.; siehe nur MünchKommBGB-*Einsele*, Bürgerliches Gesetzbuch, Band 1, 5. Aufl. 2007, § 130 Rz. 17; Palandt-*Heinrichs* (Fn. 17), § 130 Rz. 5.

²² Unstr.; siehe nur Palandt-*Heinrichs* (Fn. 17), § 130 Rz. 5.

gehört weiterhin der räumliche Machtbereich des Empfängers,²⁴ also die Wohnung, Grundstück, Betriebsgelände, Praxisräume etc.

Bei elektronischer Übermittlung von Erklärungen ist vor allem die Speicherung in einer Empfangseinrichtung von Bedeutung. Empfangseinrichtung für elektronische Nachrichten kann vor allem eine Mailbox oder ein sonstiges elektronisches Postfach des Empfängers sein. Zu den Empfangseinrichtungen gehören aber auch Webserver, soweit an diese Erklärungen übermittelt werden können,²⁵ etwa durch Ausfüllen eines Formulars auf der Website, sowie sonstige Plattformen, die für den Empfang von Nachrichten ausgestattet sind.

Gerade in Bezug auf elektronische Übermittlung wird kontrovers diskutiert, unter welchen Voraussetzungen eine Einrichtung, die technisch zum Empfang von Nachrichten geeignet ist, eine Empfangseinrichtung in diesem Sinne ist. Die Frage wird vor allem am Beispiel der E-Mail diskutiert. Im Zivilrecht wird teilweise angenommen, dass jede Mailbox eine taugliche Empfangseinrichtung für Nachrichten sei, die an den Inhaber der Mailbox gerichtet sind.²⁶ Die herrschende Meinung hingegen nimmt an, dass eine Einrichtung als Empfangseinrichtung gewidmet sein müsse und nur den Zugang der Nachricht vermittelt, wenn die Einrichtung, etwa die Mailbox, als Empfangseinrichtung für Nachrichten der betreffenden Art geeignet sei.²⁷

²³ Unstr.; siehe nur Palandt-*Heinrichs* (Fn. 17), § 130 Rz. 7.

²⁴ *Borges* (Fn. 16), S. 232 m. w. Nachw.

²⁵ *Borges* (Fn. 16), S. 254.

²⁶ *Behling*, Der Zugang elektronischer Willenserklärungen in modernen Kommunikationssystemen, 2007, S. 188 ff.; *Schmitz*, Die vertraglichen Pflichten und die Haftung der Informationsanbieter im Internet, 2000, S. 12; weitere Nachw. bei *Borges* (Fn. 16), S. 250.

²⁷ *Baetge*, in Kaminski/Henßler/Kolaschnik/Papathoma-Baetge, Rechtshandbuch E-Business, 2002, S. 106; *Borges* (Fn. 16), S. 250 m.w.Nachw.; *Dörner*, AcP 202 (2002), 363, 367; *Ultsch*, DZWIR 1997, 466, 468; *Taupitz/Kritter*, JuS 1999, 839, 841; *Vehslage*, DB 2000, 1801, 1804.

Im Anwendungsbereich des SGB ist diese Frage seit der Einführung des § 36a SGB I im Jahre 2002²⁸ gesetzlich geregelt. Gemäß § 36a SGB I, der § 3a VwVfG entspricht, ist die Übermittlung elektronischer Dokumente nur zulässig, soweit der Empfänger hierfür einen Zugang eröffnet. Wie im Zivilrecht ist also die Widmung einer Einrichtung als Empfangseinrichtung erforderlich.²⁹

Im Weiteren ist umstritten, unter welchen Voraussetzungen eine solche Widmung anzunehmen ist.³⁰ Soweit Nachrichten über spezifische Einrichtungen übertragen werden, die für eine bestimmte Geschäftsbeziehung, wie es etwa bei Internetportalen für Heilberufe der Fall ist, besteht an der Widmung der Empfangseinrichtung für Nachrichten aus der betreffenden Geschäftsbeziehung kein Zweifel.

In der Literatur ist umstritten, in welchem Stadium der Übermittlung der Zugang bewirkt wird. Diese Frage ist für die Zuordnung des Übermittlungsrisikos bedeutsam und wird daher in diesem Zusammenhang dargestellt (unten 4.).

3. Zugang durch Kenntnisnahme

Erklärungen werden nicht nur durch Zugang im Sinne der Speicherung im Bereich des Empfängers wirksam, sondern ebenso durch Kenntnisnahme. Kenntnisnahme meint die sinnliche Wahrnehmung der Nachricht, also das Lesen einer visuell wahrnehmbaren Nachricht, oder das Hören einer gesprochenen oder sonst akustisch übermittelten Nachricht. In diesem Fall kommt es auf das Vorliegen einer Speicherung nicht (mehr) an.

²⁸ Art. 2 des Dritten Gesetzes zur Änderung verwaltungsverfahrenrechtlicher Vorschriften v. 21.8.2002, BGBl. I 3322, 3325. § 36a SGB I ist am 1.2.2003 in Kraft getreten.

²⁹ Begr.RegE zu § 3a VwVfG, BT-Drucks. 14/9000, S. 30; i.V.m. Begr.RegE zu § 36a SGB I, BT-Drucks. 14/9000, S. 34; *Mrozynski*, SGB I, 3. Aufl. 2003, § 36a Rz. 3; *Waschull*, in LPK-SGB X (Fn. 13), § 37 Rz. 4 f. m.w.N., 88.

³⁰ Siehe zum Streitstand betr. § 36a SGB I *Mrozynski* (Fn. 29), § 36a Rz. 2 f.; *Waschull*, in LPK-SGB X (Fn. 13), § 37 Rz. 2; siehe zur Parallelnorm des § 41 VwVfG *Stelkens/Stelkens*, in *Stelkens/Bonk/Sachs* (Fn. 14), § 41 Rz. 14 b ff.; siehe auch die Darstellung des zivilrechtlichen Meinungsstreits bei *Borges* (Fn. 16), S. 251 ff.

4. Zugangsstörungen und Übermittlungsrisiko

Es kommt vor, dass der Zugang einer Nachricht in der soeben beschriebenen Form nicht gelingt. So können Briefe auf dem Postweg verlorengehen, der Ausdruck eines Faxes mag scheitern, ebenso die Speicherung einer E-Mail, etwa wegen der Erschöpfung der Kapazität einer Mailbox oder Funktionsstörung des Mailservers und ähnlichen Ursachen. In diesen Fällen hängt es von der Zuordnung des Übermittlungsrisikos ab, ob und ggf. unter welchen Voraussetzungen und in welchen Fällen auch bei derartigen Störungen der Übermittlung der Zugang der Nachricht anzunehmen ist.

Die Verteilung des Übermittlungsrisikos ist in der zivilrechtlichen Literatur sehr umstritten, insbesondere bei elektronischer Kommunikation. Nach einer Mindermeinung der Literatur ist der Zugang mit Passieren der Schnittstelle zum Datenverarbeitungssystem des Empfängers bewirkt.³¹ Nach einer anderen Auffassung ist der Zugang erfolgt, wenn die Speicherung aus Sicht des Absenders erfolgt ist.³² Nach beiden Ansichten trägt der Absender das Übermittlungsrisiko nur für den Datentransport bis zu dieser Schnittstelle. Für die weitere Übermittlung und die Verkörperung der Nachricht im Empfangsgerät (Fax, Mailbox etc.) trägt der Empfänger das Risiko. Störungen des Empfangsgeräts hindern somit den Zugang nicht, auch wenn der Empfänger keine Möglichkeit hat, die Nachricht zur Kenntnis zu nehmen.

Dagegen geht die herrschende Meinung davon aus, dass Zugang erst mit Vollendung der Speicherung in der Empfangseinrichtung erfolgt,³³ weist das Übermittlungsrisiko also dem Absender zu. Störungen des Empfangsgeräts gehen daher grundsätzlich zu Lasten des Absenders. Die Rechtsprechung hat zu dieser Frage für die elektronische Kommunikation noch nicht ausdrücklich Stellung genommen. Sie geht allerdings im Übrigen

³¹ *Behling* (Fn. 26), S. 186 ff.; *Burgard*, AcP 195 (1995), 74, 134.

³² *John*, AcP 184 (1984), 385, 412.

³³ Speziell zur E-Mail: *Borges* (Fn. 16), S. 248; *Dörner*, AcP 202 (2002), 363, 369 ff.; *Palandt-Heinrichs* (Fn. 17), § 130 Rz. 7a; *Köhler*, BGB AT, 30. Aufl. 2006, § 6 Rz. 18.

wie die herrschende Ansicht davon aus, dass Zugang mit vollendeter Speicherung bewirkt wird,³⁴ der Absender also das volle Übermittlungsrisiko trägt. Für die herrschende Ansicht spricht, dass es nicht zumutbar wäre, dem Empfänger Folgen aus einer Erklärung zuzuweisen, die er nicht zur Kenntnis nehmen und auf die er folglich nicht reagieren konnte. Diese Ansicht wird im folgenden zugrunde gelegt.

Auch im Anwendungsbereich des § 37 SGB X trägt der Absender, also die Behörde, das Übermittlungsrisiko. Wegen der Vermutung des § 37 Abs. 1 SGB X, wonach ein schriftlicher Verwaltungsakt als am dritten Tage nach der Aufgabe zur Post und ein elektronisch übermittelter Verwaltungsakt als am dritten Tag nach der Absendung als bekannt gegeben gilt und die Behörde lediglich „im Zweifel“ den Zugang nachzuweisen hat, wird diskutiert, unter welchen Voraussetzungen derartige Zweifel bestehen und welche Anforderungen an die Substantiierung des Vortrags zu stellen sind, wenn der Adressat den Zugang bestreitet.³⁵ Da die Vermutung aber nach dem ausdrücklichen Gesetzeswortlaut nicht gilt, wenn der Zugang nicht erfolgt ist,³⁶ bleibt es bei der Zuordnung des Übermittlungsrisikos zur Behörde.

5. Zugangsvereitelung und Obliegenheiten des Empfängers

Die traditionelle Regelung, wonach der Absender das volle Übermittlungsrisiko trägt, führt zu unbefriedigenden Ergebnissen, wenn das Empfangshindernis dem Empfänger zuzurechnen ist oder es aus seinem Bereich stammt, etwa, wenn eine Mailbox überfüllt ist und keine Mails mehr speichert, weil der Empfänger es über einen längeren Zeitraum unterlassen hat, diese zu leeren. Es gelten daher mehrere ergänzende

³⁴ Vgl. RGZ 144, 289, 292; 170, 285, 288; BGHZ 67, 271, 275; 137, 205, 208; BAG, NJW 1984, 1651; NJW 1993, 1093.

³⁵ Siehe dazu aus jüngerer Zeit etwa Hess. LSG, Urt. 9.3.2005, L 6 AL 1276/03, info also 2005, 260 m. Nachw. zum Meinungsstand; *Pickel*, in *Pickel/Marschner*, Kommentar zum SGB X, Losebl. (Stand: Juni 2005), § 37 Rz. 33; *Hauck/Noftz-Recht* (Fn. 13), § 37 Rz. 18 m.w.Nachw.

³⁶ Unstr.; siehe nur *Hauck/Noftz-Recht* (Fn. 13), § 37 Rz. 17 f.

Regeln, die unbillige Ergebnisse aus dieser Risikoverteilung vermeiden sollen. Die Notwendigkeit solcher ergänzender Regeln ist in der Sache unstrittig. Allerdings divergieren die dogmatische Einordnung und die Anforderungen im Detail.

a) Zugangsvereitelung

Eine seit langem anerkannte Modifikation der Risikoverteilung erfolgt im Fall der sogenannten Zugangsvereitelung. Eine Zugangsvereitelung im engen Sinne liegt vor, wenn der Empfänger bewusst (absichtlich) verhindert, dass die Erklärung zugeht.³⁷ Ein Beispiel bei elektronischer Kommunikation wäre etwa, dass der Empfänger seine Mailbox in Erwartung einer Erklärung bewusst „verstopft“, damit keine Erklärungen mehr gespeichert werden können, oder den Mailserver vom Netz nimmt. Das Pendant im Fall der Kenntnisnahme ist die Kenntnisnahmeverweigerung, also z.B. das Wegschauen, Weghören, um eine Erklärung nicht zu vernehmen.³⁸ Im Fall der Zugangsvereitelung in diesem engen Sinne wird der Zugang in analoger Anwendung des § 162 BGB fingiert,³⁹ der Empfänger wird also so behandelt, als wäre die Erklärung zugegangen. Die Rechtsprechung und ein Teil der Literatur stützen diese Rechtsfolge auf den Grundsatz von Treu und Glauben, § 242 BGB.⁴⁰ Ein instruktives Beispiel ergibt sich aus einer Entscheidung des LSG NRW zur Zustellung des Beschlusses eines Prüfungsausschusses der Kassenzahnärztlichen Vereinigung Westfalen-Lippe. Hier hatte der Zahnarzt die Entgegennahme eines Einschreibens verweigert. Das Gericht

³⁷ *Borges* (Fn. 16), S. 255; *Medicus*, Allgemeiner Teil des BGB, 9. Aufl. 2006, Rz. 282.

³⁸ *Borges* (Fn. 16), S. 255; *MünchKommBGB-Förschler*, Bürgerliches Gesetzbuch, 3. Aufl. 1993, § 130 Rz. 20, 28; *Enneccerus/Nipperdey*, Allgemeiner Teil des Bürgerlichen Rechts, 2. Halbbd., 15. Aufl. 1960, § 138 II. B. 1 (S. 981).

³⁹ RGZ 58, 406, 408 f.; *Borges* (Fn. 16), S. 255 f.; *Larenz/Wolf*, BGB AT, 9. Aufl. 2004, § 26 Rz. 46; *Medicus* (Fn. 37), Rz. 282.

⁴⁰ Vgl. BVerwG, NVwZ 1991, 73, 74 m. Verweis auf die Rspr. des BGH; BGHZ 137, 205, 209 f.; BGH, NJW 1983, 929, 930; *Bork*, Allgemeiner Teil des Bürgerlichen Gesetzbuchs, 2. Aufl. 2006, Rz. 637. Im Ergebnis auch *Waschull*, in LPK-SGB X (Fn. 13), § 37 Rz. 4 m.w.Nachw.

stellt fest, der Zahnarzt müsse sich nach Treu und Glauben so behandeln lassen, als sei die Zustellung erfolgt.⁴¹

b) Obliegenheits- und Pflichtverletzungen

aa) Obliegenheitsverletzungen und Zugang

Häufiger als aufgrund vorsätzlicher Zugangsverhinderung scheidet der Zugang wegen Störungen, die der Empfänger unvorsätzlich verursacht hat. Es kann etwa sein, dass der Empfänger seine Empfangseinrichtung, z.B. ein Faxgerät oder eine Mailbox, nicht angemessen kontrolliert und daher, z.B. wegen Papiermangels oder Überfüllung der Mailbox, eine Erklärung nicht vernehmbar gespeichert werden kann.

Nach im Ergebnis weitgehend übereinstimmender Ansicht ist in diesen Fällen zu differenzieren. Die Rechtsprechung geht von dem Grundsatz aus, dass derjenige, der aufgrund bestehender oder angebahnter Sonderbeziehung mit dem Zugang von Erklärungen zu rechnen hat, geeignete Vorkehrungen treffen muss, dass ihn derartige Erklärungen auch erreichen.⁴² Verstößt der Empfänger gegen diese Anforderung und geht eine Erklärung deshalb nicht zu, so muss er sich im Ergebnis so behandeln lassen, als sei die Erklärung (fristgerecht) zugegangen.⁴³ Diese Rechtsfolge wird teilweise auf den Grundsatz von Treu und Glauben gestützt,⁴⁴ teils auch als Schadensersatz aufgrund Pflichtverletzung angesehen⁴⁵. Der Bundesgerichtshof hat vor einigen Jahren eine differenzierte Wertung vertreten, die beiden Parteien Mitwirkungspflichten auferlegt. Danach muss sich der Empfänger, der nach dem o.g. Grundsatz Vorkehrungen zum

⁴¹ LSG NRW, NJW 1990, 407.

⁴² RGZ 110, 34, 36; BGHZ 67, 271, 278; 137, 205, 208; BGH, VersR 1971, 262, 263; BAG, DB 1986, 2336 f.; siehe dazu auch *Borges* (Fn. 16), S. 256 f.

⁴³ BGHZ 137, 205, 211; siehe auch *Behling* (Fn. 26), S. 164 ff.; *Borges* (Fn. 16), S. 256 f.

⁴⁴ So vor allem die arbeitsgerichtliche Rechtsprechung; vgl. etwa BGH, AP Nr. 5 zu § 130 BGB; BAG, AP Nr. 10 zu § 130 BGB.

⁴⁵ So etwa BGHZ 137, 205, 208; BGH, VersR 1971, 262, 263.

Empfang von Nachrichten treffen muss, bei Verletzung dieser Pflicht unter Umständen so behandeln lassen, als wäre die Erklärung zugegangen. Dies setzt aber einen unverzüglichen, erneuten Zustellungsversuch des Absenders voraus. Wenn der zweite Zustellungsversuch wegen erneuter Pflichtverletzung des Empfängers scheitert, gilt die Erklärung als zugegangen. Gelingt die Zustellung im zweiten Versuch, gilt die Erklärung als rechtzeitig zugegangen.⁴⁶ In der Literatur werden verschiedene Ansichten vertreten, die zu ähnlichen Ergebnissen führen.⁴⁷

Außerhalb einer bestehenden Sonderverbindung besteht eine solche Mitwirkungspflicht des Empfängers jedoch nicht. Hier trägt der Absender in vollem Umfang das Risiko, dass der Zugang mangels Speicherung fehlschlägt.⁴⁸

Im Verhältnis der Teilnehmer zum Portalbetreiber liegt regelmäßig eine rechtliche Sonderbeziehung vor, so dass die Mitwirkungspflichten des Empfängers eingreifen.

bb) Zugangsbezogene Pflichten bei elektronischer Übermittlung

Für den Zugang bei Zugangsstörungen kommt es nach den soeben dargestellten Grundsätzen entscheidend darauf an, welche Pflichten den Empfänger im Rahmen von rechtlichen Sonderbeziehungen treffen. Eine Pflicht, bestimmte Empfangseinrichtungen bereitzustellen, besteht grundsätzlich nicht,⁴⁹ kann aber vertraglich vereinbart werden.

Größere Bedeutung haben Obliegenheiten und Pflichten zur Unterhaltung und Überwachung vorhandener Empfangseinrichtungen. Diese werden vor allem für Empfangseinrichtungen bei elektronischer Kommunikation

⁴⁶ BGHZ 137, 205, 208 f.

⁴⁷ Siehe dazu *Behling* (Fn. 26), S. 165 ff. m.w.Nachw.; *Borges* (Fn. 16), S. 256 ff. m.w.Nachw.

⁴⁸ *Borges* (Fn. 16), S. 256 f.

⁴⁹ Allg. Auff.; vgl. BGHZ 67, 271, 278; BGH, NJW 1996, 1967, 1968; *Borges* (Fn. 16), S. 258 m.w.Nachw.

diskutiert. So wird etwa in Bezug auf Telefax angenommen, dass derjenige, der ein Telefaxgerät als Empfangseinrichtung einrichtet, dafür Sorge zu tragen hat, dass das Gerät betriebsbereit ist.⁵⁰ Dasselbe gilt etwa für eine Mailbox und sonstige elektronische Postfächer.

