Gutachten zur Vereinbarkeit von DMARC mit der DSGVO und anderen Rechtsvorschriften

eco Kompetenzgruppe E-Mail / CSA
Autoren: Dr. Katharina Küchler (eco),
Patrick Ben Koetter (sys4 AG)

CSA
Certified Senders Alliance

eco
VERBAND DER INTERNETWIRTSCHAFT

Inhalt

A. Sachverhalt

DMARC sammelt Daten, welche bei der Zustellung von E-Mail entstehen, verarbeitet diese, um Reports zu erstellen, und versendet diese an bestimmte EmpfängerInnen. Dieses Gutachten geht der Frage nach ob und unter welchen Bedingungen das Sammeln, Verarbeiten, Versenden und Empfangen solcher Reports rechtlich zulässig ist.

1. DMARC

DMARC ist ein Internet-Standard (RFC 7489) und die sprachliche Kurzform für „Domain-based Message Authentication, Reporting and Conformance". Entwickelt, um Identitätsmissbrauch in E-Mails zu entdecken und zu unterbinden, findet es während des E-Mail-Transports von einem Sender zu einem oder mehreren EmpfängerInnen Anwendung.

E-Mails, welche einer DMARC-Prüfung (DMARC-Authentifizierung) nicht standhalten, sollen zum Schutz der EmpfängerInnen ausgefiltert und nicht zugestellt werden; Eigentümer, deren Senderdomains zur Identitätsfälschung missbräuchlich genutzt wurden, können zusätzlich von möglichen Missbrauchsversuchen mit DMARC-Reports in Kenntnis gesetzt werden, damit diese – vom Reporter mit Daten über den Missbrauchsversuch ausgestattet – anschließend versuchen können, weiteren Missbrauch ihrer Domain zu unterbinden.

Der DMARC-Standard sieht für die Benachrichtigung der Eigentümer zwei unterschiedliche Formen des DMARC-Reports – aggregated und failure reports – vor. Diese Report-Formen unterscheiden sich sowohl in Umfang und Detailgrad der Daten, welche sie weitergeben, als auch in der Frequenz, mit welcher sie versendet werden.

Dieses Gutachten geht der Frage nach ob und unter welchen Umständen die eine oder die andere Form des DMARC-Reports, vor dem Hintergrund des Prinzips der Datensparsamkeit und auch dem Schutz personenbezogener Daten, rechtlich zulässig ist.

Für ein Verständnis des Gutachtens ist es notwendig, die DMARC-Akteure begrifflich zu bestimmen und auch die beiden genannten DMARC-Report-Typen aggregated und failure report noch weiter zu konkretisieren, damit deutlich wird, worin sich diese genau unterscheiden. Die nachfolgenden Unterabschnitte dienen dem dafür notwendigen Verständnis.

1.1 Akteure

DMARC findet im Austausch von E-Mail zwischen einem Sender und einem oder mehreren EmpfängerInnen Anwendung. Am Austausch und an der DMARC-Authentifizierung sind die nachfolgend beschriebenen Akteure beteiligt:

Akteur Definition:

Domaininhaber: Der Begriff Domaininhaber bezeichnet in diesem Dokument eine Einzelperson, eine Organisation oder eine beauftragte Einzelperson / Organisation, welche die DNS-Angaben einer Senderdomain verwaltet, die eine DMARC-Richtlinie in dieser Senderdomain veröffentlicht.

Sender: Der Begriff Sender bezeichnet eine Einzelperson, eine Organisation oder auch ein dienstleistendes Unternehmen, welche vom Domaininhaber mit dem Versand von E-Mails unter Einsatz der Senderdomain Nachrichten versendet.

Receiver: Der Begriff Receiver bezeichnet eine Einzelperson, eine Organisation oder eine Dienstleisterin wie z. B. AOL, GMX, Hotmail oder Yahoo!, welche die E-Mail einer Senderdomain entgegennehmen soll.

Report-Empfänger: Der Begriff Report-Empfänger bezeichnet eine Einzelperson, eine Organisation oder eine vom Domaininhaber beauftragte juristische Person, welche für die besagte Senderdomain DMARC-Reports entgegennehmen und verarbeiten soll.

Empfänger: Der Begriff Empfänger (engl. Recipient) bezeichnet eine Einzelperson oder eine Organisation, an welche die Nachricht einer Senderdomain gerichtet ist und zugestellt werden soll.

1.2 Funktionsweise

DMARC sieht vor, dass eine Senderdomain eine DMARC-Richtlinie (engl. DMARC-Policy) veröffentlicht, in welcher festgelegt ist, wer im Namen der Domain senden darf und womit erkannt werden kann, ob die Nachricht tatsächlich von dieser Senderdomain gesendet wurde.

Die DMARC-Richtlinie wird in Form eines DNS-Eintrags in der DNS-Zone der Senderdomain(s) veröffentlicht. Für dieses Gutachten auf das Wesentliche beschränkt besagt ein DMARC-DNS-Eintrag

a) was mit einer E-Mail geschehen soll, welche den Regeln der E-Mail-Standards SPF und / oder DKIM nicht entspricht, sowie
b) ob und wie Report-EmpfängerInnen von SPF- / DKIM-Regelverstößen benachrichtigt werden sollen und
c) welche Form des Reports – aggregated und / oder failure – dabei angewendet werden soll

Ein empfangender E-Mail-Dienst (Receiver) soll nun dem DMARC-Standard entsprechend während des Empfangs im Rahmen der DMARC-Authentifizierung prüfen,

1. ob die für den E-Mail-Transport verwendete Senderdomain eine DMARC-Policy veröffentlicht hat,
2. ob die zur Prüfung vorliegende E-Mail den Vorgaben von SPF und / oder DKIM gerecht wird,
3. wie mit der E-Mail verfahren werden soll, falls diese nicht der Überprüfung Stand hält und
4. ob die Senderdomain in Form eines DMARC-Reports vom Ergebnis der Überprüfung benachrichtigt werden möchte.

Die DMARC-Policy einer Senderdomain kann einen aggregated und/oder einen failure report sowie deren Übermittlung an eine oder mehrere EmpfängerInnen anfordern. Welche Daten in den Reports übermittelt werden – dies ist für das Gutachten von Bedeutung – und zu welchem Anlass dies, entsprechend dem DMARC-Standard, stattfindet, unterscheidet sich je nach DMARC-Report-Format – aggregated oder failure.

1.3 aggregated reports

Aggregated reports fassen mehrere Zustellereignisse in einem einzigen Report zusammen. Ein report soll laut DMARC-Standard alle Zustellereignisse der vergangenen 24 h umfassen und für gewöhnlich nur einmal täglich übermittelt werden.

