Master-Thesis

Wirtschaftsrecht

Beweisführung der Zustellung im E-Mail-Verkehr

Stefan Bauer

sb@plzk.de

01.05.2022

I. Abstract

Die Unternehmenskommunikation und Digitalisierung stellt alte Abläufe in Frage. Wird langsam aber sicher die Briefpost mit ihren Zustellformen wie dem Einschreiben-Einwurf oder dem Einschreiben-Rückschein durch E-Mail abgelöst, existieren längst neue Methoden zur rechtssicheren Beweisführung einer E-Mail-Zustellung für den Absender. Neben der Protokollauswertung von Mail- und Webserver-Logdateien, existieren Funktionen wie die Übermittlungs- und Lesebestätigung die auf Knopfdruck angefordert werden können. Bei der Beweiserhebung und Konservierung gilt es, diese bereits frühzeitig im Unternehmen zu aktivieren um im Bedarfsfall auf aussagekräftige Nachweise zurück greifen zu können. Hierzu gehört die Aktivierung und Protokollierungen von E-Mail-Zustellungen auf Systemebene sowie die Verwendung von geeichten Zeitservern. Aber auch der Einsatz von digitalen Signaturen untermauert die Echtheit. Auch die Besonderheiten beim Einsatz eines Viren- und Anti-Spam-Filters oder der automatischen Abwesenheitsnachricht im E-Mail-Verkehr können sich positiv für den Absender auswirken. Um eine positive Würdigung der eigenen Beweise vor Gericht zu erreichen, müssen diese nachvollziehbar und lückenlos sein und plausibel vorgetragen werden. Die Zugangsfiktion ist ein nötiges Instrument um Sonderfälle bei der Zustellung zu berücksichtigen und ersetzt nicht den stringenten Beweisvortrag.

E-Mail-Zustellung, Zugangsbeweis, SMTP, Zugangsfiktion, DSN, E-Mail-Annahme, MDN, Protokolle

E-Mail delivery, message acceptance, send mail transfer protocol, delivery status notification, DKIM protocols, S/MIME

II. Inhaltsverzeichnis

III. Abbildungsverzeichnis

IV. Abkürzungsverzeichnis

AG	Amtsgericht
AO	Abgabenordnung
ARPANET	Advanced Research Projects Agency Network
AZ	Aktenzeichen
BGH	Bundesgerichtshof
BVG	Bundesverfassungsgericht
DKIM	DomainKeys Identified Mail
DSN	Delivery Status Notification
eiDAS	electronic IDentification, Authentication and trust Services
EstG	Einkommenssteuergesetz
LAG	Landesarbeitsgericht
MDN	Message Disposition Notification
OLG	Oberlandesgericht
PostG	Postgesetz
RFC	Request for Comments
SMTP	Simple Mail Transfer Protocol
StPO	Strafprozessordnung
VwVfG	Verwaltungsverfahrensgesetz

WORM	write once, read many
ZPO	Zivilprozessordnung

Hinsichtlich der übrigen Abkürzungen siehe

Kirchner, Hildebert/Butz, Cornelie, Abkürzungsverzeichnis der Rechtssprache, 8. Aufl., Berlin 2015.

1. Einleitung

Durch den digitalen Charakter einer E-Mail ist häufig auch der Beweis ihrer Zustellung nur durch elektronische Nachweise zu erbringen. Aufgrund fälschbarer Protokolle, flüchtiger Computer- und Serverspeicher sowie sich ständig wechselnder Übertragungswege durch das Internet – auf dem Weg zum endgültigen Mailsystems des Empfängers – bestehen besondere Anforderungen an die Beweisführung einer erfolgreichen E-Mail-Zustellung. Diese Arbeit beschäftigt sich mit den technischen und rechtlichen Grundlagen der Beweisführung für den E-Mail-Absender. Etwaige Möglichkeiten der Empfänger, die Echtheit oder Unversehrtheit einer E-Mail digital zu überprüfen, soll in dieser Arbeit nicht im Detail behandelt werden. Weiter soll die häufig anzutreffende Zugangsfiktion (vgl. z. B. § 41 Abs. 2 VwVfG, § 122 Abs. 2 AO) den gewonnenen Erkenntnissen kritisch gegenübergestellt werden. Diese Arbeit soll dazu dienen, Absendern die nötigen Mittel und das technische Verständnis der Beweisführung an die Hand zu geben und möchte dazu folgende Fragen klären:

- Welche Beweismittel kommen als Zustellnachweis in Frage?
- Welche Aussagekraft kommt jedem Beweismittel zu und was sind deren Besonderheiten?
- Welche Beweismittel wurden in welchem Umfang bereits durch deutsche Gerichte gewürdigt?
- Welche Sonderstellung nimmt die Zugangsfiktion in der Argumentation ein?

In dieser Arbeit soll der E-Mail-Versender ein praktisches Verständnis über die zur Verfügung stehenden technischen Mittel zur Beweisführung erhalten um diese zukünftig in seiner Praxis einzusetzen. Beginnend muss die Frage geklärt werden, ab wann eine E-Mail als zugestellt gilt und wie sich dies letztlich dann beweisen lässt. Hierzu wird die Übermittlungs- und Lesebestätigung vorgestellt, die eher schwer zugänglichen Übermittlungsprotokolle von Mailservern sowie versteckte Tracking-Pixel bzw. externe Inhalte in einzelnen E-Mails. Auf diesen

Grundlagen aufbauend, folgt eine jeweilige Bewertung, mit welchem Aufwand und wie nachvollziehbar, die Beweismittel durch wen erhoben werden können, wie eine nötige gerichtsverwertbare Konservierung dieser Information umzusetzen ist und welchen Grundsätzen die Prozessführung unterliegt. Anschließend wird ausgeführt, wie deutsche Gerichte einzelne Beweismittel bereits akzeptiert haben und unter welchen Umständen davon Abstand genommen wurde. Abschließend sollen die vorgestellten Argumente für und gegen ein Beweismittel bzw. die Ansprüche an dieses, mit der Zugangsfiktion abgeglichen werden. Speziell wie sich diese Gestaltung auswirkt.

2. Methodenbeschreibung und Einschätzung – die Literaturanalyse

Grundlage dieser Arbeit war die Arbeit mit verfügbarer Literatur und Rechtsprechung. Die zu Anfang aufgestellten Leitfragen dienen als roter Faden zur Orientierung. Der primäre Fokus stellt auf die Sichtweise eines E-Mail-Versenders ab. Möglichkeiten zur Entkräftung von Beweisen für den Empfänger werden in dieser Arbeit allenfalls oberflächlich behandelt. Bei der Quellenauswahl wurde darauf geachtet – wo es möglich war – neuere Quellen bzw. Entscheidungen, gegenüber älteren zu bevorzugen. Für die Quellenrecherche wurde Google Scholar[1], der juris-Rechtsportal-Zugang für HFH-Studenten[2] sowie die Google-Suche[3] verwendet. Die Literaturrecherche wurde primär in Dokumenten über den HFH-Zugang zu Springer[4] und Wiley[5] genutzt. Wesentlicher Vorteil der online-basierten Suchmethoden war, dass in Echtzeit in jeweils indizierten Dokumenten nach Schlagwörtern gesucht werden kann. Zentrale Quelle für die recherchierte und stellenweise zitierte Rechtsprechung, war ebenso das juris-Rechtsportal. Bei der Auswahl von Artikeln und Beiträgen wurde darauf geachtet, dass die jeweiligen Autoren auch über nachweisbare Erfahrung in diesem Gebiet verfügten[6] und dass die zitierten Quellen die nötigen Antworten auf die gestellten Fragen liefern[7].

1 https://scholar.google.de (letzter Abruf am 16.01.2022)

2 https://juris.de (letzter Abruf am 16.01.2022)

3 https://www.google.de (letzter Abruf am 16.01.2022)

4 https://link.springer.com (letzter Abruf am 16.01.2022)

5 https://wiley.campus.hamburger-fh.de (letzter Abruf am 16.01.2022)

6 Bauer, Medium E-Mail, 2021, S. 2

7 Disterer, Studien- und Abschlussarbeiten schreiben, 2019, S. 66-67

Aufgrund von gefährlichen Halbwahrheiten, persönlichen Meinungen und nicht belegten Tatsachen, wurde auf Quellen wie Blogs, Communityforen und editierbaren Wissensdatenbanken (Wiki) verzichtet. Lediglich in Fällen wo der Autor eines Beitrages, Kommentars oder einer sonstigen Veröffentlichung bereits durch andere wissenschaftliche Leistungen in Erscheinung getreten ist, wurden diese Quellen berücksichtigt. Dies ist z. B. der Fall, wenn ein Fachmann oder Gutachter von einem Gericht zur Entscheidungsfindung angehört wurde und dessen Beitrag wesentlich zur Meinungsbildung beitrug.

Hinderlich war stellenweise bei der Quellen- und Literaturrecherche, dass das Medium E-Mail zwar seit mehr als 40 Jahren existiert[8], häufig jedoch in der Literatur missverständliche Fachbegriffe in Argumentationen falsch verwendet wurden oder das Vorkommen von jeweils deutschen und englischen Ausdrücken zu Problemen bei Vergleichen führten, da nicht immer klar war, was der Autor genau sagen wollte.

Dennoch war in dieser Arbeit die Literaturanalyse das geeignete Mittel um praktische Fragen aus dem Geschäftsalltag – wie der Umgang bzw. die Beweismöglichkeiten im E-Mail-Versand stattfindet – beantworten zu können. Durch den hohen Praxisbezug dieser Arbeit – da heutzutage jedermann täglich selbst E-Mails versendet – ist die Hoffnung, dass zukünftig dadurch die Digitalisierung noch weiter beschleunigt wird und auch das Medium E-Mail, in allen Bereichen als zuverlässiges Transportmittel akzeptiert wird. Bewusst verzichtet wurde in dieser Arbeit darauf, einen theoretischen Fall zu skizzieren. Das nachfolgende Kapitel beginnt mit einem kurzen Abriss der Zustellnachweise im klassischen Briefverkehr und stellt im Anschluss die verschiedenen digitalen Beweismittel in der E-Mail-Kommunikation dar.

8 Crocker, Standard for the format of arpa network text messages, 1977, S. 1

3. Beweismittel als Zustellnachweis – eine Einführung

Schon aus dem 3. Jahrhundert ist durch ein Hibe-Papyrus – der locus classicus – überliefert, dass bei der Postzustellung durch die Verwaltung in Ägypten bereits Protokollbücher geführt wurden, die über die erfolgreiche Post- bzw. Briefzustellung Aufschluss gaben und den Prozess vom Versand bis zum Empfang durch den Adressaten exakt dokumentierten. So ist den übersetzten Aufzeichnungen zu entnehmen, welcher Absender, an welchen Empfänger, zu welcher Uhrzeit durch welchen Postboten, Schriftstücke überbringen ließ[9]. Dies zeigt deutlich, dass schon in früher Zeit nicht nur der Versand von entscheidender Bedeutung war, sondern auch die nachweisbare und dokumentierte Zustellung an den richtigen Empfänger. Im 21. Jahrhundert bieten deshalb nahezu alle Post- und Transportunternehmen einen Zustellnachweis für den Absender an. Nachfolgend ein – nicht vollständiger – Auszug verfügbarer Transportleistungen im deutschsprachigen Raum.

Abb. 1 – Zustellnachweis-Transportdienstleistungen in Deutschland

Transportunternehmen	**Produkte mit Zustellnachweis**
Deutsche Post AG	Einschreiben Nachnahme Prio-Zustellung Einschreiben-Wert
DHL Paket GmbH	Paket mit Sendungsverfolgung
Hermes Germany GmbH	Paket mit Sendungsverfolgung
DPD Deutschland GmbH	Paket mit Sendungsverfolgung
United Parcel Service (UPS)	Paket- und Expressversand mit Verfolgung

Quelle: Eigene Darstellung

Die Paket- und Postnachverfolgung ist auch im Privatbereich nicht mehr wegzudenken. Nahezu kein Online-Shop versendet mehr Waren ohne einen Zustellnachweis. Dies dient der Vermeidung von Betrug und bietet dem Empfänger auch die Echtzeit-Paketnachverfolgung.

Bevor im weiteren Verlauf der Einstieg in die Beweis- und Zustellnachweise im digitalen Versand per Email erfolgt, wird an dieser Stelle noch kurz ein EU-

9 Huß, Die Verwaltungsmaßnahmen. In: Die Verwaltung des ptolemaiischen Reichs, 2011, S. 180-185

Verfahren angesprochen, welches zertifizierten Dienstleistern ermöglicht, qualifizierte elektronische Einschreiben zu transportieren bzw. in Empfang zu nehmen. Zu verstehen ist dahinter ein Zusammenschluss von Dienstleistern, die nach Erfüllung eines Anforderungskataloges berechtigt sind, in der Europäischen Union elektronische Transport- und Zustelllösungen anzubieten, die den Anspruch an ein qualifiziertes elektronisches Einschreiben erfüllen. Die Deutsche Post bietet diesen Dienst unter dem Namen E-POST an[10]. Der rechtliche und technische Rahmen findet sich zusammengefasst in der EU-Verordnung Nr. 910/2014[11] mit dem Namen eiDAS (electronic IDentification, Authentication and trust Services) wieder. Die EU-Verordnung ermöglicht sodann zertifizierten Dienstleistern, auch Zwitterlösungen anzubieten wie z. B. in der Form des E-POST-Produktes, die Annahme von Schriftstücken auf digitalem Weg mit einer Zustellung über den gewohnten Papierbrief in Form eines Einschreibens in den Briefkasten des Empfängers oder die Zustellung eines Schriftstückes in den analogen und digitalen Briefkasten gleichzeitig. Die Deutsche Post hat diese Leistung als „Digitale Kopie“ angekündigt und verspricht sich davon eine erleichterte Integration des Versandes in die internen Abläufe von Unternehmen[12].

Geht man jetzt vom klassischen Papierbrief über zur E-Mail ist festzuhalten, dass die Zustellung einer E-Mail gerade nicht mehr durch eine Person in den Haus-Briefkasten erfolgt, sondern elektronisch durch Server in das Postfach des Empfängers. Um hier die Unterschiede im Detail greifbar und verständlich zu machen, folgt dazu im nächsten Kapitel eine Ausführung, ab wann eine E-Mail als zugestellt gilt.

