Medium E-Mail - rechtliche Vorgaben und Fallstricke für die Unternehmenskommunikation

20.03.2021

Autor:
Stefan Bauer
sb AT plzk DOT de

I. Abstract

Die E-Mail Kommunikation ist die am häufigsten verwendete Kommunikationsart in Unternehmen. Hierdurch ergeben sich Fragen hinsichtlich der konkreten Verschlüsselungspflicht bei der Nachrichtenübertragung, dem Einfluss von Anti-Spam- und Anti-Malware-Software auf die Kommunikation, der Zurechenbarkeit einer empfangenen E-Mail, Fragen ab wann eine E-Mail tatsächlich als zugestellt gilt und wie dies rechtlich zu bewerten und auch zu beweisen ist und wie die Pflicht zur E-Mail-Archivierung in Unternehmen umgesetzt werden kann. Die E-Mail-Verschlüsselung ist Pflicht und die Transportverschlüsselung bis auf wenige Ausnahmen, ein geeignetes Mittel zur rechtssicheren Kommunikation. Diese sollte dauerhaft ausgehend erzwungen werden. Die technisch korrekte Konfiguration des eigenen E-Mail-Servers, zur Aufzeichnung von Übertragungsprotokollen zu Beweiszwecken ist empfohlen. Auch der dauerhafte Einsatz von Übermittlungs- und Lesebestätigungen für ausgehende E-Mails, liefert im Streitfall nötige Zustellnachweise. Beim Einsatz des E-Mail-Archivs für gesendete und empfangene Handelsbriefe, sollte OpenSource-Software mit offenen Schnittstellen gewählt werden, um einen späteren u.U. nötigen Wechsel zu vereinfachen. Die private Internetnutzung sollte aus Datenschutzgründen und zur Vereinfachung der Archivierung, durch Betriebsanweisung unterbunden werden, um eine Vermischung von privaten und geschäftlichen Daten von vorne herein zu vermeiden. Das Medium E-Mail kann rechtssicher eingesetzt werden und bietet wesentliche Vorteile gegenüber der klassischen Briefpost.

E-Mail-Verschlüsselung, Ende-zu-Ende, Revisionssichere Archivierung, Spamfilter, DSGVO, E-Mail Annahme, E-Mail-Zustellung

E-Mail encryption, end-to-end encryption, E-Mail archive, anti malware filter, spam filter, GDPR

II. Inhaltsverzeichnis

III. Abbildungsverzeichnis

IV. Abkürzungsverzeichnis & Disclaimer

AG	Amtsgericht
AO	Abgabenordnung
AZ	Aktenzeichen
BGH	Bundesgerichtshof
BVG	Bundesverfassungsgericht
DSGVO	Datenschutzgrundverordnung
DSN	Delivery Status Notification
E2E	Ende zu Ende Verschlüsselung
EstG	Einkommenssteuergesetz
GoDB	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
OLG	Oberlandesgericht
SMTP	Simple Mail Transfer Protocol
StPO	Strafprozessordnung
UWG	Unlauteres Wettbewerbsgesetz
ZPO	Zivilprozessordnung

1. Einleitung

Das Medium E-Mail nimmt einen wichtigen Stellenwert in der heutigen Unternehmenskommunikation ein. Die erste – mit der heute vergleichbaren – E-Mail wurde Anfang der 1970er verschickt. In der Anfangszeit war E-Mail primär nur in Behörden und größeren Firmenumgebungen, bzw. an technischen Forschungseinrichtungen im Einsatz. Die tatsächliche Kommerzialisierung und die somit großflächige Verbreitung begann erst durch die Verfügbarkeit von erschwinglichen Internetzugängen in den 90er-Jahren für Jedermann. Bekannte globale Anbieter waren AOL oder CompuServe – bzw. im deutschsprachigen Raum, T-Online oder Freenet (Dürscheid, 2013, S. 1). Durch die Nachrichtenübermittlung per E-Mail ergeben sich unterschiedlichste Anforderungen für den Absender und Empfänger hinsichtlich Datenschutz, Übermittlung, Archivierung und Technik. Diese Arbeit soll dazu beitragen, mehr Rechtssicherheit für Unternehmen zu schaffen und möchte folgende Kernfragen – in der üblichen Reihenfolge der Zustellung bzw. Verarbeitung – beantworten:

- Welche E-Mails müssen wann und in welcher Form bzw. Güte, bei der Übermittlung an den Empfänger verschlüsselt werden und woraus ergeben sich die rechtlichen Anforderungen?

- Wie beeinflusst ein eventueller Anti-Spam- und Virenschutz des Empfängers oder dessen Anbieters die Zustellbarkeit einer Nachricht und wer haftet für etwaige Fehler bei der Übermittlung und der sich daraus ergebenden Rechtsfolgen?

- Wann bzw. unter welchen Umständen muss sich ein Empfänger den Erhalt einer E-Mail zurechnen lassen, welche Rechtsfolge ergibt sich daraus und welche Beweis- und Dokumentationsverfahren existieren für den Absender?

- Für wen und wie lange gilt die Archivierungs- und Aufbewahrungspflicht und welche E-Mails müssen wie und in welchem Umfang archiviert werden?

Die Arbeit beginnt mit einer Einordnung der E-Mail in das Standard-Kommunikationsmodell von Shannon und Weaver. Es folgt eine Beschreibung der Begrifflichkeiten, versucht deren Ursprung zu klären und nimmt eine Einordnung des Mediums E-Mail, nach Handelsrecht vor. Es folgt die Beantwortung der gestellten Fragen unter Zuhilfenahme aktueller Literatur und Rechtsprechung. Weiter wird ausgeführt, wieso die zugrundeliegende Methode der Literaturarbeit für dieses Thema geeignet ist und welche Nachteile diese Methode besitzt. Die erarbeiteten Erkenntnisse sollen in dieser Thesis generell in einer Form dargestellt werden, in welcher sie als Handlungsempfehlung für Unternehmen in der

Praxis geeignet sind. Die Arbeit möchte einen hohen praktischen Nutzen für Entscheider liefern und schließt mit einem Fazit und weiterführenden Empfehlungen aus der Praxis ab. Die Empfehlungen stützen sich u. a. auf praktische Erfahrungen eines deutschen E-Mail-Anbieters, auf welche für diese Arbeit – neben Statistiken – zurückgegriffen werden können.

2. Methodenbeschreibung und Bewertung – die Literaturanalyse

Diese Arbeit nutzt als Methode die Literaturanalyse. Vier eingangs skizzierte Fragen aus der unternehmerischen Praxis, sollen unter Zuhilfenahme aktueller Literatur und Rechtsprechung bewertet werden. Ziel der Arbeit ist die Vermittlung des nötigen technischen Grundwissens, sowie die Bereitstellung von Handlungsanweisungen bzw. Empfehlungen aus der Praxis, für die praktische Anwendung in Unternehmen.

Bei der Auswahl der Literatur wurde nach praktischer bzw. inhaltlicher Relevanz, Fachliteratur, Internetquellen sowie Rechtsprechung herangezogen. Die Quellenrecherche erfolgte primär über den Online-Bibliotheken-Zugang der IUBH, sowie über die von Google seit 2004 angebotene freie Suchmaschine für wissenschaftliche Arbeiten, Google Scholar[1]. Besonders hilfreich hierbei war die Volltextsuchmöglichkeit über alle Dokumente hinweg (Stary, 2013, S. 42).

Da die IT heutzutage in jedem Unternehmen eine Kernfunktion einnimmt und bereichsübergreifend zur Verfügung stehen muss, geht die Arbeit an vielen Stellen – notwendigerweise – auf technische Details ein, da gerade dieses Grundverständnis für die Beurteilung essenziell ist. Durch die schnelle Veränderung der Entwicklung in der IT-Branche, wurde bei der Quellenauswahl darauf geachtet, keine veraltete Literatur zu wählen. Zusätzlich wurde – nach Möglichkeit – berücksichtigt, dass die jeweiligen Autoren von Artikeln und Fachbüchern, einen tatsächlichen Bezug zur Praxis bzw. praktische Erfahrung im jeweiligen Gebiet besitzen und die Quelle grundsätzlich geeignet ist, die gestellten Fragen zu beantworten (Disterer, 2019, S.66-67).

Auf einfach editierbare Quellen wie Blogs, private Internetseiten oder Forenbeiträge wurde aus offensichtlichen Gründen verzichtet, um akademischen Ansprüchen zu genügen. Da an manchen Stellen der Arbeit ein Bezug zur europäischen Datenschutzgrundverordnung (DSGVO) besteht, wurde zur Einschätzung von Fällen auch auf die jährlichen Berichte der unabhängigen und staatlichen Datenschutzaufsichtsbehörden der jeweiligen Bundesländer verwiesen, bzw. aus denen zitiert.

1 https://scholar.google.de

Ein großer Nachteil der Literaturanalyse für diese Arbeit zeigte sich einerseits dadurch, dass die in vielen Bereichen ausschlaggebende europäische Datenschutzgrundverordnung eine noch ziemlich junge Verordnung ist, (anzuwenden ab Mai 2018) die in der Praxis noch nicht in allen Unternehmen angekommen ist und sich deshalb noch nicht die Fülle an praxisbezogener Literatur entwickelt hat. Speziell auch der Föderalismus und der daraus entstehenden unterschiedliche Auffassungen der jeweiligen Datenschutzbeauftragten der einzelnen Bundesländer, beförderte hier unterschiedliche Meinungen. Ein weiteres Problem bei der Recherche und Auswahl von Urteilen und Rechtsprechungen bestand darin, dass manche Begriffe aus Rechtsnormen noch aus einer analogen Zeit entstammen (z. B. Handelsbrief) und erst begrifflich auf die elektronischen Ableger - wie z. B. E-Mail - übertragen werden müssen. Auch zeigte sich, dass in einem viel zitierten Urteil des AG Hamburgs[2] (Urteil vom 27.04.2018 – 12 C 214/17) zur Zurechenbarkeit von E-Mails, technische Sachverhalte falsch dargestellt wurden, die gerade für die praktische Anwendung so wichtig sind. Auf dies wird im Detail in Kapitel 7, Zurechenbarkeit und Rechtsfolgen des E-Mail-Empfangs näher eingegangen.

Die Methode der Literaturanalyse ist dafür geeignet, tatsächliche Fälle und Fragen aus der Praxis aufzugreifen und mit verfügbarer und geeigneter Literatur kritisch zu beurteilen. Nur durch eine tatsächliche Anwendung von echten Fragen bzw. Problemen aus der Praxis, kann ein Nutzen für den Leser erreicht werden. Die Arbeit hat nicht zur Aufgabe, rein theoretische oder erfundene bzw. nur skizzierte Fälle zu betrachten.

3. Kommunikation & Begriffsdefinition

Für die Nachrichtenübermittlung per E-Mail über das Internet, kann das 1949 entwickelte Sender- und Empfänger-Kommunikationsmodell von Claude E. Shannon und Warren Weaver verwendet werden (Shannon-and-Weaver Modell). Dieses Modell beschreibt auf technischer Ebene, die Kommunikation zwischen Sender und Empfänger über ein gemeinsames Medium. Auch wenn das Modell aus der Telefonzeit stammt, kann es problemlos auf das Internet bzw. die Nachrichtenübertragung – wie auch E-Mail – angewendet werden. Zu berücksichtigen ist, dass E-Mail kein Echtzeitmedium ist, die Kommunikation asynchron stattfindet (siehe auch Kapitel 7) und eine Übertragung aufgrund von Leitungsfehlern bzw. Störungen, beeinträchtigt werden kann bzw. es zu Störungen und somit zu Signalveränderungen kommt. Auch zeigt sich, dass für eine reibungslose Kommunikation, Sender und Empfänger dieselbe „Sprache“ sprechen müssen und geeignete technische Geräte benötigen, die zueinander kompatibel sind (Rohner, 2020, S. 29-30). Welche Anforderungen speziell die Verschlüsselung an Sender und Empfänger bei der E-Mail-Kommunikation stellt und wie auch die Übermittlung bei der Übertragung scheitern kann, zeigen die weiteren Kapitel.

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

Zum besseren Verständnis der weiteren Zusammenhänge, folgt eine kurze Begriffsdefinition der europäischen Datenschutzgrundverordnung (DSGVO), sowie der damit verbundenen und primär zu schützenden personenbezogenen Daten. Sie erhalten einen Überblick über die Funktionsweise der Verschlüsselung und eine Gegenüberstellung der zwei primären Verschlüsselungsarten (Ende-zu-Ende und Transportverschlüsselung) in der E-Mail-Kommunikation. Es folgt ein Einblick in die Arbeitsweise eines Spam- und Virenfilters, sowie die Beschreibung und rechtliche Anforderung an eine rechtssichere Archivierung.

3.1 DSGVO & personenbezogene Daten

Die Datenschutzgrundverordnung (DSGVO) ist eine europäische Verordnung, die seit Mai 2018 auch in Deutschland gilt. Ziel ist die Vereinheitlichung des Datenschutzes innerhalb der europäischen Union für alle Mitgliedsstaaten. Durch sie soll der Datenschutz besser und zeitgemäßer geregelt werden (Becker, 2018, S. 2). Ebenso soll der Einzelne umfangreicher vor der schier uferlosen Datensammlung, durch große Konzerne wie Google, Facebook oder Amazon geschützt werden. Die Datenschutzgrundverordnung gilt „(..) für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“ (Art. 2 DSGVO)

Unter Verarbeitung versteht man „(..) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“ (Art. 4, Abs. 2 DSGVO).

Unter Verarbeitung ist somit jeder – und nicht zwingend IT-gestützter – Vorgang zu verstehen, der in irgend einer Form etwas mit personenbezogenen Daten zu tun hat. Dies wäre z. B. die Recherche in einem elektronischen Kundensystem durch einen Verkäufer, das Ändern eines Namens in einer Personalakte, die Weitergabe von Lohnunterlagen an den Steuerberater, die Aufzeichnung eines Telefonats zu Schulungszwecken, oder der Versand einer Bestellbestätigung per E-Mail an einen Kunden.

Die IT ist ein äußerst kritisches Arbeitsmittel in nahezu allen Unternehmen und durch die elektronische Datenverarbeitung fallen in unterschiedlichsten Branchen und Bereichen, Daten an und werden automatisiert verarbeitet. Seien dies Patientendaten in der Arztpraxis oder im Labor, politische Ausrichtung oder Neigungen von Einzelnen in sozialen Netzwerken, oder das eigene Kaufverhalten oder zu

schnelles Autofahren, beim Einsatz von Rabattsystemen oder Telemetrie in der Fahrzeugortung für Arbeitgeber oder Versicherungen.

Art 1. DSGVO nennt die generellen Ziele der Datenschutzgrundverordnung wie folgt:

„(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.“

Unter natürlichen Personen sind alle Menschen zu verstehen. Dem gegenüber stehen juristische Personen, also Organisationen (Hirsch, 2020, S. 33).

Hier ist erkennbar, dass im Mittelpunkt der Schutz des Einzelnen steht. Also der Schutz personenbezogener Daten. Personenbezogene Daten nach Art. 4 Abs. 1 DSGVO sind:

„(..) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (..) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;“.

Personenbezogene Daten sind somit alle Daten die dazu dienen können, einen Einzelnen zu identifizieren. Dazu zählt beispielhaft der Name, die Adresse, das Geburtsdatum, die eigene E-Mail-Adresse, die Bankverbindung oder Telefonnummer. Ob es sich um personenbezogene Daten handelt, lässt sich selbst mit folgender Kontrollfrage beantworten:

Kann ich diese Daten einem Einzelnen korrekt zuordnen und ihn dadurch von anderen Personen – ggf. unter Zuhilfenahme von weiteren Informationen – unterscheiden? Dies wäre durch den eigenen Namen oder das Geburtsdatum möglich. Sonderfälle wie ein identischer Name oder Geburtsdatum, führen dennoch zu einer Identifizierung des Einzelnen, wenn auch nicht zwingend, zweifelsfrei.

Eine juristische Person ist nicht durch die DSGVO geschützt. Dies wäre die GmbH oder Aktiengesellschaft. Jedoch ist der einzelne Mitarbeiter oder der Geschäftsführer der GmbH oder AG, als natürliche Person durch die DSGVO geschützt. Ebenso alle natürlichen Personen, die mit der GmbH in geschäftlichem Kontakt stehen, wie z. B. Mitarbeiter von Kunden, Partner oder Lieferanten.

Generell werden durch die DSGVO, ebenso Verstöße und Datenschutzvergehen deutlich umfangreicher sanktioniert. Am Beispiel einer fehlenden Bestellung eines Datenschutzbeauftragten für das eigene Unternehmen, ergeben sich Bußgelder im Umfang von bis zu 10 Millionen Euro (Becker, 2018, S. 404). Ein kürzlich verhandelter Fall vor dem Landgericht Bonn, stellte sich wie folgt dar:

Die 1 & 1 Telecom GmbH, – eine der größten deutschen Telekommunikationsanbieter – hatte die Verarbeitung von personenbezogenen Daten im eigenen Callcenter nicht auf die DSGVO-Konformität hin überprüft. Dadurch kam es zu einer unzureichenden Legitimationsprüfung von Anrufern. Hierbei gab sich eine Ex-Partnerin eines 1 & 1 Kunden als Ehefrau aus und erlangte durch die unzureichende Prüfung durch die Call-Center Mitarbeiter, die neue Telefonnummer des Ex-Partners. Diese Nummer nutzte die Stalkerin für belästigende Anrufe gegenüber dem Ex-Partner. Dieser erstattete Anzeige. Der Bundesbeauftragte für den Datenschutz erlangte durch eine Mitteilung der Polizei davon Kenntnis und verhängte ein Bußgeld. Die ursprünglich angesetzte Bußgeldhöhe von 9.550.000 EUR wurde nachträglich zwar durch das LG Bonn auf 900.000 EUR reduziert, die erhebliche monetäre Auswirkung auf den Telekommunikationsanbieter durch dieses Bußgeld, ist jedoch weiterhin deutlich (LG Bonn, Urteil vom 11.11.2020 - 29 OWi 1/20).