Dem DMARC-Standard folgend soll ein aggregated report für Report-EmpfängerInnen nachfolgende Angaben enthalten:

- die verwendete DMARC-Policy
- wie mit der Nachricht verfahren wurde
- welche Daten zur Verifikation von SPF verwendet wurden und welches Ergebnis die SPF-Prüfung ergab
- welche Daten zur Verifikation von DKIM verwendet wurde und welches Ergebnis die DKIM-Prüfung ergab
- ob SPF und / oder DKIM in „alignment" mit den Sender-Angaben waren
- sendende und empfangende Domains
- die Richtlinie (policy), welche vom Domaininhaber vorgegeben wurde und jene, welche tatsächlich vom Receiver angewendet wurde (für den Fall, dass beide sich unterscheiden)
- die Anzahl erfolgreicher DMARC-Authentifizierungen
- die Anzahl aller Nachrichten der fraglichen Senderdomain, auch wenn diese geblockt oder anderweitig gefiltert wurden

1.4 failure Reports

Failure reports benachrichtigen im Einzelfall von fehlerhafter DMARC-Authentifizierung. Ein failure report soll anlassbezogen, idealerweise unmittelbar nach dem Auftreten eines Authentifizierungsfehlers generiert und zugestellt werden. Der Report soll ausführlicher als ein aggregated report sein.

Die DMARC-Spezifikation (RFC 7489) legt in Abschnitt 7.3. failure Reports nicht fest, welche Daten übermittelt werden sollen. Sie legt aber das AFRF-Format („Authentication Failure Reporting Using the Abuse Reporting Format", RFC 6591) als Format fest, in welchem die Daten übermittelt werden sollen. Von diesem Format lässt sich ableiten ein DMARC failure Report soll u. a. diese Daten enthalten:

- Quell-IP-Adresse des Senders
- Sender-E-Mail-Adresse
- Empfänger-E-Mail-Adresse
- Betreff der E-Mail
- E-Mail-Body

B. Rechtliche Würdigung

Bei der Prüfung der Vereinbarkeit des DMARC Verfahrens mit bestehenden Gesetzen aus Sicht der Unternehmen, die DMARC Reports versenden wollen, wird das Augenmerk auf die oben beschriebene Reportgenerierung und anschließende Übermittlung gelegt.

Hierbei sind sowohl datenschutzrechtliche als auch strafrechtliche Aspekte zu berücksichtigen.

I. Datenschutz

1. Personenbezug der übermittelten Daten

Fraglich ist, ob durch die beiden Arten von Reports („aggregated", „failure"), personenbezogene Daten verarbeitet werden. Gemäß Art. 4 Nr. 1 DSGVO sind personenbezogene Daten, „alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen." Maßgeblich ist demnach, dass sich die Daten auf eine bestimmte oder bestimmbare natürliche Person beziehen oder geeignet sind, einen Bezug zu einer natürlichen Person herzustellen.

Unter Verarbeitung fällt gemäß Art. 4 Nr. 2 DSGVO „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 personenbezogener Daten".

1.1 aggregated Reports

Wie in A. beschrieben enthalten „aggregated reports" Angaben zur sendenden und empfangenden Domain. Domains sind Folgen aus Buchstaben und Zeichen, die einer (oder mehrerer) IP-Adresse(n) zugeordnet sind. Einen unmittelbaren Personenbezug kann man mit einer Domain in der Regel nicht herstellen. Ein Bezug auf eine bereits identifizierte natürliche Person ist aus den bei einem aggregated Report übermittelten Daten daher zunächst nicht erkennbar. Nach dem Gesetz reicht es für das Vorliegen des Merkmals des Personenzugs aber aus, dass eine Person identifizierbar ist, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, identifiziert werden kann. Die Person muss also nicht anhand des fraglichen „Datums" allein identifizierbar sein, sondern Zusatzwissen ist grundsätzlich zu berücksichtigen.

Fraglich ist daher, ob aggregated reports durch die Hinzuziehung von Zusatzwissen einen mittelbaren Personenbezug aufweisen und daher als personenbezogenes Datum gelten.

Dass Domains und IP-Adressen personenbezogene Daten sein können steht heute außer Frage und wurde mehrfach durch den Europäischen Gerichtshofs (EuGH) bestätigt.[1] Die EuGH Urteile Breyer und Scarlet Extended begründen aber keine generelle Personenbeziehbarkeit von IP-Adressen, sondern gehen davon aus, dass eine IP-Adresse nicht aus sich allein heraus personenbezogen sein kann, sondern dass es stets zusätzlicher Informationen bedarf, die im Zusammenhang mit der IP-Adresse erst zu einem Personenbezug führen können. So könnte zum Beispiel mittels einer rdap-Anfrage (frühere Whois-Anfrage) ein Personenbezug im Hinblick auf Domains oder verwendete IP-Adressen hergestellt werden.

Es stellt sich daher die Frage, auf wessen „Zusatzwissen" es bei der Beurteilung eines Personenbezugs ankommt. Ist nur das Wissen des Datenverantwortlichen maßgeblich, um ein Datum zu einem personenbezogenen Datum zu machen oder müssen sämtliche, irgendeiner dritten Person bekannten Zusatzinformationen berücksichtigt werden?

Insbesondere für Domains unterhalb der Top-Level-Domain „.de" ist bei der zuständigen DENIC e.G. seit Inkrafttreten der DSGVO die Auskunftserteilung stark eingeschränkt. Informationen über den Domaininhaber können von Dritten nur noch in spezifischen Fällen und von berechtigten Behörden oder Inhabern betroffener Rechte abgefragt werden. Dritte, ohne ein glaubhaft gemachtes berechtigtes Interesse, erhalten über die DENIC keine Informationen über den Domaininhaber.

Daher können etwaige weitere Daten der DENIC e.G., die zu einer Personenbeziehbarkeit der IP-Adresse führen könnten, nur dann und denjenigen datenverarbeitenden Dritten als tatsächlich „verfügbar" zugerechnet werden, die eine Rechtsverletzung durch oder Rechte an der Domain gegenüber der DENIC e.G. glaubhaft machen können. Wäre also nur das Wissen des Datenverantwortlichen maßgeblich, könnte aus der grundsätzlichen Möglichkeit einer Whois-Anfrage kein Personenbezug hergestellt werden.

1 Rechtsprechung EuGH vom 19.10.2016 – C-582/14; Rechtsprechung EuGH vom 24.11.2011 – C-70/10.

Die Urteile des EuGHs in den Rechtssachen Breyer und Scarlet Extended sprechen dafür, dass der EuGH bei der Beurteilung des Personenbezugs auf die Perspektive des Datenverantwortlichen abstellt und nicht auf jedwede, irgendwem möglicherweise bekannten Zusatzinformationen.[2] Und auch die aktuelle Entscheidung des EuGH zur FIN (Fahrzeugidentifikationsnummer)[3] lässt sich eher so auslegen, dass von einem weniger weiten Verständnis von Personenbezug ausgegangen wird.

Die Urteile des EuGH zu Breyer und Scarlet Extended ergingen jeweils zu dynamischen IP-Adressen. Da der EuGH aber für dynamische IP-Adressen als entscheidendes Kriterium für deren Personenbezogenheit die jeweilige Verfügbarkeit von Zusatzinformationen ansieht, muss dies auch im Fall von statischen IP-Adressen angenommen werden müssen. Es kommt daher darauf an, welche Zusatzinformationen aus welchen Quellen dem Datenverantwortlichen zur Verfügung stehen, um eine IP-Adresse (und damit eine Domain) einer natürlichen Person zuordnen zu können.