In Literatur und Rechtsprechung wird kontrovers diskutiert, welche Pflichten im Einzelnen bestehen, insbesondere in welchen Intervallen die Funktionsfähigkeit einer Empfangseinrichtung zu überprüfen ist.⁵¹ Die Existenz einer Pflicht zur Überprüfung in angemessenen Abständen ist aber im Grundsatz anerkannt.⁵²

c) Zugang und Spam-Filter

Die Speicherung einer Nachricht im Eingangspostfach kann daran scheitern, dass eine Nachricht fälschlich von einem Anti-Spam-Programm gelöscht oder in einen besonderen Ordner abgelegt wird und daher vom Empfänger nicht zur Kenntnis genommen wird. In diesem Fall dürfte Einigkeit darin bestehen, dass dieses Risiko vom Empfänger zu tragen ist, wenn nach dem Inhalt der Nachricht nicht damit zu rechnen war, dass die Nachricht abgefangen würde.⁵³ Die dogmatische Begründung variiert. Nach der Mindermeinung, die das Transportrisiko beim Passieren der Schnittstelle zum System des Empfängers bzw. dessen Providers annimmt (dazu oben 4., 25 f.), ist Zugang vor, da der Spam-Filter innerhalb des Risikobereichs des Empfängers agiert.⁵⁴ Nach den Kriterien der h.M. ist je nach Fallgestaltung der Zugang erfolgt oder zwar nicht erfolgt, jedoch bestünde ein Schadensersatzanspruch bzw. müsste sich der Empfänger nach Treu und Glauben so behandeln lassen, als sei die Erklärung zugegangen.

⁵⁰ Palandt-*Heinrichs* (Fn. 17), § 130 Rz. 17; siehe auch *Borges* (Fn. 16), S. 259.

⁵¹ Siehe dazu *Borges* (Fn. 16), S. 259 ff.

⁵² Siehe dazu *Borges* (Fn. 16), S. 259 ff.

⁵³ Vgl. *Behling* (Fn. 26), S. 205.

⁵⁴ So konsequent etwa *Behling* (Fn. 26), S. 205.

6. Der Zeitpunkt des Zugangs

Der Zeitpunkt des Zugangs ist für eine Vielzahl rechtlicher Aspekte von Bedeutung. Die größte praktische Bedeutung hat der Zugangszeitpunkt für die Fristwahrung. Soweit mit einer Erklärung Fristen gewahrt werden können, wird zur Fristwahrung regelmäßig auf den Zugang der Erklärung abgestellt. Bedeutung hat dies etwa für die Abrechnung im Verhältnis der Kassen- oder Kassenzahnärztlichen Vereinigung zum Vertragsarzt (siehe dazu auch unten III.1.b).

Bei Erklärungen der Kassen- bzw. Kassenzahnärztlicher Vereinigung, die über das Portal an den Vertragsarzt übermittelt werden, ist auch in Bezug auf den Zeitpunkt des Zugangs zu differenzieren: Für Verwaltungsakte gilt, wie oben (I.) dargestellt, für den Zeitpunkt des Zugangs § 37 Abs. 2 S. 1 SGB X, wonach elektronisch übermittelte Verwaltungsakte, also etwa der Honorarbescheid, als am dritten Tag nach der Absendung zugegangen gelten. Der tatsächliche Zeitpunkt des Zugangs ist gemäß § 37 Abs. 2 S. 2 SGB X nur dann von Bedeutung, wenn der Zugang später erfolgt. Dies ist bei der elektronischen Übermittlung jedoch nur in extremen Ausnahmefällen vorstellbar, da die Übermittlung regelmäßig innerhalb sehr kurzer Zeit gelingt oder aber fehlschlägt. Für alle anderen Erklärungen der Kassen- bzw. Kassenzahnärztlichen Vereinigungen gelten die allgemeinen Grundsätze zum Zugang von Erklärungen (s. oben I., S. 20 f.). Dasselbe gilt im Anwendungsbereich des § 37 SGB X, wenn ein elektronisch übermittelter Verwaltungsakt einmal mehr als drei Tage unterwegs ist und danach noch zugeht.

Beim Zugang durch Kenntnisnahme (dazu oben 3., S. 24) erfolgt der Zugang in dem Zeitpunkt, in dem von der Nachricht Kenntnis genommen wird. Beim Zugang durch Speicherung ist der Zeitpunkt umstritten. Nach einer in der Literatur vertretenen Ansicht erfolgt der Zugang im Zeitpunkt der Speicherung.⁵⁵ Nach der herrschenden Meinung hingegen erfolgt der Zugang erst in dem Zeitpunkt, in dem die Kenntnisnahme erwartet werden kann.⁵⁶ Danach erfolgt der Zugang einer Erklärung, die etwa nach

⁵⁵ *Behling* (Fn. 26), S. 206 ff.; *Borges* (Fn. 16), S. 268 f. m.w.Nachw.

⁵⁶ Aus der zivilrechtlichen Diskussion: RGZ 99, 20, 23; 142, 402, 408 f.; BGH, VersR 1994, 586; BAG, NJW 1984, 1651; *Dörner*, AcP 202 (2002), 363, 365; Palandt-

Geschäftsschluss in einer geschäftlichen Empfangseinrichtung eingeht, erst zu Beginn des nächsten Geschäftstags. Illustrativ ist der vom OLG Rostock entschiedene Fall, in dem ein Fax am Freitag Nachmittag um 16.13 Uhr eintraf. Das Gericht nahm Zugang am folgenden Arbeitstag an.⁵⁷

Nach der herrschenden Meinung ist für den Zeitpunkt des Zugangs maßgeblich, in welchen Intervallen die Kontrolle einer Empfangseinrichtung erwartet werden kann. Die Frage ist insbesondere für die elektronische Übermittlung lebhaft umstritten.⁵⁸ Im Ergebnis besteht Einigkeit darin, dass bei elektronischen Empfangseinrichtungen von Unternehmern eine laufende Kontrolle während der Geschäftszeit erforderlich ist.⁵⁹ Bezüglich einer darüber hinausgehenden Kontrolle gehen die Ansichten auseinander, ebenso bei Empfangseinrichtungen von Privatpersonen.⁶⁰

Für die Mindermeinung, die diese Prüfung vermeidet, spricht der Grundsatz der Rechtssicherheit.⁶¹ Die Praxis freilich muss von der herrschenden Meinung ausgehen, die in der Rechtsprechung bisher weitgehend unangefochten ist.

III. Zugang bei Internetportalen für Heilberufe

Für die Übermittlung von Nachrichten des Portalbetreibers an den teilnehmenden Vertragsarzt bestehen, wie im allgemeinen Teil dargestellt, mehrere Möglichkeiten: Erklärungen könnten bereits durch Einstellen in das Postfach zugehen, das dem Teilnehmer auf dem Portal zur Verfügung gestellt wird, sie können vom Teilnehmer zur Kenntnis genommen (Lesen)

Heinrichs (Fn. 17), § 130 Rz. 5; siehe zum Meinungsstand im Einzelnen *Borges* (Fn. 16), S. 267 ff.; ebenso, zu § 41 VwVfG, *Kopp/Ramsauer* (Fn. 14), § 41 Rz. 81 m. Verweis auf die Rspr. des BGH.

⁵⁷ OLG Rostock, NJW-RR 1998, 526, 527.

⁵⁸ Siehe die Darstellung bei *Borges* (Fn. 16), S. 269 ff.

⁵⁹ *Borges* (Fn. 16), S. 272 m.w.Nachw.

⁶⁰ Siehe dazu *Borges* (Fn. 16), S. 272 m.w.Nachw.

⁶¹ *Borges* (Fn. 16), S. 268 f.

und dadurch wirksam werden. Nachrichten können auch auf dem Server des Portalbetreibers zum Abruf (download) bereitgestellt werden.

Für diese Fallgruppen wird nachfolgend erörtert, unter welchen Voraussetzungen und in welchem Zeitpunkt die Nachrichten dem Teilnehmer rechtlich wirksam zugehen. Sodann werden spezielle Aspekte des Zugangs über Internetportale erörtert, die von besonderem Interesse sind. Dies sind die Bedeutung von Eingriffen Dritter, namentlich des Zugriffs auf den Account des Teilnehmers, für den Zugang (unten 4.) sowie der Nachweis des Zugangs im Falle eines Rechtsstreits (unten 6.).

1. Zugang durch Einstellen ins Postfach

a) Die materiellrechtlichen Voraussetzungen des Zugangs

Nachrichten des Portalbetreibers, also der Berufsvereinigung, oder ggf. Dritter, für die dieser Mitteilungsweg eröffnet ist, werden regelmäßig im Postfach gespeichert, das dem Teilnehmer im Rahmen seines Accounts auf dem Portal zur Verfügung gestellt wird. Nach herrschender Ansicht ist die Nachricht, wie oben (II.) dargestellt, mit vollendeter Speicherung zugegangen, wenn die Speicherung in einer für diese Art von Nachrichten gewidmeten Empfangseinrichtung erfolgt. Das Postfach ist zweifellos für den Empfang von Nachrichten des Portalbetreibers bestimmt.

Zu erörtern ist lediglich, ob der Zugang der Nachricht daran scheitern kann, dass die Erklärung, auch wenn sie im Postfach des Teilnehmers gespeichert wurde, weiterhin auf dem Datenverarbeitungssystem des Absenders, des Portalbetreibers, gespeichert ist, so dass dieser weiterhin Zugriff auf die Erklärung hat. Diese Frage betrifft eher die Abgabe der Erklärung, der eine Entäußerung der Nachricht voraussetzt,⁶² hat aber auch für den Zugang Bedeutung. Dieser Aspekt hat gleichermaßen den Zugang von Erklärungen in allen Fällen Bedeutung, in denen Erklärungen des Providers an den Accountinhaber gesandt werden. Auch hier hat der Provider technisch die Möglichkeit, eine ins Postfach eingelegte Mail wieder zu löschen, ohne dass

⁶² Siehe zur Abgabe von Erklärungen bei elektronischer Übermittlung *Borges* (Fn. 16), S. 219 ff.

der Empfänger dies verhindern kann und ggf. ohne dass ihm erkennbar wird, dass die Mail einmal eingegangen war. Bei diesem Aspekt, der meistens nicht einmal erwähnt wird, besteht aber Einigkeit darin, dass Abgabe und Zugang von Erklärungen nicht voraussetzen, dass die Erklärung ein Datenverarbeitungssystem erreicht, auf das der Absender keinen Zugriff hat. Erforderlich und ausreichend ist lediglich eine organisatorische Zuordnung des Postfachs zum Empfänger, sofern nach dem ordnungsgemäßen organisatorischen Ablauf kein Zugriff auf das Postfach mehr möglich ist. Die lediglich faktische Zugriffsmöglichkeit durch unzulässige Maßnahmen hindert also den Zugang nicht.

Dies bedeutet, dass Nachrichten des Portalbetreibers an den Teilnehmer mit Speicherung in dessen Postfach zugehen, wenn nach der technischen und organisatorischen Ausgestaltung des Portals sichergestellt ist, dass seitens des Portalbetreibers kein Zugriff auf das Postfach erfolgt.

b) Der Zeitpunkt des Zugangs

Im Verhältnis zwischen Kassen- bzw. Kassenzahnärztlicher Vereinigung und Vertragsarzt im Anwendungsbereich des SGB ist, wie dargestellt, zu differenzieren. Elektronisch übermittelte Verwaltungsakte, also etwa der Honorarbescheid oder Änderungsbescheide, gelten gemäß § 37 SGB X als im dritten Tag nach der Absendung zugegangen (dazu oben II.6., S. 31).

Bei allen übrigen Erklärungen gelten die allgemeinen Grundsätze. Nach herrschender Meinung erfolgt der Zugang einer Erklärung, wie dargestellt, nicht stets schon im Zeitpunkt der Speicherung, sondern in dem Zeitpunkt, in dem die Kenntnisnahme erwartet werden kann. (dazu oben II.6., S. 31). Damit ist von Bedeutung, in welchen Intervallen vom Teilnehmer die Kontrolle seines Postfachs am Internetportal auf eingegangene Nachrichten erwartet werden kann.

Diese Frage wird derzeit nur selten erörtert, Literatur und Rechtsprechung orientieren sich bisher an anderen Medien wie Fax oder E-Mail (dazu oben II.6., S. 31). Wenn man die zur E-Mail vertretenen Grundsätze auf das Postfach im Internetportal überträgt, so wäre eine laufende Kontrolle während der Geschäftszeiten zu erwarten und würden Erklärungen, die vor Beginn eines Geschäftstags eingehen, zu diesem Zeitpunkt, Erklärungen,

die vor dem Ende der Geschäftszeit (Praxisschluss) gespeichert werden, zum Zeitpunkt der Speicherung zugehen. Diese Übertragung erscheint aber nur gerechtfertigt, wenn laufend Erklärungen auf dem Postfach eingehen oder der Teilnehmer Anlass hat, - aus anderem Grund - mehrfach täglich auf das Internetportal zuzugreifen. Dies hängt von der Ausgestaltung des Portals ab, erscheint derzeit aber fraglich. Mehr als eine Eingangskontrolle täglich wird daher wohl nicht erwartet werden können, möglicherweise auch nur im Abstand von zwei oder drei Tagen. Je nachdem wäre eine Erklärung dann zum Ende des Prüfintervalls zugegangen.

Anders liegt es, wenn zwischen Portalbetreiber und Teilnehmer ein bestimmtes Prüfintervall vereinbart wird oder die Kassenärztliche bzw. Kassenzahnärztliche Vereinigung eine Regelung beschließt. Es könnte auch eine Regelung dahin erfolgen, dass der Teilnehmer durch ein anderes Medium, etwa eine SMS etc., über den Eingang von Nachrichten informiert wird und verpflichtet wird, in diesem Fall das Postfach auf den Eingang von Nachrichten zu überprüfen.

2. Wirksamwerden durch Kenntnisnahme

Soweit Erklärungen durch Kenntnisnahme (Lesen) wirksam werden, erfolgt die Wirksamkeit oder der „Zugang“ im Zeitpunkt der Kenntnisnahme (dazu oben II.6., S. 31). Wenn also der Teilnehmer eine Erklärung, die ihm über das Portal gesendet wird, auf dem Bildschirm liest, ist diese ihm gegenüber wirksam geworden. Wenn er eine Erklärung nicht liest, obwohl es ihm möglich und zumutbar wäre, liegt eine Kenntnisnahmeverweigerung vor, der Teilnehmer müsste sich so behandeln lassen, als habe er die Nachricht gelesen.

Diese Grundsätze haben vor allem für solche Erklärungen praktische Bedeutung, die nicht ins Postfach eingestellt werden, sondern an anderer Stelle im Portal angezeigt werden, etwa Hinweise auf der Homepage, im Anmeldefenster etc. Sie sind aber auch anwendbar für Erklärungen, die im Postfach gespeichert werden. Hier ist freilich regelmäßig schon vorher der Zugang aufgrund der Speicherung im Postfach erfolgt. Anders liegt es aber etwa, wenn eine Nachricht am Freitag nach Praxisschluss gespeichert wird und der Teilnehmer diese am Abend oder am Wochenende liest.

3. Zugang durch Bereitstellung zum Abruf

a) Bereitstellung und Zugangserfordernis

Nachrichten können auch in der Weise elektronisch übermittelt werden, dass sie vom Absender auf einem Server zum Abruf bereitgehalten werden und der Empfänger diese auf sein Datenverarbeitungssystem herunterlädt und dann dort zur Kenntnis nimmt oder speichert. Dieses Vorgehen wird in der Praxis des elektronischen Geschäftsverkehrs bei Allgemeinen Geschäftsbedingungen angewandt, die meist auf der Website des Verwenders zur Ansicht und zum Drucken sowie Herunterladen vorgehalten werden und üblicherweise von der Homepage über einen Link erreichbar sind. Diese Technik hat auch für die Online-Abrechnung über Internetportale für Heilberufe Bedeutung. Teilweise wird der Honorarbescheid nebst Anlagen im Portal zum Abruf bereitgestellt, der teilnehmende Vertragsarzt durch eine ins Postfach eingestellte Nachricht über die Bereitstellung informiert (dazu oben B.II.4., S. 12).

Die Bereitstellung einer Nachricht zum Abruf auf dem Webserver des Absenders bewirkt nicht den Zugang beim Empfänger, denn die Nachricht befindet sich noch nicht im Bereich des Empfängers, sondern verbleibt auch organisatorisch noch im Bereich des Absenders. Der Zugang des Honorarbescheids wird daher erst dann bewirkt, wenn sie vom Teilnehmer heruntergeladen oder ausgedruckt wird.⁶³

b) Mitwirkungspflichten

Der Zugang von Erklärungen über Internetportale für Heilberufe bedarf, wie soeben dargestellt, im Fall der Bereitstellung zum Abruf der Mitwirkung des Teilnehmers. Eine Verpflichtung des Teilnehmers zu dieser Mitwirkung besteht zunächst freilich nicht. Sie könnte aber wohl durch Vereinbarung zwischen Portalbetreiber und Teilnehmer begründet werden. Gegenstand einer solchen Vereinbarung wäre die Pflicht des Teilnehmers, Erklärungen, etwa die Abrechnung, nach Eingang der Bereitstellungsnachricht unverzüglich herunterzuladen oder auszudrucken. Wenn der Teilnehmer

⁶³ Vgl. *Borges* (Fn. 16), S. 254.

dieser Pflicht schuldhaft nicht nachkommt, müsste er sich nach den oben dargestellten Grundsätzen so behandeln lassen, als wäre der Zugang erfolgt.

Als Alternative zu einer Vereinbarung zwischen Teilnehmer und Portalbetreiber kommt auch eine Regelung durch die Kassenärztliche bzw. Kassenzahnärztliche Vereinigung in Betracht. Ohnehin ergänzen diese Vereinigungen die gesetzlichen Regeln zur Honorarabrechnung regelmäßig durch eigene Regelwerke, die als Beschluss der Vereinigung gefasst werden und dann für ihre Mitglieder verbindlich sind. Eine solche Regelung könnte wohl auch Mitwirkungspflichten im Zusammenhang mit der Zustellung der Honorarbescheide enthalten. Gerichtliche Entscheidungen zu derartigen Gestaltungen liegen aber bisher, soweit ersichtlich, nicht vor.

4. Zugang und Eingriffe Dritter

Die Übermittlung von Nachrichten über Internetportale kann durch Eingriffe Dritter gestört werden. So könnte etwa ein Dritter eine ins Postfach des Teilnehmers eingelegte Nachricht löschen oder eine Datei öffnen, so dass diese als gelesen markiert und vom Teilnehmer nicht mehr als neu erkannt wird. Soweit derartige Eingriffe durch Personen erfolgen, die dem Bereich des Empfängers zuzuordnen sind, etwa durch Praxisangestellte eines Arztes, denen dieser das Passwort mitgeteilt hat, sind diese Handlungen dem Teilnehmer zuzurechnen und können den Zugang keinesfalls hindern.

Denkbar ist aber auch, dass ein außenstehender Dritter derartige Eingriffe vornimmt. So könnte der Dritte etwa durch einen Phishing-Angriff (dazu oben) in den Besitz von Zugangsdaten (Passwort) kommen, mit diesen auf den Account des Teilnehmers zugreifen und dort Nachrichten löschen. Soweit Portale das Löschen von Nachrichten durch Teilnehmer ausschließen, besteht diese Gefahr freilich nicht. Wenn das Löschen ermöglicht wird, ist fraglich, ob ein derartiger Eingriff den Zugang der gelöschten Nachricht hindert, wenn der Teilnehmer diese noch nicht gelesen hat. Wird eine Nachricht durch einen Dritten gelöscht, kann sie vom Teilnehmer nicht mehr zur Kenntnis genommen werden. Ein Wirksamwerden durch Kenntnisnahme scheidet folglich aus. Anders liegt es beim Zugang durch Speicherung. Insoweit gilt, dass der Zugang mit

Speicherung der Nachricht in der Empfangseinrichtung des Teilnehmers (hier: Postfach auf dem Portal) bewirkt ist. Spätere Eingriffe hindern folglich den Zugang nicht; das Risiko derartiger Eingriffe trägt der Empfänger. So ist beispielsweise eine E-Mail, die nach Speicherung in der Mailbox von einem Dritten gelöscht wird, gleichwohl zugegangen.⁶⁴

Diese Risikozuordnung ist im Grundsatz unstrittig. Es fragt sich aber, ob sie in dem hier interessierenden Fall bei der Übermittlung über Internetportale uneingeschränkt aufrechterhalten werden kann. Die Zuordnung dieses Risikos zum Empfänger beruht auf der Erwägung, dass der Empfänger, der die betreffende Empfangseinrichtung eingerichtet hat und vorhält, dieses Risiko am besten beherrschen kann. Es ist seine Entscheidung, ob und wo er eine Einrichtung bereitstellt und mit welchen Sicherheitsvorkehrungen gegen Eingriffe Dritter er diese ausstattet. Selbst wenn er dies faktisch nicht kann, so steht er diesem Risiko doch viel näher als der Absender, der typischerweise keinen Einfluss auf die Empfangseinrichtungen des Empfängers nehmen kann.