Neben der generellen Legitimation vor der Erteilung von Auskünften, gibt es weitere Maßnahmen zum Schutz personenbezogener Daten bei der Verarbeitung und Übertragung.

Die Verschlüsselung von Informationen ist ein wichtiger Baustein, um Informationen bei der Übermittlung vor Einblicken Dritter zu schützen. Dies ist eine wesentliche Forderung der Datenschutzgrundverordnung. Was unter Verschlüsselung zu verstehen ist, welche Einsatzzwecke für Verschlüsselung in der Praxis existieren und wie die Verschlüsselung technisch abläuft, zeigt das nächste Kapitel.

3.2 Verschlüsselung

Die Verschlüsselung bezeichnet die Veränderung einer Information in der Form, dass die ursprüngliche Information nicht mehr für Jedermann lesbar bzw. einsehbar ist. Häufig erfolgt die Verschlüsselung zwischen zwei oder mehr Parteien, welche durch ein gemeinsames Geheimnis weiter im Stande

sind, die durchgeführte Verschlüsselung wieder rückgängig zu machen. Diese Information also wieder offen zu legen. Eine Verschlüsselung ist einerseits nötig, um Informationen vor Einblicken Dritter zu schützen, aber auch um bei der Übertragung von sensiblen Informationen über ungesicherte Kanäle, die Information zu schützen (Wätjen, 2018, S. 14).

Die Pflicht zum Schutz von personenbezogenen Daten durch geeignete Verschlüsselung, findet sich auch in der zuvor vorgestellten Datenschutzgrundverordnung wieder. Die Notwendigkeit, Daten vor Unberechtigten geheim zu halten, hat viele Gründe:

Ein Unternehmen möchte bei der Kommunikation mit Partnern / Lieferanten per E-Mail, keine Daten im Klartext übermitteln.

Ein Journalist fürchtet Verfolgung bei regimekritischer Recherche und Berichterstattung und schützt so seine Aufzeichnungen auf dem eigenen Laptop durch Verschlüsselung für den Fall, dass sein Laptop gestohlen oder kontrolliert wird.

Oder aber ein Geschäftsführer nimmt täglich die Datensicherung des Firmen-Servers mit nach Hause, möchte diese Daten aber nicht im Klartext auf einer USB-Platte transportieren, um bei Verlust oder Diebstahl keine Interna offen zu legen. Auch hierzu finden sich in der DSGVO Vorgaben, angemessene Verschlüsselung einzusetzen.

Keine Verschlüsselung ist vergleichbar mit einer Postkarte, die im Klartext – und für Jedermann lesbar – Informationen beinhaltet. Die Verschlüsselung wäre vergleichbar mit einer geheimen Botschaft, die für einen Betrachter nicht direkt erkennbar ist und erst durch die Anwendung eines Verfahrens, die Informationen im Klartext wieder preisgibt.

Die Verschlüsselung am Beispiel E-Mail-Übertragung, lässt sich in zwei Arten unterteilen. Die Ende-zu-Ende Verschlüsselung sowie die Transportverschlüsselung. Die Ende-zu-Ende Verschlüsselung findet jeweils zwischen zwei Kommunikationspartnern direkt statt. Also dem Absender selbst und dem Empfänger.

In der Praxis könnte sich der Absender und Empfänger darauf einigen, dass jeder Buchstabe um eine Stelle nach hinten wandert. Dies stellt sich stark vereinfacht wie folgt dar:

Der Satz „Hallo Welt“, würde somit wie folgt verschlüsselt werden → Ibmmp Xfmu.

Der Buchstabe H wird, um eine Stelle nach hinten versetzt, dann zum Buchstaben I. Dies findet auf alle Buchstaben Anwendung. Der Empfänger kennt die Methode und kann die Information somit auch

wieder entschlüsseln, indem er alle Buchstaben jeweils um eine Stelle im Alphabet zurück versetzt (Wätjen, 2018, S. 15).

Bekanntes Beispiel für eine – wenn auch deutlich komplexere – Verschlüsselung, war die im Zweiten Weltkrieg eingesetzte Enigma-Maschine, die den Vorgang der Ver- und Entschlüsselung bereits automatisiert vollzog (Blömer, 2012, S. 1).

Zusätzlich existiert die Transportverschlüsselung. Also nicht wie bei der Ende-zu-Ende Verschlüsselung zwischen Sender und Empfänger direkt, sondern jeweils nur zwischen den E-Mail-Systemen auf dem Weg bis zum Ziel – eben für den Transport. Dies führt dazu, dass eine E-Mail zwischen einem T-Online- und einem GMX-Kunden, mehrmals ver- und entschlüsselt wird. Hierbei ist es möglich, dass der jeweilige E-Mail-Anbieter die E-Mails im Klartext zu lesen bekommt. Die Transportverschlüsselung stellt eine einfachere Verschlüsselung dar und kann ohne größeren Implementierungs- und Kostenaufwand umgesetzt werden. Die Ende-zu-Ende-Verschlüsselung verursacht höhere Kosten und die Handhabung gestaltet sich in der Praxis komplizierter (Schleipfer, 2020, S2).

So zeigt eine Umfrage[3] aus dem Jahr 2018 unter 1008 Internetnutzern ab 14 Jahren, dass der Großteil der Befragten (46,6%) angibt, die Ende-zu-Ende-Verschlüsselung sei zu aufwändig. 43,7% geben an, über nicht ausreichende Kenntnisse zu verfügen. Wäre die Ende-zu-Ende Verschlüsselung einfach nutzbar, wären gerade keine erheblichen zusätzlichen Kenntnisse nötig.

Eine zu nennende Hürde für die einfache und praktikable Anwendung der Ende-zu-Ende Verschlüsselung ist die Notwendigkeit, vor dem erstmaligen Nachrichtenaustausch, über einen sicheren Kanal, (Telefon, Brief, SMS uvw.) die Kommunikationspartner gegenseitig zu identifizieren und authentifizieren (Wätjen, 2018, S. 151). Dies ist nötig, damit das Gegenüber auch sicher sein kann, mit dem tatsächlichen Absender bzw. Empfänger zu kommunizieren. Hierauf wird jedoch in der Praxis gerne aufgrund von Bequemlichkeit verzichtet. Zusätzlich ergeben sich Probleme bei der E-Mail-Archivierung (siehe Kapitel 8.2). Hinzu kommt die derzeit noch geringe Verbreitung im geschäftlichen Umfeld.

Da im geschäftlichen E-Mail-Verkehr, häufig auch unerwünschte E-Mails – sog. SPAM – im eigenen Posteingang landen, bedarf es technischer und organisatorischer Maßnahmen zur Vermeidung. Neben organisatorischen Maßnahmen wie der zurückhaltende Umgang mit der eigenen E-Mail-Adresse

3 https://de-statista-com.pxz.iubh.de:8443/statistik/daten/studie/800374/umfrage/gruende-der-nichtnutzung-von-e-mail-verschluesselung-in-deutschland/

im Internet, existieren auch Softwarelösungen zur Spam-Abwehr. Die grundsätzliche Funktionsweise von AntiSpam-Software, soll im nächsten Kapitel ausführlich vorgestellt werden.

3.3 AntiSpam

Unter dem Begriff Spam, kann eine für den Empfänger unerwünschte Nachricht verstanden werden. Der Begriff Spam war ursprünglich ein Markenname für Dosenfleisch („SPiced hAM“). 1970 verwendete die britische Komikergruppe Monty Python, den Begriff erstmals in einem Sketch. In dem Schauspiel, welches in einem Restaurant spielt, gibt es zu jedem Gericht eine Menge Spam und der Kellner weist auch beim Serviervorgang fortlaufend darauf hin. Spam prägt sich als Begriff für etwas ein, was sich ständig wiederholt und als belästigend wahrgenommen wird (Templeton, o.J., S. 1). Lange vor der Entstehung von E-Mail, wurde bereits unerwünschte Post an Haushalte zugestellt. Die erste Spam-E-Mail wurde 1978 im damals noch existierenden ARPANET (Advanced Research Projects Agency Network) Verteidigungsnetzwerk der US-Streitkräfte verschickt (Ferrara, 2019, S. 2-3). Das damalige Netzwerk war – wie der Name bereits vermuten lässt – noch nicht der breiten Masse an Haushalten und Privatpersonen zugänglich, sondern nur ausgewählten Unternehmen, Regierungseinrichtungen und Firmen und diente primär als robustes militärisches Befehls- und Kommandonetzwerk (Crocker, 2019, S. 4). Das Aufkommen an Spam war – aufgrund der Zugangsbeschränkungen – dementsprechend gering. Erst durch die Verfügbarkeit des Internets für Jedermann, begann die Anzahl an Spam zuzunehmen. Geeignete Anti-Spam-Software war nötig.

AntiSpam-Software bzw. AntiSpam-Filter bezeichnet Computersoftware, Programme oder Vorrichtungen die dazu geeignet sind, unerwünschte E-Mails vor der Zustellung an den Empfänger durch den E-Mail-Provider auszufiltern, direkt abzuweisen oder kenntlich zu machen und mit einem Warnhinweis an den Empfänger zu übermitteln. Die Filterung dient der Vorsortierung oder Aussonderung von schädlichem Inhalt für den Empfänger. Meist finden bösartige Angriffe per E-Mail statt, um den Empfänger mit einem Virus oder Trojaner zu infizieren. Negative Berühmtheit erlangte im Jahr 2017 der Verschlüsselungstrojaner WannaCry, der über den Infektionsweg E-Mail, Daten der Opfer verschlüsselte und im Anschluss Lösegeld zur Entschlüsselung forderte (Satheesh, 2018, S. 2).

Häufig liegen zur Spamerkennung und Filterung verschiedene Methoden wie Texterkennung, Positiv- und Negativlisten oder selbst lernende Regeln der Entscheidung zugrunde (Chu, 2020, S. 1). Eine E-Mail wird auf ihren Inhalt bzw. die äußere Erscheinung hin, untersucht.

Neuerdings werden ebenso neuronale Netze – also eine Verschaltung von Computern in einem direkten Verbund – für die Entscheidung verwendet. Die Systeme lernen voneinander und nutzen die ge-

wonnenen Informationen für die Bewertung von eingehenden E-Mails. Eine prominente und kostenlos verwendbare Software ist Rspamd[4].

Unerwünschte E-Mails sind in der Regel offensichtlich unerwünschte Newsletter, bzw. tatsächliche und aufdringliche Werbung, sinnloser Text ohne erkennbaren Zusammenhang oder E-Mails die dazu geeignet sind, den Empfänger in einer unerwünschten Art und Weise zu belästigen. Obwohl für den Empfänger die Unterscheidung nicht direkt erkennbar ist, ist sie für die technische Bearbeitung bzw. Behandlung wichtig. Auf der selbstverschuldeten Seite stehen jene E-Mails, die der Empfänger – wenn auch nur irgendwann einmal – selbst angefordert hat. Dies sind Newsletter, Angebote oder Informationen von Firmen oder Service- und Supportangebote, zu einmal bezogenen Produkten.

Dem gegenüber stehen offensichtliche E-Mails, die nicht von einem bekannten Absender eintreffen oder von einem Absender, der in einem irgendwie einmal bestandenen Verhältnis zum Empfänger stand. Für ersteren Fall bietet die DSGVO die Betroffenenrechte – z. B. das Recht auf Löschung. Unabhängig davon, können beide Fälle durch einen Spamfilter erkannt oder ausgefiltert werden. Sinniger ist bei offensichtlicher Werbung von tatsächlichen und existierenden Firmen, die Inanspruchnahme der Betroffenenrechte laut DSGVO. Unter welchen Umständen eine E-Mail ohne Einwilligung als unerlaubt und somit unlauter gilt, regelt das Gesetz gegen den unlauteren Wettbewerb (UWG).

Speziell für den Newsletter und E-Mail-Versand, hat sich die doppelte Einverständniserklärung durch den Empfänger, als rechtlich gültiger Standard verfestigt. Ein unaufgeforderter Versand von Newslettern ist ohne Erlaubnis nicht gestattet (Müller, 2020, S. 132). Das Gesetz gegen den unlauteren Wettbewerb (UWG) nimmt ebenso Unterscheidungen vor, ob ein Unternehmen oder eine Privatperson per E-Mail umworben wird. Das UWG regelt neben dem Umgang mit E-Mails, ebenso die Werbung per Post und Telefon.

Dass es im Jahr 2019 immer noch über 57.000 schriftliche Anzeigen bei der Bundesnetzagentur aufgrund unerlaubter Telefonwerbung gab, zeigt der jährliche Jahresbericht[5]. Die Dunkelziffer muss als noch deutlich höher eingestuft werden, da eine schriftliche Beschwerde für den Belästigten einerseits mit bürokratischem Aufwand verbunden ist, andererseits nicht jeder die Möglichkeit der Beschwerde kennt.

Ferner kann festgehalten werden, dass der Gesetzgeber beim Versand von Werbung darauf abstellt, ob die Werbung selbst, beim Empfänger Ressourcen bindet, die Kosten verursachen oder nicht. So ist der E-Mail Empfänger damit beschäftigt, jede E-Mail einzeln zu sichten und gegebenenfalls Wider-

4 https://rspamd.com/

5 https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Jahresberichte/JB2019.pdf?__blob=publicationFile&v=6

spruch gegen den Absender einzulegen. Dies beeinträchtigt den Betriebsablauf des Empfängers (BGH[6], 14. März 2017, Az. VI ZR 721/15). Gerade durch die einfache und nahezu kostenlose Möglichkeit, mit wenigen Mausklicks tausendfach Werbemails zu versenden, sind die rechtlichen Anforderungen (vgl. doppelte Einverständniserklärung) für den E-Mail-Versand deutlich höher. Hingegen trägt der Werbende beim Versand von Briefsendungen die Portokosten, was einen massenhaften Versand von Werbung per Post erschwert, da der Absender schon aus wirtschaftlichen Gründen, seine Werbekosten gering halten möchte.

Im weiteren Verlauf geht es primär um den Sachverhalt ausfiltern und abweisen von E-Mails, jedweder Art, durch den AntiSpam-Anbieter. Dies meint die Annahme von E-Mails ohne endgültige Zustellung an den Empfänger und das Löschen der E-Mail (ausfiltern). Sowie den Fall der Abweisung von E-Mails in erkennbarer Weise für den Absender. Typische AntiSpam-Software läuft in der Regel auf hochverfügbaren E-Mail-Servern des E-Mail-Anbieters und beurteilt innerhalb von Sekunden, anhand von hunderten Erkennungsmerkmalen, wie mit einer E-Mail individuell zu verfahren ist. Neben der Möglichkeit der Ausfilterung und Erkennung von unerwünschten E-Mails, bietet ein zusätzlicher Baustein – der Virenschutz – weitere Methoden zur Erkennung von schadhaftem Inhalt. Dieser wird im nächsten Kapitel vorgestellt.

3.4 Virenschutz

Der Mathematiker Von Neumann, stellte 1948 ein Modell für sich selbst reproduzierende Systeme auf. Dies kann als erste Erklärung für einen virusähnlichen Vorgang in der Informatik bezeichnet werden (Szor, 2005, S. 13). Der Duden nennt als Wortherkunft für den Begriff Virus[7], die lateinische Übersetzung Schleim, Saft oder Gift bzw. als Synonym, den Krankheitserreger. Also einen schädlichen Gegenstand, bzw. einen Schadensverursacher. Cohen und Adleman entwickelten im Jahr 1986 und 1990 das erste abstrakte Modell zu Computerviren, was den Computervirus als ein sich selbst reproduzierendes und veränderndes System beschreibt (Gladychev, 2019, S. 3). Prominente erste Computerviren waren im Jahr 1999 der Melissa-Virus, der sich über Microsoft-Word Macros verbreitete. 2000 der LoveLetter – ein als vermeintlicher Liebesbrief getarnter Virus – der sich per E-Mail mit dem Betreff „ILOVEYOU“ verbreitete oder 2004 der MyDoom-Virus, der eine Hintertür im Betriebssystem DOS von Microsoft ausnutzte (Joshi, 2012, S. 5). Durch die rasante Entwicklung und Verfügbarkeit des Internets und der dadurch potenziellen Gefahr für den Einzelnen, entstand die Notwendigkeit, auch dieser Art Bedrohung, geeignete Schutzmaßnahmen entgegen zu setzen.

6 http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=77970&pos=0&anz=1

7 https://www.duden.de/rechtschreibung/Virus

Virenschutz – auch AntiVirus bzw. AntiViren-Schutz – bezeichnet Computersoftware bzw. Programme oder Vorrichtungen die dazu geeignet sind, Schadsoftware, Viren und/oder Trojaner zu erkennen und teilweise auch unschädlich zu machen (Eckert, 2018, S. 64).