Statische IP-Adressen, wie sie in aggregated reports enthalten sind, werden zudem in den meisten Fällen nur Unternehmen zugeteilt und nur in seltenen Ausnahmefällen natürlichen Personen. Statische IP-Adressen weisen daher auch zusammen mit dem Whois-Eintrag regelmäßig keinen Personenbezug auf. Statische IP-Adressen sind daher nur in den seltenen Fällen bereits in Kombination mit den Whois-Einträgen personenbezogen, wenn die statische IP-Adresse ausnahmsweise einer einzelnen natürlichen Person zur Benutzung zugewiesen ist.

Die enthaltenen IP-Adressen in den DMARC-Berichten sind die des sendenden Message Transfer Agent (MTA). Auch wenn jeder seinen eigenen MTA betreiben kann, wird die überwiegende Mehrheit der E-Mails über MTAs versandt, welche als zentrale Relais für E-Mails vieler einzelner Absender fungieren. In diesem Fall würden die gemeldeten IP-Adressen nicht als personenbezogene Daten gelten, da sie nicht unmittelbar einer bestimmten Person zugeordnet wären.[4] Bei den empfangenen IP-Adressen könnte dies anders aussehen, da es sich bei diesen schon eher auch um natürliche Personen handeln kann. Allerdings wäre auch hier nur durch Hinzuziehung einer weiteren, dem Datenverantwortlichen zurechenbaren, Information der Personenbezug gegeben.

In den meisten Fällen wird es sich daher bei den in aggregated reports übersandten Daten nicht um personenbezogene Daten handeln, da diese keiner natürlichen Person zugeordnet werden können. Der Anwendungsbereich der DS-GVO wäre damit nicht eröffnet, weshalb die Übermittlung der aggregated reports auch keiner datenschutzrechtlichen Ermächtigungsgrundlage bedürfte.

1.2. failure reports

„failure reports" enthalten im Gegensatz zu aggregated reports die Ausgangs- und Empfänger E-Mail-Adressen, Betreffzeilen sowie den E-Mail-Body der gesendeten E-Mail. Bei diesen Daten handelt es sich eindeutig um Daten mit einem Personenbezug im Sinne des Art. 4 Nr. 1 DS-GVO. Der Versand von failure reports kann daher nur bei Vorliegen einer der Ermächtigungsgrundlagen des § 6 Abs. 1 DSGVO gerechtfertigt werden.

2. Rechtfertigungsgründe

Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn sie durch Gesetz oder andere Rechtsvorschriften erlaubt ist oder der Betroffene einwilligt. Da nicht gänzlich auszuschließen

2 Exkurs: Das Urteil in Sachen Scarlet Extended betraf den Fall, dass die Verarbeitung der IP-Adressen durch einen Internetzugangsanbieter vorgenommen werden sollte. Dieser hat, da er selbst die Vergabe von IP-Adressen zu den Anschlüssen seiner Kunden vornimmt, im Falle der Speicherung dieser Zuordnung jederzeit auch die Möglichkeit, wieder rückwärts von der IP-Adresse auf die Identität seines Kunden zu schließen. Aus diesem Grund konnte in diesem Fall der Personenbezug von IP-Adressen bejaht werden, da hier unmittelbar über die Zusatzinformation zur Zuordnung einer IP-Adressen zu einer Kundenidentität verfügt werden konnte. In der Rechtssache Breyer ging es um eine Verarbeitung der IP-Adressen durch einen Webseitenbetreiber, der zwar nicht unmittelbar über die Zuordnung zwischen IP-Adressen und Kundenidentitäten verfügte. Dass jedoch auch in diesem Fall der EuGH zu einem Personenbezug von IP-Adressen kam, lag im vor allem an der Formulierung der Vorlagefrage durch den Bundesgerichtshof (BGH) und die weiteren Annahmen zum Sachverhalt. So verstand das Gericht die Vorlagefrage des BGH dahingehend, dass der Webseitenbetreiber die Zuordnung der IP-Adresse zu der Identität des Webseitenbesuchers zwar nicht selbst herstellen kann, sondern diese Zuordnung nur einem Dritten, nämlich dem Internetzugangsanbieter, bekannt ist. Dann allerdings führt der EuGH in Rz. 47, 48 aus, dass er die Ausführungen des BGH zum Auskunftsanspruch von Webseitenbetreibern gegen Internetzugangsanbieter bzw. das Akteneinsichtsrecht gegenüber Staatsanwaltschaften, die bei Ermittlungen (z.B. wegen Cyber-Kriminalität) ihrerseits Auskunftsverlangen an den Internetzugangsanbieter stellen können, dahingehend versteht, dass damit auch dem Webseitenbetreiber „offenbar [... die] Mittel, die vernünftigerweise eingesetzt werden könnten" zur Verfügung stünden, um anhand der IP-Adresse auch den Kunden bzw. Nutzer zu identifizieren. Aus diesen Erwägungen heraus formuliert der EuGH im Urteilstenor auch nur eine Aussage zum Personenbezug, die einer Bedingung unterliegt. Denn eine IP-Adresse stelle „für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung dar [...], wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen." Der EuGH geht also davon aus, dass die Möglichkeit zur Bestimmung einer natürlichen Person anhand einer IP-Adresse gerade deshalb bestehe, weil es einen weitgehenden und praktisch einfach umsetzbaren Auskunftsanspruch gegen den Internetzugangsanbieter gäbe. Dies entspricht in Deutschland aber nicht der Realität.

3 Rechtsprechung EuGH vom 09.11.2023 – C-319/22.

4 https://dmarc.org/wiki/FAQ#How_does_DMARC_work.2C_briefly.2C_and_in_non-technical_terms.3F

ist, dass aggregated reports doch auch personenbezogene Daten enthalten, wird im Folgenden, neben dem Vorliegen eines Erlaubnistatbestandes im Hinblick auf forensische reports, hilfsweise auch das Vorliegen eines Erlaubnistatbestands zum Versand von aggregated reports geprüft.

2.1. Einwilligung

Eine Einwilligung richtet sich nach § 4 DSGVO. Einwilligungen sind danach rechtmäßig, wenn sie freiwillig und bestimmt sind.

Im Falle von aggregated reports wie auch bei failure reports müssten die natürlichen Personen hinter der sendenden und empfangenen Domain ihre Einwilligung in die Reportzusendung geben. Da die empfangende Domain oftmals nichts von der DMARC Prüfung mitbekommt, ist die Einholung einer Einwilligung vor Versand des Reports schon praktisch schwierig. Zudem müsste die Einwilligung auch verweigert werden können oder im Nachhinein widerrufen werden können. Auch dies ist praktisch schwer vorstellbar, bzw. müsste dies dann dazu führen, dass die widersprechende Person überhaupt keine E-Mail mehr zugesandt bekommt. Zudem ist Zweck der Reports gegen Missbrauch und Pishing vorzugehen. Der „fremde" Sender oder der Verfasser einer Pishing-E-Mail wird natürlich in keinem Fall seine Einwilligung zum Versand von DMARC Reports geben. Ebenso wie der Empfänger einer Phishing-E-Mail. Eine Rechtfertigung über eine Einwilligung scheidet daher aus.