Bei Internetportalen für Heilberufe besteht aber die Besonderheit, dass es sich um Nachrichten des Betreibers der Empfangseinrichtung handelt, der Absender also über die Sicherheit der Empfangseinrichtung entscheidet. Hinzu kommt, dass diese Empfangseinrichtung ausschließlich oder jedenfalls vorrangig für den Empfang von Erklärungen des Absenders eingerichtet wurde. Dies spricht dafür, dass der Teilnehmer das Risiko jedenfalls nicht allein zu tragen hat. Stellungnahmen von Literatur und Rechtsprechung zu dieser Frage fehlen bisher. Es spricht aber einiges dafür, dass die Risikoverteilung von der Sicherheit des Portals abhängt. So könnte man wohl beim Fehlen jeglicher Sicherung schon nicht von einem Bereich des Empfängers sprechen. Auch bei völlig unzureichender Sicherung ist zweifelhaft, ob der Empfänger das Risiko tragen kann.

Die Fragen können letztlich wohl dahinstehen. Internetportale für Heilberufe verwenden sämtlich Systeme der Zugriffssicherung, Eingriffe Dritter in das Postfach von Teilnehmern sind bisher nicht bekannt geworden. Folglich bleibt es bei dem Grundsatz, dass der Teilnehmer das

⁶⁴ Dörner, AcP 202 (2002) 363, 372; siehe zu dieser Risikoverteilung dazu auch oben C.II.4. (S.25 f.).

Risiko nachträglicher Eingriffe trägt und diese den Zugang von Nachrichten nicht hindern. Sofern es zu Eingriffen kommt, sind andererseits aber Schadensersatzansprüche des Teilnehmers wegen unzureichender Zugangssicherung denkbar. Inhalt dieses Schadensersatzanspruchs wäre so gestellt zu werden, als wäre der Eingriff nicht erfolgt, d.h. die Nachricht nicht gelöscht oder verändert worden.

Diese Risikoordnung hängt wesentlich vom Risiko derartiger Eingriffe ab, das nicht zuletzt durch die Sicherheit des Systems beeinflusst wird. Es ist damit zu rechnen, dass bei geringer Sicherung das Risiko nicht uneingeschränkt beim Empfänger bleiben kann. Dies hängt aber entscheidend davon ab, ob es tatsächlich in nennenswertem Ausmaß zu Angriffen Dritter gegen Internetportale für Heilberufe kommt. Soweit diese Frage künftig akut werden sollte, wird die Risikoordnung entscheidend vom Authentisierungsverfahren abhängen. Die traditionelle Authentisierung durch Teilnehmernamen und Passwort wird möglicherweise als unzureichend angesehen werden, da sie etwa durch Phishing-Angriffe leicht zu überwinden ist. Dagegen erscheint ein Eingriff Dritter bei Authentisierung durch Chipkarte kaum denkbar.

5. Die Bedeutung von Lesebestätigungen

Soweit Internetportale vorsehen, dass das erstmalige Öffnen der ins Postfach eingestellten Datei eine Lesebestätigung auslöst, ergibt sich die Frage, welche Bedeutung derartige Lesebestätigungen für den Zugang der Nachricht haben.

Das Auslösen einer Lesebestätigung durch den Empfänger bewirkt nicht die Kenntnisnahme der in der Datei enthaltenen Nachricht. Sie hat gleichwohl praktische Bedeutung: Da die in der Datei enthaltene Nachricht im Regelfall entweder gelesen wird oder jedenfalls hätte gelesen werden können, kann vom Öffnen der Datei regelmäßig darauf geschlossen werden, dass die Kenntnisnahme der Nachricht erfolgte oder bewusst nicht erfolgte (Kenntnisnahmeverweigerung). Da im zweiten Fall die Wirkungen des Zugangs ebenfalls eintreten, kann von der Lesebestätigung auf den Zugang geschlossen werden. Da die Lesebestätigung den Zeitpunkt der Öffnung

protokolliert, zeigt sie zugleich an, zu welchem Zeitpunkt die Nachricht (spätestens) wirksam zugestellt wurde.

Für den Zugang durch Speicherung ist die Lesebestätigung nur mittelbar von Bedeutung. Sie ist insoweit lediglich ein Indiz für die Speicherung. Wenn die Lesebestätigung, etwa infolge eines Phishing-Angriffs, durch einen unbefugten Dritten ausgelöst wurde, entfaltet sie diese Wirkungen nicht. Die Möglichkeit eines solchen Angriffs hat vor allem Bedeutung für den Beweis des Zugangs.

6. Beweis des Zugangs

Wenn es zwischen Portalbetreiber und Teilnehmer zu Streitigkeiten über den Zugang einer Nachricht kommt, ist der Zugang im Falle eines Rechtsstreits zu beweisen. Die Beweislast trägt grundsätzlich die Partei, für die die zu beweisende Tatsache günstig ist (dazu unten D.). Daher muss etwa bei Verwaltungsakten der Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigung die Vereinigung den Zugang des Verwaltungsakts beweisen.

a) Beweis des Zugangs durch Speicherung

Für den Teilnehmer ist es regelmäßig nicht schwer, den Zugang der in sein Postfach eingegangenen Nachricht zu beweisen. Soweit die Nachricht nicht gelöscht ist, kann er notfalls im Wege des sogenannten Augenscheinsbeweises in der Beweisaufnahme dem Gericht Einblick in sein Postfach geben. Soweit das Gericht die betreffende Datei dort sieht, ist der Beweis des Zugangs geführt. Daher wird in dieser Konstellation ein derartiger Beweis regelmäßig nicht notwendig sein und der Zugang seitens des Portalbetreibers nicht bestritten werden.

Es ist anzunehmen, dass eher der Teilnehmer den Zugang einer an ihn gerichteten Nachricht bestreiten wird. In diesem Fall muss der Portalbetreiber beweisen, dass die Datei mit der betreffenden Nachricht im Postfach des Teilnehmers gespeichert war. Auch hier ist die Beweisführung einfach, wenn die Datei noch gespeichert ist und der Portalbetreiber dem Gericht Einblick in das Postfach des Teilnehmers vermitteln kann.

Auch ohne Präsentation des Postfachs in der Beweisaufnahme kann der Portalbetreiber den Zugang regelmäßig beweisen. Hierzu ist der Nachweis erforderlich, dass eine bestimmte Datei im Postfach gespeichert wurde und dass die gespeicherte Datei die fragliche Nachricht enthielt. In der Praxis wird in derartigen Fällen der Nachweis dadurch geführt, dass ein Ausdruck der Datei sowie Speicherprotokolle vorgelegt werden und ein Mitarbeiter des Portalbetreibers erläutert, in welcher Weise das System funktioniert. Erforderlich ist weiterhin, dass das System in dem betreffenden Zeitpunkt fehlerfrei funktioniert hat. Dies wird in der Praxis ebenfalls durch Mitarbeiter des Portalbetreibers als Zeugen bewiesen.

b) Beweis des Zugangs durch Kenntnisnahme

Soweit bewiesen werden soll, dass der Teilnehmer eine bestimmte Erklärung zur Kenntnis genommen hat, kann dieser Nachweis etwa durch die Lesebestätigung geführt werden. Hierzu ist aber im Streitfall zu beweisen, dass die Datei durch den Teilnehmer und nicht etwa durch einen Dritten geöffnet wurde. Dieser Beweis wird mittels der Authentisierung bei der Anmeldung zum Teilnehmerbereich geführt.⁶⁵ Hinreichende Sicherheit des Authentisierungsverfahrens vorausgesetzt, kann die Datei nur von der Person geöffnet worden sein, die sich bei der Anmeldung identifiziert hat. Es ist daher vom Portalbetreiber zu beweisen, dass der Teilnehmer sich authentisiert hat und nicht etwa ein Dritter, der das Authentisierungsmedium unbefugt verwendet hat.

Ob der Beweis geführt werden kann, hängt wesentlich vom jeweiligen Authentisierungsverfahren ab. Diese Frage ist insoweit dieselbe wie in allen anderen Fällen, in denen der Portalbetreiber nachweisen möchte, dass der Teilnehmer am Portal gehandelt hat und nicht etwa ein unbefugter Dritter. Daher kann auf die Ausführungen im folgenden Teil des Gutachtens verwiesen werden.

Im Ergebnis wird der Nachweis jedenfalls bei Authentisierung durch Chipkarte und PIN regelmäßig geführt werden können. Bei Authentisierung durch schlichtes Passwort hingegen ist zweifelhaft, ob der Nachweis gelingt.

⁶⁵ Siehe dazu unten D. II.2. (S. 44 f.)

D. Nachweis von Handlungen am Account des Teilnehmers

I. Die Relevanz des Beweises der Urheberschaft von Handlungen

Die Teilnehmer an Internetportalen für Heilberufe nehmen vielfach Handlungen an ihrem Account vor, die für das Verhältnis zwischen Teilnehmer und Portalbetreiber rechtlich relevant sind. So werden Erklärungen an den Portalbetreiber übermittelt oder relevante tatsächliche Handlungen vorgenommen, wie etwa das Veranlassen einer Zahlung, das Öffnen der Mitteilung über die Bereitstellung der Abrechnung zwischen Kassen- bzw. Kassenzahnärztlicher Vereinigung und Vertragsarzt, oder das Herunterladen des Honorarbescheids.

Wenn es Unstimmigkeiten über die Zuordnung einer bestimmten Handlung gibt, etwa wenn ein Teilnehmer bestreitet, eine bestimmte Erklärung abgegeben zu haben oder die Benachrichtigung über die Abrechnung geöffnet zu haben, dann kommt es im Falle eines Rechtsstreits entscheidend darauf an, ob der Nachweis geführt werden kann, dass der Teilnehmer und nicht etwa ein Dritter die betreffende Handlung vorgenommen hat. Sehr häufig wird der Nachweis vom Portalbetreiber, also der Kassen- bzw. Kassenzahnärztlichen Vereinigung zu führen sein.

Dieser Nachweis erfolgt wesentlich über die Authentisierung bei der Anmeldung zum Teilnehmerbereich und den Nachweis, dass eine bestimmte Handlung, z.B. die Abgabe einer Erklärung, innerhalb der durch die betreffende Anmeldung eröffneten Sitzung am Portal stattgefunden hat.

Damit hängt der Nachweis der Urheberschaft für Handlungen, die am Portal vorgenommen werden, wesentlich von der Authentisierung der Teilnehmer am Portal ab.

Der Nachweis, welche konkrete natürliche Person die Anmeldung am Portal vorgenommen hat, kann sehr schwierig sein. Die Aussichten, diesen Beweis in einem Rechtsstreit führen zu können, hängen stark vom jeweiligen Authentisierungsverfahren ab. Hier ist vor allem von Interesse, welche Bedeutung Angriffe auf Internetportale, die per Internet erfolgen, insbesondere Phishing und ähnliche Angriffe, für den Nachweis der Urheberschaft haben. Diese Problematik steht im Vordergrund der nachfolgenden Erörterung.

II. Der Beweis der Urheberschaft im gerichtlichen Verfahren

1. Die maßgebliche Regelung des Beweises

Die Notwendigkeit, die Urheberschaft einer am Portal vorgenommenen Handlung zu beweisen, kann sich in ganz unterschiedlichen prozessualen Situationen ergeben. Im Zivilprozess unterliegt die Beweisaufnahme den Regeln der Zivilprozessordnung (ZPO), hier den §§ 355 ff. ZPO, für die Beweiswürdigung gilt § 286 ZPO. Für Streitigkeiten zwischen einer Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigung und ihren Mitgliedern ist gemäß § 51 Abs. 1 Nr. 2 Sozialgerichtsgesetz (SGG) regelmäßig der Rechtsweg zu den Sozialgerichten eröffnet. Das Verfahren vor den Sozialgerichten ist im SGG geregelt. Die Beweisaufnahme ist in § 118 SGG, die Beweiswürdigung in § 128 SGG normiert.

Die Tatsachenfindung im sozialgerichtlichen Verfahren unterscheidet sich vom Zivilverfahren wesentlich dadurch, dass das Gericht im sozialgerichtlichen Verfahren die Tatsachen gemäß § 103 SGG von Amts wegen ermittelt (Untersuchungsmaxime), wogegen im Zivilprozess grundsätzlich den Parteien die Beibringung des Tatsachenstoffes obliegt (Dispositionsmaxime). Gleichwohl gelten in zentralen Aspekten übereinstimmende Grundsätze. Dies gilt vor allem für die Beweisaufnahme. § 118 Abs. 1 SGG verweist hierfür im Wesentlichen auf die Vorschriften der Beweisaufnahme der ZPO, die wenigen Abweichungen haben ihren Grund in den Besonderheiten des sozialgerichtlichen Verfahrens.

Die Beweiswürdigung ist in der ZPO und im SGG im Wesentlichen gleichartig geregelt. Gemäß § 286 Abs. 1 ZPO entscheidet das Gericht nach freier Überzeugung auf der Grundlage der mündlichen Verhandlung und der Beweisaufnahme über die tatsächlichen Grundlagen seiner Entscheidung. Entsprechendes gilt nach § 128 Abs. 1 SGG im sozialgerichtlichen Verfahren. Wenn eine entscheidungserhebliche Tatsache nicht festgestellt werden kann, weil die volle Überzeugung des Gerichts vom Bestehen der Tatsache nicht erzielt werden kann, bestimmt sich nach den Grundsätzen der objektiven (materiellen) Beweislast, zu wessen Nachteil sich die

fehlende Sachverhaltsaufklärung auswirkt. Dies gilt nicht nur im Zivilprozess⁶⁶, sondern auch im sozialgerichtlichen Verfahren⁶⁷.

Im Ergebnis gelten daher für die Beweisaufnahme und die Beweiswürdigung zwar verschiedene, jedoch ähnliche Grundsätze. Daher kann auch für das sozialgerichtliche Verfahren auf die Erfahrung, die im Bereich des Zivilverfahrens zum Nachweis der Urheberschaft von Handlungen an Internetportalen gewonnen wurden, zurückgegriffen werden.

2. Der Nachweis der Urheberschaft

Der Nachweis der Urheberschaft einer Handlung kann mit allen zur Verfügung stehenden Beweismitteln geführt werden. Im Zivilprozess sind dies Zeugen, Sachverständige, Vernehmung der Partei, Urkunden, Augenschein. Entsprechendes gilt im sozialgerichtlichen Verfahren, mit Ausnahme der Parteivernehmung (vgl. § 118 SGG). Außerdem können nach § 284 S. 2 ZPO, bzw. § 284 S. 2 ZPO i.V.m. § 202 SGG im Wege des sog. Freibeweises mit Einverständnis der Parteien weitere Beweismittel, etwa eine telefonische Auskunft, herangezogen werden.

Der Beweis der Urheberschaft könnte also etwa durch einen Zeugen geführt werden, der gesehen hat, wie der Teilnehmer von seinem Rechner aus zur fraglichen Zeit am Portal eine bestimmte Handlung vorgenommen hat. Dies wird freilich eher selten der Fall sein. Größere Bedeutung hat daher der Indizienbeweis, bei dem aufgrund mehrerer Indizien der Rückschluss auf die handelnde Person gezogen wird. Im Rahmen dieses Indizienbeweises können insbesondere Protokolle der Portalnutzung herangezogen werden, aus denen sich ergibt, zu welchem Zeitpunkt die jeweilige Sitzung stattgefunden hat und mit welcher Chipkarte und mit welchem Passwort der Zugang zum Portal erfolgte.

⁶⁶ Musielak-*Foerste*, ZPO, Kommentar, 5. Aufl. 2007, § 286 Rz. 32.

⁶⁷ St.Rspr.; BSGE 6, 70, 73; 19, 52, 53; 45, 283; *Bolay*, in Lüdtkke (Hrsg.), Handkommentar Sozialgerichtsgesetz, 2. Aufl. 2006 (i.F. Hk-SGG), § 128 Rz 17; *Leitherer*, in Meyer-Ladewig/Keller/Leitherer (Hrsg.), Sozialgerichtsgesetz, 8. Aufl. 2005, § 103 Rz. 19a m.w.Nachw.

Für die jeweiligen Indizien der Indizienkette gelten wiederum die allgemeinen Regeln über Beweismittel. Soweit elektronische Dateien, wie Protokolle etc., herangezogen werden, handelt es sich um Gegenstände des Augenscheins, die nach den Regeln über den Augenscheinsbeweis, §§ 371 ff. ZPO bzw. § 118 SGG i.V.m. §§ 371 ff. ZPO, in den Prozess eingeführt werden.⁶⁸ Elektronische Dateien sind danach in elektronischer Form in die Beweiserhebung einzubringen. Soweit ihr Inhalt nicht bestritten wird, kann, wie es häufig praktiziert wird, stattdessen ein Ausdruck vorgelegt werden.⁶⁹

3. Die Anforderungen an den Beweis der Urheberschaft

Zum Nachweis der Urheberschaft ist nach § 286 Abs. 1 ZPO und ebenso nach § 128 Abs. 1 SGG die volle Überzeugung des Gerichts erforderlich.⁷⁰ Dies bedeutet nicht, dass ein anderer Geschehensablauf völlig ausgeschlossen sein müsste. Es darf aber als Ergebnis der Beweisaufnahme „kein vernünftiger Zweifel“ an der Urheberschaft des Teilnehmers mehr bestehen.⁷¹

Ob und unter welchen Voraussetzungen diese hohe Anforderung beim Nachweis der Urheberschaft von Handlungen an Internetportalen in der Praxis erreicht werden kann, ist offen, da praktische Erfahrungen zu dieser Konstellation nicht vorliegen. In anderen Fällen, in denen die Urheberschaft von Erklärungen, die an Websites übermittelt wurden, streitig war, haben die Zivilgerichte aber auch bei Authentisierung durch Passwort die

⁶⁸ Siehe zum Augenscheinsbeweis mit elektronischen Dokumenten *Borges* (Fn. 16), S. 453 ff.

⁶⁹ *Borges* (Fn. 16), S. 466.

⁷⁰ BSGE 45, 285, 287; Hk-SGG-*Bolay* (Fn. 67), § 128 Rz. 13; *Meyer-Ladewig*, in Meyer-Ladewig/Keller/Leitherer (Fn. 67), § 128 Rz. 3b.; Hk-SGG-*Roller* (Fn. 67), § 118 Rz. 2; BGHZ 53, 245, 255 f.; *Pritting*, Gegenwartsprobleme der Beweislast, 1983, S. 67 ff., 71 ff.

⁷¹ Hk-SGG-*Bolay* (Fn. 67), § 128 Rz. 13; BGHZ 53, 245, 255: „Ein der Gewissheit nahekommender Grad von Wahrscheinlichkeit“; vgl. BSGE 7, 103, 106; 19, 52, 53; 45, 385, 287; *Meyer-Ladewig*, in Meyer-Ladewig/Keller/Leitherer (Fn. 67), § 128 Rz. 3b m.w.Nachw.