Schadsoftware kann generell als Software bzw. Computerprogramm bezeichnet werden, welches die Absicht hat, fremde Computersysteme zu sabotieren, Informationen zu kopieren oder zu verändern oder Kernfunktionen des Computers – negativ – zu beeinflussen. Aktuelles Beispiel für Schadsoftware war Emotet. Das kriminell operierende Betreibernetzwerk hinter Emotet, wurde im Januar 2021 durch eine internationale Zusammenarbeit zerschlagen[8]. Die Erkennung von Viren erfolgt in der Regel auf Grundlage von vorhandenen Daten, zu bereits entdeckten Viren in der Vergangenheit. Neuartige Viren können durch Virenscanner erst erkannt werden, wenn ein Virus als solcher erkannt, klassifiziert und katalogisiert wurde. Google bietet mit seinem Produkt VirusTotal[9] einen cloudbasierten Onlinedienst, um in Echtzeit vermeintlich infizierte Dateien, durch über 60 individuelle Virenscanner kostenlos prüfen zu lassen (Salem, 2020, S. 1).

Der Virenschutz bzw. die Anti-Virus-Prüfung, ist eine sinnvolle und nötige Ergänzung zur Spamabwehr und sollte möglichst weit außerhalb des eigenen Unternehmensnetzwerk erfolgen, um u.U. infizierte Dateien gar nicht erst in die sensible Unternehmens-IT einzubringen.

Neben dem Virus, der in der Regel von Anfang an schädliche Absichten verfolgt, existiert der Computer-Bug, der an dieser Stelle nicht weiter vertieft werden soll. Ein Bug ist umgangssprachlich ein unbeabsichtigter Fehler in einer Computersoftware oder elektronischen Anlage, die aufgrund von Programmierfehlern oder unzureichender Qualitätssicherung, zu Abstürzen oder Ausfällen führt (Grottke, 2007, S. 1).

3.5 Archivierung

Archivierung bezeichnet die langfristige Ablage und den Erhalt von Informationen in ihrer originären Form. Zweck der Archivierung ist es, die abgelegten Informationen zur richtigen Zeit abrufen zu können. Häufig dient ein Langzeitarchiv auch zu Beweis- und Revisionszwecken. Aufgrund der großen Anzahl von Dokumenten im täglichen Geschäftsleben ist es nachvollziehbar, dass nach einer vordefi-

8 https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html

9 https://www.virustotal.com

nierten Zeit, nicht mehr oder sehr selten benötigte Dokumente, in ein Archiv verschoben werden sollten. Die Archivierung kann abhängig vom Informationstyp, in klassischer Papierform oder IT-gestützt erfolgen. Vorteil der IT-gestützten Archivierung ist der geringe Platzbedarf, sowie die schnelle und einfache Such- und Recherchemöglichkeit in digitalen Belegen und ein möglicher Mehrfachzugriff auf das selbe Dokument, zur selben Zeit durch unterschiedliche Personen. Kann ein Papier bzw. Ordner nur durch eine Person zur selben Zeit genutzt werden, bietet ein IT-gestütztes System, keine generelle Beschränkung dieser Art.

Die grundsätzliche Pflicht zur Archivierung ergibt sich für Kaufleute u. a. aus § 257 Abs.1 HGB:

„(1) Jeder Kaufmann ist verpflichtet, die folgenden Unterlagen geordnet aufzubewahren:

1.Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse (..)“.

Eine Datensicherung stellt kein Archiv dar. Eine Datensicherung hält lediglich für einen gewissen engen Zeitraum, eine Kopie von Daten für die Wiederherstellung vor. Eine Datensicherung ist in der Regel ein automatischer Prozess, welcher ältere Daten bzw. Stände nach gewisser Zeit automatisch durch neuere Stände überschreibt. Eine Datensicherung dient der Wiederherstellung von Daten bei einem Teil- oder Totalausfall der IT-Umgebung oder zur Wiederherstellung einzelnen Dateien bei einem Überschreiben oder Löschen durch den Anwender. Der Unterschied zeigt sich deutlich in der Praxis, da eine Archivierung für bis zu 10 Jahre, Informationen konservieren muss. Eine Datensicherung hingegen arbeitet nach dem Prinzip, dass rotierend, Daten von einer Quelle auf ein Ziel übertragen werden. Eine Datensicherung kann grundsätzlich für die kurz- bis mittelfristige Wiederbeschaffung angesehen werden. Ein Archiv dient als langfristige Aufbewahrung im Rahmen rechtlicher Speichervorgaben.

4. Medium E-Mail nach Handelsrecht

Für die geschäftliche Korrespondenz und zur Beantwortung der nachfolgenden Fragen hinsichtlich Zurechenbarkeit, also ab wann eine E-Mail in den eigenen Verantwortungsbereich gelangt, Haftung und Archivierungs- sowie Aufbewahrungspflichten, muss zuallererst eine Einordnung des Begriffs E-Mail, in die gängigen Rechtsnormen erfolgen. Das Handelsrecht ist das Recht der Kaufleute. Ein Kaufmann im Sinne des Handelsgesetzbuches ist:

„(1) Kaufmann im Sinne dieses Gesetzbuchs ist, wer ein Handelsgewerbe betreibt.

(2) Handelsgewerbe ist jeder Gewerbebetrieb, es sei denn, daß das Unternehmen nach Art oder Umfang einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb nicht erfordert.“ (§ 1 HGB)

§ 1 Abs 2 HGB lässt erkennen, dass jeder Kaufmann ist, wenn seine geschäftliche Tätigkeit ausnahmsweise keinen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert. Dazu gehört z. B. eine doppele Buchführung oder die Erstellung eines Inventars. Hiervon ausgenommen sind laut § 241a HGB:

„Einzelkaufleute, die an den Abschlussstichtagen von zwei aufeinander folgenden Geschäftsjahren nicht mehr als jeweils 600.000 Euro Umsatzerlöse und jeweils 60.000 Euro Jahresüberschuss aufweisen, brauchen die §§ 238 bis 241 nicht anzuwenden. Im Fall der Neugründung treten die Rechtsfolgen schon ein, wenn die Werte des Satzes 1 am ersten Abschlussstichtag nach der Neugründung nicht überschritten werden.“.

Kaufmann ist somit jeder, der mit seinem Gewerbe die Umsatz- oder Jahresüberschüsse erreicht oder übersteigt. Ausnahmen davon bestehen jedoch z. B. für die Land- und Forstwirtschaft oder freie Berufe. Diese Sonderfälle sollen jedoch an dieser Stelle nicht weiter vertieft werden. Weitere Informationen finden sich u. a. in folgenden nicht abschließenden Normen:

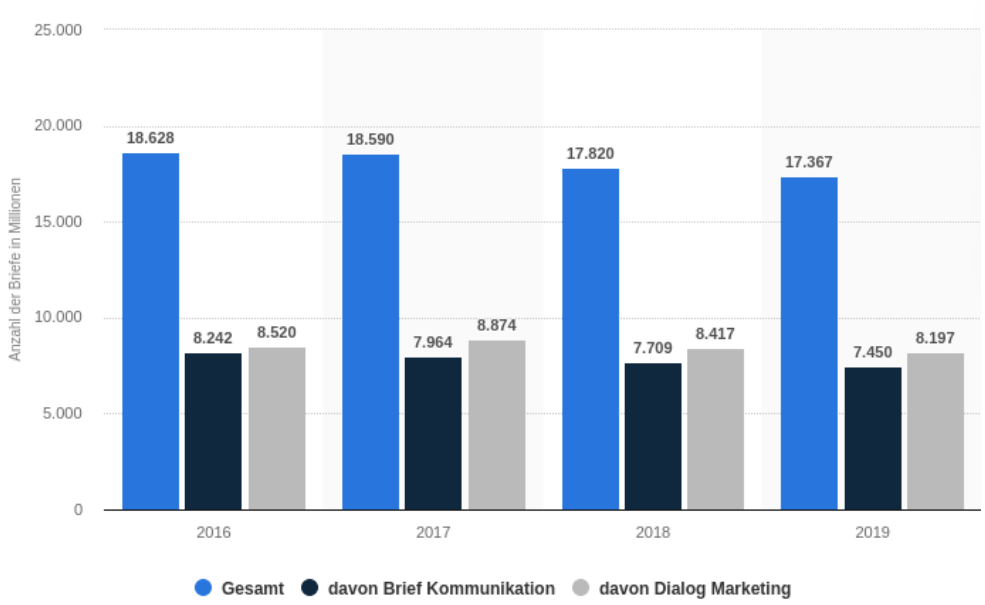
§ 18 Abs. 1 EstG sowie § 3 Abs. HGB.

Ferner steht es jedem frei, sich freiwillig in das Handelsregister einzutragen. Hierdurch wird man automatisch Kaufmann mit allen Rechten und Pflichten.

„Ein gewerbliches Unternehmen, dessen Gewerbebetrieb nicht schon nach § 1 Abs. 2 Handelsgewerbe ist, gilt als Handelsgewerbe im Sinne dieses Gesetzbuchs, wenn die Firma des Unternehmens in das Handelsregister eingetragen ist. Der Unternehmer ist berechtigt, aber nicht verpflichtet, die Eintragung nach den für die Eintragung kaufmännischer Firmen geltenden Vorschriften herbeizuführen. Ist die Eintragung erfolgt, so findet eine Löschung der Firma auch auf Antrag des Unternehmers statt, sofern nicht die Voraussetzung des § 1 Abs. 2 eingetreten ist.“ (§ 3 HGB)

Das Handelsgesetzbuch nennt in § 257 Abs. 1 - als eine von mehreren - Kaufmannspflichten, die Aufbewahrung und Archivierung von empfangenen und abgesandten Handelsbriefen. Dass es sich hier um einen sehr alten Begriff für den klassischen Brief handelt, ist unstreitig. Dass dies auch Anwendung auf die E-Mail finden muss ist nur zeitgemäß (Thomson, 2009, S. 208). Der Brief ist ein rückläufiges Medium.

Abb. 1 – Anzahl beförderter Briefsendungen durch Deutsche Post 2016-2019



Quelle: Deutsche Post Geschäftsbericht 2019[10], Seite 47 i. V. m. Statista-Auswertung

Die fehlende Differenz zur Gesamtanzahl entfällt auf nationale Paketsendungen, die in der Statistik nicht gesondert aufgeführt werden.

Demgegenüber standen im Jahr 2018, 848[11] Milliarden versandter E-Mails allein in Deutschland. Die tatsächliche Zahl ist noch höher, da eine E-Mail-Übertragung nicht zwingend über einen der großen E-Mail-Anbieter erfolgen muss, sondern in der Regel durch Firmen selbst mit eigener Infrastruktur umgesetzt werden kann.

Rechtsnormen sind bei der Verweisung auf den Handelsbrief, somit auch analog auf die E-Mail anzuwenden. Auf das Telefax wird aufgrund der veralteten Technik, obwohl dies immer noch eine praktische Relevanz hat, nicht weiter eingegangen. Fällt jedoch ebenso unter den Begriff des Handelsbriefes.

5. Wann muss welche E-Mail wie verschlüsselt werden?

Zur Beantwortung der Frage, welcher E-Mail Inhalt unter welchen Umständen verschlüsselt werden muss, hilft ein Blick in die Datenschutzgrundverordnung. Leider ist die Formulierung sehr generell und

10 https://www.dpdhl.com/content/dam/dpdhl/de/media-center/investors/documents/geschaeftsberichte/DPDHL-Geschaeftsbericht-2019.pdf

11 https://de-statista-com.pxz.iubh.de:8443/infografik/12826/anzahl-verschickter-e-mails-in-deutschland/

muss erst ausgelegt werden. Art. 5, Abs. 1f DSGVO nennt – für die Art der Verarbeitung – wozu auch der Versand bzw. die Übermittlung von E-Mails zählt:

„(..) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung (..)“. Dies muss jetzt jedoch kombiniert werden mit Art. 32, Abs. 1 DSGVO:

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (..)„

Hier ist zu erkennen, dass es keineswegs eine konkrete Verpflichtung für einen bestimmten Typ Verschlüsselung gibt, noch, dass dies eine allgemein gültige Vorgabe ist, die für alle Unternehmen oder Informationen bei der Übermittlung anwendbar sei. Dies ist auszulegen durch den hinsichtlich Implementierungskosten, Art und Umfang sowie den Umständen der Verarbeitung genannten Umständen. Stellt man auf die Vorgabe des Standes der Technik ab, ist jedoch festzuhalten, dass die Verschlüsselung für alle beteiligten IT-Systeme und Endgeräte, seit vielen Jahren verfügbar und somit die Verschlüsselung bei der Übertragung von personenbezogenen Daten verpflichtend ist. Unter personenbezogenen Daten – wie eingangs erwähnt – sind all jene Informationen zu erfassen, die dazu geeignet sind, den Einzelnen in der Masse zu identifizieren, also z. B. eine E-Mail mit einer persönlichen Auftragsbestätigung (Venzke-Caprarese, 2020, S. 4).

Wie bereits eingangs erwähnt, kommt für die Verschlüsselung eine Transport- oder Ende-zu-Ende-Verschlüsselung in Betracht, wie im Folgenden erklärt wird.

Die Transportverschlüsselung ist die einfachste Art der Verschlüsselung und erfordert lediglich, dass die beteiligten Endgeräte und E-Mail-Server, eine aktuelle Verschlüsselung unterstützen. Folgendes Ablaufschema zeigt die Nachrichtenübermittlung auf Basis einer Transportverschlüsselung. Zu erkennen ist, dass die jeweils grünen Linien eine verschlüsselte Übermittlung darstellen. Die blauen Felder zeigen jeweils die beteiligten Geräte oder Server, die den Inhalt der E-Mail im Klartext lesen können. Es kommt hier zu mehreren individuellen Ver- und Entschlüsselungsvorgängen:

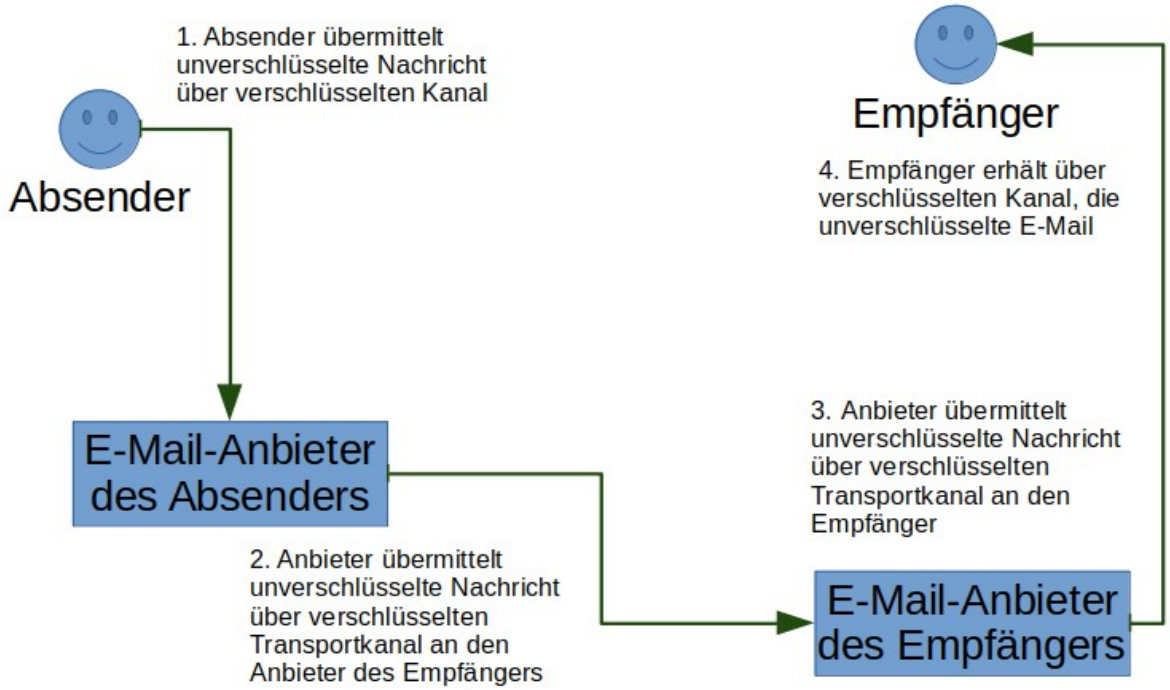
1. Der Absender übermittelt die unverschlüsselte Nachricht über einen verschlüsselten Transportkanal an seinen Anbieter

2. Der E-Mail-Anbieter übermittelt die unverschlüsselte Nachricht über einen verschlüsselten Transportkanal, an den Anbieter des Empfängers

3. Der E-Mail-Anbieter des Empfängers, übermittelt die unverschlüsselte Nachricht über einen verschlüsselten Transportkanal an den Empfänger

4. Der Empfänger erhält die Nachricht im Klartext über einen verschlüsselten Transportkanal und kann sie lesen

Abb. 2. Nachrichtenübermittlung auf Basis der Transportverschlüsselung



Quelle: Eigene Darstellung.

Jeder Pfeil ist eine Transportverschlüsselung, die je nach Unterstützung der beteiligten Parteien, einmal mehr oder weniger sicher ausfallen kann oder aufgrund von Inkompatibilität, gar nicht zum Einsatz kommt. Technisch findet pro Vorgang, eine individuelle Aushandlung der möglichen Verschlüsselung statt.