2.2 Erfüllung eines Vertragsverhältnisses nach Art. 6 Abs. 1 S.1 b) DSGVO

Zumindest mit dem illegal sendenden Phishing-Sender besteht auch kein Vertragsverhältnis. Ebenso wenig wie mit den E-Mail-Empfängern. Eine Rechtfertigung zur Vertragserfüllung scheidet damit ebenfalls aus. Dies gilt für aggregated und failure reports.

2.3 berechtigtes Interesse nach Art. 6 Abs. 1 S.1 f) DSGVO

Das Erheben und Verwenden der personenbezogenen Daten könnte gemäß Art. 6 Abs. 1 S.1 f) DSGVO gerechtfertigt sein, wenn ein berechtigtes Interesse gegeben ist. Ein berechtigtes Interesse ist gegeben, wenn die Übermittlung oder Nutzung zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.[5] Erweist sich die Verarbeitung also als zur Wahrung der berechtigten Interessen erforderlich, sind die für beide Seiten bestimmten Interessen sodann zu gewichten.[6] Einzubeziehen sind unter anderem alle relevanten Grundrechtsbezüge, die Eingriffsintensität, die Art der verarbeiteten Daten, die Art der Betroffenen, mögliche Aufgaben oder Pflichten, die Zwecke der Datenverarbeitung, Maßnahmen der Datensicherheit etc.[7]

2.3.1. aggregated reports

Im Falle von aggregated reports steht das Recht des einzelnen auf informationelle Selbstbestimmung dem Recht der Unternehmen und der Allgemeinheit auf einen möglichst sicheren Datenaustausch entgegen.

Werden personenbezogene Daten im Rahmen eines aggregated reports verarbeitet, handelt es sich hierbei um Domainadressen, die zu einer natürlichen Person zurückgeführt werden können. E-Mail-Inhalte oder Klarnamen werden bei aggregated reports nicht mitgesendet und einsehbar. Die übermittelten Daten sind daher stark begrenzt.

Dagegen bekämpft DMARC aktiv Phishing und trägt damit zum Schutz des einzelnen und des gesamten Internets bei. Letztendlich nützt das DMARC Verfahren damit auch den E-Mail-Adressaten und gewährleistet einen besseren Schutz vor Cyberangriffen, Viren, Bots oder Belästigung durch unerwünschte E-Mails. Durch DMARC wird es für E-Mail-Provider (e.g. AOL, GMX, Gmail, Yahoo) einfacher dafür zu sorgen, dass Spam und Phishing-E-Mails erst gar nicht das Postfach des Empfängers erreichen. Von daher wird man im Rahmen der aggregated reports annehmen dürfen, dass das berechtigte Interesse der Unternehmen, aber auch der Gesellschaft, an einem sichereren Internet gegenüber dem Interesse des einzelnen auf Schutz seiner informationellen Selbstbestimmung überwiegt. Der damit verbundene Eingriff in den Schutzbereich des einzelnen ist im Hinblick auf den Schutz der Funktions- und Leistungsfähigkeit der Telekommunikationsinfrastruktur und dem Schutz der personenbezogenen Daten der Betroffenen von Phishing vergleichsweise gering. Auch der Schutz, der teilweise ebenfalls grundrechtlich abgesicherten Interessen der nicht legitimen Versender und Empfänger muss hinter diesen Interessen anstehen. Der Einsatz von Aggregates Reports ist daher als verhältnismäßig zu werten und überwiegt entgegenstehende Schutzrechte Dritter.

5 Schulz, in: Gola, DS-GVO, Art.6, Rn.52.

6 Schulz, in: Gola, DS-GVO, Art.6, Rn.53.

7 Schulz, in: Gola, DS-GVO, Art.6, Rn.53.

2.3.2. failure reports

Anders als aggregated reports enthalten failure reports erheblich mehr Informationen sowohl zu dem Empfänger der E-Mails als auch zu deren Inhalt selbst. Fraglich ist daher, ob im Falle von failure reports die Abwägung zwischen dem informationellen Selbstbestimmungsrecht der natürlichen Person und dem Interesse der Unternehmen und der Allgemeinheit an einem sicheren Internet auch zugunsten der Nutzung von failure reports ausgehen kann.

Dazu müsste es sich bei den failure reports zunächst einmal um das mildeste Mitteln handeln um den verfolgten Zweck, nämlich die Abwehr von Phishing und Spam und den Schutz des Internets, erreichen zu können.

Grundsätzlich wird dieser Zweck auch bereits durch die aggregated reports verfolgt, weshalb man annehmen könnte, dass es bereits am Merkmal der Wahl des mildesten Mittel scheitern könnte. Allerdings kann durch die aggregated reports nur gesehen werden, dass überhaupt ein Angriff stattgefunden hat. Nicht gesehen werden kann, von wem der Angriff ausgegangen ist. Es sind daher zumindest Fälle denkbar, in denen aggregated reports nicht ausreichend sind, um das mit den failure reports bezweckte Ziel zu erreichen.

Unternehmen müssten weiterhin an der Erreichung des Zwecks, nämlich Kennen des tatsächlichen Absenders, ein überwiegendes Interesse gegenüber den E-Mail-Sendern- und -Empfängern und deren Recht auf Anonymität und informationelle Selbstbestimmung haben.

Bei failure reports erhalten Unternehmen eine beachtliche Anzahl von E-Mails. So rät sogar die DMARC selbst dazu failure reports nur dann zu wählen, wenn man auf die Datenflut vorbereitet ist. Argumentiert wird damit, dass „Fehlerberichte zwar sehr nützlich für die forensische Analyse sind, um sowohl Fehler in der eigenen E-Mail-Versandsoftware als auch einige Arten von Phishing- oder andere Imitationsangriffe zu identifizieren. Allerdings würde ein Fehlerbericht sofort gesendet, wenn ein Empfänger eine Nachricht aufgrund der DMARC-Richtlinie des Senders ablehnt. Der Empfänger kann sogar einen Bericht senden, wenn die E-Mail zwar angenommen wurde, aber einer der Authentifizierungsmechanismen den Abgleichstest nicht bestanden hat. Ein forensischer Bericht kann eine vollständige Kopie der zurückgewiesenen E-Mail im Abuse Reporting Format (ARF) sein. Jede E-Mail, die die sendende Domäne fälscht, wird zudem abgelehnt, und um eine Kopie gebeten. Dies kann ein Mehrfaches des Volumens der legitimen E-Mails eines Senders ausmachen, auch bei Unternehmen mit einer guten Versandpraktik".[8]