Urheberschaft des Passwortinhabers als nicht bewiesen angesehen.⁷² In der Tat sind andere Geschehensabläufe regelmäßig nicht undenkbar und auch keinesfalls rein theoretischer Art. Insbesondere ist vorstellbar, dass ein Dritter über das Authentisierungsmedium des Teilnehmers, also etwa das Passwort oder Chipkarte und Passwort, verfügt und sich damit anmeldet. Im Fall eines Arztes kommen etwa Praxismitarbeiter in Betracht. Sei es, dass der Arzt einem Mitarbeiter das Passwort mitgeteilt oder die Chipkarte übergeben hat, sei es, dass dieser sich unbefugt in den Besitz bringt.

Daher werden Zweifel an der Urheberschaft des Teilnehmers häufig nicht ausgeräumt werden können. Nach dem Grundsatz des § 128 Abs. 1 SGG bzw. des § 286 Abs. 1 ZPO wäre also der Beweis nicht erbracht. Es kommt daher in der Praxis entscheidend darauf an, ob die volle Überzeugung des Gerichts ggf. nach den Regeln des sogenannten Anscheinsbeweises erreicht wird.

III. Der Anscheinsbeweis der Urheberschaft

1. Allgemeine Grundsätze des Anscheinsbeweises

Der Anscheinsbeweis (Beweis des ersten Anscheins, prima-facie-Beweis) ist nur teilweise gesetzlich geregelt; § 371a ZPO betrifft ausdrücklich nur den Fall der qualifizierten elektronischen Signatur. Ob es sich bei diesen Regeln um einen echten Anscheinsbeweis handelt, ist fraglich.⁷³ In jedem Fall werden die allgemeinen Grundsätze des Anscheinsbeweises durch diese Bestimmung nicht berührt.

Die maßgeblichen Grundsätze des Anscheinsbeweises sind von Rechtsprechung und Literatur herausgebildet worden. Sie sind auch im sozialgerichtlichen Verfahren anwendbar.⁷⁴ Anwendungsbereich des

⁷² OLG Naumburg, NJOZ 2005, 2222, 2223 f.; LG Bonn, CR 2004, 218, 219; LG Bonn, MMR 2002, 255, 256; AG Erfurt, MMR 2002, 127, 128.

⁷³ Siehe dazu *Borges* (Fn. 16), S. 505 ff.

⁷⁴ BSGE 81, 288, 293; BSG, 22.6.1988, 9/9a BVg 4/87 SozR 1500 § 128 Nr. 35; Hk-SGG-Bolay (Fn. 67), § 128 Rz. 12; *Meyer-Ladewig*, in Meyer-Ladewig/Keller/Leitherer (Fn. 67), § 128 Rz. 9.

Anscheinsbeweises ist der Indizienbeweis.⁷⁵ Mit Hilfe des Anscheinsbeweises können fehlende konkrete Indizien durch Erfahrungssätze überbrückt werden, die auf der allgemeinen Lebenserfahrung beruhen.⁷⁶ Voraussetzung des Anscheinsbeweises ist das Bestehen eines Erfahrungssatzes, der aus einem typischen Geschehensablauf abgeleitet wird.⁷⁷ Typisch ist ein Geschehensablauf, wenn er nach der Erfahrung sehr wahrscheinlich und damit deutlich wahrscheinlicher ist als alle anderen denkbaren Geschehensabläufe.⁷⁸ Der Anscheinsbeweis wird in der Praxis vor allem zur Feststellung von Kausalverläufen und des Verschuldens eingesetzt, etwa beim Hergang eines Unfalls etc.⁷⁹ Ein klassisches Beispiel eines solchen Erfahrungssatzes ist der Grundsatz, dass ein Auffahrunfall typischerweise auf einem Fahrfehler des auffahrenden Fahrers (zu geringer Abstand oder Unachtsamkeit) beruht.⁸⁰ Der Anscheinsbeweis ist aber auch für komplexere Geschehensabläufe anerkannt, etwa bei der Verwendung von ec-Karte und PIN (dazu unten IV.3.a, S. 55 ff.).

Soweit das ungeklärte Element des Geschehensablaufs (z.B. Ursache eines Auffahrunfalls) mit Hilfe eines derartigen Erfahrungssatzes (z.B. Fehler des auffahrenden Fahrers) überbrückt werden kann, kann der Beweis für dieses Element durch den Anscheinsbeweis erbracht werden.⁸¹ Der Sache nach

⁷⁵ *Borges* (Fn. 16), S. 492 m.w.Nachw.; *Rosenberg/Schwab/Gottwald*, Zivilprozessrecht, 16. Aufl. 2004, § 112 Rz. 18.

⁷⁶ *Borges* (Fn. 16), S. 492; *Rosenberg/Schwab/Gottwald*, Zivilprozessrecht, 16. Aufl. 2004, § 112 Rz. 17; *MünchKommZPO-Prütting*, Zivilprozessordnung, 2. Aufl. 2000, § 286 Rz. 48, 64.

⁷⁷ BSGE 81, 288, 293; BSG, 27.11.986 5a – RKnU 3/85 SozR 5670 Anl. 1 Nr. 2102 Nr. 2; *Meyer-Ladewig*, in *Meyer/Ladewig/Keller/Leitherer* (Fn. 67), § 128 Rz. 9a; st. Rspr. BGHZ 100, 31, 33 m.w.Nachw.; BGH, NJW 1996, 1828; BGH, NJW 2001, 1140 f.; *Borges* (Fn. 16), S. 492; *Rosenberg/Schwab/Gottwald* (Fn. 75), § 112 Rz. 17; *MünchKommZPO-Prütting* (Fn. 76), § 286 Rz. 48.

⁷⁸ *Borges* (Fn. 16), S. 492; *Prütting* (Fn. 70), S. 106 („höchste Wahrscheinlichkeit i.S. von „wenn-dann meist““).

⁷⁹ *Hk-SGG-Bolay* (Fn. 67), § 128 Rz. 12; *Meyer-Ladewig*, in *Meyer-Ladewig/Keller/Leitherer* (Fn. 67), § 128 Rz. 9a.

⁸⁰ BGH, NJW-RR 1989, 670 ff.; *Rosenberg/Schwab/Gottwald* (Fn. 75), § 112 Rz. 26.

⁸¹ *Hk-SGG-Bolay* (Fn. 67), § 128 Rz. 21.

führt der Anscheinsbeweis somit zu einer Absenkung des Beweismaßes: der Beweis wird so aufgrund einer geringeren Wahrscheinlichkeit eines bestimmten konkreten Geschehensablaufs erreicht als es typischerweise für die volle Überzeugung des Gerichts erforderlich ist.⁸²

Allerdings kann die auf einem solchen Anschein beruhende Überzeugung des Gerichts besonders leicht widerlegt werden. So muss der Beweisgegner nicht etwa den Beweis des Gegenteils führen, um den Anschein zu widerlegen.⁸³ Vielmehr reicht es aus, wenn der Anschein durch Gegenbeweis „erschüttert“ wird.⁸⁴ Der Anscheinsbeweis lässt auch die Beweislast unberührt.⁸⁵ Wenn der Anscheinsbeweis erschüttert wird, bleibt der Beweisführer beweisfällig.

Die Erschütterung des Anscheinsbeweises setzt voraus, dass ein Sachverhalt dargelegt wird, aus dem die ernsthafte Möglichkeit eines anderen als des der allgemeinen Erfahrung entsprechenden Geschehensablaufs folgt.⁸⁶ Die Tatsachen, aus denen sich die Möglichkeit eines anderen Geschehensablaufs ergibt, müssen feststehen, also unstrittig sein oder ihrerseits vom Beweisgegner bewiesen werden.⁸⁷ Der Beweisgegner muss freilich nicht beweisen, dass sich ein solcher Geschehensablauf ereignet hat.⁸⁸

⁸² *Borges* (Fn. 16), S. 493 m.w.Nachw.

⁸³ *Borges* (Fn. 16), S. 493; *Rosenberg/Schwab/Gottwald* (Fn. 75), § 112 Rz. 36; *MünchKommZPO-Prütting* (Fn. 76), § 286 Rz. 65.

⁸⁴ BSG, 27.11.986 5a – RKnU 3/85 SozR 5670 Anl. 1 Nr. 2102 Nr. 2; Hk-SGG-*Bolay* (Fn. 67), § 128 Rz 12; *Meyer-Ladewig*, in *Meyer/Ladewig/Keller/Leitherer* (Fn. 67), § 128 Rz. 9e m.w.Nachw.; BGH, NJW 1972, 1131; *Borges* (Fn. 16), S. 493 m. w. Nachw.; *Rosenberg/Schwab/Gottwald* (Fn. 75), § 112 Rz. 36; BGHZ 39, 103, 107; 100, 31, 34; *MünchKommZPO-Prütting* (Fn. 76), § 286 Rz. 51.

⁸⁵ BGHZ 39, 103, 107; 100, 31, 34; *Baumgärtel/Prütting*, S. 63; *Rosenberg/Schwab/Gottwald* (Fn. 75), § 112 Rz. 36; *MünchKommZPO-Prütting* (Fn. 76), § 286 Rz. 51.

⁸⁶ BSG 8, 245; BSG, 27.11.986 5a – RKnU 3/85 SozR 5670 Anl. 1 Nr. 2102 Nr. 2; Hk-SGG-*Bolay* (Fn. 67), § 128 Rz 12; BGHZ 8, 239; BGH, NJW 1978, 2032; *Rosenberg/Schwab/Gottwald* (Fn. 75), § 112 Rz. 36; *Schneider*, Beweis und Beweiswürdigung, 5. Aufl. 1994, Rz. 342; *Weber*, Der Kausalitätsbeweis im Zivilprozeß, 1997, S. 49.

⁸⁷ BSG, 27.11.986 5a – RKnU 3/85 SozR 5670 Anl. 1 Nr. 2102 Nr. 2; RGZ 95, 103, 104; BGHZ 6, 169, 171, 8, 239, 240, BGH, NJW-RR 1989, 670 f.; *Borges* (Fn. 16), S.

2. Der Anscheinsbeweis für die Urheberschaft einer elektronisch übermittelten Erklärung

Für den Nachweis, dass eine bestimmte Person (z.B. ein Vertragsarzt), eine bestimmte Erklärung über ein Internetportal übermittelt hat oder eine bestimmte Handlung (z.B. Herunterladen der Abrechnung des Honorarbescheids) am Portal vorgenommen hat, sind mehrere Schritte erforderlich. Zunächst muss, wie oben (II.2., S. 44 f.) dargestellt, nachgewiesen werden, dass die betreffende Handlung am Portal vorgenommen wurde.

Für den Rückschluss auf die handelnde Person ist weiter erforderlich, dass nur diese Person die Möglichkeit hatte, sich am Portal anzumelden. Hier kommt es auf die Qualität der Zugangssicherung zum Portal und das verwendete Authentisierungsverfahren an.

Voraussetzung des Anscheinsbeweises ist insoweit das Bestehen eines Erfahrungssatzes, wonach eine Erklärung, die unter Einsatz eines Authentisierungsmediums z.B. eines Passworts, versandt wurde, nach der Lebenserfahrung stets vom Inhaber des Authentisierungsmediums (und nicht etwa einem Dritten) stammt. Dies hängt wesentlich von der Sicherheit des eingesetzten Authentisierungsverfahrens gegenüber Fälschungen ab. Folglich ist für das Bestehen des Anscheinsbeweises nach der Sicherheit der Authentisierungsverfahren zu unterscheiden.

IV. Anscheinsbeweis der Urheberschaft bei Internetportalen für Heilberufe

Der Anscheinsbeweis für die Urheberschaft des Teilnehmers richtet sich, wie soeben dargestellt, entscheidend nach dem jeweiligen Authentisierungsverfahren. Daher wird nachfolgend für die drei hier interessierenden Authentisierungsverfahren erörtert, ob ein Anschein für die

494; *Rosenberg/Schwab/Gottwald* (Fn. 75), § 112 Rz. 36; *Schneider* (Fn. 86), Rz. 342, *MünchKommZPO-Prütting* (Fn. 76), § 286 Rz. 65; *Weber* (Fn. 86), S. 50.

⁸⁸ *Borges* (Fn. 16), S. 494; *Rosenberg/Schwab/Gottwald* (Fn. 75), § 112 Rz. 36.

Urheberschaft besteht und unter welchen Voraussetzungen ein ggf. bestehender Anschein erschüttert werden kann.

1. Anscheinsbeweis bei einfachem Passwortschutz

Der volle Beweis der Urheberschaft wird bei Internetportalen, die zur Authentisierung auf einen reinen Passwortschutz vertrauen, nicht ohne weiteres gelingen, da etwa Phishing-Angriffe jedenfalls nicht völlig ausgeschlossen sein werden.

a) Bestehen eines Anscheins

Ob ein Anscheinsbeweis anzunehmen ist, ist mangels praktischer Erfahrung schwierig zu beurteilen. Es können aber Erfahrungen aus anderen Bereichen, in denen Passwörter zur Authentisierung eingesetzt werden, herangezogen werden. So hat etwa das VG Hannover kürzlich bei einem durch Passwort geschützten Userprofil eines Chatroom aufgrund der Authentisierung durch Passwort eine „tatsächliche Vermutung“ für die Urheberschaft des Passwortinhabers angenommen.⁸⁹

Das Bestehen eines Anscheins für Handlungen, die an Websites vorgenommen werden, ist in der zivilprozessrechtlichen Literatur und Rechtsprechung intensiv diskutiert worden. Die herrschende Meinung lehnt einen Anscheinsbeweis ab.⁹⁰ In der Literatur wird diese Rechtsprechung teilweise kritisiert und angenommen, dass der Passwortschutz eine hinreichende Grundlage für die Annahme biete, dass die Erklärung vom

⁸⁹ VG Hannover, 7.6.2006, 6 B 3325/06, MMR 2006, 707 (allerdings ohne die hier interessierende Passage); der Beschluss ist im Volltext abrufbar unter www.a-i3.org, Ordner „Recht“, Unterordner „Urteile“.

⁹⁰ OLG Köln, CR 2003, 55; LG Köln, Urt. v. 6.9.2005 – 8 O 15/05; LG Bonn, CR 2002, 293, 294; LG Bonn, CR 2004, 218, 219; LG Konstanz, MMR 2002, 835 f.; AG Bonn, NJW-RR 2002, 1363, AG Erfurt, MMR 2002, 127, 128; Heiderhoff, in Heiderhoff/Zmij (Hrsg.), Law of E-Commerce in Poland and Germany, 2005, S. 97, 105 f.; Noack/Kremer, AnwBl 2004, 602, 604; Wiebe, in Spindler/Wiebe (Hrsg.), Internet-Auktionen und Elektronische Marktplätze, 2. Aufl. 2005, Kap. 4 Rz. 61. A.A. AG Hannover, WuM 2000, 412.

Inhaber des Passworts stamme.⁹¹ Die meisten der den Anscheinsbeweis befürwortenden Stellungnahmen haben die besondere Problematik des Phishing und die Auswirkungen auf den Anscheinsbeweis allerdings noch nicht berücksichtigt. Teilweise wird der Anscheinsbeweis aber ausdrücklich im Hinblick auf die Probleme des Phishing⁹² oder des Identitätsdiebstahls⁹³ abgelehnt.

Dafür spricht möglicherweise der Umstand, dass internetbasierte Angriffe auf Websites und Internetportale bisher meist auf Websites gerichtet waren, über die die Täter Geld oder Leistungen (z.B. Warenlieferung oder Dienstleistungen etc.) erhalten konnten. Dagegen werden Dritte bei Internetportalen für Heilberufe meist nur ein geringes Interesse haben, in das Account des Teilnehmers einzusehen. Es ist freilich nicht auszuschließen, dass Dritte Interesse an den Daten des Teilnehmers oder seiner Patienten haben. Im Übrigen können, je nach Ausgestaltung des Portals, auch Überweisungen ausgelöst werden.

Folgt man hier der Rechtsprechung zum elektronischen Geschäftsverkehr im allgemeinen, so spricht bei der Verwendung einfacher Passwörter zur Authentisierung bei Internetportalen für Heilberufe kein Anschein dafür, dass der Teilnehmer sich angemeldet und eine bestimmte Handlung vorgenommen hat. Der Nachweis der Urheberschaft wird dann regelmäßig nicht gelingen.

b) Erschütterung des Anscheins

Wenn man mit der Gegenansicht einen Anscheinsbeweis im Grundsatz bejaht, stellt sich die Frage, ob der Anscheinsbeweis im Einzelfall erschüttert werden kann. Dies setzt voraus, wie oben (III.1., S. 46 ff.)

⁹¹ *Ernst*, MDR 2003, 1091, 1093; *Mankowski*, CR 2003, 44 ff.; *Winter*, CR 2002, 768, 769; weitergehend (Anscheinsbeweis dafür, dass die in der E-Mail-Adresse (Absenderangabe) genannte Person Urheber der Mail ist) *Mankowski*, NJW 2002, 2822 ff., 2824; *Sosnitzer/Gey*, K&R 2004, 465, 468.

⁹² So *Noack/Kremer*, AnwBl 2004, 602, 604; *Wiebe*, in Spindler/Wiebe (Fn. 90), Kap. 4 Rz. 61.

⁹³ *Heiderhoff* (Fn. 90), S. 103 ff., 106.

dargestellt, dass die ernsthafte Möglichkeit eines anderen Geschehensablaufs dargetan und ggf. bewiesen wird.

Hier sind nun ganz verschiedene andere Abläufe denkbar. Wie oben angedeutet, kommt etwa in Betracht, dass der Teilnehmer das Passwort einem Mitarbeiter seiner Praxis mitgeteilt hat und dieser gehandelt hat. Wenn also etwa dargelegt wird, dass das Passwort weitergegeben wurde, wäre dies eine ernsthafte Möglichkeit, sofern zum maßgeblichen Zeitpunkt der betreffenden Sitzung der Mitarbeiter Zugang zum Internet hatte. Der Anschein für eine Handlung des Teilnehmers persönlich wäre erschüttert. Allerdings wird in diesem Fall die Handlung des Mitarbeiters dem Teilnehmer häufig zuzurechnen sein, sei es aufgrund einer Vollmacht oder nach Grundsätzen der Rechtsscheinshaftung.

Eine andere Möglichkeit ist freilich auch, dass sich ein Mitarbeiter, der beispielsweise eine Notiz des Passworts gefunden hat, unbefugt Zugang zum Account verschafft. In solchen Fällen hat die Rechtsprechung, soweit ersichtlich, bisher keine Rechtsscheinsvollmacht angenommen. Allenfalls kommt ein Schadensersatzanspruch wegen Verletzung einer Geheimhaltungspflicht in Betracht, sofern die Geheimhaltungspflicht besteht und der Teilnehmer diese fahrlässig verletzt hat. Ein solcher Schadensersatzanspruch hat im Onlinebanking oder bei der Verwendung von ec-Karte und PIN erhebliche praktische Bedeutung.

Schließlich könnte ein Dritter durch Phishing oder ähnliche Angriffe Kenntnis des Passworts erlangt haben. Diese Möglichkeit ist angesichts der erheblichen praktischen Bedeutung, die diese Angriffe inzwischen erreicht haben, keinesfalls auszuschließen. Fraglich ist allein, ob ein solcher Angriff als ernsthaft möglich anzusehen ist, da bisher über derartige Angriffe gegen Internetportale für Heilberufe nichts bekannt geworden ist.