3.1 Wann gilt eine E-Mail als zugestellt

Bevor die Frage beantwortet werden kann, ab wann eine E-Mail als zugestellt gilt, muss sich der Frage zugewandt werden, ob ein Empfänger in allen Fällen

10 Deutsche Post, Leistungsbeschreibung E-POST, 2021, S. 1-2

11 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910 (letzter Abruf am 16.01.2022)

12 Koenig, Die digitale Kopie von Briefsendungen, Datenschutz und Datensicherheit-DuD, 2019, S. 551

überhaupt erreicht werden will bzw. dafür einen Zugang eröffnet hat. Erst wenn dies zu bejahen ist, kann über diesen Kommunikationsweg eine verbindliche Zustellung erfolgen[13]. Das Verwaltungsverfahrensgesetz (VwVfG) sieht die Zustellung bzw. Übermittlung von elektronischen Dokumenten an den Bürger nur als zulässig an, wenn dieser einen Zugang dazu eröffnet hat[14]. Speziell im Geschäftsverkehr ist dies anzunehmen, wenn ein Unternehmen die eigene E-Mail-Adresse nach außen hin darstellt[15]. Also z. B. auf Flyern, Homepage, Branchenbuch, dem eigenen Briefkopf oder einer Visitenkarte eines Mitarbeiters abdruckt[16]. So führt auch das Bundessozialgericht in einer Entscheidung aus, dass eine auf der Internetseite veröffentliche E-Mail-Adresse – ohne Beschränkung auf bestimmte Gegenstände der Kommunikation – einen Zugang per E-Mail eröffnet[17]. Eine Beschränkung auf bestimmte Gegenstände könnte dahingehend ausgelegt werden bzw. vorliegen, dass eine angegebene E-Mail-Adresse, worüber z. B. nur der externe Datenschutzbeauftragte im Falle einer Anfrage durch eine Weiterleitung sämtlicher Mails an diesen zu erreichen ist, nicht für die übliche Kommunikation mit der Firma selbst, dient und somit gerade kein Zugang eröffnet wurde. Das Bundesverwaltungsgericht konkretisiert in einem anderen Fall in seiner Entscheidung, dass eine Zugangseröffnung zu bejahen ist, wenn in objektiver Hinsicht eine technische Kommunikationseinrichtung auf Empfängerseite gegeben ist. Sowie subjektiv dieser auch damit rechnet bzw. damit rechnen muss, dass darüber Dokumente an ihn übermittelt werden[18]. Dies dürfte so dann nicht angenommen werden, wenn z. B. personalisierte Mailadressen durch den Absender nur erraten wurden oder dieser nur durch Umwege eine E-Mail-Adresse erlangt hat, die der Empfänger nur für die private Kommunikation nutzt. Diese Situationen wären möglich, wenn der Geschäftsführer im privaten Bereich mit einer privaten E-Mail-Adresse auftritt, die aber in keinem Zusammenhang mit der Tätigkeit seiner Firma steht.

13 Specht-Riemenschneider, Internetrecht Vol. 1, 2020, S. 276

14 § 3a Abs. 1 VwVfG

15 Bauer, Medium E-Mail, 2021, S. 25

16 Haug, Grundwissen Internetrecht, 3 Auflage, 2016, S. 380

17 BSG, B 14 AS 51/18 R

18 BVerwG, 6 C 12/15

Die Frage ab wann jetzt ein Schriftstück (Brief, E-Mail) tatsächlich als zugestellt gilt wird für die Willenserklärung im Bürgerlichen Gesetzbuch definiert, sobald der Zugang eröffnet ist.

Eine Willenserklärung, die einem anderen gegenüber abzugeben ist, wird, wenn sie in dessen Abwesenheit abgegeben wird, in dem Zeitpunkt wirksam, in welchem sie ihm zugeht[19]. Der BGH hat hierzu die Empfangstheorie kreiert, die besagt, dass der Zugang zu bejahen ist, wenn eine Erklärung so in den Machtbereich des Empfängers gelangt, dass dieser die Möglichkeit hat, von ihr Kenntnis zu nehmen[20].

Bei der Übertragung von Nachrichten unter Abwesenden erfolgt wie oben dargestellt die Kommunikation nicht auf direktem Weg. Man spricht von asynchroner Übertragung[21]. Eine E-Mail ist somit eine Willenserklärung unter Abwesenden, da die Übergabe nicht direkt durch Anwesende erfolgt. Eine synchrone (gleichzeitige) Übertragung ist anzunehmen, wenn Sender und Empfänger – wie bei einem Telefonat – direkt und zur selben Zeit miteinander sprechen – es also keine Relais oder Zwischenstationen gibt[22].

Das eigene E-Mail-Postfach ist zweifelsfrei im eigenen Machtbereich. Sobald eine E-Mail in den eigenen Machtbereich gelangt, kann über sie verfügt werden. Dies beinhaltet das Lesen, Beantworten oder Löschen einer E-Mail.

Das reine Absenden einer E-Mail durch den Absender begründet noch keine erfolgreiche Zustellung an den Empfänger[23].

Hingegen gilt eine E-Mail, die für den Empfänger abrufbar in seinem E-Mail-Postfach des Providers liegt, als zugestellt[24]. Liegt eine E-Mail zum Abruf für den Empfänger bereit, ist sie ja bereits in dessen Machtbereich gelangt. Hat doch der Empfänger gerade jetzt darüber die Kontrolle, ob er sie abholt oder ignoriert. Aber auch höhere Gerichtsinstanzen vertreten diese Haltung wie das folgende BGH-Urteil zeigt:

19 § 130 Abs. 1 S. 1 BGB

20 Dammann, Zahlung einfordern. In: Effizientes Forderungsmanagement, 2020, S. 17-20

21 Bauer, Medium E-Mail, 2021, S. 26

22 Baun, Computer Networks Bilingual Edition, 2019, S. 20

23 LAG Berlin-Brandenburg, Beschluss vom 27.11.2012 - 15 Ta 2066/12

24 AG Hamburg, Urteil vom 27.04.2018 – 12 C 214/17

„Ein Rechtsanwalt, der einem anderen Rechtsanwalt einen Rechtsmittelauftrag per E-Mail zuleitet, darf nicht allein wegen der Absendung der E-Mail auf deren ordnungsgemäßen Zugang beim Adressaten vertrauen. Er muss vielmehr organisatorische Maßnahmen ergreifen, die ihm eine Kontrolle des ordnungsgemäßen Zugangs ermöglichen.“[25]

Diese Auffassung ist nachvollziehbar. Bestehen doch in der E-Mail-Kommunikation für diesen Fall gerade unterschiedliche Kontrollmethoden der erfolgreichen Zustellung, die im weiteren Kapitel noch detailliert vorgestellt werden um eine nicht erfolgreiche Zustellung zu erkennen und gegebenenfalls zu wiederholen. Ganz wie im Postverkehr, wo ein retournierter – unzustellbarer – Brief nach Korrektur erneut auf den Weg gebracht wird.

Dennoch muss sich ein Empfänger – trotz Zugang – die Kenntnis über den Inhalt nicht sofort zurechnen lassen. Das Landesarbeitsgericht nennt hierzu in seiner Entscheidung, dass, ob die Kenntnis besteht, müsse nach den „gewöhnlichen Verhältnissen“ und den „Gepflogenheiten des Verkehrs“ bewertet werden und führt weiter aus, dass ein Brief, der z. B. zwischen 11:00 – 11:30 Uhr in den Briefkasten des Empfängers gelangt, dafür sorgt, dass der Empfänger noch an diesem Tag davon Kenntnis erlangt[26]. Die Gepflogenheiten des Verkehrs können dahingehend ausgelegt werden, dass üblicherweise ein Briefkasten zu üblichen Geschäftszeiten auch einmal täglich geleert wird. Vergleichsweise wäre es unüblich, dass ein gewerblicher Briefkasten eines Unternehmens nur alle paar Wochen kontrolliert wird. Dies widerspreche dem typischen Interesse eines Unternehmens am Geschäftsverkehr teilzunehmen. Ist doch gerade Brief und E-Mail ein wesentliches Kommunikationsmittel. Übertragen auf das Medium E-Mail stellt das eigene E-Mail-Postfach deshalb ebenso nur einen elektronischen Briefkasten dar, der durch den Abruf geleert, also dessen Inhalt gesichtet wird.

Um die Besonderheiten der elektronischen Nachrichtenübermittlung gegenüber der Postzustellung zu erkennen, folgt im nächsten Kapitel ein Einblick in die

25 BGH, AZ: I ZR 64/13

26 LAG RLP, 10 Sa 175/13

technischen Grundlagen des E-Mail-Transports. Dieses Verständnis ist wichtig um die Unterschiede zwischen den einzelnen Methoden der Beweisführung zu erkennen und so dann auch verständlich vortragen zu können.

3.2 Technische Grundlagen zum E-Mail-Transport

1949 entwickelte Claude E. Shannon und Warren Weaver ihr Modell zur Nachrichtenübertragung welches unter dem Namen Sender-Empfänger-Modell bzw. Shannon and Weaver Modell bekannt ist[27]. Aufgrund des Alters war das damalige zugrundeliegende Medium für das Mathematiker- und Techniker-Duo Shannon und Weaver, das Telefon, welches sich jedoch problemlos auch auf E-Mails bzw. die Nachrichtenübertragung im Internet anwenden lässt. Das Modell skizziert, dass bei jeder Nachrichtenübertragung (Sprache bei einem Telefonat, E-Mail zwischen Absender und Empfänger) jeweils ein Sender existiert sowie ein konkreter Empfänger, der Adressat und die Übertragung selbst, einer Vielzahl von Störungen unterliegen kann. Bei der Telefonie wäre dies ein temporär nicht erreichbarer Anschluss, Rauschen oder unverständliche Sprache. Erkennbarer Unterschied des Modells im Vergleich zur E-Mail ist, dass beim Medium E-Mail, der Absender und Empfänger nicht in direktem Kontakt steht, die Übertragung also nicht synchron stattfindet, sondern asynchron[28].

Grund dafür ist, dass das heutige Internet mit seinen Milliarden von Teilnehmern nicht mehr wie früher zu seinen Anfangszeiten als ARPANET (Advanced Research Projects Agency Network) als geschlossenes und kleines Verteidungsnetzwerk für die US-Armee bzw. exklusive Universitäten ausschließlich zur Verfügung stand, sondern in einer Art und Weise miteinander verschalten ist, so dass die Kommunikation nur über Zwischenstationen – sog. Router – erfolgt[29]. War es früher noch möglich, direkte Kabel bzw. Verbindungen zwischen einem Sender und Empfänger zu verschalten, wäre dies heute – aufgrund des Internets als weltweites Kommunikationsnetzwerk über alle Kontinente hinweg – weder logistisch noch wirtschaftlich sinnvoll und auch nicht mehr technisch wartbar.

27 Bauer, Medium E-Mail, 2021, S. 3

28 Röhner, Psychologie der Kommunikation, 2020, S. 19-22

29 Crocker, The Arpanet and Its Impact on the State of Networking, 2019, S. 4

Der E-Mail-Versand verläuft nach einem zertifizierten Standard in einer vordefinierten Reihenfolge[30]. Dies ist notwendig, da sich sonst alle beteiligten Parteien nicht miteinander verständigen könnten und im Fehlerfall keine einheitlichen Regeln für die Kommunikation existieren würden. Die Fehlersuche und Entstörung wäre aufwendig und jeweils individuell. Das zugrundeliegende Protokoll SMTP wurde im technischen Standard RFC5321[31] beschrieben. SMTP steht für Simple Mail Transfer Protocol und ist ausschließlich für den Versand von E-Mails. Die Abholung von E-Mails – wie aus dem Postfach des eigenen E-Mail-Anbieters – mit einem E-Mail-Programm, verwendet nicht das SMTP-Protokoll. Hierzu kann wahlweise das POP3 oder IMAP-Protokoll verwendet werden. IMAP wird bevorzugt, wenn mehrere Endgeräte mit dem selben E-Mail-Bestand arbeiten möchten bzw. die E-Mails selbst, auf dem Server des Anbieters verbleiben soll[32]. Eine E-Mail durchläuft auf dem Weg zum Ziel mehrere Zwischenstationen (Mailserver). Damit diese sich verstehen, operieren alle nach dem dargestellten SMTP-Standard. Im einfachsten Übermittlungsfall spricht der Mailserver des Absenders direkt mit dem Mailserver des Empfängers. Dies ist jedoch – aufgrund der Struktur des Internets – nicht immer direkt möglich. Häufig sind Systeme zwischenzeitlich nicht erreichbar, E-Mails werden weitergeleitet oder Störungen verhindern die Übermittlung. Die Übergabe einer E-Mail von einem Mailsystem an das Mailsystem des Empfängers, erfolgt schematisch in nachfolgender Reihenfolge. Zur Steigerung der Verständlichkeit wird die Übermittlung einer E-Mail, der Zustellung eines Briefes gegenübergestellt. Da bei der E-Mail-Übertragung die Mailserver in einer technischen Sprache miteinander sprechen (SMTP-Protokoll) gibt es hierzu für die einzelnen Schritte der Übermittlung Befehle, die sogenannten Kommandos. Die mit Zahlen vorangestellten Kommandos in der Übersicht sind jene, die der empfangende Mailserver von sich gibt. Jeder Befehl ist einem numerischen Code zugeordnet, welcher für eine bestimmte Operation steht[33].

30 Bauer, Medium E-Mail, 2021, S. 27

31 https://datatracker.ietf.org/doc/html/rfc5321 (letzter Abruf am 16.01.2022)

32 Baun, Computer Networks Bilingual Edition, 2019, S. 207-208

33 Strzyzewski, Generierung von qualifizierten E-Mail-Adressen, 2019, S. 31

Abb. 2 – Schematische Gegenüberstellung einer Post- und E-Mail-Übertragung

E-Mail	**Briefpost**
220 mx1.securepostfach.de ESMTP	Gegenseitige Vorstellung von Sender und
EHLO cubewerk.de	Absender. Dies passiert nur bei Einschreiben-
250-mx1.securepostfach.de	Zustellungen bzw. persönlichen Übergaben.
MAIL FROM: <stefan@cubewerk.de>	Absender-Adresse auf dem Briefumschlag
250 2.1.0 Ok	
RCPT TO: <max@plzk.de>	Empfänger-Adresse auf dem Briefumschlag
250 2.1.5 Ok	
DATA	
354 End data with .	
Message-ID: <fortlaufende@kennung>	Interner Vermerk. Eindeutige Briefkennung
Date: Fri, 28. Jan 2022 10:15:27 +0000	Datum auf Schriftstück im Brief
From: Stefan Bauer <stefan@cubewerk.de>	Absender auf Schriftstück im Brief
To: Max Mustermann <max@plzk.de>	Empfänger auf Schriftstück im Brief
Subject: Hallo Max, anbei meine Bestellung	Betreff auf Schriftstück im Brief
Hallo Max, wie versprochen sende ich Dir nachfolgend meine Bestellung. Ich freue mich. Bis bald. Stefan Bauer	Eigentlicher Text auf Schriftstück im Brief
.	Einwurf des Briefes in Briefkasten
250 2.0.0 Ok: queued as DTDD7G01D4	Bestätigung der Annahme durch Empfänger.