Aufgrund der Transportverschlüsselung, wird jeweils jedoch nur der Transport von einer Station (Absender, Mailserver, Empfänger) zur nächsten verschlüsselt. Hierdurch liegen die Informationen jeder Station kurzfristig im Klartext vor. Dies ermöglicht Strafverfolgungsbehörden, Informationen beim Anbieter mitzulesen. Deutsche Anbieter sind hierzu laut TKG (Telekommunikationsgesetz) verpflichtet,

geeignete Maßnahmen zu ertüchtigen, damit Informationen einfach mitgelesen werden können. § 110 TKG normiert:

"Wer eine Telekommunikationsanlage betreibt, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, hat (..) ab dem Zeitpunkt der Betriebsaufnahme (..) technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten (..)". Ein weitreichender Beschluss (2 BvR 2377/16) erging hier im Jahr 2018 durch das Bundesverfassungsgericht. Ein deutscher E-Mail-Anbieter stellte sich auf den Standpunkt, dass er keine Daten seiner Kunden erfasse und deshalb auch keine Daten den Strafverfolgungsbehörden zur Verfügung stellen könne. Zur weiteren Vertiefung sei auf die Pressemeldung[12] des BVG verwiesen.

Die Transportverschlüsselung ist jedoch in der Praxis meistens nur optional konfiguriert (Holz, 2015, S. 14). Ein Anbieter versendet lieber eine E-Mail im Klartext, als gar nicht. In der Praxis zeigt sich, dass aus Kundensicht eine nicht zustellbare E-Mail deutlich unangenehmer wahrgenommen wird, als eine unverschlüsselte E-Mail. Die Sensibilisierung für das Thema Datenschutz ist noch nicht dergestalt flächendeckend ausgebildet, dass für den Einzelnen die Vorteile der Datensicherheit, die Bequemlichkeit beim einfachen Versand überwiegen. In Anbetracht der hohen Bußgelder durch die DSGVO ist dies unverständlich.

Die Ende-zu-Ende Verschlüsselung kann als alternative oder ergänzende Sicherheitsebene zur Transportverschlüsselung betrachtet werden. Wie bei der Transportverschlüsselung, wird die zu übermittelnde Nachricht von Station zu Station transportiert und idealerweise auch verschlüsselt.

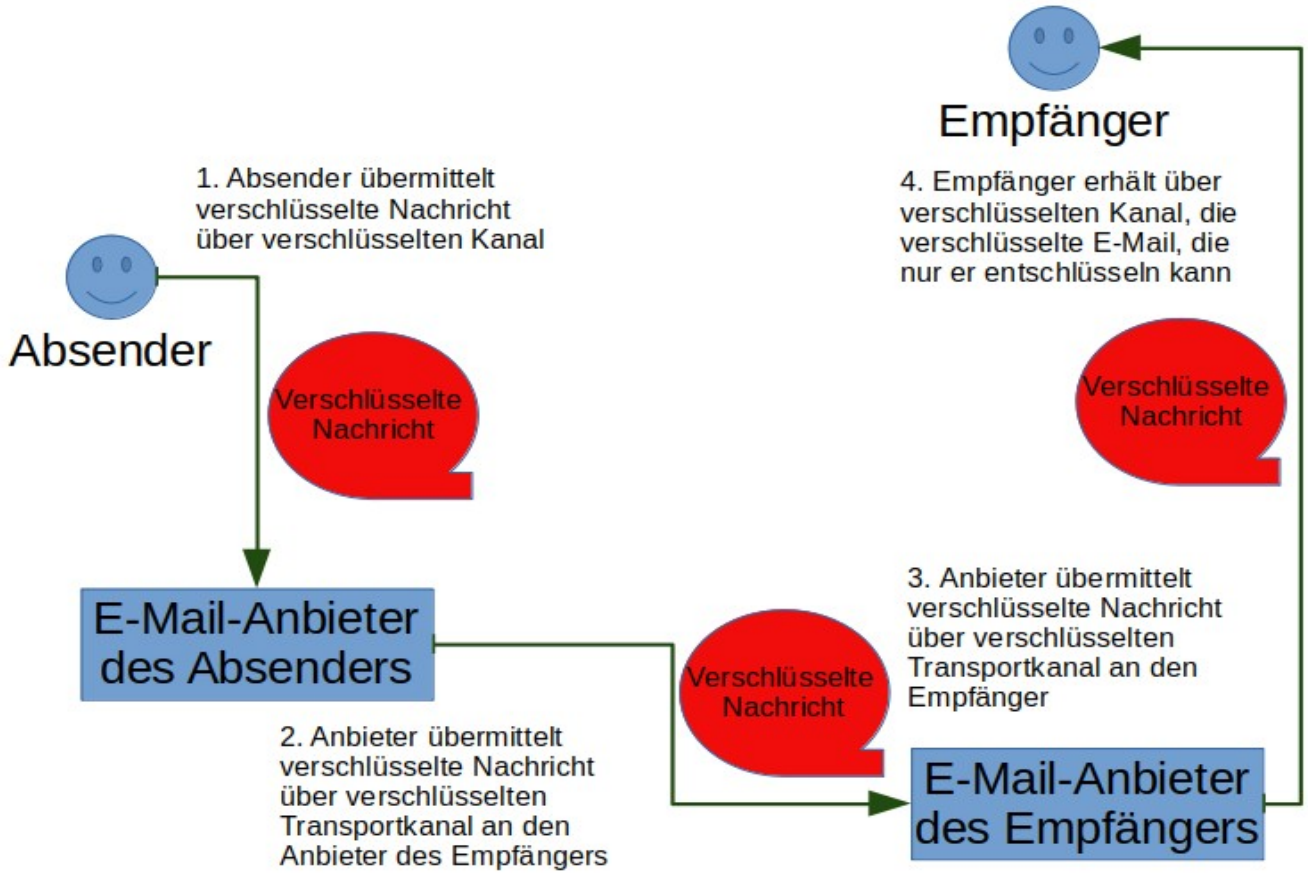
Zusätzlich verschlüsselt jedoch der Absender und Empfänger – ohne Teilnahme an der Ver- oder Entschlüsselung der Stationen dazwischen – auf Grundlage eines gemeinsamen Schlüssels, die Nachricht selbst. Am Beispiel der Strafverfolgungsbehörden kann zwar im Überwachungsfall die Nachricht beim Anbieter ausgeleitet werden, ist jedoch nicht im Klartext lesbar und somit weiterhin geschützt. Eine angemessene Verschlüsselung ist deutlich erkennbar, nicht im Interesse der Strafverfolgungsbehörden. Die Hinterlegung von Zweitschlüsseln für die Strafverfolgungsbehörden, wurde bereits vor Jahrzehnten diskutiert und gefordert. Kann jedoch als generell großes Risiko bezeichnet werden, da es faktisch einen Bruch der Verschlüsselung darstellt (Abelsen, 1997, S. 10-11). Dass zeitnah die Pflicht zur Hinterlegung von Zweitschlüsseln durch Anbieter besteht, zeigt der Resolutionsentwurf des EU-Ministerrats 12143/20 vom 21. Oktober 2020[13].

12 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2019/bvg19-007.html

13 https://data.consilium.europa.eu/doc/document/ST-12143-2020-INIT/en/pdf

Nachfolgende Abbildung zeigt die Ende-zu-Ende Verschlüsselung:

Abb. 3. Optionale Ende-zu-Ende-Verschlüsselung zur bestehenden Transportverschlüsselung



Quelle: Eigene Darstellung

Die Ende-zu-Ende Verschlüsselung besitzt jedoch hohe Hürden für Nutzer und ist in der Praxis wenig tauglich. Einerseits muss der Absender und Empfänger dasselbe Verfahren für die Ver- und Entschlüsselung benutzen. Im einfachsten Fall ist dies ein gemeinsames Kennwort, welches man z. B. telefonisch ausgetauscht hat. Hieraus ergibt sich schon ein großer Verwaltungsaufwand, kommuniziert man mit wechselnden Personen und möchte zu späterer Zeit, auch alte E-Mails erneut lesen. Müssen doch alle ausgehandelten Kennwörter, dokumentiert werden. Weiter gestaltet sich die typische Vertretungsregelung im Unternehmen schwierig. Da die Verschlüsselung zwischen zwei Teilnehmern erfolgt, kann ein Dritter (Kollege) in Abwesenheit des Empfängers, jene Mails nicht einfach lesen. Ein weiteres Problem ergibt sich bei der Langzeitablage. Alle E-Mails müssen für die dauerhafte Ablage wieder entschlüsselt werden, um sie im Klartext zu archivieren (Schleipfer, 2020, S. 1-2).

Die Meinungen ob für die Übermittlung eine Transportverschlüsselung genügt oder eine Ende-zu-Ende-Verschlüsselung nötig ist, sind uneins. Das Bayerisches Landesamt für Datenschutzaufsicht fordert

in seinem 9. Bericht[14] für Geheimnisträger (z. B. Ärzte, Rechtsanwälte, Steuerberater uvw. Laut § 53 Abs. 1ff StPO) das „(..) Vorhandensein einer Transportverschlüsselung. “Sowie bei einem hohen Risiko, eine Ende-zu-Ende Verschlüsselung. Auch wird darauf hingewiesen, dass bei einer Übermittlung in das Postfach eines FreeMail-Anbieters, (wie z. B. GMX, Yahoo, Web.de uvw.) der Absender dafür Sorge tragen muss, dass die E-Mail-Inhalte nicht zu Werbezwecken genutzt werden. Wie dies in der Praxis umzusetzen ist, ist fragwürdig. Müsste sich doch der Absender vor Versand jeder E-Mail die Informationen beschaffen, in welchem vertraglichen Verhältnis der Empfänger zu seinem FreeMail-Anbieter steht und ob hier zu Werbezwecken Daten ausgewertet werden. Dies kann nicht richtig sein, da es dem Absender nicht möglich ist, Einsicht in Vertragsdetails zu nehmen bzw. es mit erheblichem Zeit- und Kostenaufwand verbunden wäre, vor dem Versand, jeweils eine umfangreiche Recherche durchzuführen.

Eine andere Auffassung vertritt der Landesbeauftragte für den Datenschutz Baden-Württemberg in seinem 35. Tätigkeitsbericht[15] wie folgt:

„Werden regelmäßig (sensible) personenbezogene Daten zwischen Unternehmen, Arztpraxen/Kliniken oder Behörden, etc. ausgetauscht, so entspricht E-Mail ohne Ende-zu-Ende-Verschlüsselung ohnehin nicht dem Stand der Technik.“

Dass durch den Föderalismus jedoch jede Gemeinde und Stadt, in der Regel ihre eigene IT-Landschaft betreibt, trägt nicht dazu bei, einheitliche, konforme und vor allem aktuelle Kommunikationswege zu schaffen. Dies zeigt nachfolgende Auswertung der verfügbaren Verschlüsselungsmethoden der 6 größten Städte/Gemeinden im Landkreis Traunstein (Bayern).

Tab. 2. Auswertung verfügbarer Verschlüsselungsmethoden der 6 größten Städte/Märkte

Stadt/Markt	**Beste Verschlüsselungsmethode und weitere Probleme**	**Technischer Stand der Verschlüsselung**
Traunreut	TLSv1.2 + falsches Zertifikat	2008
Traunstein	TLSv1.2	2008
Trostberg	TLSv1.2 + falsches Zertifikat	2008
Tittmoning	TLSv1.3	2018

14 https://www.lda.bayern.de/media/baylda_report_09.pdf

15 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf

Waging am See	TLSv1.2	2008
Grassau	TLSv1.2 + falsches Zertifikat	2008

Quelle: Eigene Auswertung vom 18.02.2021 mit dem Testprogramm openssl s_client[16].

TLS steht für Transport Layer Security. TLS ist ein Protokoll zur Verschlüsselung der Datenübertragung im Internet und ist in seiner aktuellen Version 1.3,[17] seit 2018 verfügbar (Rescorla, 2018, S. 1). Falsches Zertifikat meint, dass der Absender keine Möglichkeit besitzt, zu prüfen, ob er tatsächlich mit dem richtigen E-Mail-System kommuniziert. Generell zeigt nachfolgende Tabelle auf, dass 1999 bereits massentaugliche Verschlüsselung veröffentlicht wurde, die bis heute Gültigkeit hat und im Einsatz ist. Diese aber keineswegs in der aktuellen Version, sofort und überall zum Einsatz kommt oder Verwendung findet. Lediglich eine von 6 Städten/Märkten nutzt bereits den aktuellsten Standard. Dies zeigt, dass es in der Praxis viele Jahre dauert, bis sich ein Stand der Technik, auch tatsächlich flächendeckend ausbreitet.

Tab. 1. Übersicht der Erscheinung der Verschlüsselungsversionen inkl. Verwendung/Gültigkeit

Version	Erscheinungsjahr	Bemerkungen
SSL 1.0	1994	
SSL 2.0	1995	Verwendung seit März 2011 unzulässig.[18]
SSL 3.0	1996	Verwendung seit Juni 2015 unzulässig.[19]
TLS 1.0	1999	Unterstützung läuft aus. Entspricht seit 30. Juni 2018 nicht mehr dem Payment Card Industry Data Security Standard (PCI DSS) im Zahlungsverkehr.[20]
TLS 1.1	2006	Unterstützung läuft aus. Da TLS 1.1 die nicht kollisionsresistente Hashfunktion SHA-1 für die Signaturerstellung verwendet, rät das BSI von dessen Nutzung ab.[21]
TLS 1.2	2008	
TLS 1.3	2018[22]	RFC 8446, enthält auch neue Anforderungen für TLS 1.2[23]

Legende:	Ältere Version; nicht mehr unterstützt	Ältere Version; noch unterstützt	**Aktuelle Version**	Zukünftige Version

Quelle: https://de.wikipedia.org/wiki/Transport_Layer_Security#Versionen

Auch der hessische Beauftragte für Datenschutz und Informationssicherheit, nennt in seinem 48. Tätigkeitsbericht[18] beim Versand von personenbezogenen Daten per E-Mail, über ein Web-Kontaktformular folgende Voraussetzung:

16 https://www.openssl.org/docs/man1.0.2/man1/openssl-s_client.html

17 https://tools.ietf.org/html/rfc8446

18 https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2019_48_TB.pdf

„Stellt ein Dienstleister ein verschlüsseltes Kontaktformular seinen Kunden zur Verfügung, sollte die automatisiert generierte Eingangsbestätigung per E-Mail ohne Mitteilung personenbezogener Daten erfolgen, da nicht sicher gestellt werden kann, dass der Anbieter des E-Mail-Dienstes des Kunden eine Transportverschlüsselung ermöglicht."

Dies kann im Umkehrschluss so ausgelegt werden, dass die Transportverschlüsselung für die Übermittlung von personenbezogenen Daten ausreichend ist, was zumindest im Hinblick auf die Einfachheit der Umsetzung und der Implementierungskosten, (siehe Art. 32, Abs. 1 DSGVO) zu begrüßen ist.

Findet jetzt eine oder keine Verschlüsselung bei der E-Mail-Übertragung statt, meldet sich beim technischen Dialog sodann in der Regel der Spam- und Virenfilter des Empfängers. In welcher Ausprägung dieser zum Einsatz kommt, zeigt das nächste Kapitel.

6. Einfluss von Spam- und Virenfilter auf E-Mails

Ein Spam- und Virenfilter kann in zwei Formen zum Einsatz kommen. Entscheidet sich der Empfänger für den eigenen Betrieb eines passenden Filters, findet dies in seinem Einflussbereich und in der Regel auf und durch eigene Hard- und Software statt. Alternativ kann er von einem Dritten diese Leistung in Anspruch nehmen. Dies wird meistens in Form einer Clouddienstleistung erbracht. Die weiteren Ausführungen – auch im Hinblick auf Vertrags- und Haftungsfragen – beschäftigen sich primär nur mit Drittdienstleistungen in Form von Clouddiensten für die Erbringung der Spam- und Filterlösungen.

Zuallererst muss das Vertragsverhältnis zwischen Kunde und Cloudanbieter betrachtet werden.

Handelt es sich nur um die für einen gewissen Zeitraum hin bereitgestellte Nutzungsmöglichkeit, in Form der Filterung von eingehenden E-Mails gegen Spam und Viren, kann von einem Mietvertrag ausgegangen werden (Nitsch, 2017, S. 208). Hierbei stellt der Anbieter selbst, dem Kunden die Nutzung der Filterung eingehender E-Mails als Dienstleistung zur Verfügung.

Die durch den Anbieter bereitgestellte Dienstleistung kann als Cloud-Computing bezeichnet werden, wenn „(..)eine ortsunabhängige Abrufbarkeit von IT-Ressourcen ermöglicht wird, die von einem Anbieter bedarfsabhängig einer Vielzahl potentieller Nutzer zur Verfügung gestellt werden." (Schneidereit, 2017, S. 41).

Dies ist zu bejahen. Der Cloudanbieter stellt die Lösung für einen großen Nutzerkreis bereit und betreibt die Lösung nicht individuell für einen einzelnen Kunden. Die IT-Ressourcen werden dafür verwendet, eingehende E-Mails zu filtern, bewerten und zu vermitteln oder abzulehnen.