Allein die Datenmengen, die ein Unternehmen durch den regelmäßigen Erhalt von failure reports erhält, lassen schon an der Verhältnismäßigkeit des berechtigten Interesses der Unternehmer gegenüber den Interessen der E-Mail-Empfänger zweifeln. Failure reports werden nicht nur gesendet, wenn ein Phishing oder DDOS-Angriff vorliegt, sondern in allen Fällen, in denen irgendeine Art Fehler oder Abweichung von den Authentifizierungsmerkmalen des Domaininhabers vorliegt. Failure reports können auch Repost zu E-Mails enthalten, bei denen ggfs. nur ein Fehler in der Senderadresse vorlag oder eine E-Mail fehlgeleitet wurde. Auch in diesen Fällen sieht der Reportempfänger aber die E-Mail-Adressen der sendenden und empfangenden Partei sowie den Inhalt und Zweck ihres E-Mailverkehrs, obwohl die Abweichung keinen kriminellen Hintergrund hatte. Es lässt sich daher auch nicht argumentieren, dass ausschließlich E-Mail-Adressen des kriminellen Senders publik werden, sowie Spaminhalte, und diese personenbezogenen Daten weniger schützenswert sind, da hier rechtswidrig eine fremde Domain missbraucht wird um Phishing und DDoS Angriffe durchzuführen. Auch die E-Mail-Adressen und -Inhalte völlig unbeteiligter Dritter könnten durch die failure reports an den Reportempfänger gelangen. Anders als bei aggregated reports ist der Eingriff auch nicht als nur gering einzustufen, da eben nicht nur IP-Adressen weitergegeben werden, sondern klar zuzuordnende Mailadressen, Betreffzeilen und der E-Mail-Body. Insbesondere Kommunikationsinhalte stellen ein besonders schützenswertes Gut dar und werden deshalb auch von Art. 10 GG geschützt. Sender und Empfänger einer E-Mail haben grundsätzlich ein Recht auf eine vertrauliche Kommunikation sowie darauf, dass ihre E-Mail-Adressen nicht Dritten zugänglich gemacht werden. Der nachvollziehbare Wunsch eines Unternehmens Fehler in der eigenen Versandsoftware besser nachvollziehen zu können wird hinter diesen Rechten des Einzelnen zurücktreten müssen. Ebenso das berechtigte Interesse daran, potenzielle Risiken für die eigene Infrastruktur frühzeitig zu erkennen. Einzig in der Einzelfallabwägung, zum Beispiel bei Bestehen eines massiven Phishing- oder DDoS Angriffs, der sowohl die Infrastruktur des Domaininhabers aber auch die Rechte Dritter wie der Empfänger solcher Schad E-Mails, gefährdet, könnte der Empfang von failure reports gerechtfertigt sein.

8 https://dmarc.org/wiki/FAQ#How_does_DMARC_work.2C_briefly.2C_and_in_non-technical_terms.3F

II. Fernmeldegeheimnis

Dazu kommt, dass es sich bei E-Mail-Inhalten um Daten handelt die, neben der DSGVO, auch durch das Fernmeldegeheimnis geschützt sind.

Dem Fernmeldegeheimnis unterfallen gem. § 3 Abs. 1 TTDSG der „Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war". Geschützt ist also alles, was während des jeweiligen Telekommunikationsvorgangs ausgesandt, übermittelt oder empfangen wird.[9] Hierzu zählen unter anderem ob und wie oft jemand eine Telekommunikationsverbindung aufgebaut hat, wann jemand eine Telekommunikationsverbindung aufgebaut hat und wie lange sie aufgebaut war.[10] Zu den „näheren Umständen der Telekommunikation" zählen zudem auch alle „Verkehrsdaten" i.S.v. § 3 Nr. 17 TKG, § 9 TTDSG.[11] Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche. Der Schutz des Fernmeldegeheimnisses beschränkt sich dabei nicht auf die klassische Sprachtelefonie, sondern ist umfassend und technologieneutral ausgestaltet. Erfasst werden insbesondere auch IP-vermittelte Kommunikation und E-Mail.[12] Entscheidend ist, dass die Kommunikation nicht für einen unbegrenzten Adressatenkreis bestimmt ist, sondern es sich um Individualkommunikation handelt.[13] Bei den in failure reports enthaltenen Angaben wie E-Mail-Adressen, IP-Adressen, Betreffzeile und E-Mail-Body handelt es sich damit um Inhalt der Telekommunikation und ihrer näheren Umstände. Der Schutzbereich des § 3 TTDSG ist eröffnet. Da unter den Schutzbereich der §§ 1 ff. TTDSG Verbindungsdaten natürlicher wie auch juristischer Personen fallen, kommt es hier zudem auch nicht darauf an, ob personenbezogene Daten betroffen sind oder nicht.[14]

Gemäß § 3 Abs. 3 TTDSG dürfen die nach dem TTDSG Verpflichteten über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste, den Betrieb eines Telekommunikationsnetzes oder einer Telekommunikationsanlage erforderliche Maß hinaus, weder sich noch anderen Kenntnis von Fernmeldegeheimnissen i.S.v. § 3 Abs. 1 TTDSG verschaffen. Neben dem „sich verschaffen" ist den Verpflichteten also auch die Weitergabe von Fernmeldegeheimnissen an Dritte untersagt.

Verpflichteter ist gemäß § 3 Abs. 2 TTDSG jeder

- Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
- Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
- Betreiber öffentlicher Telekommunikationsnetze und
- Betreiber von Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden. Nr. 6 TKG „jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt."

Sender sind somit als Verpflichtete im Sinne des TTDSG anzusehen.

Durch den Erhalt von failure reports erhalten die Report-Empfänger Kenntnis von E-Mail-Inhalten, ohne dass diese für die Erbringung eines Telekommunikationsdienstes benötigt werden. In dem Erhalt von failure reports ist somit eine Verletzung des § 3 Abs. 3 TTDSG zu sehen.

Allerdings kann nach dem TTDSG eine Kenntnisnahme von Fernmeldedaten dann gerechtfertigt sein, wenn das TTDSG oder eine andere gesetzliche Vorschrift dies vorsieht.

Ein Erlaubnistatbestand könnte sich aus § 12 TTDSG ergeben.

9 Eckhardt, in: TTDSG, § 3 Rn.13.
10 Eckhardt, in: TTDSG, § 3 Rn.15; BverfG, Beschluss der 1. Kammer des Ersten Senats vom 27.10.2006 – 1 BvR 1811/99 -, Rn.12.
11 Eckhardt, in: TTDSG, § 3 Rn.14.
12 Eckhardt, in: TTDSG, § 3 Rn.9.
13 Eckhardt, in: TTDSG, § 3 Rn.10.
14 Eckhardt, in: TTDSG, § 3 Rn.11.