Quelle: Eigene Darstellung in Anlehnung[34]

Der Dialog selbst erfolgt i.d.R. innerhalb weniger Sekunden vollautomatisch. Wichtig zu erwähnen ist der Punkt „.“ in der vorletzten Zeile. Dies ist die

34 Wittmaack, Vertrauensvolle E-Mail-Kommunikation, Datenschutz Und Datensicherheit – DuD 2016, S. 3

Signalisierung des Absenders, dass die Nachrichtenübertragung abgeschlossen ist[35]. Darauf folgt im Erfolgsfall der Statuscode „250“ durch den Empfänger, welcher die erfolgreiche Annahme – also die Zustellung – quittiert.

Nachdem die Grundlagen einer E-Mail-Übertragung jetzt vermittelt wurden, werden im nächsten Kapitel die einzelnen Beweismöglichkeiten erörtert und detailliert ausgeführt. Es folgt die Übermittlungsbestätigung (DSN).

3.3 Die Übermittlungsbestätigung (DSN)

Wie zuvor ausgeführt, liegen i.d.R. allen technischen Abläufen bzw. Protokollen, jeweilige Beschreibungen – die Standards – zugrunde. Diese finden sich in RFCs (Request for Comments) wieder. Für die Übermittlungsbestätigung (DSN) existiert RFC3464[36]. DSN steht für Delivery Status Notification. DSN selbst kann als eigenständige E-Mail angesehen werden, die der Absender als eine Art elektronische Zustellquittung erhält. Mit DSN werden mehrere Ziele verfolgt (nicht abschließend):

- Benachrichtigung des Absenders über den Status der Nachrichtenübertragung inkl. ggf. der Gründe bzw. Fehlermeldungen bei einer gescheiterten Übertragung
- E-Mail-Programmen die Möglichkeit zu geben, eine DSN einer erfolgreichen oder gescheiterten Zustellung, einer zuvor versandten E-Mail zuordnen zu können
- Den Übertragungsstatus in einer sprach- und mediumunabhängigen Art und Weise darzustellen[37].

Eine DSN selbst ist textbasiert und trifft als E-Mail in das Postfach des Absenders ein. Im Fall eines falsch adressierten Briefes erhält der Absender

35 Bauer, Medium E-Mail, 2021, S. 29

36 https://datatracker.ietf.org/doc/html/rfc3464 (letzter Abruf am 16.01.2022)

37 Moore, An Extensible Message Format for Delivery Status Notifications, 2003, S. 3

des Briefes die Unzustellbarkeitsmeldung per Post inkl. seinem Schriftstück zurück. Also üblicherweise den eigenen Brief mit einem Vermerk zurück. Hieraus ist erkennbar, dass auch eine DSN zwingend an den ursprünglichen Absender gerichtet sein muss. Analog zum Postversand kann bei einem Brief ohne gültigen Absender nur schwer eine Unzustellbarkeitsmeldung erfolgen. Im Briefverkehr existiert hier die Briefermittlungsstelle der Deutschen Post AG, die in Marburg Briefe mit ungültigem Absender durch Öffnen der Briefe ermittelt und sodann retourniert[38]. Generell unterliegt der Inhalt von Briefen dem Postgeheimnis. Dies wird jedoch zur Feststellung von Empfänger und Absendern durch § 39 Abs. 4 PostG ausgenommen um auch den Inhalt zur Recherche des Absenders bzw. Empfängers zu nutzen.

Diese – durchaus sinnvolle – Adressermittlung ist bei automatisch verarbeiteten E-Mails nicht vorgesehen und findet nicht statt. E-Mails mit ursprünglich falschem bzw. verschleiertem Absender erhalten deshalb auch nie eine DSN. Um zu vermeiden, dass unzustellbare E-Mails für immer aufbewahrt werden, existiert ein empfohlenes Ablaufdatum von 4-5 Tagen, welches der verantwortliche Mailserver-Administrator selbst individuell festlegen kann[39]. Ist der Absender einer E-Mail, also der vorgesehene Empfänger der DSN-Nachricht ungültig, wird die E-Mail gelöscht. Ist der Absender nur temporär nicht erreichbar bzw. nicht zu ermitteln, erfolgen fortlaufend Zustellversuche, bis das genannte Ablaufdatum von 4-5 Tagen überschritten ist.

Im weiteren Verlauf muss nun herausgearbeitet werden, welche Entität unter welchen Umständen eine DSN generiert und ob dies in allen Fällen erfolgt. Im E-Mail-Versand sind wie oben dargestellt häufig mehrere Mailserver beteiligt. Eine mögliche Übermittlung stellt sich wie folgt dar:

Abb. 3 – Beteiligte Entitäten bei der Anforderung & Generierung einer DSN

E-Mail-Programm des Absenders	=>	Server des Absenders bzw. dessen Providers	=> DSN-generierender Server	=> Server des Empfängers

Quelle: Eigene Darstellung in Anlehnung[40]

38 Abels, Der Brief: eine Kulturgeschichte der schriftlichen Kommunikation, 1996, S. 288-292

39 Klensin, Simple Mail Transfer Protocol, 2008, S. 67

40 Moore, An Extensible Message Format for Delivery Status Notifications, 2003, S. 5

Hieraus ist erkennbar, dass eine E-Mail im E-Mail-Programm des Absenders erzeugt wird und sodann an den E-Mail-Server des eigenen E-Mail-Anbieters bzw. in firmeninternen Umgebungen an den eigenen Mailserver übermittelt wird. Dieser stellt dann den weiteren Transportweg fest und übermittelt die E-Mail weiter an den finalen Empfänger. Festzuhalten ist, dass der DSN-generierende Server jeweils jener Mailserver ist, der als letztes Glied in der Kette, die E-Mail an den Mailserver des Empfängers übergibt. Also an jenen Mailserver, der öffentlich erkennbar für die Domain des Empfängers als verantwortlicher Mailserver hinterlegt wurde. Hierzu existieren DNS MX-Einträge im DNS-Server für die Empfängerdomain[41]. Ein DNS-Server kann mit einem globalen Telefonbuch verglichen werden, wo eine Zuordnung zwischen Mail-Domain (der Teil hinter dem @-Zeichen) und den dafür zuständigen Mailservern für die Annahme vorgenommen wird.

Die verantwortlichen Mailserver können mit dem Befehl „nslookup“ einfach in jedem Betriebssystem abgefragt werden und stellen sich am Beispiel der Domain „cubewerk.de“ wie folgt dar:

nslookup -type=MX cubewerk.de

cubewerk.de mail exchanger = 10 mx2.securepostfach.de.

cubewerk.de mail exchanger = 10 mx3.securepostfach.de.

Hier ist erkennbar, dass die zuständigen Mailserver „mx2.securepostfach.de“ und „mx3.securepostfach.de“ sind. Diese Einträge können sich ändern. Nämlich wenn zukünftig andere Mailserver die E-Mails annehmen sollen. Deshalb prüfen übermittelnde Mailserver in regelmäßigen Abständen, ob die Einträge im DNS noch aktuell sind und aktualisieren ihre zwischengespeicherten Informationen bei Bedarf dementsprechend.

41 Schwenk, Sicherheit und Kryptographie im Internet, 2020, S. 332

Der Mailserver, der somit als letzte Instanz die zuzustellende E-Mail an das Zielsystem übergibt, erkennt im Dialog mit dem empfangenden SMTP-Server, ob die Zustellung erfolgreich, gescheitert, oder temporär nicht möglich ist. Bei einer erfolgreichen Zustellung ist die Situation einfach. Dem übergebenden Mailserver wird die Übergabe der E-Mail vom Zielsystem mit der Ausgabe

„250 2.0.0 Ok: queued as DTDD7G01D4“

(vgl. Abb. 2) quittiert. „DTDD7G01D4“ ist eine zufällig vergebene Nachrichten-ID des Empfangssystems. Hier quittiert also das empfangene Mailsystem nicht nur die Einlieferung mit „250 2.0.0 Ok“ sondern bestätigt auch durch eine selbst und zufällig erzeugte Zeichenfolge, dass die E-Mail sodann im Mailsystem des Empfängers unter der Kennung „DTDD7G01D4“ registriert wurde. Übertragen auf das Briefpostsystem wäre dies vergleichbar mit einer erfolgreichen Empfangsbestätigung inkl. Unterschrift des Empfängers oder einer Person seines Haushaltes bzw. ein Empfangsbevollmächtigter. Ob hier der Mailserver des Empfängers oder eben der Mailserver seines vorgeschalteten Providers die Mail annimmt und somit u.u. nicht der Empfänger selbst ist irrelevant. Der Provider ist nur der ausgewählte und somit durch den Empfänger/Kunden eingesetzte Gehilfe, welcher im Interesse des Kunden handelt. Und so normiert auch das Bürgerliche Gesetzbuch:

Der Schuldner hat ein Verschulden (...) der Personen, deren er sich zur Erfüllung seiner Verbindlichkeit bedient, in gleichem Umfang zu vertreten wie eigenes Verschulden[42].

In Fällen wo der übermittelnde Mailserver jedoch bei der Übergabe der E-Mail temporär scheitert, werden innerhalb der o.g. Ablaufzeit weitere Zustellversuche unternommen. Wie bereits ausgeführt für bis zu 5 Tage. Scheitern alle Versuche, erhält der Absender eine DSN über die gescheiterte Zustellung. Dies kann verglichen werden mit dem Postzusteller, der an mehreren unterschiedlichen Tagen versucht, ein Einschreiben persönlich zu übergeben und es am Ende als unzustellbar zurück an den Absender sendet. In Fällen wo jedoch der Empfangsmailserver bereits beim ersten Zustellversuch die E-Mail

42 § 278 BGB

ablehnt oder nicht annehmen kann oder will, erfolgt hierüber umgehend eine DSN. Gründe für eine sofortige Unzustellbarkeit sind, dass das adressierte Postfach auf dem Ziel-Mailsystem nicht (mehr) existiert, dauerhaft voll ist oder aufgrund eines technischen Fehlers permanent keine Nachrichten angenommen werden können. Ganz wie im Briefverkehr, wo der Empfänger unter einer bestimmten Postanschrift nicht erreichbar ist (kein Briefkasten, kein beschrifteter Briefkasten) oder die Sendung konkludent abgelehnt wird. Die laut RFC3464 möglichen Zustände einer Zustellung sind

failed	→	*fehlgeschlagen*
delayed	→	*verzögert*
delivered	→	*erfolgreich zugestellt*
relayed	→	*zur endgültigen Zustellung weitergeleitet*
expanded	→	*zugestellt, jedoch für einen erneuten Weitertransport vermerkt*[43]

Wissenswert an dieser Stelle ist, dass es vom DSN-generierenden Mailsystem abhängt (vgl. Abb. 3) ob DSN-Nachrichten erzeugt werden oder nicht. Nicht alle Mailsysteme bzw. Anbieter generieren DSN-Nachrichten. Es handelt sich dabei um eine i.d.R. konfigurierbare Einstellung der Mailserver-Anwendung. Wie nachfolgend zu erkennen, gibt es sogar E-Mail-Anbieter, die eine laut Standard freie und vorgesehene Funktion zur Zustellverfolgung, bewusst deaktivieren um sie als kostenpflichtige Zusatzleistung wiederum anzubieten[44]. In allen Fällen muss ein DSN-Bericht vom Absender bereits beim Versand über einen Schalter in seinem E-Mail-Programm explizit angefordert werden. Aufgrund unterschiedlicher Übersetzungen und Produktbegriffe, unterscheidet sich diese Funktion namentlich wesentlich von Programm zu Programm. Nachfolgend eine – nicht vollständige – Aufstellung von Bezeichnungen für die Anforderung eines DSN-Berichtes in unterschiedlichen Anwendungen.

43 Moore, An Extensible Message Format for Delivery Status Notifications, 2003, S. 17

44 Bauer, Medium E-Mail, 2021, S. 33

Abb. 4 – DSN-Funktionsbezeichnung in unterschiedlichen Mailclients

Mailclient	**Funktionsbezeichnung**
Microsoft Outlook	Zustellbestätigung anfordern
Mozilla Thunderbird	Übermittlungsstatus (DNS) anfordern
web.de Webmail	E-Mail Einschreiben (kostenpflichtig)
Mutt Mailclient	Delivery Status Notification

Quelle: Eigene Darstellung

Unabhängig von der Anforderung eines DSN-Berichtes erhält der Absender immer eine Benachrichtigung, wenn eine E-Mail nicht zugestellt werden konnte. Das Ausbleiben einer Unzustellbarkeitsnachricht ist jedoch kein sicherer Beweis, dass die E-Mail auch zugestellt wurde. Ferner ist es primär – wie bereits ausgeführt – von der jeweiligen Konfiguration eines Mailservers abhängig, ob die DSN-Berichte generiert und an den ursprünglichen Absender übermittelt werden. Ob also der Mailserver den Wunsch des Absenders erfüllt, einen DNS-Bericht zu erzeugen.

Abb. 5 – Standardmäßige Einstellungen von E-Mail-Servern zur DSN-Funktion

Mailserverprodukt	**DSN standardmäßig aktiv**	**DSN konfigurierbar**
Microsoft Exchange 2019[45]	Nur für unzustellbare Mails.	Ja. Durch Rechteanpassung pro Benutzer.
Postfix Mailserver[46]	Aktiv für jeden Status.	Ja.
Exim Mailserver[47]	Nur für unzustellbare Mails.	Ja.
HCL Domino (IBM Lotus Notes)[48]	Nur für unzustellbare Mails.	Ja.