In der Praxis stellt der Anbieter in der Regel dem Kunden ein Kundencenter zur Verfügung, in welchem der Kunde selbst individuelle Feinanpassungen der Lösung vornehmen und somit das endgültige Verhalten des verwendeten Filters, beeinflussen kann. Für die Beurteilung ob eine E-Mail abgelehnt, angenommen oder gelöscht wird, bedienen sich Anbieter vordefinierter Regelwerke. Jene legt der Anbieter erstmals selbst fest. Zusätzlich ist es jetzt möglich, dass der Kunde Empfehlungen des Anbieters aus eigener Überzeugung abändert, um das Verhalten der Filter an eigene Bedürfnisse anzupassen. Ein Unterschied ist zu erkennen, wenn die Spamfilterung nur eine Nebenleistung ist und dem Kunden primär ein E-Mail-Postfach zur Verfügung gestellt wird.

Unter welchen Kriterien eine E-Mail als angenommen gilt, beantwortet das nächste Kapitel. Im Umgang mit Spam- und Viren, ergeben sich für den Diensteanbieter zwei generelle Prüfmethoden. Die Prüfung vor Annahme, sowie die Annahme und anschließende Prüfung. Dies kann verglichen werden mit einer Sichtprüfung eines Paketes auf etwaige Beschädigung, vor der Annahme des Paketes an der Haustür gegenüber dem Postboten. Zweiter Fall wäre die Annahme und anschließende Prüfung. Je nach Ergebnis, wird sodann das Paket ausgepackt oder zurück geschickt. Dieses Verhalten kann analog auf das Medium E-Mail übertragen werden.

Diensteanbieter können E-Mails bereits vor Annahme prüfen oder diese annehmen und erst dann prüfen. Abhängig vom Ergebnis der Prüfung löst dies unterschiedliche weitere Schritte aus. Nachfolgend sollen einige Beispiele aus der Praxis erörtert und bewertet werden.

Beispiel 1: Prüfung einer unauffälligen E-Mail vor Annahme und anschließender Zustellung

In diesem Fall wird die E-Mail in Echtzeit geprüft, während der Absender auf die erfolgreiche Annahme wartet. Nach erfolgreicher Prüfung wird dem Absender die Annahme quittiert. Die E-Mail wird an den Empfänger zugestellt. Unter welchen konkreten Umständen eine E-Mail als angenommen gilt und wie hierzu auch Gerichte geurteilt haben, wird im nächsten Kapitel noch weiter präzisiert.

Beispiel 2: Prüfung einer verdächtigen E-Mail vor Annahme und Ablehnung

Hier wird ebenso die E-Mail vor Annahme geprüft. Das Ergebnis ist jedoch negativ. Die E-Mail wird als verdächtig eingestuft und dem Absender gegenüber die Annahme verweigert. Der Empfänger bemerkt

diesen Zustellversuch in der Regel nicht. Dies ist vergleichbar mit einem im Unternehmen beauftragten Mitarbeiter, der gegenüber dem Postzusteller eine Werbesendung ablehnt.

Beispiel 3: Prüfung einer auffälligen E-Mail nach Annahme und anschließender Zustellung

Dem Absender wird die Zustellung der E-Mail ungeprüft quittiert. Anschließend prüft der Cloudanbieter die E-Mail und bemerkt einen verdächtigen Inhalt. Der E-Mail-Betreff wird durch den Anbieter um den Zusatz [Spam] oder [Virus] ergänzt und die E-Mail an den Empfänger übermittelt.

Beispiel 4: Prüfung einer virulenten E-Mail nach Annahme und nachträglichen Ablehnung

Auch hier erfolgt eine umgehende Annahmebestätigung gegenüber dem Absender. Nachträglich wird die E-Mail geprüft und als Schadsoftware erkannt. Da der Empfänger keine virulenten E-Mails wünscht, wird durch den Cloudanbieter eine neue E-Mail – die Unzustellbarkeitsmeldung – an den ursprünglichen Absender verschickt. Hierdurch entsteht ein neues Problem für den Cloudanbieter. Das sogenannte Backscatter-Problem.

Das Backscatter-Problem entsteht dadurch, dass häufig Spam- und Viren-E-Mails einen gefälschten Absender tragen. Durch die nachträgliche Unzustellbarkeitsmeldung des Cloudanbieters, bekommt somit ein häufig völlig Unbeteiligter eine Unzustellbarkeitsnachricht für eine E-Mail, die er selbst gar nicht verschickt hat. Er jedoch der einzige Kontakt ist, der aufgrund des gefälschten Absenders über die Unzustellbarkeit informiert werden kann. Der Cloudanbieter wird also häufig unwissend und unabsichtlich, selbst zum Spam- oder Virenversender und der Empfänger der Unzustellbarkeit wundert sich über eine Unzustellbarkeit für eine E-Mail, die er nicht auf den Weg gebracht hat (Fuhrmann, 2008, S. 1).

Zusätzlich ändert auch das nachträgliche Zurücksenden einer E-Mail, durch den E-Mail-Anbieter des Empfängers nichts daran, dass die E-Mail bereits einmal als erfolgreich zugestellt, bzw. angenommen quittiert wurde. Wie dies weiter zu bewerten ist, wird im Kapitel 6 noch ausführlicher erläutert. Auf die Briefzustellung übertragen würde dieser Sachverhalt bedeuten, dass am Postschalter ein Paket mit falschem Absender eingeliefert wird, welches der Empfänger nach Annahme als ungeeignet deklariert und zurück sendet. Dadurch erhält jedoch ein Fremder ein Paket zurück, welches er nie abgeschickt hat.

Beispiel 5: Prüfung einer virulenten E-Mail nach Annahme und nachträglichen Löschung

Annahme der E-Mail sowie Prüfung und Beurteilung, mit dem Ergebnis, dass der Inhalt unerwünscht bzw. schadhaft ist. Jetzt entscheidet sich der Anbieter aufgrund eigener Vorgaben oder Kundenvorgaben, dass virulente E-Mails ungesehen gelöscht werden sollen (drop). Dem Absender wurde also auch hier die Annahme quittiert. Der Empfänger bemerkt jedoch die unterdrückte E-Mail nicht. Ein Urteil – wenn auch aus der analogen Postzustellung – was jedoch ebenso auf die digitale Übermittlung per E-Mail anwendbar ist aus dem Jahr 2003, (AZ: 4 Ss 1058/02 OLG Hamm) liefert folgenden Leitsatz:

„Ein Briefzusteller der Deutschen Post AG, der Postwurfsendungen, wie z.B. Reklameflyer einer Möbelfirma nicht austeilt, sondern in einen Abfallcontainer wirft, unterdrückte unbefugt die der Deutschen Post AG zur Übermittlung anvertrauten Sendungen und macht sich wegen Unterdrückung von Postsendungen nach § 206 Abs. 2 Nr. 3 StGB strafbar."

Für die Praxis ist jeweils wichtig zu erkennen, dass in der Regel der Anbieter bzw. Cloudanbieter mit seinem Kunden vertraglich – oder durch Allgemeine Geschäftsbedingungen – regelt, wie sich das Produkt Spamfilter bzw. Virenfilter in jeweiligen Fällen zu verhalten hat. Viele Anbieter wählen ebenso den rechtssicheren Weg, dem Kunden lediglich das Werkzeug Spamfilter an die Hand zu geben, so dass dieser letztlich die invasive Einstellung selbst, erstmalig aktivieren muss. Ohne eine vertragliche Regelung, macht sich der Cloudanbieter der eigenmächtigen Unterdrückung strafbar.

7. Zurechenbarkeit und Rechtsfolgen des E-Mail-Empfangs

Ab wann sich ein Empfänger eine E-Mail zurechnen lassen muss, hängt zuallererst davon ab, ob der Empfänger überhaupt per E-Mail erreichbar sein will. Dies setzt voraus, dass der Empfänger grundsätzlich einen Zugang per E-Mail eröffnet. Also ob er über das Medium E-Mail, grundsätzlich erreichbar sein will. Dies kann angenommen werden, wenn er nach außen hin, im Geschäftsverkehr mit seiner E-Mail-Adresse auftritt (Specht-Riemenschneider, 2020, S. 276). Diese Voraussetzung ist zu prüfen, da es möglich ist, dass ein Dritter dem Absender eine E-Mail-Adresse des Empfängers mitteilt, welche der Empfänger seit Jahren nicht mehr verwendet oder diese eine rein private Adresse darstellt, die nicht für die geschäftliche Kommunikation vorgesehen ist.

Weiter kann dann definiert werden, unter welchen Umständen eine E-Mail als zugestellt gilt. Zur weiteren Vereinfachung wird davon ausgegangen, dass es sich beim Inhalt der E-Mail um eine Willenserklärung im rechtlichen Sinne handelt. § 130 Abs. 1 BGB nennt hierzu:

„(1) 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. (…)“

Man spricht hier von der Empfangstheorie (Gerstberger, 2018, S. 85-87).

Eine E-Mail wird nicht persönlich und materiell unter Anwesenden übergeben, sondern virtuell und über Zwischenstationen bei der Übermittlung und somit unter Abwesenden. Es handelt sich hierbei um eine asynchrone Kommunikation. Absender und Empfänger sprechen nicht direkt miteinander.

Bei der synchronen Datenübertragung, bleibt die Verbindung während der Übertragung bestehen. Ein Beispiel ist das persönliche Gespräch oder Telefonat oder eine direkte Nachrichtenübertragung zwischen Absender und Empfänger, ohne Zwischenstationen (Baun, 2019, S. 20). Eine E-Mail wird gerade nicht unter Anwesenden übergeben, bzw. übertragen, sondern über mehrere Zwischenstationen hinweg, – auf dem Weg zum Ziel – übermittelt.

Hinsichtlich der Frage der Zustellung, muss der Absender die Zustellung beweisen. Also der, der sich darauf beruft, dass die E-Mail zugestellt wurde (Specht-Riemenschneider, 2020, S. 279).

Eine E-Mail geht einer Person zu, wenn die E-Mail in dessen Einflussbereich, gelangt. Also wenn der Empfänger über sie verfügen kann. Dies ist dann der Fall, wenn er sie z. B. aussortieren, beantworten, löschen oder vernichten kann, also uneingeschränkten Zugriff auf sie hat. Beauftragt er einen Dritten mit diesen Aufgaben, handelt es sich um einen Erfüllungsgehilfen, (siehe § 278 BGB), der nur im Interesse des Auftraggebers handelt, somit im übertragenen Sinn, von diesem gesteuert wird. Dies wäre der Fall bei der Inanspruchnahme von E-Mail-Diensten eines E-Mail-Anbieters oder Cloud-Dienstleistungen, zur Spam- oder Virenprüfung.

Ein Empfänger muss sich somit den Empfang einer E-Mail zurechnen lassen, wenn diese in dessen Einflussbereich gelangt. Die Rechtsfolgen sind jeweils abhängig von der konkreten Vertragsgestaltung, bzw. dem Inhalt der übermittelten Willenserklärung. Häufig beginnt der Ablauf einer gesetzten Frist oder aber auch die Annahme eines Geschäfts, durch Schweigen im Geschäftsverkehr bei Zugang eines Auftrages. § 362 HGB normiert:

„Geht einem Kaufmanne, dessen Gewerbebetrieb die Besorgung von Geschäften für andere mit sich bringt, ein Antrag über die Besorgung solcher Geschäfte von jemand zu, mit dem er in Geschäftsverbindung steht, so ist er verpflichtet, unverzüglich zu antworten; sein Schweigen gilt als Annahme des

Antrags. Das gleiche gilt, wenn einem Kaufmann ein Antrag über die Besorgung von Geschäften von jemand zugeht, dem gegenüber er sich zur Besorgung solcher Geschäfte erboten hat.“

Hier ist zu erkennen, dass eine E-Mail – analog zum Brief – die im Einflussbereich des Empfängers landet, als Vertragsannahme zu werten ist, wenn eine Antwort unterbleibt.

Der Schwerpunkt der weiteren Betrachtung dient der Definition, ab wann eine E-Mail – technisch – als zugestellt gilt und wie sich dies für den Absender beweisen lässt. Abschließend wird ein AG Hamburg Urteil vom 27.04.2018 (12 C 214/17) hinsichtlich der Zurechenbarkeit von E-Mail-Zustellungen betrachtet und aufgezeigt, wieso das Urteil im Kern richtig, die technische Argumentation jedoch irreführend ist.

7.1 Beweismittel als Zustellnachweis – die Empfangsquittung

Wie in Abb. 2 aufgezeigt, findet eine E-Mail-Übermittlung jeweils zwischen einem Absender und Empfänger, in Richtung des Empfängers statt. Auf technischer Ebene sprechen jedoch nur die E-Mail-Server des Absenders und Empfängers, in einer für den Nachrichtenversand vorgesehenen Sprache miteinander. Die Art und Weise wie hier miteinander kommuniziert wird, wurde bereits 1982 in einem Internet-Standard definiert, der zuletzt 2001 in einer überarbeiteten Version[19] veröffentlicht wurde. Dieser hat weltweite Gültigkeit. Um die reibungslose Übermittlung zu ermöglichen, operieren alle heute verfügbaren E-Mail-Server nach diesem Standard. Das zugrundeliegende Protokoll nennt sich SMTP und steht für Simple Mail Transfer Protocol. SMTP kann mit der Straßenverkehrsordnung verglichen werden. Ohne die Einhaltung von Regeln durch alle Teilnehmer eines Systems, wäre ein geordnetes Miteinander nicht möglich (Wittmaak, 2016, S. 1-2).

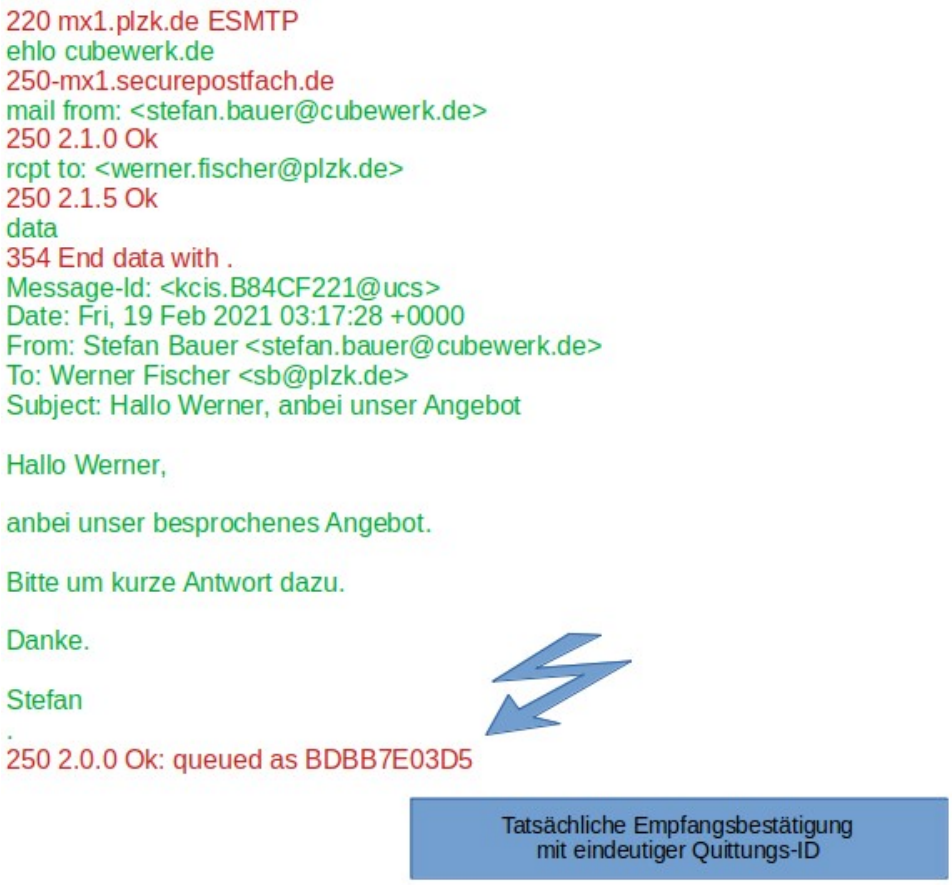
Schaltet ein Unternehmen zur Spam- und Virenprüfung, eine Dienstleistung eines Cloud-Anbieters vor seinen E-Mail-Server, da dieses die Leistungen nicht selbst erbringen kann oder will, operieren auch diese Systeme nach aufgezeigtem SMTP-Standard.

Wichtig anzumerken ist, dass die Abholung einer E-Mail aus dem durch einen Anbieter bereitgestellten Postfaches, in das lokale E-Mail-Programm wie z. B. Microsoft Outlook, nicht dem SMTP-Standard folgt und hier nicht weiter betrachtet wird. Rechtlich entscheidend für die Erbringung des Beweises der Zustellung, ist in der Regel nur die Kommunikation zwischen den ersten zwei Akteuren. Dem Server des Absenders sowie der Server des Empfängers, bzw. der Server eines vorgeschalteten Anti-Spam

19 https://tools.ietf.org/html/rfc2821

und Anti-Virus-Anbieters. Dies kann verglichen werden mit der Briefpostzustellung an ein Sammelpostfach. Ob, wie und in welchem zeitlichen Ablauf, nachträglich die Post den Weg innerhalb des Hauses zum Empfänger findet, ist für den Absender unerheblich. Nachfolgende Abbildung zeigt einen echten technischen Dialog zwischen Absender und Empfangsserver, zur Einlieferung einer E-Mail. Der Dialog ist aus Sicht des Absenders. Jedoch liegen auch dem Empfänger identische Informationen vor, da dieser ja mit dem Absender in bilateralem Kontakt steht. Der Dialog ist für den Absender und sein E-Mail-Programm grundsätzlich nicht direkt ersichtlich und passiert binnen weniger Sekunden automatisch im Hintergrund.