Gemäß § 12 TTDSG darf der Verpflichtete, soweit erforderlich, zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen Verkehrsdaten der Endnutzer verarbeiten. Der Störungsbegriff ist dabei weit zu verstehen. Gemeint ist jede vom Verpflichteten nicht gewollte Veränderung der von ihm für seine Leistungserbringung genutzten technischen Einrichtungen.[15] Als Störung gilt also zum Beispiel auch, wenn die von einem Verpflichteten genutzten IP-Adressbereiche zur Verbreitung von Schadsoftware oder Spam-Mails genutzt werden. Hierzu zählt auch die Durchführung von DDoS-Attacken. Die eingesetzte Technik kann nämlich nicht mehr die ihr zugedachten Funktionen richtig oder vollständig erfüllen.[16] Eine Datenverarbeitung ist nach der Rechtsprechung sogar bereits dann zulässig, um abstrakten Gefahren für die Funktionstüchtigkeit der genutzten technischen TK-Anlage entgegenzuwirken. Anhaltspunkte für eine Störung oder einen Fehler müssen im Einzelfall nicht unbedingt vorliegen.[17] Unter den Begriff der Verarbeitung kann auch die Übermittlung an Dritte fallen, soweit dies zur konkreten Missbrauchsbekämpfung erforderlich ist.[18] Beachtet werden muss allerdings immer der Verhältnismäßigkeitsgrundsatz.[19] Die in Rede stehende Datenerhebung und –verwendung muss geeignet, erforderlich und im engeren Sinn verhältnismäßig sein, um abstrakten Gefahren für die Funktionstüchtigkeit des Telekommunikationsbetriebs entgegenzuwirken.

Fraglich ist zunächst, ob alle in failure reports enthaltenen Daten als Verkehrsdaten zu qualifizieren sind und damit dem Erlaubnistatbestand des § 12 TTDSG unterliegen. Verkehrsdaten sind gemäß § 3 Nr. 70 TKG „Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind." Verkehrsdaten beziehen sich dabei auf einen konkreten Telekommunikationsvorgang.

IP-Adressen, E-Mail-Adressen, Datum und Uhrzeit des Zugriffes bzw. der Zustellung oder Routing Informationen sind als Verkehrsdaten zu qualifizieren.[20] Soweit IP-Adressen oder E-Mail-Adressen demnach der Erkennung und des Eingrenzens von Spam und Phishing dienen, um eine massive Schädigung und erhebliche Störung der Telekommunikationsinfrastruktur zu vermeiden, ist die Erhebung und Übermittlung dieser gerechtfertigt. Die Sicherheit, Funktions- und Leistungsfähigkeit des Telekommunikationsverkehrs stellen hohe Schutzgüter dar, sodass die Erhebung und Übermittlung der IP-Adressen und anderer Daten dahinter zurückstehen können. Failure reports sollen dazu dienen, den E-Mail-Verkehr von Phishing und Spam E-Mails freizuhalten sowie den Domaininhabern und Versendern eine Möglichkeit zu geben, weitergehenden Einblick in ihre Infrastruktur bzw. in die des beauftragten Versenders zu erhalten. Gewährleistet werden soll die Sicherheit, die sich an den Interessenlagen der Nutzer und der Betreiber orientiert. Die Datenverarbeitung zum Erkennen und Verhindern einer „Störung" im Sinne des TTDSG ist daher gegeben.

Problematisch ist es aber, wenn der gesamte E-Mail-Body oder Betreffzeilen gesehen werden können. Darin sind keine Verkehrsdaten zu sehen. Der Rechtfertigungstatbestand des § 12 TTDSG greift in diesen Fällen nicht.

Durch § 12 TTDSG gerechtfertigt werden können daher die Übersendung der Quell-IP-Adresse des Senders sowie die Sender-E-Mail-Adresse und die Empfänger-E-Mail-Adresse. Die Betreffzeile der E-Mail und der E-Mail-Body sind demgegenüber nicht als Verkehrsdaten zu qualifizieren. Sollten diese in failure reports mitgesendet werden, kann dies nicht durch § 12 TTDSG gerechtfertigt werden.

15 Eckhardt, in: TTDSG, § 12, Rn.27.
16 Eckhardt, in: TTDSG, § 12, Rn.27.
17 Eckhardt, in: TTDSG, § 12, Rn.28.
18 Eckhardt, in: TTDSG, § 12, Rn.73.
19 Eckhardt, in: TTDSG, § 12, Rn.28

20 Braun, in: Geppert/Schütz, Beck´scher TTDSG-Kommentar, 2023; Rückert, in: MüKo zur StPO 2023, § 100 a, Rn. 72 ff.

III. Ergebnis zu I. und II.

Failure reports sind vor allem dann problematisch, wenn nicht nur IP-Adressen, sondern auch Betreffzeilen und E-Mail-Bodys mitversandt werden. Dies stellt einen starken Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen dar. Dieser Eingriff lässt sich auch nicht damit rechtfertigen, dass mit Hilfe der Reports Phishing oder Spam besser und nachhaltiger bekämpft werden kann als durch die Generierung bloßer aggregated reports. Bei Abwägung im Rahmen einer Einzelfallprüfung kann möglicherweise zu einem anderen Ergebnis gelangt werden, zum Beispiel bei Vorliegen eines besonders massiven Angriffs auf die Netzinfrastruktur des betroffenen Systems. Grundsätzlich sind failure reports aber nicht durch das berechtigte Interesse des Senders gedeckt. Zudem sind failure reports, die Betreffzeilen und E-Mail-Bodys enthalten, auch nicht durch § 12 TTDSG gedeckt und stellen eine Verletzung des Fernmeldegeheimnisses dar.

Unternehmen sollten daher in ihrer DMARC-Policy keine failure reports anfordern oder sicherstellen, dass failure reports keine E-Mail-Bodys oder Betreffzeilen enthalten oder diesen nur geschwärzt enthalten.

Sender eines failure reports, die vom Domaininhaber angewiesen werden, einen solchen zu versenden, müssen ebenfalls prüfen, inwiefern sie überhaupt berechtigt sind einen solchen Report zu verschicken. Dabei ist auch zu prüfen, ob sie als eigenständige Verantwortliche handeln oder Auftragsverarbeiter und damit als „verlängerter Arm" des Domaininhabers. Als eigenständig Verantwortlicher muss auch der Sender eine Ermächtigungsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO haben. Es gelten hierzu die oben gemachten Ausführungen. Eine Ermächtigungsgrundlage wird von dem Sender kaum zu argumentieren sein. Aber auch im Falle einer Auftragsverarbeitung bedeutet dies nicht, dass der Sender die Verantwortung allein auf den Domaininhaber abschieben kann und nur „nach Weisung" handelt. Denn gemäß Art. 82 DSGVO haften Aufraggeber und Auftragsverarbeiter gegenüber den Betroffenen erst einmal gesamtschuldnerisch. Die Unterstützung von failure reports sollte von Sendern daher vermieden werden.