Quelle: Eigene Darstellung

45 https://docs.microsoft.com/de-de/Exchange/permissions/feature-permissions/mail-flow-permissions?view=exchserver-2019 (letzter Abruf am 16.01.2022)

46 http://www.postfix.org/DSN_README.html (letzter Abruf am 16.01.2022)

47 https://exim.org/exim-html-4.94/doc/html/spec_html/ch-main_configuration.html (letzter Abruf am 16.01.2022)

48 https://help.hcltechsw.com/domino/11.0.0/conf_definingwhentosendtransferanddeliverydelayreports_t.html (letzter Abruf am 16.01.2022)

Sind alle Voraussetzungen durch den DSN-generierenden Mailserver erfüllt und hat der Absender einen DSN-Bericht angefordert, erhält dieser automatisiert einen Statusbericht zur jeweiligen Mailzustellung. Da eine DSN jedoch wie eine übliche E-Mail auf dem selben Transportweg übermittelt wird, unterliegt diese auch Übertragungs- und Zustellungsproblemen und kann auf dem Übertragungsweg untergehen. Zu erwähnen sei ein Spamfilter oder Virenscanner der selbstständig E-Mails aussortiert oder ablehnt.

Leider hat der Absender nicht immer Einfluss auf den DSN-generierenden Mailserver. In diesen Fällen kommt die Lesebestätigung als Beweismittel in Frage. Diese wird im nächsten Kapitel vorgestellt.

3.4 Die Lesebestätigung (MDN)

Die Lesebestätigung (MDN) ist ein alternatives Instrument um die erfolgreiche Mailzustellung nachzuweisen. Weiter noch, sie kann als höherwertiges Beweismittel im Vergleich zu DSN angesehen werden, da sie nicht nur die Zustellung – die für sich betrachtet bereits ausreichen würde – dokumentiert, sondern ebenso die unmittelbare Kenntnisnahme einer E-Mail durch den Adressaten aufgrund einer aktiven Handlung dessen. Der Quittierung der Nachricht gegenüber dem Absender als empfangen bzw. gelesen. Die Lesebestätigung wird im RFC3798[49] unter dem sperrigen Begriff „Message Disposition Notification“ (MDN) erfasst. Erklärte Ziele einer MDN sind:

- Die Benachrichtigung des Absenders nach einer erfolgreichen Mailzustellung, dass seine E-Mail auch verarbeitet wurde

- Die Zuordnung von Verarbeitungsberichten des Empfängers, zu tatsächlich versandten E-Mails

- Den Verarbeitungsstatus in einer sprach- und mediumunabhängigen Art und Weise darzustellen[50]

49 https://datatracker.ietf.org/doc/html/rfc3798 (letzter Abruf am 16.01.2022)

50 Hansen, Message Disposition Notification 2004, S. 3

Eine MDN wird – analog zu SDN – in der Form einer Text-E-Mail an den Absender gesendet und enthält häufig auch einen Auszug jener Nachricht, deren Empfang bestätigt wird[51]. Auch die Übermittlung einer MDN kann wie die SDN – und alle anderen E-Mails – bei der Übertragung scheitern oder untergehen.

Wie bei einer SDN muss der Absender der E-Mail zum Zeitpunkt des Versandes in seinem E-Mail-Programm eine MDN anfordern. Auch hier existieren je nach eingesetztem E-Mail-Programm unterschiedliche Namen für diese Funktion.

Abb. 6 – Funktionsname für MDN-Einstellungen gängiger E-Mail-Clients

Mailclient	**Funktionsbezeichnung**
Microsoft Outlook	Lesebestätigung anfordern
Mozilla Thunderbird	Empfangsbestätigung anfordern (MDN)
web.de Webmail	Lesebestätigung
Evolution Mailclient	Lesebestätigung anfordern

Quelle: Eigene Darstellung

Wie stellenweise schon ausgeführt, bedarf es für den Empfang einer MDN zweier Dinge. Die Anforderung einer MDN durch den Absender in seinem eigenen E-Mail-Client, sowie die aktive Handlung des Empfängers in seinem – also die Auslösung einer MDN.

Wesentlicher Unterschied zu SDN ist, dass eine SDN selbst, automatisiert durch einen Mailserver erzeugt wird und dies für den Empfänger völlig unbemerkt erfolgt und er diese auch i.d.R. nicht unterbinden kann[52]. Eine MDN hingegen wird durch den Empfänger manuell oder durch Standardeinstellungen seines E-Mail-Clients ausgelöst. Im Vergleich zur Briefpost wäre eine SDN ein Einwurf-Einschreiben, welches der Postbote dem Absender als „in den Briefkasten geworfen“ quittiert. Eine MDN hingegen wäre eine Bestätigung des Empfängers, dass er Kenntnis über den Brief im eigenen Briefkasten erlangt hat, also das Einschreiben mit persönlicher Übergabe.

51 Hansen, Message Disposition Notification 2004, S. 7

52 Bauer, Medium E-Mail, 2021, S. 33

Der Standard für MDN sieht mehrere Zustände vor, die der Empfänger dem Absender quittieren kann[53]. Diese sollen an dieser Stelle jedoch nicht weiter ausgeführt werden, da diese beweisunerheblich sind. Für den Absender ist es ausschließlich relevant, ob eine Zustellung erfolgte bzw. der Empfänger sich eine E-Mail zurechnen lassen muss. Deshalb ist es unbedeutend, welchen Status der Empfänger dem Absender quittiert. In allen Fällen ist zu diesem Zeitpunkt die E-Mail selbst, bereits zugestellt.

Aufgrund der weitreichenden rechtlichen Konsequenzen einer automatischen Empfangsbestätigung durch den E-Mail-Client des Empfängers, neigen viele Unternehmen dazu, diese Art der Bestätigung firmenweit über Richtlinien zu deaktivieren[54]. Dem Anwender bzw. Mitarbeiter also die individuelle Möglichkeit zu nehmen, eigenmächtig empfangene E-Mails zu bestätigen. In Microsoft-Windows Umgebungen ist dies durch Gruppenrichtlinien[55] zu erreichen. Generell handelt es sich um eine oder mehrere Einstellungen pro E-Mail-Client.

Im weiteren Verlauf soll die Möglichkeit vorgestellt werden über Transportprotokolle der eigenen übermittelnden Mailserver eine Zustellung nachzuweisen.

3.5 Das Mailserverprotokoll

Die Aufzeichnung von Ereignissen in IT-Systemen in Form von Protokollen ist gängige Praxis. Aber auch außerhalb der IT, finden Protokolle Anwendung. So wird z. B. der Einlass von Personen, die Ausgabe von Waren oder Artikel oder die Dauer von Arbeitsleistungen genau dokumentiert. Sie dienen der nachträglichen Rekonstruktion von Vorgängen und können als Beweismittel herangezogen werden[56]. Hierunter fällt ebenso die Erfassung der Mailserver-Ereignisse während einer Zustellung. Wie zuvor bereits ausgeführt, quittiert ein

53 Hansen, Message Disposition Notification, 2004, S. 17

54 Bauer, Medium E-Mail, 2021, S. 34

55 https://docs.microsoft.com/de-de/windows-server/networking/branchcache/deploy/use-group-policy-to-configure-domain-member-client-computers (letzter Abruf am 16.01.2022)

56 Pohlmann, Cyber-Sicherheit, 2019, S. 308

empfangender Mailserver die Annahme einer E-Mail in Form eines standardisierten Codes sowie einer selbst und fortlaufend vergebenen Kennung, der Sendungs- oder Quittungs-ID. Diese Information schreibt so dann der empfangene und übermittelnde Mailserver in das eigene Übertragungsprotokoll. In der Vergangenheit sind jedoch immer wieder Mailprovider[57] aufgefallen, die aus Datenschutzgründen damit werben, keine Protokolle zu erstellen. Die Protokollierung selbst führen die E-Mail-Server automatisch durch und schreiben die Ereignisse chronologisch in eine Textdatei oder Datenbank mit jeweils dazugehörigem Zeitstempel. In dieser Datenbank bzw. Textdatei kann nachträglich nach Kriterien wie der Empfänger- oder Absenderadresse oder einem bestimmten Zeitfenster gesucht werden um einen Übermittlungsvorgang zu belegen. Exemplarisch nachfolgend ein – vereinfachter – Protokollauszug der erfolgreichen Übergabe einer E-Mail an das Empfangs-Mailsystem.

00:40:32 4406B5F523: from=<stefan@cubewerk.de>, size=4431

00:40:36 Connection established to gmail-smtp-in.l.google.com TLSv1.3

00:40:38 4406B5F523: to=<mustermann@gmail.com>, relay=gmail-smtp-in.l.google.com status=sent (250 2.0.0 OK 1640562038 x10si7309113wmc.104 – gsmtp)

Nachfolgend soll das Protokoll bzw. der Informationsgehalt kurz übersetzt werden:

00:40:32 Eingang einer E-Mail von stefan@cubewerk.de am Absender-Mailsystem

00:40:36 Verbindungsaufbau zum Ziel-Mailsystem inkl. verwendete Verschlüsselung

00:40:38 Erfolgreiche Übergabe der E-Mail (250 2.0.0 OK) an das Mailsystem von Google mit dem Namen (gmail-smtp-in.l.google.com) für den

57 https://www.theregister.com/2021/09/07/protonmail_hands_user_ip_address_police/ (letzter Abruf am 16.01.2022)

Empfänger (mustermann@gmail.com) und Bestätigung der Annahme der E-Mail durch den Empfänger durch Bereitstellung einer fortlaufenden eindeutigen Nachrichten-ID (1640562038 x10si7309113wmc.104 – gsmtp).

Das Mailserverprotokoll enthält nahezu identische Informationen wie eine empfangene SDN. Dies hat den Grund, da der Mailserver i.d.R. jene Entität ist, die die SDN auch generiert. Da nicht davon auszugehen ist, dass der Empfänger einen Einblick in seine eigenen Protokolle zulässt, da er sich dadurch selbst belasten könnte, stehen nur die eigenen Protokolle des eigenen Mailsystems zur Verfügung. Der Inhalt eines Mailserverprotokolls kann nicht vollumfänglich den Informationen einer SDN gleichgesetzt werden. Zwar beinhalten SDN sowie Protokolle die Informationen über die generelle Übermittlung, jedoch hängt an einer SDN üblicherweise ein Teil der ursprünglichen E-Mail als Zitat an, was zumindest den Nachweis vereinfacht, dass die SDN tatsächlich auch zweifelsfrei einer konkreten E-Mail zuzuordnen ist. Für Einblicke in die Protokolle des eigenen Mailservers ist üblicherweise eine Abstimmung mit der IT-Abteilung in Verbindung mit dem Betriebsrat nötig, da diese Protokolle personenbezogene Informationen in Form von Kommunikationsbeziehungen enthalten. Es handelt sich hierbei um Metainformationen. Nämlich wer kommuniziert – erfolgreich oder nicht – wann, mit wem und wie häufig, ohne einen konkreten Bezug zu einem Inhalt[58]. Der Abruf bzw. die Einsicht in zentrale Protokolle stellt einen erhöhten Aufwand dar, da dies häufig außerhalb der Möglichkeiten des Absenders liegt und Mailprotokolle auch häufig als flüchtig anzusehen sind. Um Speicherplatz zu sparen, rotieren üblicherweise Protokolle in einem Wochen- oder Monatsrhythmus und überschreiben sich selbst. Dem kann durch ein WORM-System entgegen gewirkt werden. WORM steht für „write once, read many“ und bezeichnet ein Speichersystem, welches das Überschreiben bzw. Löschen von Daten bzw. Informationen verhindert und somit nur ein Anhängen von Daten ermöglicht[59]. Dies ist hilfreich um auch ein irrtümliches Überschreiben zu verhindern. Ein WORM-System ersetzt keine regelmäßige Datensicherung.

58 Mittag, Statistik, 2020, S. 30

59 Pohlmann, Cyber-Sicherheit, 2019, S. 145

Nach der Darstellung von SDN, MDN sowie die Möglichkeit der lokalen Auswertung von Systemprotokollen, soll im nächsten Kapitel der Einsatz von Tracking-Pixel bzw. versteckter Inhalte in E-Mails ausgeführt werden.

3.6 Tracking-Pixel und versteckte Inhalte in E-Mails

Für die Formatierung bzw. Darstellung von E-Mails existieren mehrere Optionen. Die gängigste Methode ist die rein textbasierte Darstellung sowie die Formatierung einer E-Mail in der Form einer webseitenähnlichen Struktur in HTML-Code. Der Versand von rein textbasierten E-Mails gestattet keine weitere Formatierung wie die farbliche Hervorhebung oder die direkte Integration von Bildern, Videos, anklickbaren Links oder weiteren Medien. Bietet jedoch die größte Kompatibilität über alle weltweiten E-Mail-Anwendungen hinweg, da die Darstellung von reinem Text wenig Ansprüche an das darzustellende Mailprogramm stellt und auch reibungslos auf älteren Geräten funktioniert. HTML hingegen erlaubt die Formatierung und grafische Aufbereitung von E-Mails. Also die Ausgestaltung von E-Mails. Ebenso den Einsatz von Zähl-Pixel, den sogenannten Tracking-Pixel[60].

Zählpixel sind unsichtbare Bilder in HTML-basierten E-Mails, welche aufgrund ihrer Größe von 1 Pixel und häufig in weißer Farbe auf weißem Hintergrund, in einer E-Mail nicht sofort erkannt werden können. Diese jedoch aufgrund der Art und Weise wie die E-Mail erstellt wurde nicht Teil der eigentlichen E-Mail selbst sind, sondern durch einen Verweis, von einer externen Webseite erst nach dem Empfang nachgeladen werden. Dies ist vergleichbar mit Internetseiten, die Videos von Medienplattformen wie z. B. YouTube in die eigene Homepage einbinden. Der Inhalt selbst – also das eigentliche Video – jedoch beim Aufruf der Internetseite von extern erst nachgeladen werden. Da dieses Nachladen technisch ein Abruf von fremden Inhalt darstellt, taucht dieser Zugriffsversuch auch im Protokoll der externen Webseite auf. Wie stellt sich dies am Beispiel einer E-Mail schematisch dar:

1. Der Absender übermittelt eine unscheinbare E-Mail an den Empfänger und bindet neben dem üblichen Inhalt der E-Mail und einem Anhang wie z. B. eine

60 Lammenett, E-Mail-Marketing. In: Praxiswissen Online-Marketing, 2019, S. 107

Rechnung, auch ein verstecktes Zähl-Pixel ein, welches er nicht direkt in die E-Mail integriert, sondern von seiner eigenen Homepage unter der Adresse

http://zaehlpixel.cubewerk.de/pixel37343.png

als Verweis darauf nachladen lässt.