Die abstrakte Möglichkeit eines Phishing-Angriffs reicht sicher nicht aus. Wenn aber Anzeichen vorgetragen und zur Überzeugung des Gerichts festgestellt werden, aufgrund derer ein Phishing-Angriff oder ein Angriff durch Trojaner im konkreten Fall möglich erscheint, wird diese Möglichkeit als ernsthaft anzusehen sein, so dass der Anschein erschüttert ist. Für das Vorliegen einer solchen Möglichkeit trägt der Beweisgegner, meist der Teilnehmer, die Beweislast.

c) Ergebnis

Im Ergebnis wird der Nachweis der Urheberschaft bei Internetportalen, die auf ein schlichtes Passwort als Authentisierungssystem setzen, häufig nicht gelingen. Die volle Überzeugung des Gerichts wird nicht ohne weiteres erzielt werden können, so dass es auf den Anscheinsbeweis ankommt. Insoweit ist aufgrund der bisherigen Rechtsprechung zum Anscheinsbeweis bei schlichtem Passwortschutz schon zweifelhaft, ob die Gerichte einen Erfahrungssatz der Urheberschaft des Passwortinhabers annehmen würden. Selbst wenn ein Gericht einen Anscheinsbeweis annimmt, gibt es mehrere andere Geschehensabläufe, die als ernsthaft möglich in Betracht zu ziehen wären und damit den Anschein erschüttern würden. In diesem Fall ist der Beweis der Urheberschaft des Teilnehmers nicht erbracht.

2. Anscheinsbeweis bei Softzertifikat

Ob der Nachweis der Urheberschaft bei Authentisierung durch Passwort und Softzertifikat im Wege des Anscheinsbeweises geführt werden kann, ist derzeit schwierig zu beurteilen, da es an praktischer Erfahrung mangelt.

Man wird einen solchen Anschein der Urheberschaft aber wohl annehmen können. Die Rechtsprechung zum Anscheinsbeweis bei schlichten Passwörtern verweist zur Begründung meist darauf, dass einfache Passwörter einen sehr geringen Schutz bieten und leicht geknackt werden könnten.⁹⁴ Dies wird man bei Softzertifikaten nicht in gleicher Weise annehmen können.

Allerdings kann der Anschein, wenn er besteht, durchaus erschüttert werden. So kann die Möglichkeit, dass ein Mitarbeiter des Teilnehmers das Passwort verwendet hat, insbesondere dann ernsthaft in Betracht kommen, wenn der Mitarbeiter zum Zeitpunkt der betreffenden Sitzung Zugang zu dem Computer des Teilnehmers hat, auf dem das Softzertifikat gespeichert

⁹⁴ OLG Köln, CR 2003, 55; erstinstanzlich LG Bonn, CR 2002, 293, 294; LG Bonn, CR 2004, 218, 219. OLG Naumburg, NJOZ 2005, 2222, 2224 (keine andere Beweislastverteilung).

war. Denkbar ist auch, dass ein Mitarbeiter das Softzertifikat dupliziert und von einem anderen Rechner aus verwendet hat.

Auch Phishing-Angriffe können ernsthaft möglich sein. Softzertifikate können durch Trojaner kopiert und an den Angreifer gesendet werden. Wenn also die Möglichkeit eines Angriffs durch Trojaner plausibel dargestellt wird, dürfte der Anschein erschüttert sein. Im Fall einer derartigen Erschütterung des Anscheins ist der Beweis der Urheberschaft nicht erbracht.

3. Anscheinsbeweis bei Chipkarte

Zum Anscheinsbeweis der Urheberschaft von Handlungen auf Internetportalen, die zur Authentisierung eine Chipkarte mit PKI sowie eine PIN verwenden, liegen, soweit ersichtlich, keine veröffentlichten Entscheidungen vor.

Es kann aber das Beispiel der qualifizierten elektronischen Signatur herangezogen werden, da diese bei den heute verfügbaren Verfahren unter Verwendung von Chipkarte und PIN erzeugt wird. Zudem kann auf andere Fälle der Authentisierung mittels Besitz und Wissen zurückgegriffen werden, da die Authentisierung durch Chipkarte und PIN ein Anwendungsfall dieses Authentisierungsverfahrens darstellt.

Der Anscheinsbeweis der Urheberschaft von elektronisch übermittelten Erklärungen und Handlungen bei Verfahren, die das Konzept der Authentisierung durch Besitz und Wissen verwenden, ist seit Jahren Gegenstand vor allem der zivilrechtlichen Diskussion. Die Diskussion bezieht sich insbesondere auf ec-Karten-Systeme, die bei Verfügungen am Geldautomaten eine Authentisierung durch ec-Karte und PIN voraussetzen. Daher wird nachfolgend zunächst der Diskussionsstand zum Anscheinsbeweis bei Verwendung von ec-Karte und PIN skizziert, sodann der Anscheinsbeweis bei durch Chipkarte und PIN gesicherten Internetportalen erörtert.

a) Anscheinsbeweis bei Verwendung von ec-Karte und PIN

Der Anscheinsbeweis aufgrund Verwendung von ec-Karte und PIN hat sein Einsatzgebiet vor allem bei Verfügungen an Geldautomaten. Hier wird der Anscheinsbeweis relevant, wenn die Verantwortlichkeit des Bankkunden für einen Geldbetrag streitig ist, der von einem Geldausgabeautomaten abgehoben wurde.

Materiellrechtlicher Hintergrund des Beweises ist die Frage, ob die Bank das Konto des Kunden mit dem abgehobenen Betrag belasten kann, mithin, ob ihr ein Zahlungsanspruch gegen den Kunden in dieser Höhe zusteht. Dieser Anspruch besteht als Aufwendungsersatzanspruch, wenn der Kunde das Geld selbst abgehoben hat oder wenn eine andere Person als bevollmächtigter Vertreter des Kunden – und sei es aufgrund einer Rechtsscheinsvollmacht – das Geld abgehoben hat. Ein Anspruch der Bank besteht auch, wenn ein unbefugter Dritter das Geld abgehoben hat und der Kunde dies durch grob fahrlässigen Umgang mit der PIN verursacht hat, denn in diesem Fall hat der Kunde seine Geheimhaltungspflicht verletzt und haftet der Bank auf Schadensersatz.⁹⁵ Daher kann für das Ergebnis des Rechtsstreits regelmäßig dahinstehen, welcher der drei Sachverhalte tatsächlich vorlag.

Vor diesem materiellrechtlichen Hintergrund wird bei Verwendung von ec-Karte und PIN und ordnungsgemäßem Funktionieren des Geldautomaten im Ergebnis einhellig ein Anscheinsbeweis dahin angenommen, dass entweder der Kunde die Verfügung vorgenommen oder Karte und PIN weitergegeben hat oder dem Täter die Kenntnis der PIN durch grob fahrlässige Verletzung der Geheimhaltungspflicht ermöglicht hat.⁹⁶

⁹⁵ Siehe dazu *Bieber*, WM-Sonderbeilage Nr. 6/1987, S. 1, 12 ff.; *Borges* (Fn. 16), S. 497 ff. m.w.Nachw.; a.A. (kein Anscheinsbeweis) etwa LG Osnabrück, WM 2003, 1951.

⁹⁶ BGHZ 160, 308, 315 f. m zahl. Nachw.; OLG Frankfurt a.M., WM 2002, 2101, 2102 f.; OLG Stuttgart, NJW-RR 2002, 1274, 1275 f.; Heymann-Balzer, HGB, Bd. 4, 2. Aufl. 2005, Anh. § 372 Rz. V/162; a.A. OLG Hamm, NJW 1997, 1711 ff.; OLG Frankfurt a.M., NJW-RR 2002, 682, 693; ausdrückl. offengelassen bei OLG Oldenburg, WM 2000, 2337, 2339 sowie BGH, NJW 2001, 286; weitere Nachw. bei *Borges* (Fn. 16), S. 499 (Fn. 180).

Der BGH hat in seinem Urteil vom 5.10.2004, das den aktuellen Stand der höchstrichterlichen Rechtsprechung zum Anscheinsbeweis bei Verwendung von ec-Karte und PIN darstellt, diesen Anscheinsbeweis mit den genannten drei Varianten ausdrücklich bestätigt.⁹⁷

Allerdings wird der durch die Verwendung von ec-Karte und PIN hervorgerufene Anschein teilweise auch anders beschrieben. So wird nicht selten explizit ein Anschein dahin angenommen, dass der Kunde den Geldautomaten persönlich bedient hat.⁹⁸

Andere Stellungnahmen hingegen verweisen sogleich auf den dargestellten, dreifach gestaffelten Anschein, ohne auf die Möglichkeit eines Anscheins für das Handeln des Kunden selbst hinzuweisen.⁹⁹

Darin liegt aber nicht notwendig eine unterschiedliche Auffassung zum Anscheinsbeweis bei Verwendung von ec-Karte und PIN. Der zu führende Anscheinsbeweis richtet sich grundsätzlich nach der Beweisfrage. Diese hängt entscheidend davon ab, welche Tatsachen im Verfahren umstritten sind. Diese Interdependenz von Anscheinsbeweis und Tatsachenvortrag der Parteien wird auch am Beispiel des BGH-Urteils vom 5.10.2004 sehr deutlich. Hier war zwischen den Parteien unstrittig, dass der Kunde das Geld nicht selbst abgehoben hatte. Folglich kam es für den Beweis allein darauf an, ob der Kunde seine Geheimhaltungspflicht verletzt hatte, und entsprechend fokussiert der BGH, obwohl er zuvor den Anscheinsbeweis mit den drei Varianten ausdrücklich anerkennt, den Anschein im konkreten Fall auf die Sachverhaltsvariante einer Verwendung durch einen Dieb und die Pflichtverletzung des Kunden.¹⁰⁰

⁹⁷ BGHZ 160, 308 = NJW 2004, 3623.

⁹⁸ OLG Stuttgart, WM 2003, 125, 126; LG Bonn, WM 1995, 575, 576; AG Hannover, WM 1997, 64, 65; AG Schöneberg, WM 1997, 66, 68; AG Wuppertal, WM 1997, 1209; *Bieber*, WM-Sonderbeilage Nr. 6/1987, S. 1, 12; *Fervers*, WM 1988, 1037, 1043 wohl auch: *Werner*, in: Hellner/Steuer (Hrsg.), Bankrecht und Bankpraxis (Losebl.), Rz. 6/1510); ähnl. AG Frankfurt a.M., BKR 2006, 297, 298 (Anschein für eigene Abhebung oder durch von ihm autorisierten Dritten).

⁹⁹ Vgl. z.B. LG Berlin, WM 2003, 128, 129.

¹⁰⁰ BGHZ 160, 308, 312 ff.; ebenso in dieser Konstellation etwa OLG Frankfurt a.M., NJW-RR 2007, 198 f.; LG Duisburg 8.5.2003 – 5 S 63/02; LG Duisburg, 13.1.2006 – 7 S 176/05.

Diese Abhängigkeit des Anscheinsbeweises vom Streitstand ist auch keine Besonderheit des Anscheinsbeweises bei Verwendung mit ec-Karte und PIN. Auch beim Auffahrunfall wird regelmäßig offengelassen, ob der auffahrende Kraftfahrer zu geringen Abstand hielt oder unachtsam war, da dies für das Ergebnis – Verantwortlichkeit des Hintermanns für den Unfall – nicht erheblich ist.

Nach der Lebenserfahrung liegt bei Bedienung des Geldautomaten durch ec-Karte und PIN in aller Regel eine Verfügung durch den Kunden selbst oder durch eine von ihm autorisierte Person vor. Es besteht also ein beweisrelevanter Anschein dahin, dass der Kunde selbst oder ein von ihm bevollmächtigter Dritter gehandelt hat. Dieser Anschein ist freilich besonders leicht zu erschüttern, etwa durch den Nachweis, dass sich der Kunde zum Zeitpunkt der Verfügung an einem anderen Ort befunden hat. Der gestaffelte Anscheinsbeweis mit den o.g. drei Varianten vereinfacht also lediglich die Beweisaufnahme, ohne einen Anschein für die Urheberschaft des Kunden in Abrede zu stellen.

Gerade zum Anscheinsbeweis bei Verwendung von ec-Karte und PIN ist auch die Möglichkeit einer Erschütterung des Anscheins Gegenstand intensiver Diskussion. In der Praxis wurde meist geltend gemacht, ein Dieb habe die ec-Karte entwendet und die PIN entweder durch Ausnutzung von Sicherheitslücken des Systems oder durch Ausspähen in Erfahrung gebracht¹⁰¹.

Der BGH hat in seinem Urteil vom 5.10.2004 die in der Praxis besonders häufig vorgetragene Variante eines Ausspähens der PIN bei früheren Verfügungen erheblich eingeschränkt und ein Errechnen der PIN für nur theoretisch möglich gehalten. Damit gelten für die Möglichkeit, den Anschein zu erschüttern, aufgrund des BGH-Urteils ausgesprochen hohe Anforderungen, die in der Praxis kaum erreicht werden. In den seither veröffentlichten Urteilen ist eine Erschütterung des Anscheins jeweils abgelehnt worden.¹⁰²

¹⁰¹ Vgl. z.B. LG Osnabrück, WM 2003, 1951, 1954, das wegen dieser Möglichkeit gar den Anscheinsbeweis insgesamt ablehnt.

¹⁰² Siehe etwa OLG Frankfurt a.M., NJW-RR 2007, 198; LG Duisburg, Urteil v. 13.1.2006 – 7 S 176/05; LG Kaiserslautern, Urteil v. 26.11.2004 – 2 O 394/04; AG

b) Der Anscheinsbeweis bei qualifizierter elektronischer Signatur nach § 371a ZPO

Der Gesetzgeber hat mit § 371a ZPO im Jahr 2001, damals als § 292a ZPO, erstmals eine gesetzliche Regelung des Anscheinsbeweises in das deutsche Recht eingeführt.

Nach § 371a ZPO, der freilich sehr unklar formuliert ist,¹⁰³ begründet die qualifizierte elektronische Signatur einen Anschein dahin, dass die signierte Datei vom Inhaber der Signaturkarte signiert wurde. Dieser Anschein kann nur durch den Nachweis der ernsthaften Möglichkeit, dass ein Dritter ohne Willen des Signaturschlüsselinhabers die Signatur erstellt hat, erschüttert werden. Auch wenn § 371a ZPO bisher offenbar ohne praktische Bedeutung geblieben ist und die genaue rechtliche Bedeutung des § 371a ZPO in der Literatur umstritten ist,¹⁰⁴ wird doch deutlich, dass nach Auffassung des Gesetzgebers die Verwendung der Signaturkarte einen Anschein der Echtheit der signierten Datei und damit dafür begründet, dass der Inhaber der Chipkarte, die den geheimen Schlüssel enthält, Urheber der Datei ist.

c) Anscheinsbeweis bei Internetportalen mit Chipkartenschutz

Der Anscheinsbeweis setzt einen auf praktischer Lebenserfahrung beruhenden Erfahrungssatz voraus. Eine solche Erfahrung liegt in Bezug auf die Authentisierung bei Internetportalen mit Chipkarte und PIN bisher nur in geringem Maße vor. Jedoch können aber wohl die Erfahrungen und Wertungen bei der ec-Karte und des Anscheinsbeweises aufgrund der elektronischen Signatur herangezogen werden.

Der deutsche Gesetzgeber geht davon aus, dass bei Dateien, die mit einer qualifizierten elektronischen Signatur versehen sind, ein Anschein dafür spricht, dass die Datei mit Willen des Karteninhabers signiert wurde (dazu

Düsseldorf, Urteil vom 26.1.2005 – 37 C 18086/00; AG Frankfurt a.M., BKR 2006, 297, 298 f.

¹⁰³ *Borges* (Fn. 16), S. 505 ff.

¹⁰⁴ Siehe dazu etwa *Armgaradt/Spalka*, K&R 2007, 26 ff.; *Borges*, S. 505 ff.; *MünchKommZPO-Prütting*, 2. Aufl., Aktualisierungsband ZPO-Reform 2002 und weitere Reformgesetze, 2002, § 292a Rz. 7 ff.

oben b). Für die Zuordnung der Signatur zu einer natürlichen Person streiten einerseits die Authentisierung durch den Besitz an der Signaturkarte und die Kenntnis der PIN, die beim Signaturvorgang zusätzlich erforderlich ist, und andererseits die Sicherheit des Systems, die die Erstellung einer identischen Signatur ohne Verwendung des geheimen Schlüssels weitestgehend ausschließt. Internetportale, die zur Authentisierung auf PIN und Chipkarte setzen, vertrauen in gleicher Weise auf die Authentisierung durch Besitz an der Chipkarte und Kenntnis der PIN. Auch in Bezug auf die Systemsicherheit werden, jedenfalls bei den im ZOD zugelassenen Karten, technisch dieselben Anforderungen erfüllt wie bei einer Karte, die für qualifizierte elektronische Signaturen zugelassen ist. Auch wenn insoweit ein Unterschied besteht, als die Karte für die Authentisierung und nicht, wie bei der elektronischen Signatur, zum Signieren einer einzelnen Datei genutzt wird, werden hier für die Authentisierung der handelnden Person die gleichen Sicherheitsmechanismen verwendet.

Dies spricht dafür, dass nach der Wertung des § 371a ZPO auch bei Authentisierung durch Chipkarte und PIN ein Anschein für die Urheberschaft des Karteninhabers besteht.

Auch das Beispiel der ec-Karte spricht für einen Anschein der Urheberschaft des Karteninhabers. Das Prinzip der Authentisierung durch Besitz (der ec-Karte) und Wissen (der PIN), auf der der Anscheinsbeweis bei der ec-Karte beruht, verwendet die Authentisierung durch Chipkarte und PIN ebenfalls. Da eine Chipkarte, die den Vorgaben des ZOD entspricht, weitaus sicherer ist als die ec-Karte, muss aus technischer Sicht der auf der Verwendung der ec-Karte beruhende Anschein erst recht bei Verwendung der Chipkarte gelten.

Im Übrigen kommt es für das Bestehen des Anscheins nicht nur auf die Sicherheit des Authentisierungssystems, sondern genauso auf die Gefahr von Fälschungen an. Insoweit ist anzunehmen, dass das Gefahrenpotential bei Chipkarten zur Authentisierung bei Internetportalen für Heilberufe erheblich geringer ist als bei der ec-Karte, die etwa dem Dieb ermöglicht, Bargeld zu erlangen, wogegen der Dritte über das Internetportal regelmäßig weder Bargeld noch Buchgeld erhalten kann. Aus heutiger Sicht besteht also kein vergleichbares Interesse Dritter am Missbrauch von Chipkarten für Internetportale. Wenn Internetportale für Heilberufe Überweisungen auf frei definierbare Konten zulassen sollten, könnte ein Interesse am Missbrauch

bestehen. Allerdings zeigen die aktuellen Angriffe gegen das Onlinebanking, dass die Täter eher über das Internet vorgehen und nicht versuchen, in den Besitz der Chipkarte zu kommen. Ist demnach das Missbrauchsrisiko bei Internetportalen für Heilberufe jedenfalls nicht höher als bei der ec-Karte, muss der Anschein der Urheberschaft aufgrund der Authentisierung durch Chipkarte und PIN am Internetportal erst recht bestehen.

Im Ergebnis kann daher aus heutiger Sicht kein Zweifel daran bestehen, dass aufgrund der Authentisierung am Portal mit Chipkarte und PIN ein Anschein dafür besteht, dass entweder der Karteninhaber oder eine Person, der der Inhaber Chipkarte und PIN weitergegeben hat, gehandelt hat.

d) Erschütterung

Der durch Verwendung von Chipkarte und PIN hervorgerufene Anschein kann gemäß den allgemeinen Regeln zum Anscheinsbeweis erschüttert werden, wenn im konkreten Fall die ernsthafte Möglichkeit eines atypischen Geschehensablaufs besteht. Bei der Verwendung von Chipkarte und PIN zur Authentisierung an Internetportalen für Heilberufe sind ganz unterschiedliche Geschehensabläufe vorstellbar.

aa) Unbefugte Verwendung der Chipkarte durch Dritte

Als atypischer Geschehensablauf kommt eine Verwendung der Authentisierungsmedien durch Dritte in Betracht. Diese Möglichkeit können insbesondere Personen aus dem Bereich des Teilnehmers haben, etwa Mitarbeiter der Praxis. Soweit der Teilnehmer Chipkarte und PIN dem Mitarbeiter überlassen hat oder mit der Verwendung einverstanden ist, ist das Verhalten dieses Mitarbeiters dem Teilnehmer zuzurechnen; eine Erschütterung des Anscheins erfolgt hier also nicht.