Abb. 4 – Technischer E-Mail-SMTP-Dialog zwischen Absender- und Empfangsserver



Quelle: Eigene Darstellung in Anlehnung an (Wittmaak, 2016, S. 3)

Der Dialog, bzw. die Übertragung beginnt in der ersten Zeile in roter Farbe. Rot steht jeweils im gesamten Dialog für Befehle bzw. Informationen, die der Empfänger bei der Übertragung von sich gibt Grün für Befehle, die der Absender übermittelt. Der Dialog beginnt zur Vereinfachung mit der Erstmeldung des Empfängers, der sich dem Absender gegenüber vorstellt. Dem voraus geht der Verbindungsaufbau des Absenders zum Empfänger. Im gezeigten Dialog, erfolgt die erste Meldung durch den Empfänger. Dies mag verwirrend erscheinen. Kann jedoch verglichen werden mit einem Tele-

fonat, wo zwar der Anrufer das Gespräch sucht, der Angerufene sich aber zuerst mit seinem Namen meldet.

Im weiteren Verlauf des technischen SMTP-Dialoges, übermittelt der Absender seine eigene E-Mail-Adresse (mail from) sowie die Adresse des Empfängers (rcpt to). Der Empfänger quittiert jeden Befehl. Dies hat den Grund, dass es hierbei bereits zu Fehlern der Übertragung kommen kann. Vergleichbar ist dies mit einer Person, die am Empfangsschalter der Post ein Paket aufgeben möchte und bereits das Paket über die Theke schiebt, der Postmitarbeiter jedoch darum bittet, in 30 Minuten nochmal zu kommen, da der Schalter gerade geschlossen ist, oder die Post keine Beförderung in spezielle Länder, bzw. die Beförderung von übergroßen Paketen übernimmt.

Es folgt der typische Aufbau der E-Mail, bestehend aus einer durch den Absender eindeutig generierten Nachrichtenkennung (Message-ID), dem Datum (Date) sowie erneut dem Absender inkl. Namen (From) und einem oder mehrerer Empfänger (To). Ergänzt wird jede E-Mail in der Regel mit einem Betreff, (Subject) gefolgt vom tatsächlichen E-Mail Inhalt. Die vermeintliche Dopplung der Nennung von Absender und Empfänger kommt daher, dass wie bei der Briefpost, der Umschlag selbst einen anderen Absender und Adressaten tragen kann, wie der Brief selbst, der vielleicht eine persönlichere Anrede enthält.

Beachtenswert und ein wesentlicher Schritt in der Nachrichtenübermittlung, ist der abschließende Punkt „.“ in der vorletzten Zeile. Hierdurch signalisiert der Absender das Ende seiner Nachricht. Dies kann verglichen werden mit der versuchten Übergabe einer Postkarte am Postschalter, in Richtung des Postmitarbeiters.

Mit der abschließenden Rückmeldung in der Form

„250 2.0.0 Ok: queued as BDBB7E03D5“

durch den Empfänger, wird die E-Mail angenommen und die Annahme quittiert. Dies kann verglichen werden mit der physikalischen und somit tatsächlichen Annahme der Postkarte am Postschalter, durch den Postmitarbeiter. Weiter noch, der Empfänger quittiert nicht nur die Annahme, sondern nimmt ebenso mit einer durch sich selbst generierten fortlaufenden Kennung, (BDBB…..) – die die Nachricht im System des Empfängers kennzeichnet – eine Kennzeichnung vor und und teilt diese dem Absen-

der mit. Dies ist vergleichbar mit der Aushändigung einer Quittung am Postschalter, in Form eines Quittungsbelegs zur Nachverfolgung.

An diesem Dialog ist zu erkennen, dass im Rechtsverkehr, dem E-Mail-System des Absenders, bei der Nachrichtenübermittlung klar signalisiert wird, ob eine E-Mail durch den Empfänger angenommen wurde oder nicht und sogar unter welcher Kennung, die E-Mail im System des Empfängers weiter transportiert wird. Im Vergleich zur Abgabe eines Briefes am Schalter, bzw. der Einwurf am Postkasten, stellt die Übermittlung per E-Mail deutlich aussagekräftigere Möglichkeiten in Form von Rückmeldungen bzw. Protokollen zur tatsächlichen Einlieferung zur Verfügung und vereinfacht somit die Beweisführung.

Trotz der eindeutigen Protokollierung des Empfängers, dass eine E-Mail angenommen wurde, findet sich in der Literatur eine teilweise andere Auffassung:

„Scheitert eine Übermittlung der Willensklärung (..) ist zu differenzieren, ob der Absender hierüber in Kenntnis gesetzt wurde (sog. „Bounce-Mail“) oder nicht. Wurde der Absender nicht von der Fehlübermittlung informiert, so muss er davon ausgehen können, dass die Erklärung dem Empfänger zugegangen ist. Demgegenüber ist der Zugang der Erklärung zu verneinen, wenn den Empfänger[sic] eine Bounce-Mail erreicht hat.“ (Specht-Riemenschneider, 2020, S. 278).

Eine Bounce-Mail ist eine Unzustellbarkeitsmeldung – anders wie im Text erwähnt, an den Absender – nach der Annahme. Obige Auffassung würde bedeuten, dass man eine als empfangen quittierte E-Mail, nachträglich wieder als unzustellbar zurückweisen könnte. Das kann nicht richtig sein. Lediglich falls die Unzustellbarkeitsmeldung vom eigenen E-Mail-System generiert wird, kann dies teilweise bejaht werden, da hier gerade noch keine erfolgreiche Übergabe an den Empfänger, durch diesen quittiert wurde. Ein Unterbleiben einer Fehlermeldung des eigenen Systems ist jedoch weiterhin noch kein Beweis, dass eine E-Mail tatsächlich übermittelt bzw. zugestellt wurde.

Zur Vertiefung und weiteren Forschung, sollen diese Informationen nun mit den Erkenntnissen aus Kapitel 6 kombiniert und ansatzweise weiter ausgeführt werden. In den Fällen wo die Spam- oder Virenprüfung vor der Annahme erfolgt, bedient sich der Empfangs-Mailserver eines Umstandes, dass die Quittierung der Nachrichtenannahme nicht sofort erfolgen muss. Dies ist vergleichbar mit dem Postmitarbeiter, dem zwar eine Postkarte entgegen gestreckt wird, dieser aber noch unschlüssig ist, ob er diese befördern kann oder will. Er kann jedoch den Text der Postkarte bereits lesen. Dies ist je-

doch – auf die E-Mail angewandt – nur möglich, wenn der Nachrichteninhalt der E-Mail nicht mit einer Ende-zu-Ende-Verschlüsselung auf den Weg gebracht wurde.

Nach dem Abschluss der Nachricht durch den Absender durch einen Punkt, „.“ (vgl. Abb. 4) kennt der Mailserver des Empfängers zwar bereit die Nachricht und kann diese prüfen, lesen und auswerten, hat aber dem Absender noch nicht quittiert, dass er diese annimmt oder gar komplett erhalten hat.

Viele Spam- und Anti-Viren Anbieter nutzen diesen Umstand für ihre Lösungen, um im letzten Dialog Mails noch ablehnen zu können, wenn der Inhalt der E-Mail, für den Empfänger unangemessen oder durch diesen nicht gewünscht ist. Aus juristischer Sicht ist dies für den Empfänger deutlich günstiger, da er sich die E-Mail nicht direkt zurechnen lassen muss und diese auch nicht als angenommen quittiert hat, den Inhalt aber technisch schon zu sehen bekommt. Wie die technische Annahme in der Praxis durch das AG Hamburg beurteilt wurde, wird im nächsten Kapitel noch näher ausgeführt.

Weitere Überlegungen wie der Umstand datenschutzrechtlich zu bewerten ist, dass dem Empfänger zwar der Inhalt einer E-Mail gezeigt wurde, er die ganze E-Mail jedoch technisch ablehnen kann und ob nicht doch dem Empfänger dadurch eine E-Mail unter diesem speziellen Sonderfall zuzurechnen ist, sollte noch weiter untersucht werden. Aufgrund der Schwierigkeit, dass solange der Empfänger die E-Mail nicht quittiert hat, es nicht bewiesen werden kann ob er die E-Mail tatsächlich erhalten hat, gestaltet sich die Beweisführung nahezu unmöglich. Besteht ja doch genau in diesem Fall die plausible Möglichkeit, dass er die E-Mail aufgrund eines Übertragungsfehlers tatsächlich nicht erhalten hat und deshalb auch die Annahme nicht quittieren kann. Auch ob der Empfänger, – der den E-Mail-Inhalt kennen könnte, diesen zur Spam- und Virenprüfung prüft und somit verarbeitet – datenschutztechnische Informationspflichten dem Absender gegenüber hat, sollte Gegenstand weiterer Untersuchungen sein.

Abschließend sei genannt, dass der zuvor verwendete Begriff der Ablehnung eine konkludente Handlung des Empfangsservers sein kann oder aber auch ein Schweigen, also keine Reaktion. Der SMTP-Standard sieht vor, dass eine Ablehnung oder keine Reaktion, wie ein temporärer oder dauerhafter Fehler zu bewerten ist und die E-Mail als nicht zugestellt bzw. erfolgreich übermittelt gilt.

Zuletzt soll für weitere Forschungen hinsichtlich der Zurechenbarkeit der Sachverhalt genannt werden, wo der Empfangsmailserver dauerhaft nicht erreichbar ist, bzw. immer ablehnt. Hier fehlt es dem Me-

dium E-Mail derzeit noch – anders wie im Briefverkehr – der Möglichkeit einer öffentlichen Zustellung wie in § 185 ZPO erwähnt.

7.2 Betrachtung des AG Hamburg Urteils - 12 C 214/17

Nachfolgend soll ein Urteil des Amtsgerichtes Hamburg, mit engem Bezug zur zuvor geschilderten Zurechenbarkeit betrachtet werden.

Die Absenderin war Kundin einer Fluggesellschaft und begehrte Ausgleichszahlungen aus einem Luftbeförderungsvertrag, für einen Flug zwischen Hamburg und Enfidha, Tunesien. Dies machte sie per E-Mail mit Fristsetzung geltend. Der Anbieter/Veranstalter stritt den Empfang der E-Mail ab. Die Absenderin konnte jedoch durch Protokolle belegen, dass der Empfänger die E-Mail angenommen hatte.

Das Gericht erkennt an, dass das bloße Absenden einer E-Mail nicht für die Zurechenbarkeit ausreicht, da dies auch kein Indiz dafür ist, dass eine E-Mail in den Einflussbereich des Empfängers gelangt. Dies ist nur schlüssig. Was das Gericht jedoch als Beweis akzeptiert, ist ein Protokoll des Mailsystems der Absenderin, welches belegt, dass eine E-Mail erfolgreich übermittelt wurde. Dieses Protokoll enthält – wie zuvor skizziert – mindestens das Datum, und die Kennung des Empfangssystems sowie die Bestätigung der Annahme. Ärgerlich ist hierbei die falsche technische Begründung des Urteils wie folgt:

„Allerdings hat die Klägerin durch Vorlage eines Ausdrucks aus ihrem Postausgangssystem die Bestätigung des Abrufs der E-Mail von dem Mailserver auf das E-Mail-Konto der Beklagten dargelegt. Diese Eingangsbestätigung setzt den Anschein der ordnungsgemäßen Ablieferung der Erklärung der Klägerin bei der Beklagten, sodass ein Anscheinsbeweis für den Zugang begründet wird (…)."

(AG Hamburg Urteils - 12 C 214/17).

Gemeint ist hier augenscheinlich wie in Abb. 4 dargestellt, die Quittierung der Annahme einer E-Mail. Ein Abruf selbst, ist nicht erfolgt. Dies wäre auch aus folgendem Grund nicht möglich gewesen:

Hätte ein tatsächlicher Abruf stattgefunden, hätte die abzuholende Partei beim Bereitsteller der E-Mail einen Zugang benötigt, um selbstständig die Abholung zu starten. Dies war in diesem genannten Urteil nicht der Fall. Der Absender war weder E-Mail-Anbieter, noch bot dieser ein E-Mail-Postfach für die Abholung an.

Hinsichtlich der Manipulationsmöglichkeit durch die Absenderin, da die Protokolle lediglich in Textform vorliegen und somit manipuliert werden könnten, führt das Gericht wie folgt aus:

„Zwar besteht die Möglichkeit, dass entweder der technische Vorgang oder die Aufzeichnung durch die beweisbelastete Partei manipuliert wird, allerdings ist diese Möglichkeit jeder Datenerhebung inhärent und reicht alleine nicht aus, einen Anschein zu zerstören. Ein Anscheinsbeweis verlangt nur Typizität des Geschehensablaufs, aber nicht den Ausschluss jedes Restrisikos(..)“.

Dies ist nur angemessen, da dem Empfänger ebenso identische Protokolle über die E-Mail-Kommunikation vorliegen und dieser entweder der Annahme entgegen halten könnte, dass sein E-Mail-System die Nachricht nachweislich abgelehnt hat oder dass keinerlei Übermittlung zu diesem Zeitpunkt durch den Absender versucht wurde.

7.3 Beweismittel als Zustellnachweis – Übermittlungs- und Lesebestätigung

Eine weitere bzw. zusätzliche Möglichkeit der Beweissicherung für den Absender, stellt die Lese- und/oder Übermittlungsbestätigung dar. Die Übermittlungsbestätigung (Delivery Status Notification[20] - DSN) ist eine zusätzliche Quittierung gegenüber dem Absender, ob und wann, erfolgreich eine E-Mail im weiteren Transport auf dem Weg zum Empfänger, transportiert wurde (Specht-Riemenschneider, 2020, S. 279).

Diese Bestätigung kann in der Regel durch den Absender selbst, in dessen E-Mail-Programm angefordert werden. Nicht alle E-Mail-Anbieter bieten die Rückmeldung von Übermittlungszuständen an den Absender an. Etliche DSGVO-konforme Produkte zur E-Mail-Verschlüsselung, bietet dies jedoch als Zusatzleistung In Form eines elektronischen Einschreibens für Absender an.

Die Übermittlungsbestätigung ist ein sinnvolles Mittel zur Beweisführung, falls auf die Protokolle des eigenen E-Mail-Servers oder die des eigenen E-Mail-Anbieters – um den tatsächlichen und erfolgreichen Übermittlungsdialog zu dokumentieren – nicht direkt zurückgegriffen werden kann.

Die Übermittlungsbestätigung wird in der Regel automatisch durch den E-Mail-Server des Empfängers generiert. Der tatsächliche Empfänger erhält hierüber keine Information oder kann dies direkt verhindern.

20 https://tools.ietf.org/html/rfc3463#section-3

Ferner besteht die Möglichkeit der Anforderung einer Lesebestätigung für den Absender. Da dies jedoch erfordert, dass der Empfänger bewusst eine Lesebestätigung auslöst, ist davon auszugehen, dass bewusst oder unbewusst, nicht jeder eine empfangene E-Mail quittiert, bzw. quittieren will oder gar technisch kann. Dies kann z. B. durch entsprechende IT-Richtlinien[21], auch unternehmensweit blockiert werden. Das OLG Koblenz bestätigte im AZ: 3 U 1895/19 am 20.03.2020 die Beweiskraft einer Lesebestätigung wie folgt:

„Bei E-Mails bedarf es zur Annahme eines Anscheinsbeweises vielmehr einer Lesebestätigung (BGH, NJW 2014, 556, 557, Rn. 11)(…)“ und präzisiert weiter: „Der bloße Nachweis des Absendens (…) genügt zur Begründung eines Anscheinsbeweises jedenfalls nicht“.

Dies ist nur konsequent. Der Versand bzw. das auf den Weg bringen einer E-Mail durch den Absender aus seinem E-Mail-Programm heraus, garantiert weder die korrekte Übermittlung an dessen E-Mail-Server, noch die Übergabe und Annahme der E-Mail durch den Empfänger durch seinen E-Mail-Server. Auf diesem Weg (vgl. Abb. 2) existieren mehrere potenzielle Fehlerquellen bei der Übermittlung, die nicht pauschal zu Lasten des Empfängers ignoriert werden dürfen. Nur weil ein Absender erfolgreich einen Brief in den Briefkasten wirft, erbringt dies nicht den Beweis der erfolgreichen Zustellung. Auch beim klassischen Postversand existieren ähnliche Fehlerquellen wie z. B. die unzureichende Frankierung oder die falsche oder unvollständige Adressierung.

8. Archivierungs- und Aufbewahrungspflicht für E-Mails

Unter einer Archivierung kann die Konservierung von Dokumenten bzw. Informationen verstanden werden, um diese bei Bedarf wieder abrufen zu können.

Ein Handelsbrief und somit eine E-Mail die unter diesem Begriff zu erfassen ist, durchläuft im Unternehmen unterschiedliche Etappen. Von der erstmaligen Sichtung bzw. Bearbeitung über die Aufbewahrung und Archivierung, bis zum endgültigen Vernichten und somit Ausscheiden aus dem eigenen Bestand bzw. Archiv (Riggert, 2019, S. 11).

21 https://docs.microsoft.com/de-de/windows-server/networking/branchcache/deploy/use-group-policy-to-configure-domain-member-client-computers

Abb. 5 – E-Mail Lifecycle im Unternehmen

Quelle: Eigene Darstellung in Anlehnung an (Riggert, 2019, S. 11)

Abhängig vom tatsächlichem Inhalt einer E-Mail oder deren Anhang, muss diese archiviert werden.