2. Der Empfänger erhält diese E-Mail und öffnet diese. Der E-Mail-Client des Empfängers lädt alle externen Bilder in der E-Mail nach um eine optimale Darstellung des in der Regel aufeinander abgestimmten Textes und der Bilder zu erreichen. Dieses Nachladen veranlasst den E-Mail-Client des Empfängers so dann, von der externen Webseite

http://zaehlpixel.cubewerk.de/pixel37343.png

das Bild und ggf. weiterer Bildern/Medien abzurufen.

3. Im Webserver-Protokoll des Absenders taucht ein Eintrag in folgender Form auf:

1.2.3.4 – - [27/Dec/2021:01:45:49 +0100] "GET /pixel37343.png HTTP/1.1" 200 6096 "-" "Thunderbird/78.14.0"

1.2.3.4 steht hier für die öffentliche IP-Adresse des Empfängers gefolgt von einem Zeitstempel und im hinteren Bereich, der dokumentierte Abruf des eindeutig hinterlegten Zähl-Pixels (pixel37343.png).

4. Der Empfänger besitzt somit ein Beweisstück welches dokumentiert, dass ein Dritter (in der Regel der Empfänger, da nur dieser die exakte Adresse des Zähl-Pixels kennt) eine E-Mail erhalten haben muss, wodurch er erst Kenntnis von der Zähl-Pixel-Adresse erlangt hat, welcher er anschließend abgerufen hat.

5. Wird jetzt im weiteren Verlauf der Erhalt der Rechnung nach mehreren Mahnungen bestritten, existiert ein Beweismittel in Form eines Abrufprotokolls.

Häufig ist der Dateiname des Zähl-Pixels personalisiert und lässt eine direkte Zuordnung zur abgeschickten E-Mail des Absenders zu. Die Verwendung von Zähl-Pixel findet oft auch beim Versand von Newslettern Anwendung, da hierdurch überwacht werden kann, welche E-Mails bzw. ob E-Mails von einem bestimmten Kundenkreis gelesen werden oder ob ein bestimmtes Angebot besonderes Interesse auslöst. In Kombination mit der Abrufuhrzeit kann sogar festgestellt werden, zu welchen Zeiten bestimmte Personengruppen E-Mails sichten und mit welchem E-Mail-Programm dies erfolgte. Häufig hinterlassen die E-Mail-Programme beim Abruf im Protokoll sogar ihre eigenen Softwarestand („Thunderbird/78.14.0“) *wie im o.g. Auszug ersichtlich.*

Der Einsatz von Zähl-Pixel setzt voraus, dass der Absender die Hoheit über einen Webserver besitzt, für welchen er die Log-Dateien auslesen kann. Ebenso, dass das eingesetzte E-Mail-Programm des Empfängers, externe Bilder automatisiert nachlädt oder der Empfänger das Nachladen manuell anstoßt. Häufig muss dies erst einmal manuell bestätigt werden.

Zusätzlich oder alternativ enthalten E-Mails oft einen Link, welcher den Empfänger dazu auffordert, eine E-Mail in einer Web-Version für die bessere Darstellung, zu lesen. In welchem Verhältnis ein Empfänger eher einem Verweis auf eine externe Seite folgt oder eine Lesebestätigung bestätigt, wurde nicht weiter untersucht. Es darf jedoch davon ausgegangen werden, dass bei der Aufforderung des Empfängers, eine Lesebestätigung zu bestätigen dem Empfänger bewusst sein dürfte, was er hier aktiv bestätigt, also dass er dem Absender eine Zustellung quittiert. Wogegen der Klick eines unscheinbaren Links, die technische Möglichkeit der Dokumentierbarkeit aufgrund Unwissenheit des Empfängers, eher verschleiert.

Nach der abschließenden Vorstellung der möglichen Beweiserhebungsmethoden für die erfolgreiche E-Mail-Zustellung, folgt im nächsten Kapitel eine kurze Beschreibung der Zivilprozess-Grundsätze sowie der Fallstricke bei der Beweiserhebung bzw. Konservierung.

4. Prozessführung und Beweisqualität

Steht man nun in einem Zivilprozess vor deutschen Gerichten greift der Beibringungsgrundsatz welcher besagt, dass es den beteiligten Parteien überlassen ist, die nötigen Beweise beizubringen die für die eigene Partei förderlich sind. Also jene Beweise dem Richter vorzulegen, welche die eigenen Behauptungen unterstreichen bzw. dokumentieren. Dies sind sodann SDN, MDN sowie Mail- und Webserverprotokolle. Zusätzlich normiert die Zivilprozessordnung:

„Die Beweisaufnahme erfolgt vor dem Prozessgericht.“[61]. Hierunter ist der Unmittelbarkeitsgrundsatz zu verstehen, der dafür sorgt, dass Beweise unmittelbar vor Gericht vorgetragen werden sollen um Verzögerungen bzw. Rückfragen zu vermeiden[62].

Dies ist insoweit nachvollziehbar, als dass der Richter frei ist in seiner Würdigung der vorgelegten Beweise und diese deshalb auch persönlich – unmittelbar – in Augenschein nehmen können soll. Das heißt die Beweise müssen für den Richter persönlich in Augenschein genommen werden können. Explizit nennt der Gesetzgeber hier auch elektronische Dokumente:

„Ist ein elektronisches Dokument Gegenstand des Beweises, wird der Beweis durch Vorlegung oder Übermittlung der Datei angetreten.“[63]

Elektronische Protokolle und Ausdrucke sind grundsätzlich dazu geeignet, als Anscheinsbeweis durch den Richter berücksichtigt zu werden[64]. Dies wäre der Ausdruck einer erhaltenen SDN oder MDN, bzw. die Vorlage eines Mail- oder Webserverprotokolls mit passendem Zeitstempel.

Generell stellt sich die Frage, ob ein Beweismittel welches in den Prozess eingebracht werden soll geeignet ist, den Richter dadurch in seiner Entscheidung zu beeinflussen und ob das Beweismittel der Wahrheitsfindung dient, also hilft, einen Sachverhalt aufzuklären[65].

---

61 § 355. Abs. 1 ZPO

62 Haas, Internetquellen im deutschen Zivilprozessrecht. In: Internetquellen im Zivilprozess. Juridicum – Schriften zum Zivilprozessrecht, 2019, S. 38-39

63 § 371 Abs. 1 S. 2 ZPO

64 Marschall, Rechtliche Kriterien für IT-forensische Systeme (K). In: Rechtsverträgliche Gestaltung IT-forensischer Systeme. DuD-Fachbeiträge 2019, S. 226

65 Marschall, 2019, S. 213-214

So ist zur Qualität von Beweismitteln festzuhalten, dass je zweifelsfreier ein Beweismittel sich darstellt, umso höher die Chance einer wirksamen Würdigung ist. Ist es jedoch sehr zweifelhaft, ob ein Protokoll oder E-Mail-Ausdruck nicht doch nachträglich manipuliert wurde, schwächt dies wesentlich die Qualität des Beweismittels[66].

Hier bietet es sich grundsätzlich an, Maßnahmen zu ergreifen die die Authentizität der Beweismittel sicherstellen oder gar verstärken. Dies kann für die Mail- und Webserverprotokolle bedeuten, dass die Log-Dateien automatisiert in ein Drittsystem überführt werden, welches einen nur lesenden Zugriff erlaubt, sich geografisch an anderer Stelle befindet und die Echtheit von Log-Auszügen bestätigt – sog. Logserver[67]. Oder aber ein Dritter bzw. z. B. der externe IT-Dienstleister bestätigt, dass die Log-Dateien nach aktuellem Stand der Technik erfasst und gespeichert wurden. Ferner ist festzuhalten, dass speziell in Log-Dateien nicht nur die Uhrzeit selbst entscheidend ist, sondern auch die jeweilige Zeitzone in welcher sich das protokollierende System befindet. Für die Zeitsynchronisation bieten sich öffentlich verfügbare Zeitserver an. Hier sollte eine Internet-Zeitquelle gewählt werden, die nach dem DCF77-Signal eine gesetzlich anerkannte Zeit liefert. Diese automatische Synchronisation der lokalen Systemzeit von einem entfernten Zeitserver stellt sicher, dass Zeitstempel in Protokollen jeweils korrekt sind. Dies in Kombination mit einer Verfahrensdokumentation gewährleistet, dass bei einem Beweisvortrag keine beweisvernichtenden Einreden der Ungenauigkeit entgegen gehalten werden können[68]. Nicht vergessen werden darf, dass speziell bei länderübergreifender Kommunikation per E-Mail und im Falle der Wahrung von Fristen, auch die jeweilige Zeitzone berücksichtigt werden muss. Kann sich doch die lokale Uhrzeit des Absenders wesentlich von der Uhrzeit des Empfängers unterscheiden. Muss eine Frist eingehalten werden, richtet sich diese jeweils nach der Uhrzeit des Empfängers. Kommuniziert beispielhaft ein deutsches Unternehmen mit einem Unternehmen an der Westküste in den Vereinigten Staaten von Amerika, kommt es hier zu einem größeren Zeitunterschied, der bei der Aufbereitung der Protokolle berücksichtigt werden muss. Nachdem jetzt erörtert wurde auf welche Besonderheiten in einem

66 Marschall, 2019, S. 269

67 Anussoya, Importance of centralized log server and log analyzer software for an organization. (IRJET), 2015, S. 1

68 Kersten, IT-Sicherheitsmanagement nach der neuen ISO 27001, 2020, S. 165

Zivilprozess zu achten sind, folgt im nächsten Kapitel die weitere Bewertung der einzelnen Beweismittel wie die DSN, MDN sowie die Mail- und Webserverprotokolle mit ihren jeweiligen Besonderheiten.

4.1 Bewertung – Die Übermittlungsbestätigung (DSN)

Eine DSN gelangt als herkömmliche E-Mail in das Postfach des Absenders und hat folgenden Aufbau.

Abb. 7 – DSN-Nachricht – Ausdruck aus Mozilla-Thunderbird

This is the mail system at host mx02.cubewerk.de.

Your message was successfully delivered to the destination(s)
listed below. If the message was delivered to mailbox you will
receive no further notifications. Otherwise you may still receive
notifications of mail delivery errors from other systems.

<max@plzk.de>: delivery via mx3.securepostfach.de[138.201.159.146]:25: 250
2.0.0 Ok: queued as 0FD985DCCF

To: max@plzk.de
From: Stefan Bauer <stefan@cubewerk.de>
Subject: DSN Test mit Mozilla-Thunderbird
Message-ID: <4567f138-5f8d-fe24-c741-69cb42bfad3d@cubewerk.de>
Date: Mon, 27 Dec 2021 11:01:38 +0100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Thunderbird/78.14.0
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit
Content-Language: en-US

Quelle: Eigene Darstellung

Wie zu erkennen ist, hängt an der DSN selbst im unteren Bereich ein Auszug der Original E-Mail an, wie zuvor bereits erwähnt, um eine direkte Zuordnung zur abgesandten E-Mail herstellen zu können. Dies ist eine konfigurierbare Einstellung des jeweils DSN-generierenden Mailsystems. Hier muss ein Spagat erfolgen zwischen dem Datenschutz und der Dokumentations- und Beweiserhebung. Wird der Anhang weiter gekürzt, reduziert man die vorhandenen Informationen die bei einem Vortrag die Echtheit untermauern können. Erleichtert dadurch aber auch die Datenspeicherung und reduziert die Anforderungen an den Datenschutz.

Generell stellt sich beim Medium E-Mail seit Anbeginn die Frage, wie der Nachweis erbracht werden kann, ob eine E-Mail tatsächlich von einem bestimmten Absender stammt oder ob eine E-Mail gefälscht wurde. Hierzu existieren unterschiedliche Methoden der elektronischen Signierung bzw. Unterzeichnung. Ein häufig in der öffentlichen Verwaltung gefordertes Verfahren ist der Einsatz einer qualifizierten elektronischen Signatur laut Vertrauensdienstegesetz (VDG). War die öffentliche Verwaltung doch lange Zeit stark papiergestützt, kann nunmehr die häufig geforderte Schriftform auch durch elektronisch signierte Dokumente gewahrt werden[69]. Eine qualifizierte elektronische Signatur verhindert die Veränderung bzw. Manipulation an Dokumenten und bietet die Möglichkeit, rechtsverbindlich ein Dokument zu unterzeichnen. Die Ausstellung von qualifizierten digitalen Signaturen kann z. B. nach Beantragung mit dem eigenen Personalausweis mit eID-Funktion erfolgen[70]. Damit ist es u.a. möglich, Mahnverfahren online einzureichen oder die Kommunikation mit Behörden papierlos abzuwickeln. Offensichtlich erkennbarer Sinn dahinter ist, dass die Behörden sicherstellen müssen, dass im Einzelfall mit dem richtigen Bürger kommuniziert wird.

Unter dem Begriff „DomainKeys Identified Mail (DKIM) Signatures“ existiert ein weiteres Verfahren welches ermöglicht, E-Mails mit einer digitalen Signatur durch einen Mailserver selbst zu versehen, welche der Empfänger auf Echtheit prüfen kann[71]. Dieses Verfahren signiert die gesamte E-Mail. Das Verfahren

69 § 3a Abs. 2 VwVfG

70 Stemper, Aktuelle Entwicklungen zum E-Government, 2021, S. 117, 126

71 Crocker, DomainKeys Identified Mail (DKIM) Signatures, 2011, S. 1

wird im RFC6376[72] Standard beschrieben und kann für alle E-Mails verwendet werden (DSN, MDN, reguläre E-Mail).

Das DKIM-Verfahren ist wie folgt – vereinfacht – beschrieben:

1. Ein Mailsystem, welches die erfolgreiche Zustellung einer E-Mail dem ursprünglichen Absender quittieren möchte, sendet hierzu eine E-Mail (SDN). Diese E-Mail enthält eine digital erzeugte Signatur welche nur dem Mailsystem möglich ist zu erzeugen. Damit diese digitale Signatur durch Dritte nachprüfbar bleibt, hinterlegt das Mailsystem im DNS-System (siehe Kapitel 3.3) seinen öffentlichen Schlüssel. Nur aus der Kombination des öffentlichen und privaten Schlüssels, können gültige Signaturen erzeugt werden. Es handelt sich hierbei um Public-Key-Kryptographie[73].

2. Der ursprüngliche Absender der die DSN-Bestätigung erhält, kann anhand der Signatur in der E-Mail in Kombination mit dem öffentlichen Schlüssel im DNS-System nachprüfen, ob die E-Mail tatsächlich vom DSN-generierenden Mailsystem erzeugt wurde und ferner ob diese nachträglich verändert wurde[74]. DKIM muss durch die Mailserver selbst unterstützt werden.