Als ein atypischer Geschehensablauf, der zur Erschütterung des Anscheins führen kann, kommt etwa der unbefugte Zugriff von Dritten auf die Chipkarte und eine Notiz der PIN in Betracht. Allerdings sind derartige Eingriffe wenig plausibel. Anders als im Fall der ec-Karte hätte der Dieb

typischerweise keinen Nutzen durch den Diebstahl der Chipkarte, da er kein Bargeld erlangen kann. Personen, die ein Interesse haben könnten, werden sich regelmäßig nicht als Taschendiebe betätigen. Am wahrscheinlichsten wäre wohl noch der Zugriff durch einen Mitarbeiter. In allen derartigen Fällen reicht aber die abstrakte Möglichkeit eines solchen Eingriffs nicht aus. Vielmehr muss die ernsthafte Möglichkeit eines solchen Angriffs vorgetragen und im Bestreitensfalle bewiesen werden.

bb) Erschütterung durch Phishing-Angriffe

Denkbar sind auch Phishing-Angriffe. Allerdings ist die Authentisierung durch Chipkarte und PIN aus heutiger Sicht weitgehend sicher gegen Phishing. Wie eine aktuelle Studie des renommierten Kryptologen *Prof. Dr. Buchmann* ausdrücklich feststellt, sind Angriffe des klassischen Phishing nicht geeignet, die chipkartenbasierte Authentisierung zu überwinden.¹⁰⁵

Denkbar sind allenfalls hochkomplexe Trojaner-Angriffe, die bei jedem Authentisierungsverfahren im Grundsatz möglich sind.¹⁰⁶ Auch soweit diese Art von Angriffen in Betracht kommt, ist allerdings zu bedenken, dass solche Angriffe, etwa in Bezug auf die elektronische Übertragung von Abrechnungsdaten an die Kassenärztliche bzw. Kassenzahnärztliche Vereinigung auch bisher schon möglich wären, ohne dass jemals ein derartiger Angriff bekannt geworden wäre. Im Übrigen ist unter dem Gesichtspunkt des Missbrauchsrisikos zu berücksichtigen, dass derartig komplexe Trojaner-Angriffe zum Missbrauch von Accounts an Internetportalen in der Praxis bisher nicht beobachtet wurden. Zudem richten sich die derzeit zu beobachtenden Angriffe mit Trojanern regelmäßig gegen Ziele, die dem Täter Lieferung von Daten oder Dienstleistungen oder den Zugriff auf Buchgeld ermöglichen. Dies ist aber bei Internetportalen für Heilberufe jedenfalls dann nicht möglich, wenn

¹⁰⁵ Johannes Buchmann, Passwörter oder Smartcards zur Absicherung von Portalen?, Technical Report No. TI-2/06, Oktober 2006, abrufbar unter www.cdc.informatik.tu-darmstadt.de/, Ordner „Veröffentlichungen“.

¹⁰⁶ Siehe etwa zur Verfälschung von Dateien, die mit einer qualifizierten elektronischen Signatur versehen sind, durch Trojaner *Armgardt/Spalka*, K&R 2007, 26, 28 m.w.Nachw.

diese nicht mit dem Zugriff auf ein Bankkonto verbunden sind. Daher erscheinen Trojaner-Angriffe gegen Internetportale für Heilberufe derzeit als eine äußerst unwahrscheinliche Möglichkeit.

Dies bedeutet, dass eine Erschütterung des Anscheins aufgrund von Phishing und ähnlicher Angriffe aus heutiger Sicht kaum vorstellbar und auch für die nähere Zukunft nicht zu erwarten ist.

V. Ergebnis

Als Gesamtergebnis zeigt sich, dass sich beim Beweis der Urheberschaft von Handlungen, die an Internetportalen für Heilberufe vorgenommen werden, entscheidende Vorteile für sichere Authentisierungsverfahren ergeben, da diese für den Anscheinsbeweis der Urheberschaft zentrale Bedeutung haben.

Im Fall der Authentisierung durch einfaches Passwort ist schon zweifelhaft, ob überhaupt ein Anschein für die Urheberschaft des Passwortinhabers besteht, die zivilrechtliche Rechtsprechung verneint dies regelmäßig. Jedenfalls wäre dieser Anschein wohl relativ leicht zu erschüttern, da Dritte durch Phishing oder ähnliche Angriffe in den Besitz des Passworts gelangen können.

Bei zusätzlicher Verwendung von Softzertifikaten zur Authentisierung wird man einen Anschein der Urheberschaft wohl annehmen können. Auch hier kommt aber eine Erschütterung des Anscheins durch die Möglichkeit eines Trojaner-Angriffs in Betracht.

Erst recht ist bei Authentisierung durch Chipkarte und PIN der Anschein dahin zu bejahen, dass entweder der Karteninhaber selbst oder eine von ihm bevollmächtigte Person gehandelt hat. Anders als beim Softzertifikat erscheint eine Erschütterung dieses Anscheins durch die Möglichkeit von Phishing oder ähnlichen Angriffen aus heutiger Sicht weitgehend ausgeschlossen, da allenfalls hochkomplexe, aufwendige Angriffe in Betracht kommen, die aus heutiger Sicht nicht plausibel erscheinen.

Dies rechtfertigt die Erwartung, dass der Nachweis der Verantwortlichkeit der Teilnehmer für eine an ihrem Account vorgenommene Handlung bei Authentisierung durch Chipkarte und PIN regelmäßig gelingen, bei weniger sicheren Verfahren hingegen häufig scheitern wird.

E. Anforderungen an die Datensicherheit bei Internetportalen

Für die Gestaltung von Internetportalen für Heilberufe ist von Interesse, welche Anforderungen sich aus dem Datenschutzrecht für die Authentisierungssysteme ergeben. Bedeutung hat diese Frage vor allem wegen der Patientendaten, die in den Abrechnungsdaten enthalten oder im Internetportal abrufbar sind.

Diese Frage wird nachfolgend erörtert. Zunächst werden die Anforderungen an die Datensicherheit beschrieben und sodann die Anforderungen bei Internetportalen für Heilberufe, insbesondere die hier interessierenden Verfahren der Authentisierung unter datenschutzrechtlichen Gesichtspunkten untersucht.

I. Die gesetzlichen Anforderungen an die Datensicherheit

1. Datensicherheit im SGB X und den allgemeinen Datenschutzgesetzen

Die allgemeinen Anforderungen an den Datenschutz sind im Bundesdatenschutzgesetz (BDSG) bzw. den Landesdatenschutzgesetzen¹⁰⁷ geregelt. Für das Sozialrecht enthalten die §§ 67 ff. SGB X die maßgeblichen datenschutzrechtlichen Bestimmungen. Die Regeln sind überwiegend an das BDSG angelehnt; gelegentlich wird auf das BDSG verwiesen.

Die Datenschutzgesetze regeln den Umgang mit personenbezogenen Daten, die in § 3 Abs. 1 BDSG als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person definiert sind. Entsprechend lautet die Definition der Sozialdaten in § 67 Abs. 1 S. 1 SGB X, die Gegenstand der §§ 67 ff. SGB X sind. Diese Definition ist in einem weiten Sinne zu verstehen und soll alle

¹⁰⁷ Abgedr. bei *Schaffland/Wiltfang*, Bundesdatenschutzgesetz (Losebl, Stand 2006); siehe zu den Gemeinsamkeiten und Unterschieden der Regeln *Heibey*, in Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 4.5 Rz. 75 ff.

Informationen umfassen, die über die Bezugsperson und ihre Verhältnisse etwas aussagen.¹⁰⁸

Bei Internetportalen für Heilberufe kommt dem Datenschutz höchste Bedeutung zu, da im Rahmen der Online-Abrechnung Patientendaten verarbeitet werden, die über das Portal einsehbar sind und übertragen werden. Die Abrechnungsdaten enthalten auch Diagnosen und sonstige gesundheitsbezogene Daten von Patienten, mithin hochsensitive Daten, die in besonderer Weise des Datenschutzes bedürfen.

Zum Datenschutz gehört auch die Datensicherheit.¹⁰⁹ Datensicherung, als Gesamtheit der Maßnahmen zur Herstellung von Datensicherheit, bedeutet den Schutz von Daten vor Beeinträchtigung oder Missbrauch. Ziel der Datensicherung ist es einerseits, die Integrität und Verfügbarkeit von Daten zu sichern, andererseits auch, einen unzulässigen Umgang mit Daten zu verhindern.¹¹⁰

Die zentrale Norm der Datensicherheit ist § 9 BDSG, der die Anforderungen an die Datensicherung regelt. § 9 BDSG hat in den Landesdatenschutzgesetzen ein – meist wortgetreues – Pendant. Für das Sozialrecht enthält § 78a SGB X eine dem § 9 BDSG weitestgehend entsprechende Regelung. Auch das Teledienstedatenschutzgesetz (TDDSG) und der Mediendienstestaatsvertrag (MDStV) enthalten Bestimmungen zur Datensicherung. So hat der Anbieter von Telediensten nach § 4 Abs. 3 Nr. 3 TDDSG durch technische und organisatorische Maßnahmen sicherzustellen, dass der Nutzer bei Inanspruchnahme eines Teledienstes gegen Kenntnisnahme durch Dritte geschützt ist.

Für die Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigungen sind die Vorschriften des SGB X maßgeblich. Da diese dem BDSG nachgebildet sind, können dessen Regeln zur Auslegung herangezogen werden. Daher bezieht sich die nachfolgende Erörterung auf BDSG und SGB X.

¹⁰⁸ Simitis-Dammann, Bundesdatenschutzgesetz, 6. Aufl. 2006, § 3 Rz. 7. Ähnlich Gola/Schomerus, Bundesdatenschutzgesetz, 8. Aufl. 2005, § 3 Rz. 3.

¹⁰⁹ Simitis-Ernestus (Fn. 108), § 9 Rz. 2.

¹¹⁰ Simitis-Ernestus (Fn. 108), § 9 Rz. 2; vgl. auch die Def. der Datensicherheit in DIN 44300.

2. Die Anforderungen an die Datensicherheit

§ 78a SGB X und ebenso § 9 BDSG sowie die Parallelnormen in den Landesdatenschutzgesetzen beschreiben die Anforderungen an die Datensicherung durch eine Generalklausel. Danach sind die Maßnahmen der Datensicherung rechtlich geboten, die erforderlich sind, um die gesetzlichen Anforderungen an den Datenschutz zu erfüllen. Zu den dort genannten Anforderungen des Gesetzes gehört vor allem der Grundsatz, dass personenbezogene Daten bzw. Sozialdaten nur erhoben, verarbeitet oder verwendet werden dürfen, wenn der Betroffene eingewilligt hat oder das Gesetz die Nutzung der Daten erlaubt (§ 35 SGB I, § 4 Abs. 1 BDSG).

Die Verpflichtung zur Datensicherung nach § 9 BDSG bzw. § 78a SGB X macht deutlich, dass der Adressat, also die datenverarbeitende Stelle, die gesetzliche Verpflichtung zum Datenschutz nicht nur selbst einzuhalten hat, sondern darüber hinaus auch den unbefugten Zugriff Dritter auf die geschützten Daten abwehren muss. Damit ist der Schutz von personenbezogenen Daten gegenüber dem unbefugten Zugriff Dritter integraler Bestandteil des gesetzlichen Datenschutzes.

Die Generalklausel des § 9 BDSG, § 78a SGB X wird jeweils in einer (weitestgehend übereinstimmenden) Anlage konkretisiert, die Bestandteil des Gesetzes ist. Die Anlage ist nicht abschließend. Vielmehr können sich darüber hinausgehende Anforderungen aus der Generalklausel ergeben.¹¹¹

Der Begriff der technischen und organisatorischen Sicherheit ist weit auszulegen¹¹² und umfasst alle Bereiche der Datenerhebung, -speicherung und -übermittlung. Umfasst sind etwa Maßnahmen, um den Zugang Unbefugter zum Datenverarbeitungssystem, etwa dem Server, auf dem die Daten gespeichert sind, zu unterbinden. Ferner ist der Schutz vor unbefugtem elektronischen Zugriff auf geschützte Daten umfasst, etwa durch Passwortschutz und sonstige Authentisierungssysteme. Schließlich

¹¹¹ Simitis-Ernestus (Fn. 108), § 9 Rz. 56; Hauck/Noftz-Rombach (Fn. 13), § 78a Rz. 23.

¹¹² Simitis-Ernestus (Fn. 108), § 9 Rz. 20; Gola/Schomerus (Fn. 108), § 9 Rz. 5; Hauck/Noftz-Rombach (Fn. 13), § 78a Rz. 14; Schaffland/Wiltfang (Fn. 107), § 9 BDSG Rz. 3.

sind Daten auch während der Übermittlung vor dem Zugriff Dritter zu schützen.

In der Anlage zu § 9 BDSG und zu § 78a SGB X werden diese Anforderungen in verschiedene Gruppen zusammengefasst. Erforderlich sind nach Nr. 1 der Anlagen zu § 9 BDSG und zu § 78a SGB X Maßnahmen, um den Zutritt Unbefugter zu den Datenverarbeitungsanlagen zu verhindern, auf denen die geschützten Daten gespeichert sind, die sogenannte Zutrittskontrolle. Hiermit ist vor allem der Zugang zum Datenverarbeitungssystem als Sache gemeint.¹¹³ Diese Anforderungen betreffen etwa den Server, auf dem die Daten beim Portalbetreiber gespeichert sind.

Erforderlich sind gemäß Nr. 2 der Anlagen weiter Maßnahmen, um den Zugang Unbefugter zu dem Datenverarbeitungssystem zu unterbinden, in dem die Daten gespeichert sind, die sogenannte Zugangskontrolle. Die Zugangskontrolle in diesem Sinne meint nicht den Zugriff auf Geräte (Hardware), der unter dem Gesichtspunkt der Zutrittskontrolle in Nr. 1 erfasst ist,¹¹⁴ sondern im Kern den Zugang zu den geschützten Daten.¹¹⁵ Die Zugangskontrolle schließt daher nicht zuletzt den elektronischen Zugriff auf Daten über Datennetze ein.¹¹⁶

Unter dem Gesichtspunkt der Zugriffskontrolle, Nr. 3 der Anlagen, wird vor allem der Zugriff der zur Benutzung des Datenverarbeitungssystems Berechtigten erfasst.¹¹⁷ Hier ist sicherzustellen, dass der Berechtigte nur auf

¹¹³ Vgl. *Simitis-Ernestus* (Fn. 108), § 9 Rz. 70; *Gola/Schomerus* (Fn. 108), § 9 Rz. 23.

¹¹⁴ *Hauck/Noftz-Rombach* (Fn. 13), § 78a Rz. 26.

¹¹⁵ Vgl. *Simitis-Ernestus* (Fn. 108), § 9 Rz. 91 f., *Gola/Schomerus* (Fn. 108), § 9 Rz. 24; *Hauck/Noftz-Rombach* (Fn. 13), § 78a Rz. 26; *Schaffland/Wiltfang* (Fn. 104), § 9 BDSG Rz. 28.

¹¹⁶ Vgl. *Simitis-Ernestus* (Fn. 108), § 9 Rz. 89; *Heibey*, in *Roßnagel* (Fn. 104), Kap. 4.5 Rz. 43; *Hauck/Noftz-Rombach* (Fn. 13), § 78a Rz. 26.

¹¹⁷ *Gola/Schomerus* (Fn. 108), § 9 Rz. 25, *Hauck/Noftz-Rombach* (Fn. 13), § 78a Rz. 27.

die Daten zugreifen kann, für die er die Nutzungsberechtigung besitzt.¹¹⁸ Zur Zugriffskontrolle gehört aber auch der Zugriff Unbefugter zu gespeicherten Daten.¹¹⁹

Schließlich sind Daten nach Nr. 4 der Anlagen zu § 78a SGB X und zu § 9 BDSG auch während der Übermittlung vor dem Zugriff Unbefugter zu schützen, die sogenannte Weitergabekontrolle.

Als Maßstab für die erforderlichen Maßnahmen nennt § 78a SGB X und ebenso § 9 BDSG den Gesichtspunkt der Erforderlichkeit. Geboten sind danach die Maßnahmen, die erforderlich, also insbesondere geeignet sind, um Missbrauch von Daten zu verhindern (§ 78a S. 1 SGB X, § 9 S. 1 BDSG). Jedoch steht dieser Maßstab ausdrücklich unter dem Vorbehalt der Verhältnismäßigkeit. Gemäß § 9 S. 2 BDSG, § 78a S. 2 SGB X sind erforderlich nur solche Maßnahmen, deren Aufwand in einem angemessenen Verhältnis zum angestrebten Schutz steht.

Von entscheidender Bedeutung für die Anforderungen an die Datensicherung ist das Gefährdungspotential.¹²⁰ Unter diesem Gesichtspunkt ist zum einen die Sensibilität der gespeicherten Daten von Bedeutung,¹²¹ zum anderen das tatsächliche Risiko eines Missbrauchs.¹²²

Damit ist zur Bestimmung des rechtlich gebotenen Maßes an Datensicherheit jeweils eine Abwägung zwischen dem Interesse an einem möglichst effektiven Schutz personenbezogener Daten einerseits, und den damit verbundenen Kosten andererseits notwendig. Das konkrete Ergebnis der Abwägung hängt dabei nicht zuletzt aber von der Schutzbedürftigkeit

¹¹⁸ Vgl. Simitis-Ernestus (Fn. 108), § 9 Rz. 104, Heibey, in Roßnagel (Fn. 104), Kap. 4.5 Rz. 45; Hauck/Noftz-Rombach (Fn. 13), § 78a Rz. 27; Schaffland/Wiltfang (Fn. 104), § 9 BDSG Rz. 29.

¹¹⁹ Simitis-Ernestus (Fn. 108), § 9 Rz. 106.

¹²⁰ Hauck/Noftz-Rombach (Fn. 13), § 78a Rz. 22.

¹²¹ Simitis-Ernestus (Fn. 108), § 9 Rz. 27; Heibey, in Roßnagel (Fn. 104), Kap. 4.5 Rz. 32; Hauck/Noftz-Rombach (Fn. 13), § 78a Rz. 22; Schaffland/Wiltfang (Fn. 104), § 9 BDSG Rz. 35.

¹²² Simitis-Ernestus (Fn. 108), § 9 Rz. 27, Heibey, in Roßnagel (Fn. 104), Kap. 4.5 Rz. 32; Schaffland/Wiltfang (Fn. 104), § 9 BDSG Rz. 7.

der Daten¹²³ und dem Missbrauchsrisiko¹²⁴ ab, denn je sensitiver die Daten sind und je größer die Gefahr des Missbrauchs ist, desto höher ist auch der unter dem Gesichtspunkt der Verhältnismäßigkeit zu fordernde Aufwand an Schutzmaßnahmen.¹²⁵

3. Datensicherheit und Haftung

Die Anforderungen des § 9 BDSG bzw. des § 78a SGB X an die technische Datensicherung sind für die Betreiber von Internetportalen verbindlich. Verstöße gegen die Anforderungen stellen zwar keine Ordnungswidrigkeit dar.¹²⁶ Wenn aber wegen mangelhaften Schutzes personenbezogene Daten von unbefugten Dritten missbraucht werden, kommt eine Haftung des Portalbetreibers auf Schadensersatz in Betracht.