Aus unterschiedlichen Normen, Rechtsquellen und wirtschaftlichen Gepflogenheiten, ergeben sich für Unternehmen, Freiberufler, Kaufleute und Land- und Forstwirte, die Archivierungspflichten für Handelsbriefe und E-Mails. Zu nennende Rechtsquellen sind z. B. das Handelsgesetzbuch oder die Abgabenordnung im Steuerrecht. Sobald eine E-Mail, die nach deren Inhalt bzw. Umfang in eine der nachfolgend genannten Kategorien (Handelsbrief, Handelsbücher, Steuerbescheid uvw.) fällt, in den eigenen Zuständigkeitsbereich gelangt, besteht die Pflicht zur Archivierung (Ripper, 2010, S.2). Weiter zu nennen sind die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoDB). Speziell in Hinblick auf die Handelsbriefe aus § 238 und § 239 HGB definieren sich die Anforderungen wie folgt: (Riggert, 2019, S. 117)

„Der Kaufmann ist verpflichtet, eine mit der Urschrift übereinstimmende Wiedergabe der abgesandten Handelsbriefe (Kopie, Abdruck, Abschrift oder sonstige Wiedergabe des Wortlauts auf einem Schrift-, Bild- oder anderen Datenträger) zurückzubehalten.“ (§ 238 Abs. 2 HGB) sowie durch die Präzisierung in § 239 HGB wie folgt:

„Die Eintragungen in Büchern und die sonst erforderlichen Aufzeichnungen müssen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden.“.

Dies ergibt für den Verantwortlichen bei der Archivierung die Pflicht „eine mit der Urschrift übereinstimmende Wiedergabe der abgesandten Handelsbriefe (...) zurückzubehalten.“.

Die Grundsätze ordnungsgemäßer Buchführung, gelten für alle Betriebe die zur Buchhaltung verpflichtet sind und somit auch die Pflicht zur Archivierung und Aufbewahrung von Unterlagen. Hierunter fallen neben den klassischen Kaufleuten, auch alle weiteren gewerblichen Unternehmen und Land- und Forstwirte, sobald bestimmte jährliche Umsatzgrenzen überschritten werden. (vgl. hierzu § 141 Abgabenordnung). Aber eben auch alle weiteren freiberuflich Tätigen, die zwar nicht zu einer ordnungsgemäßen Buchführung verpflichtet sind, jedoch dem Finanzamt gegenüber durch Einnahmeüberschussrechnung zur Rechenschaft verpflichtet sind (vgl. § 147 Abs.1ff)(Goldshteyn, 2016, S. 13).

Die einschlägigen Gesetze zählen weiter auf, welcher Typ E-Mail bzw. welcher tatsächliche Inhalt, unter die Archivierungs- und Aufbewahrungspflicht fällt. Nachfolgend sollen die typischen Dokumente bzw. Vorgänge unter Nennung der einschlägigen Gesetzesquellen, genannt werden.

Bei Handelsbücher, Inventare, Bilanzen, Abschlüsse, Lageberichte, Konzernabschlüsse, Arbeitsanweisungen und Organisationsunterlagen, handelt es sich primär um für Steuer- und über feste Zeiträume relevante Abrechnungsunterlagen bzw. Unterlagen, die primär mit der Führung und Organisation des Unternehmens verbunden sind, statt konkrete Geschäftsabläufe oder Vorgänge zu dokumentieren. Bei empfangenen und versandten Handelsbriefen oder Geschäftsbriefen, handelt es sich um all jene Schriftstücke von Kaufleuten im Sinne des § 1 HGB, oder jener Personen, die zur Vorbereitung, Anbahnung, dem Abschluss oder dem Widerruf eines Handelsgeschäftes, dienen. Somit z. B. Angebote, Auftragsbestätigungen, Bestellungen, Reklamationen usw. (Speichert, 2007, S. 292).

Buchungsbelege sind all jene Belege die dazu dienen, nachträglich einen erfassten Buchungsvorgang zu validieren. Also jene Belege, die die Grundlage für eine Buchung darstellen wie z. B. Rechnungen, Steuerbescheide, Lieferscheine, Lohnzettel, Zahlungsanweisungen, Kassenzettel oder Bons (Goldshteyn, 2016, S. 18).

Unter sonstigen Unterlagen werden weitere steuerbezogene Dokumente zusammengefasst, die dazu dienen, einen Sachverhalt oder Umstand zu belegen oder nachzuvollziehen.

Für alle genannten Belegarten ist die gesetzliche Grundlage jeweils § 257 HGB (für Kaufleute) bzw. § 147 AO. Nicht abschließend existieren weitere Rechtsquellen, die die Archivierung bzw. Aufbewahrung von Dokumenten je nach Umstand erforderlich werden lassen. Wie z. B. § 14 UStG oder § 103 EnergieStV (Goldshteyn, 2016, S. 14).

8.1 Archivierungsdauer von E-Mails

Neben der grundsätzlichen Pflicht zur E-Mail-Archivierung, sollte ein Unternehmen die Archivierung aber auch als große Chance und wichtigen Schritt zur vollumfänglichen Digitalisierung der Geschäftsprozesse im eigenen Unternehmen sehen. Dies beginnt beim Ersparen von Platz- und Ablagefläche und zieht sich über die bessere und schnellere Auffindbarkeit von Dokumenten und einer möglichen und komfortablen Suche in Altbeständen. Die tatsächlichen Speicherpflichten bzw. die Dauer lässt sich nachfolgender Tabelle entnehmen:

Tab. 3 – Archivierungsdauer von E-Mails

Dokumenttyp	**Gesetzliche Speicherdauer**
Handelsbücher, Inventare Bilanzen, Abschlüsse, Lageberichte, Konzernabschlüsse, Arbeitsanweisungen und Organisationsunterlagen sowie Buchungsbelege (§ 257 Abs. 1 i.V.m. § 257 Abs. 4 S.1)	10 Jahre
Empfangene und versandte Handelsbriefe oder Geschäftsbriefe (§ 257 Abs. 1 i.V.m. § 257 Abs. 4 S2)	6 Jahre

Quelle: Eigene Darstellung.

§ 147 AO Abs. 3, S. 1 nennt analog zu § 257 HGB identische Aufbewahrungsfristen. Interessant ist in diesem Zusammenhang die Definition, ab wann die jeweilige Speicherdauer beginnt. § 257 Abs. 5 nennt hierzu:

„Die Aufbewahrungsfrist beginnt mit dem Schluß des Kalenderjahrs, in dem die letzte Eintragung in das Handelsbuch gemacht, das Inventar aufgestellt, die Eröffnungsbilanz oder der Jahresabschluß festgestellt, der Einzelabschluss nach § 325 Abs. 2a oder der Konzernabschluß aufgestellt, der Handelsbrief empfangen oder abgesandt worden oder der Buchungsbeleg entstanden ist.“

Wurde somit am 05. Januar 2021 ein Handelsbrief per E-Mail verschickt, beginnt die 6-jährige Archivierungsdauer erst mit Ende des Jahres. Diese E-Mail muss somit mindestens bis zum 31.12.2027 in Form einer Archivierung aufbewahrt werden.

Das Ende der Archivierungsdauer meint lediglich das Ende der Pflicht zur Archivierung nach Ablauf der vorgesehenen Zeiträume. Häufig sind jedoch gerade historische Werte bzw. Daten für die Prognose von zukünftigen Entscheidungen wichtig. Gerade Produkte und Dienstleistungen im Bereich der Datenanalyse (BigData), nutzen Vergangenheitswerte um Trends bzw. Veränderungen der Entwicklung zu erklären. Hierbei ist jedoch stets die Datenschutzgrundverordnung zu berücksichtigen, die weitere Anforderungen hinsichtlich Datenverarbeitung stellt.

8.2 Art und Speicherform der zu archivierenden E-Mails

Ist das Original-Dokument elektronisch eingegangen, (E-Mail) muss auch die Ablage in dieser Form erfolgen. Ein Ausdruck von E-Mails ist nicht zulässig, bzw. erfüllt nicht die Anforderungen an die Archivierung in ihrer Ursprungsform (Ripper, 2010, S.4). Da die E-Mail selbst jedoch auch nur als Träger verwendet werden kann, – wie der Briefumschlag im Postversand – muss eine E-Mail nicht archiviert werden, wenn deren Inhalt für sich betrachtet archiviert wird. Hängt also an einer E-Mail der tatsächliche Handelsbrief als Anhang im PDF-Format an, ist es ausreichend, nur den Anhang zu archivieren. Dies findet sich in Tz 131 GoBD[22] wie folgt:

„Eingehende elektronische Handels- oder Geschäftsbriefe und Buchungsbelege müssen in dem Format aufbewahrt werden, in dem sie empfangen wurden (z. B. Rechnungen oder Kontoauszüge im PDF- oder Bildformat).“ (Macht, 2019, S. 26).

In Fällen wo die tatsächliche und relevante Information nicht als Anhang per E-Mail übermittelt wird, sondern in der E-Mail selbst als Text enthalten ist, muss die E-Mail archiviert werden. Dennoch kann es Gründe geben, die tatsächliche E-Mail zusätzlich aufzubewahren. Dies ist vergleichbar mit einer von Amts wegen förmlichen Zustellung, wo auf dem Umschlag das Datum der tatsächlichen Zustellung vermerkt ist. Auch bei der E-Mail trägt die E-Mail selbst, wichtige Informationen zum Einlieferungszeitpunkt, dem Betreff und dem tatsächlichen Absender bzw. Verfasser der E-Mail und kann aus Gründen der Dokumentation, nachträglich Beweiskraft entfalten. Leider hält sich der Glaube an die korrekte Umsetzung durch Ausdruck einer E-Mail und Ablage in Papierform, in vor allem kleineren Unternehmen noch hartnäckig aufrecht. Ausnahme hiervon finden sich wiederum z.B. in § 257 Abs. 3 HGB wie folgt:

22 https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf?__blob=publicationFile&v=9

„Sind Unterlagen auf Grund des § 239 Abs. 4 Satz 1 auf Datenträgern hergestellt worden, können statt des Datenträgers die Daten auch ausgedruckt aufbewahrt werden“.

In Kombination mit der Archivierung und einer Ende-zu-Ende E-Mail-Verschlüsselung ist sicherzustellen, dass „(..) die verschlüsselten Unterlagen im DV-System in entschlüsselter Form zur Verfügung stehen. Werden Signaturprüfschlüssel verwendet, sind die eingesetzten Schlüssel aufzubewahren. Die Aufbewahrungspflicht endet, wenn keine der mit den Schlüsseln signierten Unterlagen mehr aufbewahrt werden müssen.“ (Tz 134 GoBD).

Existiert bereits ein E-Mail-Archiv und wurden darin verschlüsselte E-Mails abgelegt, sollte bereits jetzt sichergestellt werden, dass diese auch noch in mehreren Jahren, lesbar sind. Also müssen die nötigen Kennwörter bzw. Schlüssel zur Entschlüsselung ebenso lange vorgehalten werden, wie die Archivierungspflicht besteht. Die E-Mail-Archivierung sollte keine primäre und alleinige Aufgabe der IT-Abteilung sein, da sie bereichsübergreifend in alle Abteilungen ausschlägt und wie zuvor erwähnt, auch über die gesetzliche Speicherpflicht hinaus, wichtige Informationen für die BigData-Analyse liefern kann.

8.3 Datenschutzrechtliche Abwägung für die Archivierung

Ein primär technisches Problem, zeigt sich bei der Betrachtung des Einflusses durch den Datenschutz auf die Archivierung. Die Pflicht zur Archivierung entbindet den Archivierenden nicht von seinen datenschutzrechtlichen Verbindlichkeiten. Dies ist z. B. die Löschpflicht (Kremer, 2020, S. 153). Die Datenschutzgrundverordnung nennt hierzu in § 17 Abs. 1 DSGVO:

„Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft“„.

Da einerseits jetzt der Gesetzgeber durch Archivierungsvorgaben fordert, dass Daten zu archivieren sind, diese jedoch in der Regel personenbezogen sind und somit der Löschpflicht unterliegen, stehen sich zwei grundsätzlich widersprüchliche Forderungen gegenüber. Dies lässt sich durch Art. 6 1f DSGVO auflösen, welcher als Rechtfertigungsgrund für die Speicherung ausführt:

„die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen(…)“ (Kremer, 2020, S. 155).

Dass die DSGVO bereits berücksichtigt hat, dass eine Ausnahme von der Löschfrist bestehen muss, wenn eine rechtliche Verpflichtung zu erfüllen ist, normiert Art. 17 Abs. 3 DSGVO wie folgt:

Die Absätze 1 und 2 gelten nicht (Art. 17 DSGVO - Recht auf Löschung) „(…) soweit die Verarbeitung erforderlich ist (…) zur Erfüllung einer rechtlichen Verpflichtung“. Ebenso normiert § 35 Abs. 3, dass eine Löschung nicht erforderlich ist, wenn dieser Aufbewahrungsfristen entgegenstehen:

(Voigt, 2018, S. 215).

„Ergänzend zu Artikel 17 Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 gilt Absatz 1 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679, wenn einer Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen.“

Dies ist nur logisch, da sonst unter dem Vorwand der Betroffenenrechte Dritter, z. B. steuerrelevante Unterlagen gelöscht werden könnten, die eine lückenlose Nachvollziehbarkeit von Geschäftsvorfällen für die Steuerprüfung, durch den Fiskus unmöglich machen würden. Ein weiteres Problem aus der Praxis ist, dass sich häufig private und dienstliche E-Mails vermischen, da die Arbeitgeber die private Nutzung des dienstlichen Kontos erlauben oder nicht explizit verbieten. Kommt es jetzt auch zu einer – meistens automatisierten – Archivierung jener privaten Mails, fehlt hierzu die Rechtsgrundlage und die Verarbeitung ist rechtswidrig. Zusätzlich ist der Arbeitgeber wie ein Kommunikationsanbieter zu behandeln. So erwähnt bereits die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, in einer 2016 erschienen Handreichung[23]:

„Sofern der Arbeitgeber seinen Beschäftigten die Möglichkeit zur Nutzung des betrieblichen E-Mail-Accounts für private E-Mail-Kommunikation ermöglichen möchte, sollte er bedenken, dass er dann an das Fernmeldegeheimnis gebunden ist. Dies führt in der Praxis regelmäßig zu erheblichen Konflikten, nämlich dann, wenn der Arbeitgeber für den Geschäftsablauf auf das betriebliche Postfach der Beschäftigten zugreifen möchte.“

23 https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf

Dennoch kam das Landesarbeitsgericht Berlin-Brandenburg mit Urteil vom 16.02.2011 (AZ 4 SA 2132/10) zu folgendem anderen Entschluss:

„Ein Arbeitgeber wird nicht allein dadurch zum Dienstanbieter i. S. d. Telekommunikationsgesetzes, dass er seinen Beschäftigten gestattet, einen dienstlichen E-Mail-Account auch privat zu nutzen."

Dies kann als praxistauglich bewertet werden, da der Arbeitgeber generell nicht die Absicht oder das Interesse hat, Kommunikationsdienstleistungen für seine Mitarbeiter zur Verfügung zu stellen.

9. Handlungsempfehlungen

Aus den bislang erlangten Erkenntnissen, lassen sich nachfolgende Empfehlungen für die Praxis herleiten. Diese haben das Ziel, die Themen E-Mail-Verschlüsselung, Archivierung, Zurechenbarkeit und Stolperfallen hinsichtlich E-Mail Kommunikation in Unternehmen aufzugreifen und konkrete praktische Vorschläge zu bieten.

Die Transportverschlüsselung sollte für alle ausgehenden E-Mails, generell auf dem eigenen IT-Mailsystem erzwungen werden. So werden pauschal alle ausgehenden E-Mails verschlüsselt. Auch wenn manche Empfänger vereinzelt noch keine Verschlüsselung anbieten und die E-Mail-Zustellung scheitert, stellt die erzwungene Transportverschlüsselung den größten gemeinsamen Nenner dar. Ist ein Empfänger nicht verschlüsselt erreichbar, sollte unkompliziert Kontakt zu dessen IT-Abteilung oder IT-Dienstleister gesucht werden um eine Kompatibilität herzustellen.

Die Ende-zu-Ende Verschlüsselung sollte nur bei zwingendem Bedarf und besonders schützenswerten Daten zum Einsatz kommen. Das verwendete System sollte in Zusammenarbeit mit den Kommunikationspartnern ausgewählt werden um hier Reibungsverluste zu vermeiden. Nach Möglichkeit sollte freie und quelloffene Software zum Einsatz kommen (OpenSource-Software). Bereits bei der Auswahl der Verschlüsselungssysteme, sollte die langfristige Archivierung mit berücksichtigt werden. Eine arbeitsrechtlich saubere Vertreterregelung, empfiehlt sich vor Einsatz des neuen Systems in Zusammenarbeit mit dem Betriebsrat zu erarbeiten, falls dieser den betrieblichen Umständen nach, erforderlich ist.

Zur Beweissicherung sollten die E-Mail-Protokolle ausgehender E-Mails, auf dem zentralen Mailsystem zu Dokumentationszwecken langfristig gespeichert werden. Die Anforderung von Übermittlungs-

und Lesebestätigungen ist zusätzlich dauerhaft empfohlen und kann über firmenweite Richtlinien aktiviert werden.