Unabhängig davon kann der bloße Inhalt einer E-Mail durch den Absender selbst signiert und verschlüsselt werden. Für die Signierung und Verschlüsselung von E-Mails hat sich das Verfahren S/MIME etabliert, welches die Authentizität von E-Mails sicherstellen kann[75]. S/MIME steht für „Security Multiparts for MIME“ und ist im RFC1847[76] ausführlich beschrieben. S/MIME ist ein Verfahren welches unabhängig von den beteiligten E-Mail-Servern verwendet werden kann. Dieses Verfahren kann ebenso mit DKIM kombiniert werden. Also die Signierung der gesamten E-Mail durch den Mailserver sowie

72 https://datatracker.ietf.org/doc/html/rfc6376/ (letzter Abruf am 16.01.2022)

73 Galbraith, Mathematics of public key cryptography, 2012, S. 485-491

74 Crocker, 2011, S. 6

75 Galvin, Security Multiparts for MIME, 1995, S. 1

76 https://datatracker.ietf.org/doc/html/rfc1847 (letzter Abruf am 16.01.2022)

die Signierung des Inhaltes der E-Mail, durch den Absender. Für die Signierung von E-Mails bedarf es – wie bei DKIM – eines Schlüsselpaares aus privatem und öffentlichen Schlüssel (Public-Key-Kryptographie). Das nötige Schlüsselpaar wird i.d.R. von öffentlichen Zertifizierungsstellen für die Dauer von 12 Monaten ausgestellt. Nachfolgend eine Übersicht von S/MIME-Zertifikatsanbietern:

Abb. 8 – Übersicht S/MIME-Zertifikatsanbieter

Anbieter	**Jahrespreis für S/MIME-Zertifikat**
GlobalSign[77]	59 – 189 €
Sectigo[78]	19 – 39 €
D-Trust (Bundesdruckerei)[79]	39 – 299 €
Digicert[80]	29 – 39 €

Quelle: Eigene Darstellung

Die digitale Signatur einer E-Mail, egal ob selbst signiert in Form einer S/MIME-Signierung oder durch eine serverplatzierte DKIM-Signatur, untermauert sodann die Echtheit einer E-Mail und erleichtert die Beweisführung. Im weiteren Verlauf soll die Lesebestätigung mit ihren Besonderheiten nochmal thematisiert werden.

4.2 Bewertung – die Lesebestätigung (MDN)

Die Lesebestätigung (MDN) ist wie die SDN eine herkömmliche E-Mail, die wie im Kapitel SDN bereits dargestellt, ebenso durch eine digitale Signatur (DKIM) abgesichert sein sollte. Wie bereits zuvor ausgeführt, erfordert die MDN anders wie die SDN, ein aktives Handeln des Empfängers. Hier soll nun nachfolgend aufzeigt werden, wie sich die Zustimmung einer Lesebestätigung für den ursprünglichen Absender darstellt. Der Empfänger erhält i.d.R. beim Anklicken bzw. erstmaligen Öffnen einer empfangenen E-Mail die Aufforderung zur

77 https://www.globalsign.com/de-de (letzter Abruf am 16.01.2022)

78 https://sectigo.com (letzter Abruf am 16.01.2022)

79 https://www.d-trust.net/de/index.html (letzter Abruf am 16.01.2022)

80 https://www.digicert.com (letzter Abruf am 16.01.2022)

Abgabe einer Lesebestätigung. Ist dies erfolgt, generiert das E-Mail-Programm des Empfängers daraus eine neue E-Mail mit minimalem Inhalt.

Der entscheidende Vorteil hierbei ist, dass die E-Mail durch den Empfänger generiert wird und durch sein E-Mail-System auf den Weg gebracht wird. Im Idealfall also enthält diese E-Mail eine digitale DKIM-Signatur des Empfängers, welche die Beweiskraft der Lesebestätigung zusätzlich erhöht.

Aus Sicht des Absenders stellt sich eine Lesebestätigung wie folgt dar. Er erhält eine neue E-Mail des Empfängers:

Abb. 9 – Empfangene Lesebestätigung in Mozilla Thunderbird

Ihre Nachricht

> *An: Max Mustermann (max@plzk.de)*
> *Betreff: Rechnungsübersendung INV37439*
> *Gesendet am: Mon Dec 27 11:44:04 2021*

wurde gelesen am Mon Dec 27 11:52:56 2021

Quelle: Eigene Darstellung

Die Lesebestätigung zeigt, dass der Empfänger Max (max@plzk.de) eine E-Mail mit dem Betreff „Rechnungsübersendung INV37439“ welche am 27.12.21 um 11:44:04 Uhr zugestellt, um 11:52:56 auch durch diesen gelesen wurde.

Lehnt es der Empfänger hingegen ab auf die Anforderung einer Lesebestätigung zu reagieren, also diese auszulösen, erfolgt keine Information an den Absender. Zumindest bei den Tests für diese Arbeit hat sich jedoch gezeigt, dass bei einer Aufforderung durch eine neu empfangene E-Mail und der Ablehnung durch den Empfänger, dadurch die E-Mail nicht entschärft wird, sondern jedes Mal, wenn die E-Mail wieder als ungelesen markiert wird, ein

erneuter Versuch unternommen wird eine Lesebestätigung einzuholen durch den E-Mail-Client des Empfängers. Dies könnte dazu führen, dass der Empfänger – aus Versehen – doch ungewollt irgendwann einer Bestätigung zustimmt.

Ein weiterer Sonderfall zeigte sich bei der Erstellung der Arbeit, dass häufig E-Mail-Programme in Abwesenheit des Empfängers – aufgrund von Urlaub oder Krankheit – jede eingehende E-Mail automatisch mit einer Out-of-Office / Abwesenheitsnachricht beantworten. Auch wenn dies vermutlich nicht das gewünschte Ziel des Empfängers in diesem Fall ist, generiert dies für den Absender eine Zustellungsbestätigung, da hierbei mindestens immer der Ursprungsbetreff zitiert wird. Auch wenn der Empfänger in einem Gerichtsverfahren u.u. entgegen halten wird, im Urlaub gewesen zu sein, kann man erwarten, dass in regelmäßigen Abständen ein Postfach/Briefkasten gesichtet wird. Die E-Mail ihm also auch zugerechnet wird.

Ein spezieller Umstand der noch weiter untersucht werden sollte sind jene Fälle, wo der Spam- oder Virenscanner des Empfängers die E-Mails nachträglich – nach der Zustellung – lokal prüft und entscheidet, dass bestimmte E-Mails aufgrund verdächtiger Inhalte an den Absender wieder als unzustellbar zurückgeschickt werden sollen[81]. Hierdurch würde der Spam- bzw. Virenscanner – mittelbar – einen Nachweis der Zustellung erbringen. Verglichen mit dem Briefverkehr wäre dies die Situation in welcher ein Empfänger nachträglich, erkennbar einen Brief an den Absender zurück schickt. Hierdurch wäre zweifelsfrei bewiesen, dass der Brief dem Empfänger bereits einmal zuging. Dieser Umstand tritt häufig bei falsch oder unzureichend konfigurierten Spam- und/oder Virenfiltern des Empfängers auf und ist äußerst günstig für den Absender.

Im nächsten Kapitel sollen die Besonderheiten der Mailserverprotokolle noch näher ausgeführt werden.

81 Al-Saleh, Investigating the detection capabilities of antiviruses under concurrent attacks, 2015, S. 393

4.3 Bewertung – das Mailserverprotokoll

Das bereits angesprochene Mailserverprotokoll erfasst die erfolgreichen und fehlgeschlagenen Zustellversuche des Mailausgangssytems. Dass dem Empfänger auf seiner Seite der Kommunikation, ein identisches Protokoll vorliegt führt dazu, dass dieser sämtliche Beweise vor Gericht, grundsätzlich durch eine plausible Gegendarstellung widerlegen kann. Üblicherweise ist der Status zu einer Zustellung auf dem Sende- und Empfangssystem jedoch identisch, da hier beide Parteien, ein und den selben Dialog – miteinander – führen. Wie in Abb. 2 zur technischen Übertragung ausgeführt, gilt die E-Mail erst mit der Quittierung des Empfängers als zugestellt. Dies muss bei der Auswertung der Mailserverprotokolle berücksichtigt werden. Der reine Verbindungsaufbau zur Gegenseite stellt noch keine erfolgreiche Zustellung dar. Ohne exakte Uhrzeit von einer geprüften NTP-Zeitquelle ist die Auswertung von Log-Einträgen zwar noch zielführend, aber zeitlich u.u. nicht mehr präzise. Bevor ein Logdatei-Auszug vor Gericht als Beweismittel deshalb eingebracht wird, sollten alle Ungereimtheiten bezüglich Uhrzeit und Zeitzone ausgeschlossen werden um eine unzureichende Würdigung zu verhindern. Die Aufbereitung der Log-Datei in einer Form, die die wesentlichen Informationen für den Richter enthält, trägt zu einer optimierten und schnellen Würdigung bei. Speziell komplexe und nur schwer lesbare Protokolle die sich nicht auf das Wesentliche beschränken – auch u.u. in anderer Sprache – sorgen dafür, dass das Gericht möglicherweise einen Gutachter hinzuzieht, welcher andere Maßstäbe an die Qualität der Beweise legt. Liegt keine SDN oder MDN vor, ist die Log-Datei ein angemessenes Mittel, die Zustellung der E-Mail an den Empfangsserver zu belegen. Zu beachten ist in allen Fällen, dass häufig in Rechtsstreitigkeiten erst Monate oder gar Jahre nach dem Versand einer E-Mail, ein Prozess droht. Es ist also sinnvoll, bereits generell und präventiv, Log-Dateien zu erzeugen und zu archivieren. Speziell die Archivierung von E-Mails ist neben der sinnvollen Beweiskraft, für viele Unternehmensformen verbindliche gesetzliche Vorgabe zur Einhaltung der Unternehmens-Compliance. Diese ergeben sich u.a. aus der Abgabenordnung sowie dem Handelsgesetzbuch[82].

Abschließend muss auf die Deutung der Zeitstempel in E-Mails hingewiesen werden. Jede E-Mail kann – wie auch ein Brief – durch den Absender mit einem

82 Riggert, ECM – Konzepte und Techniken rund um Dokumente, 2019, S. 114-116

beliebigen Datum sowie einer Uhrzeit versehen werden. So ermöglicht es auch dem Absender einer E-Mail, seine eigene Computer-Systemzeit vor- oder zurück zu datieren[83]. Diese Information findet sich im sog. Nachrichtenheader der E-Mail im Date-Feld:

„Date: Wed, 5 Jan 2022 20:32:14 +0100“

Der Nachrichtenheader wird durch jedes Mailsystem – während des Transports der E-Mail auf dem Weg zum Ziel – um eigene Transportinformationen ergänzt. Es kann mit einem Logbuch verglichen werden. Dem Empfänger liegen deshalb immer umfangreichere Informationen im Header vor, als dem Absender. Sieht doch der Empfänger alle Zwischenstationen auf dem Weg bis zu seinem Postfach. Jedes weitertransportierende Mailsystem erweitert den Header um eine Received-Zeile sowie dem eigenen Zeitstempel des Empfanges und optionaler weiterer Informationen wie z. B. den Status einer durchgeführten Viren- oder Spamprüfung. Ein Header-Eintrag der durch ein Mailsystem ergänzt wurde, zeigt sich wie folgt:

Abb. 10 – SMTP-Nachrichtenheader

Received: from mail-qk1-x72f.google.com (mail-qk1-x72f.google.com [IPv6:2607:f8b0:4864:20::72f])

by mx2.securepostfach.de (Postfix) with ESMTPS id 2432D7E0C7

for <stefan.bauer@cubewerk.de>; Wed, 5 Jan 2022 20:32:27 +0100 (CET)

X-securePostfach-checked: yes

Quelle: Eigene Darstellung

Hier ist zu erkennen, dass der Mailserver „mx2.securepostfach.de“ am „5 Jan 2022 20:32:27 +0100 (CET)“ eine E-Mail vom Mailsystem „mail-qk1-x72f.google.com“ mit der Nachrichtenkennung „2432D7E0C7“ für „stefan.bauer@cubewerk.de“ erhalten hat und ein „securePostfach-Check“ erfolgreich war. Diese Informationen können i.d.R. aus jedem E-Mail-Programm

83 Hlawon, In: Herberger/Martinek/Rüßmann/Weth/Würdinger, jurisPK-BGB, 9. Aufl., Art. 20 CISG, 2020, Rn. 11

extrahiert werden. Es ist sinnvoll, bei der Beweisführung diesen Umstand zu berücksichtigen, dass hier dem Empfänger umfangreichere Informationen zum Nachrichtenverkehr vorliegen, die er möglicherweise auch entgegen hält.

Im nächsten Kapitel soll die Verwendung von Zähl-Pixel – umgangssprachlich Tracking-Pixel – nochmal aus einem anderen Licht betrachtet werden.

4.4 Bewertung – Tracking-Pixel und versteckte Inhalte

Aufgrund des erheblichen Aufwandes für jede ausgehende E-Mail ein individuelles Pixel-Bild oder einen individuellen Link einzufügen und auf der Gegenseite die nötige Infrastruktur vorzuhalten um den tatsächlichen Zugriff dann auszuwerten, ist dies nur in einer automatisierten Art und Weise sinnvoll. Wie z. B. beim Versand von automatisierten Newslettern. Dennoch mag es Umstände geben, wo gerade nur dies als Beweismittel in Frage kommt bzw. gerade nur diese Zugriffe protokolliert werden können bzw. wurden. An dieser Stelle muss auf eine Besonderheit von Spam- und Virenfiltern hingewiesen werden, die u.u. das Ergebnis verfälschen und selbstständig – ohne das Zutun des Empfängers – Links klicken bzw. Bilder verfolgen. Zum Vorteil des Absenders.

Spamfilter operieren in zwei Betriebsmodi. Die Prüfung der E-Mail vor und nach der Annahme. (Pre- und Post-Processing[84]). Der Pre-Processing-Modus wertet den Inhalt einer E-Mail bereits aus, bevor dem Absender die Zustellung quittiert wurde – also noch während des stattfindenden SMTP-Dialogs zwischen dem übergebenden und empfangenden Mailserver[85].