Aggregated reports sind dagegen mit den Bestimmungen sowohl der DSGVO als auch des TTDSG vereinbar. Zwar schützt das TTDSG auch Daten juristischer Personen, so dass der Anwendungsbereich regelmäßig geöffnet ist. Anders als bei den failure reports werden in den aggregated reports aber nur Verkehrsdaten ausgetauscht. Dies ist durch den Tatbestand des § 12 TTDSG geschützt. Zu beachten ist jedoch stets der Verhältnismäßigkeitsgrundsatz. Zudem sollten Daten, sobald sie nicht mehr benötigt werden, gelöscht werden. Dies sollte in der Regel nach 7 Tagen passieren, in Anlehnung an die Grundsätze des BGH zur Speicherdauer bei Anbietern von Internetdiensten.[21]

21 BGH, Urteil v. 03.07.2014, III ZR 391/13.

IV. Strafrecht

Einschlägige Strafvorschriften sind §§ 206 Abs. 2 Nr. 2 sowie 303 a Abs. 1 StGB.

1. §206 StGB

Sofern der Receiver eine Nachricht nicht zustellt, könnte er sich nach § 206 Abs. 2 Nr. 2 StGB strafbar machen.

Dazu müsste er als Inhaber oder Beschäftigter eines Unternehmens, das geschäftsmäßig Telekommunikationsdienste erbringt, eine diesem Unternehmen zur Übermittlung anvertraute Sendung unterdrücken.

a) Inhaber iSd. § 206 StGB sind natürliche Personen in ihrer Eigenschaft als Träger der Einzelnen kaufmännischen Unternehmen oder als (Mit-)Eigner von Personenhandels- und Kapitalgesellschaften, soweit diese ebenfalls als Unternehmensträger fungieren. Beschäftigte sind sämtliche Mitarbeiter dieser Unternehmen.

Dieses Tatbestandsmerkmal ist bei einem Provider, der E-Mail-Dienste anbietet, erfüllt.

b) Geschäftsmäßiges Erbringen von Telekommunikation ist gemäß § 3 Nr. 10 TKG a.F.[22] das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht.

Auch dieses Tatbestandsmerkmal ist vorliegend erfüllt.

c) Die Sendung muss dem Unternehmen anvertraut sein

Tatobjekt des § 206 Abs. 2 Nr. 2 StGB ist jede Form der dem Fernmeldegeheimnis unterliegenden Telekommunikation. Die E-Mail ist geeignetes Tatobjekt iSd. § 206 Abs. 2 Nr. 2 StGB. Der Begriff der Sendung erstreckt sich auch auf unkörperliche Gegenstände, da § 206 Abs. 2 Nr. 2 StGB nicht, wie § 206 Abs. 2 Nr. 1 StGB auf verschlossene Sendungen beschränkt ist.[23] Anvertraut ist eine Sendung dann, wenn sie auf vorschriftsmäßige Weise in den Verkehr gelangt ist und sich im Gewahrsam des Unternehmens befindet. Da das Fernmeldegeheimnis alle Beteiligten schützt, muss auch davon ausgegangen werden, dass Spam und Phishing-E-Mails zunächst vom Schutzbereich erfasst werden und unter das Tatbestandsmerkmal des vorschriftsmäßig in den Verkehr gelangen fallen. Unproblematisch liegt darüber hinaus der Gewahrsam an einer E-Mail spätestens dann vor, wenn die Anfrage zur Übermittlung von Daten den Mailserver des Unternehmens erreicht hat und der versendende Mailserver die Daten dem empfangenden Server übermittelt hat.[24] Dies ist hier der Fall, da die E-Mails beim Receiver eingehen und dann bestimmt wird, wie mit diesen E-Mails verfahren wird. Unterdrücken setzt voraus, dass die Sendung dem ordnungsgemäßen Telekommunikationsverkehr entzogen wird. Ein Unterdrücken ist anzunehmen, wenn durch technische Eingriffe in den technischen Vorgang des Aussendens, Übermittelns oder Empfangens von Nachrichten mittels Telekommunikationsanlagen verhindert wird, dass die Nachricht ihr Ziel, ihren Empfänger erreicht.[25] Insbesondere ist der E-Mail-Verkehr von diesem Schutzbereich umfasst.[26]

Das Tatbestandsmerkmal ist hier durch die verschiedenen Möglichkeiten, die in den jeweiligen Richtlinien festgelegt werden, erfüllt. Insbesondere durch die Möglichkeiten „reject" und „quarantine", da in diesem Fall die Übermittlung der eingehenden E-Mail vom Receiver an den einzelnen Empfänger nicht bzw. modifiziert stattfindet. Eine andere Beurteilung würde dann vorliegen, wenn „quarantine" durch „Zustellung als Spam" umgesetzt wird: In diesem Fall wird das automatische Verschieben in einen Spamordner als Zustellung gewertet. Der Empfänger hat vorliegend immer noch die Möglichkeit, die E-Mails im Spamordner aufzurufen.

e) Der Täter müsste unbefugt handeln

Dies ist nicht der Fall, soweit Rechtfertigungsgründe gegeben sind. Als Rechtfertigungsgrund für Eingriffe in das Fernmeldegeheimnis kommt zunächst das ausdrückliche oder konkludente Einverständnis in Betracht, das bereits die Tatbestandsmäßigkeit und damit die Strafbarkeit ausschließt.

aa) Tatbestandsausschließendes Einverständnis

Streitig ist, ob das Einverständnis von allen an dem konkreten Fernmeldeverkehr Beteiligten erteilt werden muss[27] oder ein einseitiges Einverständnis ausreicht. Geschützt ist die Telekommunikation als solche, sodass alle Beteiligten hieran dem Schutzbereich unterfallen.

Allerdings ist hier zu beachten, dass strafrechtlich relevant die Nichtzustellung bzw. -übermittlung einer E-Mail ist und nicht der

22 Das neue TKG enthält keine Legaldefinition von „geschäftsmäßiger Erbringung von Telekommunikation" mehr, die historische und systematische Auslegung führt aber dazu, dass § 3 Abs, 2 Nr.2 TTDSG nach Maßgabe des § 3 Nr.10 TKG a.F. auszulegen ist – siehe dazu Eckhardt, TTDSG, § 3 Rn.73.

23 OLG Karlsruhe 1 Ws 152/04 Rn.21; Fischer, 58. Aufl. § 206 StGB Rn. 13

24 OLG Karlsruhe 1 Ws 152/04 Rn.21

25 OLG Karlsruhe 1 Ws 152/04 Rn.22

26 Fischer, 58. Aufl. § 206 Rn. 15

27 OLG Karlsruhe 1 Ws 152/04 Rn. 23; Fischer, 58. Auflage, § 206 Rn. 9

Inhalt der Telekommunikation als solcher. Der Empfänger erwartet den rechtmäßigen und ordnungsgemäßen Umgang mit seiner E-Mail. Daneben betrifft § 206 StGB aber auch das Interesse an der Funktions- und Leistungsfähigkeit sowie der Sicherheit der Telekommunikationsinfrastruktur. Nach hiesiger Auffassung müsste es demnach reichen, wenn eine einseitige Einwilligung des Empfängers gegeben ist. Grundsätzlich dürfte hier, mangels vertraglicher Vereinbarungen von einer mutmaßlichen Einwilligung des Empfängers auszugehen sein, was Phishing-E-Mails betrifft, um weitergehende Gefahren für die betroffenen Personen zu vermeiden. Hinsichtlich der Möglichkeit bestimmte E-Mails durch den Mailboxprovider als Spam zu behandeln oder ähnliches, kann jedoch nicht allgemein davon ausgegangen werden. Aus Art. 2 Abs.1 iVm. Art. 1 Abs. 1 GG (informationelle Selbstbestimmung) folgt vielmehr, dass der Empfänger in der Regel selbst entscheiden möchte, wie er mit solchen E-Mails verfahren will, das heißt, ob er Kenntnis von ihr nehmen möchte, sie unberücksichtigt lässt oder als Spam deklariert und selbst in den „Papierkorb" verlegt. Die Beurteilung, ob eine E-Mail für den jeweiligen Empfänger Spam ist, unterliegt einer individuellen Beurteilung des Empfängers. In der Praxis ist die Beurteilung, ob eine E-Mail für den jeweiligen Empfänger Spam ist, regelmäßig die Aufgabe des Receivers. Dies lässt das Recht auf informationelle Selbstbestimmung jedoch unberührt.