Der Spam- und Anti-Virus-Filter, – wenn auch nur auf dem eigenen Mailsystem betrieben – sollte ausschließlich im Modus Prüfen vor Annahme betrieben werden. Nur so kann die Annahme von E-Mails bei tatsächlicher Ablehnung verneint werden.

Bei der E-Mail-Archivierung sollte ein automatisiertes Archivsystem zum Einsatz kommen. Manuelle Archivierung ist fehleranfällig, kann vergessen werden und ist nicht lückenlos. Bei der Auswahl des Anbieters sollte berücksichtigt werden, dass dieser auch noch in 6-10 Jahren am Markt aktiv ist. Eine spätere Umstellung des Archivsystems, gestaltet sich kostspielig und aufwendig. Bei der Auswahl der Software sollte ein quelloffenes System (OpenSource-Software) mit zusätzlichen Schnittstellen genutzt werden um einen eventuellen späteren und nötigen Export, bei einem Softwareumstieg, in ein neues System zu vereinfachen.

Die private Internetnutzung generell im Unternehmen durch Betriebsvereinbarung bzw. Arbeitsvertrag zu unterbinden, vermeidet Probleme bei der E-Mail-Archivierung und eine mögliche Vermischung von dienstlicher und privater Kommunikation. Der Betriebsrat ist hier – falls vorhanden – einzubeziehen.

10. Fazit und Ausblick

Ziel der Arbeit war die Beantwortung der eingangs gestellten Fragen, wann eine Verschlüsselungspflicht zu bejahen ist, wie eine Anti-Spam- und AntiVirus Software die Übermittlung beeinflusst und wer für Übertragungsfehler haftet. Aber auch unter welchen Umständen sich ein Empfänger eine E-Mail zurechnen lassen muss und wie dies der Absender rechtssicher beweisen kann. Und zuletzt, für wen und in welchem Umfang die Archivierungspflicht besteht und wie dies tatsächlich zu bewerkstelligen ist.

Generell kann festgehalten werden, dass alle dem geschäftlichen Ablauf dienlichen E-Mails, die personenbezogenen Inhalt aufweisen, auf Grundlage der DSGVO verschlüsselt werden müssen. Die Pflicht zur deutlich aufwendigeren Verschlüsselung – für alle E-Mails – auf Basis einer Ende-zu-Ende-Verschlüsselung ist zwar wünschenswert und teilweise durch die Datenschützer gefordert, jedoch we-

der praktikabel noch nach herrschender Meinung verpflichtend. Ausnahmen stellen hier lediglich besonders schützenswerte Daten dar, wozu im Einzelfall eine Abwägung vorzunehmen ist.

AntiSpam- und AntiVirus-Filter dienen zur Abwehr von Angriffen, bzw. zur Ablehnung von schadhaften oder unerwünschten Sendungen. Lehnt hier der Anbieter die E-Mails ohne Auftrag eigenmächtig ab, macht dieser sich u.a. der eigenmächtigen Unterdrückung nach § 274 StGB strafbar. Handelt der Anbieter lediglich im Auftrag, ist er nur der verlängerte Arm des Kunden, handelt nicht eigenmächtig und muss sich deshalb auch kein Fehlverhalten zurechnen lassen. Da jeweilige Abwehr- und Filtersoftware, Nachrichten zu unterschiedlichen Zeitpunkten der Einlieferung ablehnen kann, gelangt eine E-Mail nicht in jedem Fall in den Einflussbereich des Empfängers. Dem Absender – und Empfänger – stehen ausführliche Protokoll- und Beweismöglichkeiten zur Verfügung um eine Nachrichtenübermittlung zu dokumentieren. Dies sei die Lese- und Übermittlungsbestätigung oder ein Einlieferungsnachweis in Form eines Protokolls der eigentlichen Nachrichtenübertragung.

Zuletzt ergibt sich für Handelsbriefe und steuerrelevante Unterlagen eine Aufbewahrungsfrist zwischen 6 und 10 Jahren je nach Dokumententyp. Die E-Mail selbst dient einerseits nur als Träger – wenn der E-Mail das eigentliche Dokument als Anhang angehängt ist – und ist vergleichbar mit dem Briefumschlag. Hier muss die E-Mail nicht archiviert werden. Andererseits kann die E-Mail selbst die Informationen enthalten und fällt unter die Archivierungspflicht. Die Aufbewahrung des Umschlages selbst ist jedoch in manchen Fällen hilfreich, um Einlieferungszeiten und Zusatzinformationen zusätzlich zu dokumentieren.

Aufgrund hoher Strafen für DSGVO-Vergehen, sollten Unternehmen die eigenen Richtlinien für die E-Mail-Kommunikation prüfen. Cloud- und IT-Anbieter sollten zur Vermeidung von strafrechtlichen Konsequenzen, die eigenen AGBs bzw. individuelle Verträge mit Kunden überprüfen. Bewährt hat sich hier die reine Bereitstellung von Prüfungs und Sicherungsmethoden, die der Kunde erstmals selbst aktivieren muss und individuell auf die Bedürfnisse des eigenen Unternehmens ausrichten kann.

Gegenstand weiterer Forschung sollte das kostenpflichtige Kommunikationsmittel De-Mail sein (vgl. § 1 Abs. 1 DE-Mail-Gesetz[24]) sowie das von der Deutschen Post verfügbare Produkt E-Postbrief[25]. Aber auch die Möglichkeit des Einsatzes von digitalen Signaturen, zur Authentifizierung von Handelsbriefen bei der Übermittlung per E-Mail, bietet Raum für weitere Forschung.

24 https://www.gesetze-im-internet.de/de-mail-g/BJNR066610011.html

25 https://www.deutschepost.de/de/e/epost.html

V. Literaturverzeichnis

1 & 1 Mail & Media (2019). Umfrage zur sicheren Ende-zu-Ende-Verschlüsselung, letzter Abruf am 28.02.21 von https://de-statista-com.pxz.iubh.de:8443/statistik/daten/studie/800374/umfrage/gruende-der-nichtnutzung-von-e-mail-verschluesselung-in-deutschland/

Abelson, H. et al. (1997). *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*. https://doi-org.pxz.iubh.de:8443/10.7916/D8GM8F2W

Aleieldin, S., Banescu, S., & Pretschner, A. (2020). "*Maat: Automatically Analyzing VirusTotal for Accurate Labeling and Effective Malware Detection.*" http://search.ebscohost.com.pxz.iubh.de:8080/login.aspx?direct=true&db=edsarx&AN=edsarx.2007.00510&site=eds-live&scope=site.

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

Bayerisches Landesamt für Datenschutzaufsicht (2019). *9. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht für das Jahr 2019*, Letzter Abruf am 27.02.21 von https://www.lda.bayern.de/media/baylda_report_09.pdf

Becker, T. et al. (2018). *Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG*. in: Plath, K.-U. (Hrsg.) Köln Otto Schmidt.

Brand, M. (2019). Die Deutschen verschicken immer mehr Mails. Letzter Abruf am 27.02.21 von https://de-statista-com.pxz.iubh.de:8443/infografik/12826/anzahl-verschickter-e-mails-in-deutschland/

Brink, S. (2019). 35. Datenschutz-Tätigkeitsbericht, letzter Abruf am 27.02.21 von www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf

Blömer, J. (2012). *Turing und Kryptografie*. (German). *Informatik Spektrum*, *35*(4), 261.

Bundesnetzagentur (2019). Jahresbericht 2019, letzter Abruf am 28.02.21 von https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Jahresberichte/JB2019.pdf?__blob=publicationFile&v=6

Bundesverfassungsgericht (2019). *Erfolglose Verfassungsbeschwerde gegen die Verpflichtung zur Übermittlung von IP-Adressen*, letzter Abruf am 27.02.21 von bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2019/bvg19-007.html

Chu, K.-T. et al. (2020). Effective spam filter based on a hybrid method of header checking and content parsing. *IET Networks (Institution of Engineering & Technology)*, *9*(6), 338. https://ietresearch-onlinelibrary-wiley-com.pxz.iubh.de:8443/doi/full/10.1049/iet-net.2019.0191

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

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

Dürscheid, C. & Frehner, C. (2013). Email communication. Letzter Abruf am 06.03.21 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-Ministerrat (2020). *Resolutionsentwurf des EU-Ministerrats 12143/20*, letzter Abruf am 27.02.21 von https://data.consilium.europa.eu/doc/document/ST-12143-2020-INIT/en/pdf

Ferrara, E. (2019). The History of Digital Spam. *Communications of the ACM*, *62*(8), 82–91. https://doi-org.pxz.iubh.de:8443/10.1145/3299768

Fuhrman, C. P. (2008). Forensic Value of Backscatter from Email Spam. *2008 Third International Annual Workshop on Digital Forensics and Incident Analysis, Digital Forensics and Incident Analysis, 2008. WDFIA '08. Third International Annual Workshop On*, 46–52. https://doi-org.pxz.iubh.de:8443/10.1109/WDFIA.2008.10

Generalstaatsanwaltschaft Frankfurt. (2021). *Infrastruktur der Emotet-Schadsoftware zerschlagen*, letzter Abruf am 27.02.21 von bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html

Gerstberger, D. (2018). *Der Zugang von Willenserklärungen bei gewandelten Kommunikationsstrukturen – Die Empfangstheorie auf dem Prüfstand* in: Husemann, T. et al. (Hrsg.) (2019) Strukturwandel und Privatrecht, Helbing Lichtenhahn Basel.

Gladychev N. Computer Viruses: The Abstract Theory Revisited. (2019). Letzer Abruf am 06.03.21 von http://search.ebscohost.com.pxz.iubh.de:8080/login.aspx?direct=true&db=edsbas&AN=edsbas.F15EBD63&site=eds-live&scope=site

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

Grottke, M., & Trivedi, K. S. (2007). Fighting bugs: remove, retry, replicate, and rejuvenate. *Computer*, *40*(2), 107–109. Letzter Abruf am 06.03.21 von https://doi-org.pxz.iubh.de:8443/10.1109/MC.2007.55

Hirsch, C. (2020). *BGB Allgemeiner Teil*. Baden-Baden Nomos, 2020. http://search.ebscohost.com.pxz.iubh.de:8080/login.aspx?direct=true&db=cat05114a&AN=ihb.47974&site=eds-live&scope=site.

Holz, R. et al. (2015). *TLS in the wild: an Internet-wide analysis of TLS-based protocols for electronic communication*. https://doi-org.pxz.iubh.de:8443/10.14722/ndss.2016.23055

Joshi, M. J., & Patil, B. V. (2012). Computer Virus: Their Problems & Major attacks in Real Life. *Journal of Advanced Computer Science and Technology*, *1*(4), 316-324. Letzter Abruf am 06.03.21 von https://core.ac.uk/download/pdf/193780319.pdf

Klensin, J. (2001), *Simple Mail Transfer Protocol*, letzter Abruf am 27.02.21 von tools.ietf.org/html/rfc2821

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2016), *Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz*, letzter Abruf am 21.02.21 von datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf

Kremer, K., (2020). *Datenschutzkonformes Löschen in IT-Systemen. (2020)*. *Revisionspraxis PRev*, *3*, 152–157. viewed 17 February 2021, <http://search.ebscohost.com.pxz.iubh.de:8080/login.aspx?direct=true&db=bsu&AN=143837371&site=eds-live&scope=site>.

Kumar, S., M., Ben-Othman, J., & Srinivasagan, K. G. (2018). *An Investigation on Wannacry Ransomware and its Detection*. *2018 IEEE Symposium on Computers and Communications (ISCC), Computers and Communications (ISCC), 2018 IEEE Symposium On*, 1–6. https://doi-org.pxz.iubh.de:8443/10.1109/ISCC.2018.8538354

Macht, W. (2020). *GoBD – auch im Mandantenalltag relevant*. Haufe Gruppe. Zuletzt abgerufen am 20. Februar 2021, https://www.lexoffice.de/wp-content/uploads/ebook-gobd-auch-im-mandantenalltag-relevant-wolfgang-macht-lexoffice-rechnungsprogramm-buchhaltungssoftware.pdf

Microsoft (2018). *Verwenden von Gruppenrichtlinie zum Konfigurieren von Domänen Mitglieds-Client Computern*, letzter Abruf am 21.02.21 von docs.microsoft.com/de-de/windows-server/networking/branchcache/deploy/use-group-policy-to-configure-domain-member-client-computers

Müller, R. (2020). *Datenschutz im Verein : Leitfaden für den sicheren Umgang mit der DSGVO: Vol. 1. Auflage 2020*. Haufe.

Nitsch, K. (2017). *IT-Vertragsrecht. Informatikrecht : Grundlagen, Rechtsprechung Und Fallbeispiele, 161*. https://doi-org.pxz.iubh.de:8443/10.1007/978-3-658-16426-3_4

OpenSSL Software Foundation (2018). O*penssl manpage*, letzter Abruf am 21.02.21 von https://www.openssl.org/docs/man1.0.2/man1/openssl-s_client.html

Rescorla, E. (2018), *The Transport Layer Security (TLS) Protokol Version 1.3*. Letzter Abruf am 14.03.21 von https://tools.ietf.org/html/rfc8446

Riggert, W. V. (2019). *ECM - Enterprise Content Management Konzepte und Techniken rund um Dokumente*. Springer Vieweg. https://doi-org.pxz.iubh.de:8443/10.1007/978-3-658-25923-5

Ripper, J. (2010). *E-Mail-Archivierung: Revisionssicher ist nicht gleich rechtskonform. Wirtschaftsinformatik und Management*, *2*(6), 44. https://doi-org.pxz.iubh.de:8443/10.1007/bf03250520

Röhner, J. V. (2020). *Psychologie der Kommunikation*. Springer. Letzter Abruf am 06.03.21 von https://doi-org.pxz.iubh.de:8443/10.1007/978-3-662-61338-2

Ronellenfitsch, M. (2019). Achtundvierzigster Tätigkeitsbericht zum Datenschutz, letzter Abruf am 21.02.21 von datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2019_48_TB.pdf

Schleipfer, S. (2020). *Ende-zu-Ende-Verschlüsselung von E-Mails: Ungeeignet für den betrieblichen Einsatz*. *Datenschutz Und Datensicherheit - DuD*, *44*(11), 748. https://doi-org.pxz.iubh.de:8443/10.1007/s11623-020-1360-7

Schneidereit, P. (2017). *Haftung für Datenverlust im Cloud Computing*. Nomos Verlagsgesellschaft mbH & Co. KG.

Specht-Riemenschneider, L., Riemenschneider, S., & Schneider, R. (2020). *Internetrecht: Vol. 1. Aufl. 2020*. Springer.

Speichert, H. (2007). *Praxis des IT-Rechts Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung*. https://doi-org.pxz.iubh.de:8443/10.1007/978-3-8348-9205-8

Stary, J., & Franck, N. (2013). *Die Technik wissenschaftlichen Arbeitens - eine praktische Anleitung*. 2013 UTB. Letzter Abruf am 06.03.21 von http://search.ebscohost.com.pxz.iubh.de:8080/login.aspx?direct=true&db=cat05114a&AN=ihb.26697&site=eds-live&scope=site

Szor, P. (2005). The Art of Computer Virus Resarch and Defense. Addison Wesley Professional. ISBN: 0-321-30454-3.

Templeton, B. (o.J.) *Origin of the term "spam" to mean net abuse.* Letzter Abruf am 14.03.21 von https://www.templetons.com/brad/spamterm.html

Thomsen, I. (2009). *Buchführung Grundlagen: Kompakte Lerneinheiten mit Abschlusstest und Teilnahmebestätigung*, Haufe-Lexware; Auflage: 1., Auflage 2009, ISBN 978-3-4480-9357-5

Vaudreuil, G. (2003). *Enhanced Mail System Status Codes*,letzter Abruf am 21.02.21 von https://tools.ietf.org/html/rfc3463#section-3

Venzke-Caprarese, S. (2020). *Zur Praxistauglichkeit des Datenschutzes in der digitalen Kommunikation*. (German). *Datenschutz Und Datensicherheit - DuD*, *44*(12), 796.

Voigt. P., & Von dem Bussche, A. (2018). *EU-Datenschutz-Grundverordnung (DSGVO) : Praktikerhandbuch.* Springer.

Wätjen, D. (2018). *Kryptographie [electronic resource] : Grundlagen, Algorithmen, Protokolle.* Wiesbaden : Springer Fachmedien Wiesbaden : Imprint: Springer Vieweg, 2018.

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

Urteile:

AG Hamburg, Urteil vom 27.04.2018 – 12 C 214/17, abgerufen am 21.02.21 von https://rabüro.de/bei-vorlage-von-ausdruck-aus-postausgangssystem-fuer-abruf-der-e-mail-vom-server-auf-e-mail-konto-des-empfaengers-gilt-anscheinsbeweis-fuer-den-zugang/

BGH, Urteil vom 14. März 2017, AZ: VI ZR 721/15, abgerufen am 14.03.21 von http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=77970&anz=1&pos=0&Frame=4&.pdf

LAG Berlin-Brandenburg, Urteil vom 16.02.2011 – 4 Sa 2132/10, abgerufen am 06.03.21 von https://openjur.de/u/168249.html

LG Bonn, Urteil vom 11.11.2020 – 29 Owi 1/20, abgerufen am 28.02.21 von https://openjur.de/u/2310641.html

OLG Hamm, Urteil vom 03.01.2003 – 4 Ss 1058/02, abgerufen am 27.02.21 von https://www.burhoff.de/rspr/texte/ap_00021.htm