So sehen das BDSG, ebenso die Landesdatenschutzgesetze und § 82 SGB X eine Schadensersatzhaftung vor, die eintritt, wenn Personen durch unbefugte Verwendung ihrer Daten einen Schaden erleiden (§ 7 BDSG). Der Schadensersatzanspruch setzt Verschulden voraus, enthält aber eine Beweislastumkehr zugunsten des Verletzten (§ 7 S. 2 BDSG). Die datenverarbeitende Stelle, hier also der Portalbetreiber, muss beweisen, dass sie kein Verschulden trifft.

Für öffentliche Stellen gilt nach § 8 BDSG, der nach § 82 S. 2 SGB X ebenfalls maßgeblich ist, ebenso nach den Landesdatenschutzgesetzen, daneben eine verschuldensunabhängige Haftung, wenn Daten unzulässig oder unzutreffend erhoben oder verarbeitet werden. Die §§ 7, 8 BDSG, 82 SGB X greifen auch bei Verletzung der Datensicherungspflicht nach § 78a SGB X ein¹²⁷.

¹²³ *Gola/Schomerus* (Fn. 108), § 9 Rz. 9.

¹²⁴ *Simitis-Ernestus* (Fn. 108), § 9 Rz. 27.

¹²⁵ *Simitis-Ernestus* (Fn. 108), § 9 Rz. 38.

¹²⁶ *Hauck/Noftz-Rombach* (Fn. 13), § 78a Rz. 35.

¹²⁷ *Hauck/Noftz-Rombach* (Fn. 13), § 78a Rz. 21, 35; *Wagner*, Mitt.LVA Württ. 1991, 268, 270.

Neben der Haftung aus den §§ 7, 8 BDSG i.V.m. § 82 SGB X sind in jedem Fall die allgemeinen Vorschriften anwendbar.¹²⁸ Soweit Internetportale von Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigungen im Rahmen ihrer öffentlichrechtlichen Tätigkeit betrieben werden, gelten die allgemeinen Regeln des Staatshaftungsrechts. Danach können ggf. Ansprüche auf Folgenbeseitigung¹²⁹ und auf Schadensersatz nach Art. 34 GG i.V.m. § 839 BGB geltend gemacht werden.¹³⁰

Soweit zivilrechtliche Regeln zur Anwendung kommen, die etwa für die Haftung der Vertragsärzte gegenüber ihren Patienten maßgeblich sind, können die Patienten, deren Daten missbraucht wurden, neben dem Schadensersatzanspruch aus § 7 BDSG Ansprüche nach § 823 Abs. 1 BGB geltend machen. Im Übrigen ist § 9 BDSG ein Schutzgesetz i.S.d des § 823 Abs. 2 BGB.¹³¹ Neben der Haftung auf Schadensersatz nach BDSG und BGB kommt die zivilrechtliche Störerhaftung in Betracht, die für Betreiber von Websites und Portalen in der aktuellen zivilrechtlichen Rechtsprechung stark an Bedeutung gewinnt.

Die Haftung nach allgemeinen Regeln des öffentlichen Rechts oder des Zivilrechts sind nicht Gegenstand dieser Untersuchung. Betreiber von Internetportalen für Heilberufe sollten aber die damit verbundenen Haftungsrisiken bedenken.

¹²⁸ *Gola/Schomerus* (Fn. 108), § 7 Rz. 16, § 8 Rz. 2; *Hauck/Noftz-Rombach* (Fn. 13), § 82 Rz. 44; *Simitis* (Fn. 108), § 7 Rz. 52, § 8 Rz. 35; *Seidel*, in *LPK-SGB X* (Fn. 13), § 82 Rz. 8.

¹²⁹ *Seidel*, in *LPK-SGB X* (Fn. 13), § 82 Rz. 8.

¹³⁰ *Hauck/Noftz-Rombach* (Fn. 13), § 82 Rz. 44; *Seidel*, in *LPK-SGB X* (Fn. 13), § 82 Rz. 8.

¹³¹ *Simitis* (Fn. 108), § 7 Rz. 68 m.w.Nachw.

II. Anforderungen an Authentisierungssysteme bei Internetportalen

1. Authentisierungssystem und Missbrauchsgefahren

Die Anforderungen an die Datensicherheit bei Internetportalen für Heilberufe sind bisher kaum Gegenstand öffentlicher Diskussion. Diese überaus komplexe Fragestellung weist zahlreiche Aspekte auf, die nicht Gegenstand dieser Untersuchung sind, wie etwa die Sicherheit der Daten innerhalb der Kassen- bzw. Kassenzahnärztlichen Vereinigungen. Hier interessiert vor allem die Sicherung gegenüber Zugriffen auf Daten über die Accounts der Teilnehmer, denn dies stellt einen spezifischen Aspekt der neuen Internetportale für Heilberufe dar. Diese Sicherung umfasst Maßnahmen zur Gewährleistung der Vertraulichkeit der Kommunikation und vor allem die Authentisierung der Teilnehmer.

Eine abschließende Beurteilung der Erforderlichkeit von Authentisierungssystemen zum Schutz vor Zugriff auf Daten an Internetportalen setzt umfassende tatsächliche Erhebungen voraus und kann hier nicht erfolgen, zumal in Bezug auf Internetportale für Heilberufe noch keine ausreichenden Erfahrungen vorliegen.¹³² Diese Untersuchung kann lediglich, auf der Grundlage von Erfahrungen in anderen Bereichen, Anhaltspunkte geben.

Beim Schutz von Daten gegenüber Angriffen, die über die Accounts berechtigter Teilnehmer geführt werden, sind aus heutiger Sicht die Gefahren des Phishing und ähnlicher Angriffe zu betrachten, die, wie die gegenwärtigen Angriffe gegen das Onlinebanking und gegen Internetauktionshäuser zeigen, durchaus geeignet sind, Dritten Zugang zu den Accounts der Teilnehmer zu verschaffen, wenn diese nicht hinreichend gesichert sind (S. dazu oben B.III.2., S. 14 ff.).

Der Schutz von Daten gegenüber Phishing und ähnlichen Angriffen berührt sowohl die Zugangskontrolle i.S. der Nr. 2 der Anlagen zu § 9 BDSG, § 78a SGB X als auch die Zugriffskontrolle nach Nr. 3 der Anlagen. Unter beiden

¹³² Eine umfassende Übersicht von denkbaren Angriffen auf Datenverarbeitungssysteme enthalten die "IT-Grundschutz-Kataloge" des Bundesamts für Sicherheit in der Informationstechnik, abrufbar unter <http://www.bsi.de/gshb/>.

Gesichtspunkten werden die Anforderungen an die Authentisierungssysteme diskutiert.¹³³ Eine genaue Abgrenzung kann daher dahinstehen.

Im Rahmen der datenschutzrechtlichen Anforderungen kommt es darauf an, welche Authentisierungssysteme erforderlich i.S. des § 78a SGB V, § 9 BDSG sind, um den Zugang Unbefugter zu geschützten Daten abzuwehren. Wegen der hier gebotenen Verhältnismäßigkeitsprüfung sind zwei Schritte erforderlich. So ist zunächst die Eignung der Authentisierungssysteme zum Schutz vor Angriffen zu prüfen, im zweiten Schritt die Verhältnismäßigkeit der jeweiligen Maßnahme unter Berücksichtigung der damit verbundenen Kosten.

Gegenstand der folgenden Betrachtung sind die Authentisierungssysteme des Passwortschutzes, des Softzertifikates und der Chipkarte, die derzeit für die Authentisierung an Internetportalen für Heilberufe am meisten diskutiert werden und charakteristische Unterschiede aufweisen, somit als Beispiele für verschiedenartige Sicherungssysteme gut geeignet sind. Sonstige Authentisierungssysteme bleiben außer Betracht.

2. Eignung zur Abwehr „konventioneller“ Angriffe

Der Zugriff Unbefugter auf das Account des Teilnehmers kann etwa dadurch ermöglicht werden, dass der Täter im Bereich des Teilnehmers auf Authentisierungsmedien zugreift und diese missbraucht. Unter Berücksichtigung der Erfahrungen in anderen Bereichen, in denen Authentisierungsmedien missbraucht werden (z.B. Bankautomaten, Onlinebanking), kommt etwa in Betracht, dass der Täter eine Notiz des Passworts entdeckt, Zugang zum Rechner des Berechtigten erhält oder sich in den Besitz einer Chipkarte bringt. Solche Angriffe kommen häufig aus dem Bereich des Berechtigten, etwa von seinen Angehörigen, Bekannten oder Mitarbeitern. Denkbar ist freilich auch, dass Dritte ohne Nähebeziehung zum Berechtigten, etwa ein Praxisbesucher, ein Dieb etc., auf die Authentisierungsmedien des Teilnehmers zugreifen.

¹³³ So etwa bei Simitis-Ernestus (Fn. 108), § 9 Rz. 88 f., insb. Rz. 97, Rz. 99 ff., 108 f.

Derartige Angriffe sind in Bezug auf die Gefährdung von Patientendaten, die über das Internetportal einsehbar sind, freilich sehr unwahrscheinlich, da Personen aus dem Umfeld des Teilnehmers häufig mindestens ebenso leicht auf die Datenverarbeitungssysteme der Praxis zugreifen können – oder auf Patientendaten in Papierform –, wo die Patientendaten weitaus umfassender gespeichert sind als in den Abrechnungsdaten.

Auch wenn diese Angriffe eher theoretisch erscheinen, ist doch festzustellen, dass das Passwort insoweit den geringsten Schutz bietet und das Softzertifikat den Schutz nicht entscheidend erhöht, da Personen aus dem Umfeld häufig Zugriff auf den Rechner des Teilnehmers haben werden und von dort aus agieren oder das Zertifikat kopieren können. Dagegen ist der Missbrauch der Chipkarte, deren Daten nicht kopiert werden können, deutlich schwieriger, so dass die Authentisierung durch Chipkarte zur Abwehr derartiger Angriffe besser geeignet erscheint.

3. Eignung zur Abwehr internetbasierter Angriffe

Internetbasierte Angriffe gegen Authentisierungssysteme sind aus heutiger Sicht eine wesentliche Bedrohung für die Datensicherheit im Internet. Die unter dem Stichwort des Phishing bekannt gewordenen Angriffe, die sich derzeit vor allem gegen das Onlinebanking, Internetauktionshäuser und sonstige Anbieter im elektronischen Geschäftsverkehr richten, gewinnen ihr besonderes Gefahrenpotential auch dadurch, dass die Täter, da sie meist nur über Internet und häufig aus dem Ausland agieren, kaum zu fassen sind. Verglichen mit konventionellen Angriffen ist das Risiko für die Täter bedeutend geringer, entsprechend steigt die Attraktivität solcher Angriffe für die Täter.

a) Authentisierung durch Passwort

Phishing und ähnliche Angriffe richten sich heute meist gegen die Authentisierung durch einfache Passwörter. Wie das Beispiel etwa des Onlinebanking zeigt, gelingt es den Tätern häufig genug schon durch klassisches Phishing mit gefälschter E-Mail und gefälschten Websites, das Passwort des Teilnehmers zu erfahren. Im Bereich des Onlinebanking führt

diese Problematik derzeit bekanntlich dazu, dass die meisten Kreditinstitute das traditionelle PIN/TAN-Verfahren durch aufwendigere Authentisierungsverfahren ersetzen.

Während beim klassischen Phishing der Erfolg des Angriffs davon abhängt, ob der Teilnehmer sich täuschen lässt, kann der Teilnehmer Pharming-Angriffe, also den Angriff gegen einen Name-Server oder die Veränderung der hosts-Datei auf seinem Rechner durch Trojaner kaum abwehren. Im Übrigen können Passwörter durch sog. Keylogger relativ leicht ausgespäht werden, wie die Erfahrung im Onlinebanking lehrt. Im Ergebnis kann der Passwortschutz durch internetbasierte Angriffe relativ leicht überwunden werden.

b) Softzertifikate

Wenn zur Authentisierung der Teilnehmer neben einem Passwort ein Softzertifikat erforderlich ist, sind Angriffe wie das klassische Phishing durch E-Mail und gefälschte Website aus heutiger Sicht ausgeschlossen. Auch durch Keylogging des Passwortes kann das Authentisierungssystem nicht überwunden werden.

Jedoch ist durchaus nicht ausgeschlossen, dass der Täter, der durch Trojaner Zugang zum Rechner des Teilnehmers hat, das auf dem Rechner des Teilnehmers gespeicherte Softzertifikat kopiert. Denkbar ist auch, dass der Täter durch Trojaner während der Kommunikation des Teilnehmers mit dem Internetportal Daten abrufen und an sich übermitteln lässt. Derartige Angriffe sind deutlich aufwendiger als etwa klassisches Phishing, bedürfen aber keinesfalls sehr hohen Aufwandes oder eines nur Spezialisten vorbehaltenen Könnens.

c) Chipkarte und PIN

Authentisierungssysteme, die Chipkarte und PIN verlangen, können durch klassisches Phishing nicht überwunden werden. Auch ein Keylogging der PIN hilft dem Täter nicht weiter. Anders als beim Softzertifikat kann der geheime Schlüssel des Teilnehmers nicht kopiert werden, da der Schlüssel

nur auf der Chipkarte gespeichert ist und der Täter selbst dann, wenn er Trojaner auf dem Rechner des Teilnehmers platziert hat, diese nicht auslesen kann. Im Übrigen ist Keylogging ausgeschlossen, wenn mindestens ein Class 2-Kartenleser verwendet wird.

Freilich sind erfolgreiche Angriffe durch Trojaner auch bei Authentisierung durch Chipkarte und PIN durchaus denkbar. Solche Angriffe gelten aber als sehr schwierig und aufwendig. Insoweit ist daher auf die schon erwähnte Studie von *Buchmann* zu verweisen, der ausdrücklich feststellt, dass die Authentisierung durch Chipkarte und PIN bei den heute relevanten Angriffen gegen Phishing und gegen Trojaner-Angriffe sicheren Schutz bietet, sofern die PIN über eine gesicherte Tastatur des Chipkartenlesegeräts eingegeben wird.

d) Zwischenergebnis

Die hier betrachteten Authentisierungssysteme unterscheiden sich in Bezug auf ihre Eignung, den Zugriff Unbefugter auf geschützte Daten zu verhindern, deutlich. Alle Authentisierungssysteme können durch gezielte Eingriffe von Personen aus dem Bereich des Teilnehmers, etwa Praxismitarbeiter, überwunden werden. Insoweit bietet die Authentisierung durch Passwort den geringsten Schutz, die Authentisierung durch Chipkarte und PIN den höchsten Schutz. Freilich sind derartige Angriffe gegen Internetportale für Heilberufe höchst unwahrscheinlich.

Bei den hier vor allem interessierenden internetbasierten Angriffen sind die Unterschiede gravierender. Hier bietet die Authentisierung durch schlichtes Passwort nur geringen Schutz, denn Passwörter können durch klassisches Phishing, durch Keylogging und zahlreiche sonstige Angriffe relativ leicht überwunden werden. Die Authentisierung durch Passwort und Softzertifikat kann zwar nicht durch klassisches Phishing, wohl aber durch Trojaner-Angriffe einfach überwunden werden, da das Softzertifikat vom Rechner des Teilnehmers kopiert werden kann. Verfahren, die zur Authentisierung Chipkarte und PIN verlangen, sind aus heutiger Sicht gegen internetbasierte Angriffe weitestgehend sicher, auch wenn ihre Überwindung theoretisch in Betracht kommt.

III. Erforderlichkeit von Schutzmaßnahmen

Die Erforderlichkeit i.S. des § 78a SGB X und des § 9 BDSG setzt, wie gesagt, eine Abwägung zwischen dem durch eine jeweilige Maßnahme zu erreichenden Schutz und dem damit verbundenen Aufwand voraus.

1. Die maßgeblichen Kosten der Authentisierungssysteme

Unter dem Gesichtspunkt des mit der Schutzmaßnahme verbundenen Aufwands sind alle Kosten zu berücksichtigen, die durch die Maßnahme entstehen.¹³⁴ Im Fall der Zugriffssicherung sind dies die Gesamtkosten des Authentisierungssystems.

Die Kosten, die durch die hier interessierenden Maßnahmen entstehen, können im Rahmen dieser Untersuchung nicht erörtert werden. Es lässt sich aber auch ohne eingehende Untersuchung feststellen, dass die Authentisierung durch Teilnehmernamen und Passwörter die geringsten Kosten unter den hier betrachteten Alternativen verursacht und die Authentisierung durch Chipkarte und PIN die höchsten. Bei der Chipkarte fallen gegenüber dem Softzertifikat zusätzliche Kosten für die Chipkarte an, die jeder Teilnehmer erhalten muss. Außerdem muss ggf. ein Kartenlesegerät angeschafft werden.

Auf Seiten des Portalbetreibers können zudem zusätzliche Kosten für die Einrichtung dieses Systems anfallen. Es ist jedoch fraglich, ob die Kosten nennenswert höher sind als die Systemkosten bei Authentisierung durch Teilnehmernamen und Passwörter oder Softzertifikate und Passwörter.

Bei Internetportalen für Heilberufe ist in Bezug auf die Kosten der Authentisierungssysteme zu beachten, dass derartige Portale derzeit erst geplant oder in Errichtung sind. Dies bedeutet, dass Umstellungskosten, die in anderen Bereichen (z.B. Onlinebanking) einen erheblichen Anteil der Gesamtkosten für neue Authentisierungsverfahren ausmachen, nicht anfallen. Ebenso entfallen Abschreibungen auf bereits getätigte

¹³⁴ Simitis-Ernestus (Fn. 108), § 9 Rz. 34; Pickel, in Pickel/Marschner (Fn. 35), § 78a Rz. 4; Schaffland/Wiltfang (Fn. 104), § 9 BDSG Rz. 7.

Investitionen, so dass die Kosten für aufwendige Verfahren wie etwa der Authentisierung durch Chipkarte und PIN in der hier betrachteten Konstellation verhältnismäßig niedrig sein dürften.

2. Schutzwürdigkeit der Daten

Für das Maß an erforderlichen Schutzmaßnahmen zur Gewährleistung der Datensicherheit kommt es wesentlich darauf an, in welchem Maß die Daten schutzwürdig sind.¹³⁵

Die damit notwendige Einstufung personenbezogener Daten nach ihrer Schutzbedürftigkeit ist teilweise vom Gesetz vorgegeben. SGB X und BDSG treffen übereinstimmend eine, auf die EG-Datenschutzrichtlinie zurückgehende Unterscheidung dahin, dass für bestimmte Arten von personenbezogenen Daten besondere Schutzregeln¹³⁶ gelten.¹³⁷ Diese Gruppe der „besonderen personenbezogenen Daten“ ist in § 67 Abs. 12 SGB X und § 3 Abs. 9 BDSG wörtlich übereinstimmend definiert. Diese Definition, die auf Art. 8 der EG-Datenschutzrichtlinie zurückgeht,¹³⁸ nennt unter anderem Angaben über „Gesundheit“. Daraus folgt, dass Gesundheitsdaten nach dem Willen des Gesetzes besonders schutzbedürftig sind.

Das SGB X enthält daneben noch eine weitere Kategorie von Daten, die besonders geschützt werden. § 76 SGB X schränkt die Übermittlung sogenannter medizinischer Sozialdaten ein. Danach dürften Sozialdaten, die von einem Arzt oder einer anderen nach § 203 StGB zur Verschwiegenheit verpflichteten Person zugänglich gemacht worden sind, nur unter den Voraussetzungen weitergegeben werden, unter denen der Arzt die Daten weitergeben dürfte. Durch § 76 SGB X, der eine Verlängerung des

¹³⁵ *Simitis-Ernestus* (Fn. 108), § 9 Rz. 27 ff., 39 ff.; Hauck/Noftz-Rombach (Fn. 13), § 78a Rz. 22.

¹³⁶ Vgl. §§ 13 Abs. 2, 28 Abs. 6, 9, 29 Abs. 5 BDSG.