bb) andere Rechtfertigungsgründe

Das Tatbestandsmerkmal „unbefugt" hat eine Doppelfunktion.[28] Neben dem Einverständnis können allgemeine Rechtfertigungsgründe ebenfalls zum Tragen kommen, um den Straftatbestand auszuschließen. Zu beachten ist allerdings, dass nur Erlaubnissätze in Betracht kommen, die in einer gesetzlichen Vorschrift niedergelegt sind, und die sich ausdrücklich auf Telekommunikationsvorgänge beziehen, § 3 Abs.3 TTDSG.

Hier kommen jedenfalls die Vorschriften der StPO in Betracht. Die Übermittlung von Kommunikationsinhalten an Strafverfolgungsbehörden kann aufgrund eines wirksamen Beschlusses gem. §§ 99, 100, 100 a, 100 b, 100 g , 100 h, 100 i, 101 StPO erfolgen.[29]

Ob daneben auch allgemeine Rechtfertigungsgründe, wie § 34 StGB eingreifen können, ist umstritten.[30] Nach Ansicht des OLG Karlsruhe, der auch hier gefolgt wird, gelten dann, wenn besondere Fallgestaltungen vorliegen, die den Rahmen des § 3 Abs. 3 Satz 3 TTDSG sprengen, auch die allgemeinen Rechtfertigungsgründe.[31] Unter Umständen kann es daher gerechtfertigt sein, eine E-Mail herauszufiltern bzw. nicht zuzustellen, da bei deren Verbreitung Störungen oder Schäden der Telekommunikations- und Datenverarbeitungssysteme eintreten und darüber hinaus im Fall von Phishing, weitergehende Schäden für die Betroffenen nicht auszuschließen sind.[32]

Hier kann wieder auf die oben bereits ausführlich dargestellte Argumentation zurückgegriffen werden.

2. Datenveränderung, §303 a StGB

Eine Strafbarkeit könnte sich ferner nach § 303 a Abs. 1 Alt. 2 StGB ergeben. § 303 a StGB schützt das Interesse des Verfügungsberechtigten.

Der Straftatbestand ist einschlägig, wenn E-Mails unterdrückt werden. Hierzu kann auf die Ausführungen zu § 206 Abs. 2 Nr. 2 StGB verwiesen werden.[33]

Eine Rechtfertigung kann aber auch hier durch eine mutmaßliche Einwilligung geschehen[34], wobei auch hier auf die oben bei § 206 Abs. 2 Nr. 2 StGB dargestellten Grundsätze verwiesen wird.

Fazit: Unter strafrechtlichen Gesichtspunkten ist sowohl § 206 StGB als auch § 303 a StGB erfüllt. Ein Ausschluss der Strafbarkeit kommt allerdings zum einen aufgrund einer anzunehmenden mutmaßlichen Einwilligung des Empfängers betreffend der Phishing E-Mails in Betracht, zum anderen durch allgemeine Rechtfertigungsgründe, wie den Schutz des Empfängers vor betrügerischen Absichten und dem Interesse des Receivers an der Aufrechterhaltung der Telekommunikationssicherheit, welches ein überwiegendes Interesse darstellt.

28 OLG Karlsruhe 1 Ws 152/04 Rn.23.
29 Fischer, 58. Auflage, § 206 Rn. 9
30 Fischer, 58. Auflage, § 206 Rn. 9
31 Fischer, 58. Auflage, § 206 Rn. 9
32 OLG Karlsruhe 1 Ws 152/04 Rn.25
33 Fischer, 58. Auflage, § 303 a StGB, Rn. 10
34 Fischer, 58. Auflage, § 303 a StGB, Rn. 13

C. Gesamtergebnis und Empfehlungen

Die Implementierung von DMARC ist vereinbar mit der DSGVO unter Beachtung einiger Einschränkungen.

Während aggregated reports rechtmäßig eingesetzt werden können, bestehen bei der Implementierung von failure reports erhebliche datenschutzrechtlichen Bedenken.

Im Einzelnen:

a) aggregated reports:

Die in den reports enthaltenen IP-Adressen werden in den meisten Fällen nicht als personenbezogene Daten einzuordnen sein und unterliegen damit bereits nicht dem Anwendungsbereich der DSGVO. Sollten doch personenbezogene Daten enthalten sein, ist die Verarbeitung dieser grundsätzlich durch ein berechtigtes Interesse der Unternehmen an einer fehlerfreien Versandsoftware und dem Schutz vor Spam und Phishing sowie zum Schutz der Telekommunikationsanlagen gerechtfertigt. Eine konkrete Störung muss dafür nicht vorliegen.

Eine zweckmäßige Anonymisierung sollte - wo möglich und zumutbar - vorgenommen werden.

b) failure reports:

Im Vergleich zu aggregated reports enthalten failure reports eine Vielzahl von personenbezogenen Daten. Der Erhalt von failure reports kann daher grundsätzlich nicht durch das berechtigte Interesse der Unternehmen gerechtfertigt werden, da die Interessen des einzelnen auf informationelle Selbstbestimmung und Vertraulichkeit der Kommunikation überwiegen.

Der Erhalt von failure reports kann höchsten im Einzelfall gerechtfertigt werden. Allerdings wird empfohlen auch in diesen Fällen auf redacting zurückzugreifen, um zu vermeiden, dass personenbezogene Daten des Empfängers einer betrügerischen Mail übermittelt werden. Zu diesen Daten zählen zwingend Betreff und Body einer E-Mail sowie die E-Mail-Adresse des Empfängers.

Gutachten zur Vereinbarkeit von DMARC mit der DSGVO und anderen Rechtsvorschriften

eco Kompetenzgruppe E-Mail / CSA
Autoren: Dr. Katharina Küchler (eco),
Patrick Ben Koetter (sys4 AG)

eco –Verband der Internetwirtschaft e.V.
Lichtstraße 43h, 50825 Köln
fon +49(0)221/700048-0
fax +49(0)221/700048-111
info@eco.de
www.eco.de

CSA Certified Senders Alliance

eco VERBAND DER INTERNETWIRTSCHAFT