Dies führt dazu, dass der Absender keine Bestätigung in seinen Log-Dateien findet, dass eine Zustellung schon abgeschlossen ist. Ebenso wird kein SDN ausgelöst, da die Zustellung tatsächlich noch nicht erfolgreich war. Weiter aber, dass der Spamfilter des Empfängers, Links, Bilder und Verweise automatisiert auf Spam- und Viren prüft – also im Protokoll Spuren hinterlässt. Abhängig vom

84 Bauer, Medium E-Mail, 2021, S. 23

85 Muhammad, A spam rejection scheme during SMTP sessions based on layer-3 e-mail classification, 2009, S. 236

Ergebnis wird dann die E-Mail abgelehnt oder angenommen, also als zugestellt quittiert.

Diese Art der Spamfilterung ist für den Empfänger auf den ersten Blick äußerst günstig. Hat er dadurch nämlich schon – mittelbar – den Inhalt zur Kenntnis nehmen können, ist der gesamte SMTP-Dialog aber noch nicht abgeschlossen und es fehlt an den üblichen Beweismitteln wie einem erfolgreichen Log-Eintrag, einer SDN oder gar einer MDN[86]. Einzig allein in diesem Fall, ist in der Log-Datei des Webservers zu erkennen, dass Links in der E-Mail schon geklickt bzw. externe Inhalte nachgeladen wurden. Dies kann für den Empfänger jedoch auch negative Folgen mit sich bringen, da er von der temporären Annahme zur Spam- und Virenprüfung nichts mitbekommt und somit gar nicht in Kenntnis gesetzt ist, dass die E-Mail in seinem Einflussbereich war. Da sich der Empfänger hier aber eines Gehilfen zur Spamfilterung bemächtigt, muss er sich auch die Zustellung zurechnen lassen, da die E-Mail, wenn auch nur kurz, in seinem – mittelbaren – Einflussbereich war. Dies wäre im Postverkehr damit zu vergleichen, dass der Empfänger aus unbekannten Gründen Kenntnis über den Inhalt einer Postsendung erlangt, dem Zusteller selbst, aber die Annahme verweigert. Das kann nicht richtig sein und bietet Raum für weitere Untersuchungen. Im nächsten Kapitel werden die vorgestellten Beweismittel daraufhin geprüft, ob deutsche Gerichte diese – wenn auch nur in modifizierter Version – gewürdigt haben und welche Argumentation damit einher ging.

5. Akzeptanz der Beweismittel vor Gericht – eine Bestandsaufnahme

Ausgewählt wurden 4 Urteile an Bundesgerichten zum Thema E-Mail-Kommunikation und Beweiswürdigung von Unterlagen. Diese werden nachfolgend in der Form eines jeweiligen Falles, vorgestellt und kurz bewertet.

5.1 BSG – B 14 AS 51/18 R

Die Bestandsaufnahme beginnt mit einem Fall eines Arbeitssuchenden, den letztlich das Bundessozialgericht am 11.07.2019 zu entscheiden hatte. Streitig war ob ein per E-Mail übermittelter Antrag auf Sozialhilfe an das Jobcenter letztlich in den Einflussbereich des Amtes gelangt ist und fristgerecht

86 Bauer, Medium E-Mail, 2021, S. 31

Sozialhilfeleistungen auslöste. Obwohl der arbeitssuchende Kläger weder eine SDN, MDN oder ein Protokoll eines Servers vorlegen konnte, kam das Gericht zum Entschluss, dass eine Sendebestätigung mit korrekter Angabe der E-Mail-Adresse des Jobcenters als Beweismittel ausreiche um im Rahmen der Beweiswürdigung, eine vollständige Übermittlung der E-Mail als bewiesen anzusehen. Der Kläger hat dem Gericht einen Ausdruck aus seinem Postausgangsordner seines E-Mail-Programms als Beweis vorgelegt.

Diese Entscheidung ist fragwürdig. Allein das Absenden eines Briefes oder einer E-Mail begründet noch keine erfolgreiche Zustellung. Da laut Urteil jedoch das Jobcenter weder eine interne Nachforschung betrieben hat und E-Mails binnen 6 Monaten automatisch in den Postfächern des Jobcenters gelöscht werden, ging das Gericht von einer Beweisvereitelung aus und gewährte bei der Entscheidung eine Beweiserleichterung zu Gunsten des Klägers[87]. Die angesprochene Sendebestätigung war lediglich ein Ausdruck einer E-Mail aus dem „Gesendete Objekte“-Ordner seiner E-Mail-Anwendung.

5.2 BVerfG – BvR 1633/09

In einem weiteren Fall begehrten mehrere Personen Schadensersatz gegen ein Luftfahrtunternehmen, da dieses es mutmaßlich unterließ, fristgerecht über geänderte Abflugzeiten zu informieren was dazu führte, dass den Klägern Unkosten für Flugumbuchungen entstanden. Die Personen beantragten Klage gegen das Luftfahrtunternehmen.

Die beklagte Partei trug erstinstanzlich vor, es könne die nötigen Mailserver-Protokolle inkl. Status-Code vorlegen, also die Zustellung belegen. Das Amtsgericht Dortmund würdigte jedoch den Ausdruck eines Mailserverprotokolls nicht ausreichend, wogegen das Luftfahrtunternehmen Beschwerde einlegte und letztlich das Bundesverfassungsgericht am 20.09.2012 darüber zu entscheiden hatte. Laut Einschätzung des BVerfG verstand das Amtsgericht Dortmund die technischen Zusammenhänge nicht oder falsch. Dagegen richtete sich die Beschwerde der Beklagten. Die Beklagte führte aus, dass sie laut eigenem Mailserverprotokoll nachweisen könne, dass der Mailserver der Kläger

87 BSG 14. Senat, B 14 AS 51/18 R

die E-Mail akzeptiert habe, diese also fristgerecht zugestellt wurde. Die Beklagte legte dazu den Ausdruck mit dem Statuscode „250 – message accepted“ vor[88].

Dies ist nachvollziehbar. Zusätzlich hätte die Beklagte nicht nur den Nachweis der Zustellung erbringen können, sondern auch die Sendungs-ID des empfangenen Mailservers mitteilen, welche die Beweiskraft noch verstärkt hätte, da diese ausschließlich durch den Empfangsserver generiert wird. Auch wenn dieses Verfahren letztlich nicht durch das BVerfG im Schadensersatzfall entschieden und zurück an das AG verwiesen wurde zeigt dies deutlich, dass es sich beim Thema E-Mail-Zustellung um ein komplexes Gebiet der Beweisführung handelt und Sachverstand bei der Beweiswürdigung nötig ist.

5.3 BGH – I ZR 64/13

Aufgrund eines selbstverschuldeten Fristversäumnisses bat der Kläger um Wiedereinsetzung in den vorherigen Stand[89] gegenüber dem OLG Karlsruhe. Da das Berufungsgericht die Revision nicht zugelassen hat, musste sich der BGH mit den Einwänden des Klägers beschäftigen. Er führte aus, dass aufgrund eines technischen Problems im E-Mail-Server seine abgesandte E-Mail nicht zugestellt werden konnte. Der BGH konkretisiert in seiner Entscheidung, dass das bloße Absenden für die Annahme einer erfolgreichen Zustellung nicht genüge und für diese Fälle eine Lesebestätigung als Funktion im E-Mail-Client aktiviert werden sollte um nachträglich die Zustellung auch zu beweisen[90].

Dies bestätigt die vorherigen Ausführungen zur MDN. Unabhängig davon darf erwartet werden, dass jede prozessführende Partei schon aus eigenem Interesse heraus, bei Schriftstücken dieser Art die erfolgreiche Zustellung nachhaltig kontrolliert.

88 BVerfG 1. Senat 3. Kammer, 1 BvR 1633/09

89 § 233 ZPO

90 BGH 1. Zivilsenat, I ZR/64/13

5.4 BGH – I ZB 17/06

In einem weiteren Fall vor dem 1. Zivilsenat des BGH musste sich dieser mit der Beweiskraft eines abgesandten Schriftstückes beschäftigen. Es ging um die Entscheidung ob der Beklagte die Klage veranlasst habe und dafür die Gerichtskosten tragen müsse, da dieser bestritt, eine vorherige Abmahnung erhalten zu haben. Das Gericht führt aus, dass in diesen Fällen bewusst eine besondere Versandform wie ein Einschreiben mit Rückschein gewählt werden solle um die Beweisführung zu erleichtern[91].

Wie bereits ausgeführt ist das Einschreiben mit Rückschein wie ein MDN zu werten. Also technisch nicht nur die Zustellung selbst in das Postfach des Empfängers, sondern auch die i.d.R. persönliche Bestätigung des Empfängers, dass eine Zustellung erfolgt ist.

Es muss an dieser Stelle auf eine Besonderheit hingewiesen werden, worin sich die Post- und E-Mail-Zustellung unterscheidet. Bei einem Einwurf-Einschreiben per Post, wirft der Briefträger lediglich den Brief in den Briefkasten. Eine Handlung des Empfängers ist nicht nötig. Bei einem Einschreiben mit Rückschein jedoch, muss der Empfänger die Zustellung schriftlich bestätigen und bekommt so dann erst den Brief überreicht. Bei der elektronischen Zustellung einer E-Mail stellt sich dies – zum Nachteil des Empfängers – anders dar. Ein Einschreiben ist hier schon die bloße Zustellung in das Postfach des Empfängers. Ein Einschreiben-Rückschein (MDN) hingegen entfaltet, wenn der Empfänger eine Lesebestätigung auslöst, eine erhöhte Beweiskraft. Jedoch kann er die E-Mail-Zustellung selbst, nicht einfach verhindern, weshalb die Zustellung immer gegeben ist. Er kann lediglich die Lesebestätigung verhindern. Bei einem Einschreiben mit Rückschein in Briefform jedoch kann der Empfänger die Sendung ablehnen und es kommt zu keiner Zustellung. Die Übermittlung per Post hat hier – neben der Laufzeit des Schriftstückes – klare Nachteile für den Absender. Aufgrund eines wichtigen Urteils des zweiten Zivilsenats des BGH im Jahr 2016 wurde deshalb festgestellt, dass ein persönlich übergebenes Schriftstück (Einschreiben-Rückschein) dem Einwurf-

91 BGH 1. Zivilsenat, I ZB 17/06

Einschreiben gleichzusetzen ist, da ein böswilliger Empfänger sonst einfach die Zustellung verhindern könne[92].

Anders stellt sich dies bei der Zustellung per E-Mail dar. Der tatsächliche Empfänger hat nur mittelbar bei einer E-Mail die Möglichkeit, diese abzulehnen. In Frage kommen hierfür Absender-Sperrlisten, so genannte „Blacklisten“[93]. Alternativ könnte der Empfänger – mit erhöhtem technischen Aufwand – auch sein E-Mail-System für eine gewisse Zeit nicht empfangsbereit schalten, also versuchen, sich der Kenntnisnahme zu entziehen.

Wie dies noch berücksichtigt wird, zeigt das nächste Kapitel mit der Zugangsfiktion.

Holt der Empfänger ein für ihn hinterlegtes Einschreiben mit Rückschein bzw. Einschreiben-Persönlich bei der Post nicht ab, gilt dies als nicht zugestellt. Ausnahmen davon ergeben sich durch die Zugangsfiktion die in Kapitel 6 ausführlich dargestellt wird. Liegt eine E-Mail schon abrufbereit im Postfach des Empfängers, gilt diese schon als zugestellt. Wie bereits dargestellt ist diese E-Mail dann schon im Einflussbereich des Empfängers und ihm zuzurechnen.

Abschließend sollen die bis hier gewonnen Erkenntnisse, nach einer kurzen Darstellung der Zugangsfiktion mit dieser abgeglichen werden.

6. Die Zugangsfiktion

Wie im letzten Kapitel ausgeführt gibt es Umstände, die für eine Partei unvorteilhaft, nein sogar ungerecht wären. Könnte doch der Empfänger einer Zustellung entgehen, würde er nur die Einschreiben nicht von der Post abholen und sich somit der Kenntnis des Inhaltes entziehen. Oder würde er seinen Provider anweisen, bestimmte E-Mails von bestimmten Absendern generell abzulehnen. In der analogen Welt wäre dies damit zu vergleichen, dass der Empfänger seinen eigenen Briefkasten absichtlich demontiert. Dieses Verhalten nennt sich Zugangsvereitelung. Eine Vereitelung kann durch aktives Tun oder Unterlassen hervorgerufen werden. Dies ist auch dann anzunehmen, wenn für

92 BGH 2. Zivilsenat, II ZR/299/15

93 Darms, IT-Sicherheit und Datenschutz im Gesundheitswesen, 2019, S. 141

den Empfänger erwartbar und absehbar ist, dass ihm ein Schreiben zugehen wird. Er also damit rechnen muss, sich also den Umstand sehend, dem Empfang dennoch versucht zu entziehen[94].

Ist der Absender für die unmögliche Zustellung verantwortlich, darf dies nicht dem Empfänger angelastet werden. Ist die Ablehnung, Verhinderung oder Vereitelung jedoch durch den Empfänger verursacht und deshalb unberechtigt, darf dies nicht dem Absender angelastet werden. Um diese unberechtigten Umstände zu heilen, wird die erfolgreiche Zustellung dann angenommen. Man spricht von der Zugangsfiktion[95]. Diese findet sich in vielen Gesetzen an unterschiedlicher Stelle wie dem BGB wieder.

„Ist eine dem Antragenden verspätet zugegangene Annahmeerklärung dergestalt abgesendet worden, dass sie bei regelmäßiger Beförderung ihm rechtzeitig zugegangen sein würde, und musste der Antragende dies erkennen, so hat er die Verspätung dem Annehmenden unverzüglich nach dem Empfang der Erklärung anzuzeigen, sofern es nicht schon vorher geschehen ist. Verzögert er die Absendung der Anzeige, so gilt die Annahme als nicht verspätet.“[96]

Eine weitere Besonderheit im Briefverkehr, die in der E-Mail-Kommunikation nicht abgebildet ist, ist die öffentliche Zustellung laut Zivilprozessordnung[97]. Ist eine Person unter keiner bekannten Postanschrift zu erreichen, kann ein behördliches Schriftstück im Gerichtsgebäude ausgehängt werden. Also öffentlich zugestellt werden[98]. Mit dem Medium E-Mail stellt sich dies anders dar. Aufgrund der örtlichen Unabhängigkeit eines E-Mail-Servers vom tatsächlichen Empfänger, existieren hier keine vergleichbaren öffentlichen Zustellmöglichkeiten. Der RFC2821 SMTP-Standard – wie zuvor bereits ausgeführt – sieht dennoch eine zentrale E-Mail-Adresse pro Empfänger-Domain (der Teil hinter dem @-Zeichen) vor, über welche eine Kontaktmöglichkeit zum Zielsystem- bzw. Unternehmen bei Zustellproblemen

94 Powietzka, Praxishandbuch Arbeitsverträge für Unternehmer, 2016, S. 315-316

95 Zerres, Bürgerliches Recht, 2019, S. 34

96 § 149 BGB

97 § 185 ZPO

98 Duchstein, Zwangsvollstreckungsrecht, 2020, S. 152

bestehen soll[99]. Diese sogenannte Postmaster-Adresse (postmaster@...) ist zwar nicht als Sammelpostfach zu werten und dient primär für die Kommunikation auf technischer Ebene zwischen Administratoren einzelner Mailsysteme. Die Argumentation ist jedoch zulässig, dass eine erfolgreich zugestellte E-Mail an das postmaster-Postfach, auch dem Unternehmen zuzurechnen ist. Könnte dies doch mit einem Pförtner oder einer Postsammelstelle verglichen werden, die bei der finalen Zustellung im Unternehmen unterstützend tätig ist und gerade auch dafür vorgehalten wird, die Abläufe und Kommunikation aufrecht zu erhalten.