¹³⁷ Sehr kritisch zu dieser Vorgabe der Richtlinie *Simitis* (Fn. 108), § 3 Rz. 250 ff.

¹³⁸ *Simitis* (Fn. 108), § 3 Rz. 250.

Geheimnisschutzes bezweckt,¹³⁹ wird der Bereich der medizinischen Sozialdaten unter den besonderen personenbezogenen Daten nochmals hervorgehoben und die besondere Schutzwürdigkeit dieser Daten betont.

§ 78a SGB X und § 9 BDSG enthalten keine ausdrückliche Bezugnahme auf die besonderen personenbezogenen Daten oder medizinische Sozialdaten. Vielmehr ist, wie gesagt, die besondere Schutzwürdigkeit der Daten im Rahmen der Prüfung der Erforderlichkeit von Schutzmaßnahmen zu berücksichtigen. Dies bedeutet, dass für Gesundheitsdaten, erst recht für medizinische Sozialdaten, die in den Abrechnungsdaten enthalten sind, regelmäßig ein sehr hohes Schutzniveau erforderlich ist.¹⁴⁰

3. Abwägung

Die Prüfung der Verhältnismäßigkeit der Schutzmaßnahme erfordert letztlich eine Abwägung zwischen dem erstrebten Schutzniveau und dem für die Gewährleistung des Schutzes erforderlichen Aufwand. Zu dieser Frage fehlt es in Bezug auf Internetportale für Heilberufe bisher an veröffentlichten Stellungnahmen. Ebenso ist noch weitestgehend unerforscht, welche Maßnahmen bei Internetportalen, über die personenbezogene Daten einsehbar sind, in Bezug auf das Risiko von internetbasierten Angriffen erforderlich sind.

a) Bisherige Anforderungen an Sicherung von Patientendaten

Anhaltspunkte für die Abwägung lassen sich aber aus der bisherigen Handhabung der Online-Abrechnung gewinnen. Insoweit besteht bei den Kassen- und Kassenzahnärztlichen Vereinigungen in der Sache Einigkeit dahin, dass sehr hohe Anforderungen zum Schutz von Patientendaten bei der Online-Abrechnung gelten. So wurde etwa gefordert, dass für die Online-Übermittlung von Abrechnungsdaten ein Stand-alone-Rechner

¹³⁹ Seidel, in LPK-SGB X (Fn. 13), § 76 Rz. 1.

¹⁴⁰ Heibey, in Roßnagel (Fn. 104), Kap.4.5 Rz. 26; Hauck/Noftz-Rombach (Fn. 13), § 78a Rz. 22.

genutzt wird, der keine Anbindung zu den übrigen Datenverarbeitungssystemen hat. Hierdurch wird ein hohes Maß an Schutz gegen internetbasierte Angriffe (Hacking) gegen die beim Arzt gespeicherten Daten erreicht. Dieses Verfahren ist freilich sehr aufwendig, denn es muss vom Teilnehmer ein Rechner für die Online-Übermittlung vorgehalten werden, der nur sehr eingeschränkt für andere Zwecke eingesetzt werden kann. Auch wenn es bei der hier interessierenden Frage der Authentisierung nicht nur um die Abwehr von Hacking-Angriffen, sondern vor allem um Phishing und ähnliche Angriffe geht, so zeigt sich doch, dass nach Auffassung der Kassen- bzw. Kassenzahnärztlichen Vereinigungen auch ein recht hoher Aufwand zum Schutz gegen internetbasierte Angriffe gerechtfertigt ist.

Diese Linie spiegelt sich auch in der Literatur wieder. So wird vertreten, dass der Einsatz des Internet zur Übermittlung von Sozialdaten nur auf der Grundlage der elektronischen Signatur i.S. des SigG – gemeint ist wohl die qualifizierte elektronische Signatur – eine den Anforderungen des § 78a SGB X genügende Anwendung betrieben werden könne.¹⁴¹

In die gleiche Richtung geht die Auffassung der Datenschutzbeauftragten. Schon 2002 haben Vertreter des Bundesbeauftragten für den Datenschutz und mehrerer Landesbeauftragte für den Datenschutz zu den datenschutzrechtlichen Anforderungen an Medizinetze Stellung genommen.¹⁴² In dieser Studie wird dem Schutz der Vertraulichkeit der Patientendaten ausdrücklich auch unter dem Gesichtspunkt des Schutzes gegen Einsichtnahme durch unbefugte Dritte bei allen Diensten der Telemedizin große Bedeutung zugemessen.¹⁴³ Die Studie äußert sich nicht ausdrücklich zu dem hier relevanten Schutz gegen den Zugriff auf Ärzteportale durch unbefugte Dritte, geht aber davon aus, dass die Erfordernisse des Datenschutzes bei der Telemedizin nur unter Einsatz starker Verschlüsselung und Authentisierung durch qualifizierte

¹⁴¹ *Grunert*, DAngVers 2002, 52, 55; Hauck/Noftz-Rombach (Fn. 13), § 78a Rz. 18b.

¹⁴² Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig: Datenschutz und Telemedizin – Anforderungen an Medizinetze, Oktober 2002, abrufbar z.B. unter www.dimdi.de/static/de/ehealth/literatur/index.

¹⁴³ Datenschutz und Telemedizin (Fn. 142), unter V. 1. (S. 19 f.).

elektronische Signaturen, also durch eine Chipkarte mit PKI-Infrastruktur erforderlich ist.¹⁴⁴

In der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 verlangen die Datenschutzbeauftragten für den gesamten Bereich der öffentlichen Verwaltung unmissverständlich die Einführung sicherer Authentisierungsverfahren. So wird das Authentisierungssystem des ELSTER-Verfahrens ausdrücklich als unzureichend verworfen und eine Authentisierung durch Chipkarte mit PKI sowie die Verwendung qualifizierter elektronischer Signaturen gefordert.¹⁴⁵

b) Verhältnismäßigkeit hochwertiger Authentisierungssysteme

Die Frage, welche Anforderungen sich aus dem Gebot der Datensicherheit nach § 78a SGB X, § 9 BDSG bzw. der Landesdatenschutzgesetze ergeben, konzentriert sich unter Berücksichtigung der hier betrachteten Verfahren der Authentisierung auf die Frage, ob ein Schutzniveau, wie es durch Einsatz von Chipkarte und PIN erreicht wird, unter Berücksichtigung der damit verbundenen Kosten verhältnismäßig und damit erforderlich i.S. des § 78a SGB X, § 9 BDSG ist. Dabei ist klarzustellen, dass die Verpflichtung des § 78a SGB X, § 9 BDSG im Grundsatz nicht auf eine konkrete Schutzvorrichtung weist, da in aller Regel ein bestimmtes Schutzniveau durch verschiedene Mittel erzielt werden kann.

Unter dem Gesichtspunkt der Verhältnismäßigkeit ist auch jeweils zu prüfen, ob ein niedrigeres Schutzniveau, das mit geringeren Kosten zu erreichen ist, für den bezweckten Schutz ausreichend ist.¹⁴⁶ Folglich kommt es darauf an, ob die Authentisierung durch Teilnehmernamen und Passwort,

¹⁴⁴ Datenschutz und Telemedizin (Fn. 142), unter V. (S. 19 ff.).

¹⁴⁵ Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11.10.2006 „Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren“; abrufbar etwa unter www.sachsen-anhalt.de/LPSA/index.php?id=20565.

¹⁴⁶ *Bergmann/Möhrle/Herb*, Datenschutzrecht (Losebl.; Stand: 8/2006), § 9 BDSG Rz. 16; *Simitis-Ernestus* (Fn. 108), § 9 Rz. 23.

die die geringsten Kosten verursacht, zur Sicherung von Gesundheitsdaten ausreicht. Da Gesundheitsdaten in besonderer Weise schutzwürdig sind, wird man diese Frage angesichts des aktuellen Gefährdungspotentials durch internetbasierte Angriffe wohl verneinen müssen.

Entscheidend ist, ob der durch die Authentisierung mit Chipkarte und PIN erzielte höhere Schutz bei Internetportalen für Heilberufe, die Einblick in Patientendaten vermitteln, den Zuwachs an Kosten rechtfertigt. Diese Frage kann hier mangels konkreter Zahlen nicht abschließend beurteilt werden. Es ist aber nicht zu verkennen, dass aus Sicht der Teilnehmer die Kosten für die Beschaffung der Chipkarte und ggf. eines Lesegeräts wesentlich geringer sein dürften als der Aufwand für einen Rechner, der etwa als Stand-alone-Rechner für den Datentransfer genutzt wird.

Da durch die Authentisierung mit Chipkarte und PIN im Vergleich zum Schutz durch einfaches Passwort oder durch Softzertifikat ein wesentlich höherer Schutz gegen Phishing und ähnliche Angriffe erzielt wird, sprechen gute Gründe dafür, dass ein Schutzniveau, wie es durch Chipkarte und PIN erzielt wird, erforderlich i.S. des § 78a SGB X, § 9 BDSG ist.

Dies schließt nicht aus, ein vergleichbares Schutzniveau durch andere Authentisierungssysteme zu erzielen. Anbieter von Internetportalen für Heilberufe müssen aber damit rechnen, dass Datenschutzbehörden und Gerichte, jedenfalls dann, wenn internetbasierte Angriffe auf die Portale auftreten und Patientendaten von unbefugten Dritten eingesehen werden sollten, die Auffassung vertreten werden, dass ein geringeres Schutzniveau hinter dem gesetzlich gebotenen Schutz zurückbleibt. Dies würde die oben (I.3.) beschriebenen Haftungsrisiken auslösen.

IV. Ergebnis

Auch wenn eine abschließende Beurteilung der datenschutzrechtlichen Anforderungen an die Authentisierung von Internetportalen für Heilberufe im Rahmen dieser Untersuchung nicht möglich ist, lassen sich doch einige Anhaltspunkte für diese Anforderungen gewinnen.

Das SGB X und das BDSG fordern für Patientendaten als besonders sensitive Daten einen besonders hohen Schutz gegenüber Angriffen Dritter.

Bei Internetportalen sind auch Phishing und ähnliche Angriffe in Betracht zu ziehen.

Die Authentisierung durch Chipkarte und PIN hat unter den hier betrachteten Authentisierungssystemen die eindeutig beste Eignung, um internetbasierte Angriffe abzuwehren.

Dagegen lassen sich die Authentisierung durch Teilnehmernamen und Passwort schon durch klassisches Phishing, erst recht durch Pharming oder Trojaner-Angriffe relativ leicht umgehen. Auch Softzertifikate können durch Trojaner-Angriffe überwunden werden. Dagegen ist die Authentisierung durch Chipkarte und PIN aus heutiger Sicht gegen internetbasierte Angriffe weitestgehend sicher.

Die Erforderlichkeit von Schutzmaßnahmen i.S. des § 78a SGB X und des § 9 BDSG setzt ein angemessenes Verhältnis von Kosten und erstrebtem Schutz voraus.

Angesichts der hohen Bedeutung, die das Gesetz dem Schutz von Gesundheitsdaten beimisst, sprechen gute Gründe dafür, dass die mit der Authentisierung durch Chipkarte und PIN verbundenen Kosten nicht unverhältnismäßig sind. Betreiber von Internetportalen für Heilberufe müssen daher damit rechnen, dass das damit erreichte Schutzniveau gesetzlich geboten ist.

Soweit das gesetzlich gebotene Schutzniveau nicht erreicht wird, kommt im Fall eines erfolgreichen Angriffs und des Missbrauchs von Patientendaten eine Haftung der Betreiber von Internetportalen in Betracht.

F. Zusammenfassung der Ergebnisse

Die Einrichtung von Internetportalen wirft zahlreiche, durchaus schwierige Rechtsfragen auf. Die Gestaltung der Portale muss an die rechtlichen Vorgaben angepasst werden, damit Rechtssicherheit erzielt wird und Haftungsrisiken vermieden werden. Dies wird nicht zuletzt an den hier untersuchten Aspekten des Zugangs, der Beweisführung und des Datenschutzes deutlich.

I. Sicherer Zugang von Nachrichten in Internetportalen

Für die Betreiber der Internetportale (Kassenärztliche bzw. Kassenzahnärztliche Vereinigungen) ist es von Bedeutung, den Teilnehmern (Vertragsärzte) zugangsbedürftige Erklärungen, etwa den Honorarbescheid, rechtswirksam über das Portal übermitteln zu können. Diese Anforderung kann bei sachgerechter Gestaltung des Portals erreicht werden.

Der Zugang von elektronisch übermittelten Erklärungen setzt die Speicherung der Erklärung in einer Empfangseinrichtung des Teilnehmers voraus. Das Postfach des Teilnehmers im Portal ist eine solche Empfangseinrichtung, da die exklusive organisatorische Zuordnung des Postfachs für die Eigenschaft als Empfangseinrichtung ausreicht. Ebenso liegt die erforderliche Widmung zum Empfang von Erklärungen des Portalbetreibers vor.

Der Zugang erfolgt mit gelungener Speicherung. Das Übermittlungsrisiko, das grundsätzlich der Absender trägt, wird minimiert, da die Übermittlung innerhalb des Datenverarbeitungssystems des Portalbetreibers erfolgt. Sofern der Teilnehmer die Speicherung schuldhaft verhindert, wird er nach dem Grundsatz von Treu und Glauben so behandelt, als wäre die Erklärung zugegangen.

Erklärungen, die nicht im Postfach gespeichert, sondern etwa an anderer Stelle des Portals abgebildet sind, werden mit Kenntnisnahme durch den Teilnehmer wirksam.

Die Bereitstellung von Erklärungen zum Herunterladen (download) bewirkt nicht den Zugang. Dieser erfolgt erst, wenn der Teilnehmer die Erklärung

tatsächlich heruntergeladen hat. Sofern der Teilnehmer gegenüber dem Portalbetreiber verpflichtet ist, am Zugang der Erklärung durch Herunterladen einer bereitgestellten Erklärung mitzuwirken, kann auf diesem Wege der Zugang gesichert werden. Mit einer Lesebestätigung kann der Nachweis vereinfacht werden, dass der Teilnehmer über die Bereitstellung zum Herunterladen informiert wurde.

Eingriffe Dritter in das Account, z.B. Löschen von Daten, hindern den Zugang der zuvor gespeicherten Erklärung jedenfalls nicht, wenn der Zugriff auf das Account hinreichend gesichert ist.

II. Nachweis von Handlungen am Account des Teilnehmers

Für Betreiber von Internetportalen kann es wichtig sein, den Nachweis führen zu können, dass der Teilnehmer, und nicht etwa ein unbefugter Dritter, eine bestimmte Handlung am Account vorgenommen hat. Dieser Nachweis erfolgt wesentlich über die Authentisierung bei der Anmeldung zum Teilnehmerbereich.

Der Beweis der Urheberschaft einer bestimmten Handlung kann im sozialgerichtlichen Verfahren, wie im Zivilverfahren, mit allen zugelassenen Beweismitteln geführt werden. Beim Nachweis der Urheberschaft aufgrund der Authentisierung erfolgt ein Indizienbeweis aufgrund mehrerer Umstände, insbesondere der Anmeldung am Portal und der Herrschaft des Teilnehmers über das Authentisierungsmedium (z.B. Passwort, Chipkarte).

Der volle Beweis der Urheberschaft wird häufig nicht gelingen, da es nicht nur theoretisch möglich ist, dass ein unbefugter Dritter sich in den Besitz des Authentisierungsmediums gebracht und damit die Anmeldung vorgenommen hat. Umso größere Bedeutung kommt dem sogenannten Anscheinsbeweis zu, durch den der Nachweis der Urheberschaft gleichwohl geführt werden kann. Dieser Anscheinsbeweis setzt voraus, dass nach der Lebenserfahrung davon ausgegangen werden kann, dass der Teilnehmer und nicht ein Dritter sich unter Einsatz des Authentisierungsmediums angemeldet hat. Ein etwa bestehender Anschein kann erschüttert werden, wenn die ernsthafte Möglichkeit eines atypischen Geschehensablaufs besteht.

Bestehen und Erschütterung des Anscheins hängen entscheidend von der Qualität des Authentisierungssystems ab. Für die Authentisierung durch Teilnehmernamen und Passwort haben die Zivilgerichte bisher ganz überwiegend einen solchen Erfahrungssatz und damit den Anscheinsbeweis abgelehnt, da dieses Authentisierungsverfahren zu unsicher sei. Sofern man einen Anschein annimmt, kann dieser relativ leicht, durch die Möglichkeit von Phishing oder eines Trojaner-Angriffs, erschüttert werden.

Zum Anscheinsbeweis bei Authentisierung durch Passwort und Softzertifikat liegen keine veröffentlichten Gerichtsentscheidungen vor. Man wird aber einen Anschein der Urheberschaft annehmen können. Auch dieser kann aber durch die ernsthafte Möglichkeit eines Trojaner-Angriffs erschüttert werden.

Die Authentisierung durch Chipkarte und PIN begründet den Anschein der Urheberschaft des Karteninhabers. Insoweit kann die Wertung des § 371a ZPO herangezogen werden, wonach die qualifizierte elektronische Signatur, die zur Authentisierung ebenfalls Chipkarte und PIN verwendet, einen Anscheinsbeweis der Urheberschaft begründet. Auch der bei der Verwendung von ec-Karte und PIN anerkannte Anscheinsbeweis spricht für den Anschein der Urheberschaft. Der Anschein wird kaum zu erschüttern sein, da die Authentisierung durch Chipkarte durch Phishing und herkömmliche Trojaner-Angriffe nicht überwunden werden kann.

Dies rechtfertigt die Erwartung, dass der Nachweis der Urheberschaft des Teilnehmers für eine an seinem Account vorgenommene Handlung bei Authentisierung durch Chipkarte und PIN regelmäßig gelingen, bei weniger sicheren Verfahren hingegen häufig scheitern wird.

III. Anforderungen an die Datensicherheit bei Internetportalen für Heilberufe

Der Betrieb von Internetportalen unterliegt hohen datenschutzrechtlichen Anforderungen. Dazu gehört unter anderem der Schutz gespeicherter personenbezogener Daten gegenüber unbefugter Verwendung durch Dritte. Dieser Aspekt ist für Internetportale von besonderer Bedeutung, da die Abrechnungsdaten Gesundheitsdaten von Patienten enthalten und auf diese Daten, anders als bei herkömmlicher Abrechnung, über Internet zugegriffen

werden kann. Bei Internetportalen sind auch Phishing und ähnliche Angriffe in Betracht zu ziehen.

Das SGB X und das BDSG fordern für Gesundheitsdaten von Patienten als besonders sensitive Daten einen besonders hohen Schutz gegenüber Angriffen Dritter. Die Authentisierung durch Chipkarte und PIN hat unter den hier betrachteten Authentisierungssystemen die eindeutig beste Eignung, um internetbasierte Angriffe abzuwehren. Dagegen lassen sich die Authentisierung durch Teilnehmername und Passwort schon durch klassisches Phishing, erst recht durch Pharming oder Trojaner-Angriffe relativ leicht umgehen. Auch Softzertifikate können durch Trojaner-Angriffe überwunden werden.

Gemäß § 78a SGB X sind erforderlich und damit rechtlich geboten nur solche Maßnahmen, deren Kosten in einem angemessenen Verhältnis zum erstrebten Schutz stehen. Angesichts der hohen Bedeutung, die das Gesetz dem Schutz von Gesundheitsdaten beimisst, sprechen gute Gründe dafür, dass die mit der Authentisierung durch Chipkarte und PIN verbundenen Kosten nicht unverhältnismäßig sind. Betreiber von Internetportalen für Heilberufe müssen daher damit rechnen, dass das damit erreichte Schutzniveau gesetzlich geboten ist.

Soweit das gesetzlich gebotene Schutzniveau nicht erreicht wird, kommt im Fall eines erfolgreichen Angriffs und des Missbrauchs von Patientendaten eine Haftung der Betreiber von Internetportalen in Betracht.