Wie sich jetzt die Anwendung der Zustellfiktion in der Praxis an einem Fall darstellt und wie dies einzuschätzen ist, zeigt sich im nächsten Kapitel.

7. Eigenart Zugangsfiktion – eine Einordnung

Konstruiert man nun die Situation, dass das Finanzamt Steuerbescheide versendet die üblicherweise einer Widerspruchsfrist von einem Monat unterliegen, wäre es für den Empfänger durchaus vorteilhaft, wenn die Frist durch Entzug der Kenntnisnahme weiter verlängert werden könnte. Der Steuerbescheid ist ein hoheitlicher Verwaltungsakt und wird erst mit Bekanntgabe wirksam[100]. Für Verwaltungsakte wird die Fiktion in der Abgabenordnung[101] wie folgt ausführlich normiert:

„Ein schriftlicher Verwaltungsakt, der durch die Post übermittelt wird, gilt als bekannt gegeben (...)

bei einer Übermittlung im Inland am dritten Tage nach der Aufgabe zur Post (...)

außer wenn er nicht oder zu einem späteren Zeitpunkt zugegangen ist; im Zweifel hat die Behörde den Zugang des Verwaltungsakts und den Zeitpunkt (…) nachzuweisen.“

99 Klensin, Simple Mail Transfer Protocol, 2001, S. 15, 53

100 Meier, Bekanntgabe eines Verwaltungsaktes. Der Einspruch im Steuerrecht, 2019, S. 9,15

101 § 122 Abs. 2 Nr. 1 Abgabenordnung (AO)

Hier ist ersichtlich, dass es sich nicht um behördliche Willkür handelt, sondern um ein Instrument, sicherzustellen, dass i.d.R. ein Verwaltungsakt nach 3 Tagen Wirkung entfaltet. Jedoch nicht, wenn der Empfänger angibt, dass ihn ein Brief verspätet oder gar nicht erreicht hat. Die Behörde hat hier – wie in der Abgabenordnung[102] normiert – die erfolgreiche Zustellung im Zweifel nachzuweisen, trägt also letztlich weiter die Beweislast.

Die Zustellfiktion muss von einem Anscheinsbeweis unterschieden werden. Auch wenn der Absender im E-Mail Verkehr nur einen Ausdruck aus seinem Postausgang vorlegt, der als schwaches Beweismittel zu werten ist, genügt dies u.u. schon für eine Überzeugung des Gerichtes als Anscheinsbeweis. Davon unabhängig ist die vorgestellte Zustellfiktion, die – ohne Beweiserhebung – fingiert, dass eine gewisse Zustellung nach Ablauf einer definierten Zeit als gegeben anzunehmen ist.

Wie sich abschließend das Thema E-Mail-Beweismöglichkeiten für Absender in einer Gesamtwürdigung darstellt, wird im letzten Kapitel zusammengefasst.

8. Zusammenfassung und Ausblick

Die inhaltliche Ausrichtung der Arbeit orientierte sich an den zu Anfang gestellten Fragen, welche Beweismittel für den Nachweis einer erfolgreichen E-Mail-Zustellung zur Verfügung stehen, welche Aussagekraft diesen beizumessen ist, zu welchen Entscheidungen Gerichte im Einzelfall gekommen sind und wie sich die Zustellfiktion in die Argumentation fügt. Es darf zusammengefasst werden, dass die Übermittlung von E-Mails durch die Vorlage von Mail- und Webserverprotokollen bzw. einer durch den Absender angeforderten Übermittlungs- und/oder Lesebestätigung die erfolgreiche Zustellung belegen kann und durch die Ergänzung durch digitale Signaturen, die Echtheit der Bestätigungen untermauert, was sich förderlich auf die Beweiswürdigung auswirkt.

Wann immer möglich sollte eine Lesebestätigung (MDN) angefordert werden, da diese den bestmöglichen Beweis der Zustellung erbringt, da hierbei eine

102 § 122 AO

Interaktion mit dem tatsächlichen Empfänger erfolgt. Aber auch eine Übermittlungsbestätigung oder ein Ausdruck der eigenen Mail- und Webserverprotokolle kann in einer Gesamtschau die Zustellung ausreichend nachweisen. So ist es nicht verwunderlich, dass selbst Gerichte in Urteilsbegründungen die Lesebestätigung als probates Mittel empfehlen. Generell sollte jedoch erwähnt werden, dass jeglicher Beweis vor Gericht ausreichend sein kann, wenn dieser substanziiert vorgetragen wird und keine Zweifel an seiner Echtheit lässt. So kann es schon genügen, wenn der Absender nur glaubhaft belegt, dass er eine E-Mail auf den Weg gebracht, also abgesendet hat. Wann immer möglich sollte das Thema Beweiserhebung und Protokollierung lange vor dem Eintritt eines Streitfalls firmen- bzw. unternehmensweit berücksichtigt und vorbeugend umgesetzt werden. Speziell die Dokumentation des Verfahrens hilft bei der späteren Interpretation. Abschließend wurde die Erkenntnis gewonnen, dass die Zugangsfiktion ein wichtiges Mittel ist um dem Umstand Rechnung zu tragen, dass Empfänger absichtlich den Empfang bzw. die Zustellung von Nachrichten vereiteln.

Ziel für weitere Forschungen bietet der Sachverhalt, dass ein E-Mail-Server die E-Mail jeweils vollständig erhält und erst dann die Zustellung quittieren kann. Dieser also Kenntnis vom Inhalt erlangt ohne sich diesen zurechnen lassen zu müssen.

V. Literaturverzeichnis

Abels, N. (1996). Der Brief: eine Kulturgeschichte der schriftlichen Kommunikation. Deutschland: Ed. Braus.

Al-Saleh, M. et al. (2015). Investigating the detection capabilities of antiviruses under concurrent attacks. *Int. J. Inf. Secur.* 14, 387–396.

https://doi.org/10.1007/s10207-014-0261-x

Anussoya, R. et al. (2015). Importance of centralized log server and log analyzer software for an organization. *International Research Journal of Engineering and Technology (IRJET)*, *2*, 2244-2249. Letzter Abruf am 17.01.22 von https://www.academia.edu/download/38290467/Irjet-v2i3365.pdf

Bauer, S. (2021). Medium E-Mail. Letzter Abruf am 17.01.22 von cubewerk.de/wp-content/uploads/2021/12/Bachelorarbeit_Medium_E-Mail_DSGVO_Stefan_Bauer.pdf

Baun, C. (2019). *Computer Networks Bilingual Edition: English – German*. Springer Vieweg.

Corfield, G. (2021). ProtonMail deletes „we don‘t log your IP‘ boast from website. Letzter Abruf am 17.01.22 von https://www.theregister.com/2021/09/07/protonmail_hands_user_ip_address_police/

Crocker, D. et al. (1977). Standard for the format of arpa network text messages. Letzter Abruf am 17.01.22 von https://datatracker.ietf.org/doc/html/rfc733

Crocker, D. et al. (2011). DomainKeys Identified Mail (DKIM) Signatures. Letzter Abruf am 17.01.22 von https://datatracker.ietf.org/doc/html/rfc6376/

Crocker, S. (2019). The Arpanet and Its Impact on the State of Networking. *Computer*, *52*(10), 14–23. https://doi-org.pxz.iubh.de:8443/10.1109/MC.2019.2931601

Dammann, U. (2020). Zahlung einfordern. In: Effizientes Forderungsmanagement. essentials. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-30182-8_4

Darms, M. et al. (2019). IT-Sicherheit und Datenschutz im Gesundheitswesen. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-21589-7

Deutsche Post. (2021). Leistungsbeschreibung E-POST, letzter Abruf am 17.01.22 von https://www.deutschepost.de/content/dam/dpag/images/E_e/epost/downloads/pk/dp-epost-pk-leistungsbeschreibung-012021.pdf

Disterer, G. 1957-, V. (2019). *Studien- und Abschlussarbeiten schreiben Seminar-, Bachelor- und Masterarbeiten in den Wirtschaftswissenschaften*. Springer Gabler.

Duchstein, M. (2020). Zwangsvollstreckungsrecht. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-59444-5

Dürscheid, C., Frehner, C. (2013). Email communication. Letzter Abruf am 17.01.22 von https://www.zora.uzh.ch/id/eprint/71867/1/%5B9783110214468_-_Pragmatics_of_Computer-Mediated_Communication%5D_2._Email_communication.pdf

Eckert, C. (2018). *IT-Sicherheit : Konzepte – Verfahren – Protokolle: Vol. 10., erweiterte und aktualisierte Auflage*. De Gruyter Oldenbourg.

EU-Verordnung 910/2014 (2014). Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, letzter Abruf am 17.01.22 von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910

Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge University Press.

Galvin, J. et al. (1995). Security Multiparts for MIME. Letzter Abruf am 17.01.22 von https://datatracker.ietf.org/doc/html/rfc1847

Goldshteyn, M., Thelen, S. (2016). *Praxishandbuch digitale Betriebsprüfung: Anforderungen der neuen GoBD an Buchführung, Datenspeicherung und Datenzugriff*. Schäffer-Poeschel.

Haas, G. (2019). Internetquellen im deutschen Zivilprozessrecht. In: Internetquellen im Zivilprozess. Juridicum – Schriften zum Zivilprozessrecht. Springer, Wiesbaden. https://doi.org/10.1007/978-3-658-27256-2_2

Hansen, T., Vaudreuil, G. (2004). Message Disposition Notification, letzter Abruf am 17.01.22 von https://datatracker.ietf.org/doc/html/rfc3798

Haug, Volker M. (2016). Grundwissen Internetrecht, 3. Auflage, Kohlhammer. Stuttgart.

Hirsch, C. (2020). *BGB Allgemeiner Teil*. Baden-Baden Nomos, 2020.

Hlawon in: Herberger/Martinek/Rüßmann/Weth/Würdinger, jurisPK-BGB, 9. Aufl., Art. 20 CISG (Stand: 01.03.2020)

Huß, W. (2011). Zweites Kapitel: Die Verwaltungsmaßnahmen. In: *Die Verwaltung des ptolemaiischen Reichs.* C.H.Beck. doi:10.4000/books.chbeck.1237

Kersten, H. et al. (2020). IT-Sicherheitsmanagement nach der neuen ISO 27001. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-27692-8

Klensin, J. (2001). *Simple Mail Transfer Protocol*, letzter Abruf am 17.01.22 von tools.ietf.org/html/rfc2821

Klensin, J. (2008). Simple Mail Transfer Protocol, letzter Abruf am 17.01.22 von https://datatracker.ietf.org/doc/html/rfc5321

Koenig, C. (2019). Die Digitale Kopie von Briefsendungen. *Datenschutz und Datensicherheit-DuD*, *43*(9), 551-558.

Lammenett, E. (2019). E-Mail-Marketing. In: Praxiswissen Online-Marketing. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-25135-2_3

Marschall, K. (2019). Rechtliche Kriterien für IT-forensische Systeme (K). In: Rechtsverträgliche Gestaltung IT-forensischer Systeme. DuD-Fachbeiträge. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-26237-2_7

Meier ,S., Rakowski, U. (2019). Bekanntgabe eines Verwaltungsaktes. In: Der Einspruch im Steuerrecht. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-27022-3_2

Microsoft. (2018). *Verwenden von Gruppenrichtlinie zum Konfigurieren von Domänen Mitglieds-Client Computern*, letzter Abruf am 17.01.22 von docs.microsoft.com/de-de/windows-server/networking/branchcache/deploy/use-group-policy-to-configure-domain-member-client-computers

Mittag, H.J., Schüller, K. (2020). Statistik. Springer Spektrum, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-61912-4

Moore, K., Vaudreuil, G. (2003). An Extensible Message Format for Delivery Status Notifications, letzter Abruf am 17.01.22 von https://datatracker.ietf.org/doc/html/rfc3464

Muhammad, N. et al. (2009). A spam rejection scheme during SMTP sessions based on layer-3 e-mail classification. https://doi.org/10.1016/j.jnca.2008.03.005.

Pohlmann, N. (2019). Cyber-Sicherheit. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-25398-1

Powietzka, A. (2016). Praxishandbuch Arbeitsverträge für Unternehmer. Berlin, Boston: De Gruyter. https://doi.org/10.1515/9783110364057

Riggert, W. V. (2019). ECM – Enterprise Content Management Konzepte und Techniken rund um Dokumente. Springer Vieweg.

Röhner, J. V., Schütz, A. (2020). *Psychologie der Kommunikation*. Springer, Berlin, Heidelberg

Schwenk, J. (2020). Sicherheit und Kryptographie im Internet. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-658-29260-7

Specht-Riemenschneider, L. et al. (2020). *Internetrecht: Vol. 1. Aufl. 2020*. Springer.

Stemper, J. et al. (2021). Aktuelle Entwicklungen zum E-Government. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-33586-1

Strzyzewski, F., Karpa-Tovar, C. (2019). Generierung von qualifizierten E-Mail-Adressen. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-26755-1

Vaudreuil, G. (2003). *Enhanced Mail System Status Codes*,letzter Abruf am 17.01.22 von https://tools.ietf.org/html/rfc3463#section-3

Wittmaack, L. et al. (2016). *Vertrauensvolle E-Mail-Kommunikation. (German). Datenschutz Und Datensicherheit – DuD*, *40*(5), 271.

Zerres, T. (2019). Bürgerliches Recht. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/978-3-662-58460-6