WIR GESTALTEN DAS INTERNET.

Verband der deutschen Internetwirtschaft e.V.

Gutachten zur Vereinbarkeit von DMARC mit dem deutschen Recht

eco Kompetenzgruppe E-Mail

Inhaltsverzeichnis

A. Sachverhalt

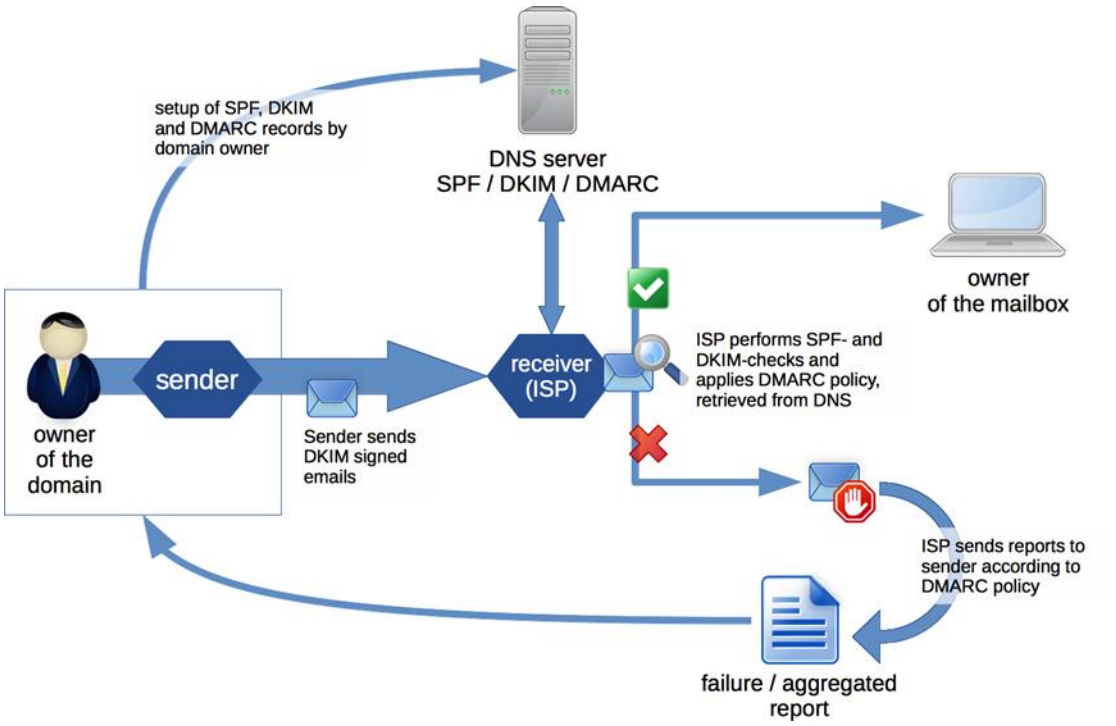
DMARC steht für: Domain-based Message Authentication, Reporting and Conformance: Domainbasierte Authentifizierung, Meldung und Konformität von Nachrichten.[1]

Hintergrund der DMARC.org ist es, die Sicherheit im E-Mailverkehr zu erhöhen und einen größeren Schutz von E-Mail-Empfängern vor Phishing Mails zu gewährleisten, sowie eine Domainreputation zu ermöglichen. Ziel ist es, bestimmte Formen krimineller E-Mails (Phishing) vorzeitig herauszufiltern bzw. abzugreifen, damit sie die Nutzer nicht erreichen.[2] Beim Phishing handelt es sich um gefälschte E-Mail-Nachrichten an Internet-Anwender , bei denen z.B. ein Link, der in der E-Mail enthalten ist, nicht auf den seriösen Anbieter zurückführt, sondern verdeckt zu den Angreifern, die damit in den Besitz der sensiblen privaten Daten gelangen wollen. Phishing kann auch durch Anhänge oder Aufforderungen in einer Mail erfolgen. Häufig wird die Absenderadresse maskiert, um dem Empfänger einer Mail einen validen Absender vorzutäuschen. Dies wird u.a. von DMARC verifiziert, um etwaige „Fälschungen" erkennen zu können.

Mit DMARC als Standard soll ein Zusammenspiel zwischen den Beteiligten im E-Mailverkehr ermöglicht werden, indem ein Informationsaustausch zwischen bzw. zu ihnen stattfindet. Folgende Beteiligte sind dabei zu unterscheiden:

1. Der Domaininhaber – z.B. Facebook, Paypal etc. – (bzw. Domainverwalter, der vom Domaininhaber beauftragt wird, alle Einstellungen in Bezug auf die Domain zu verwalten, darunter also auch den DMARC Eintrag)
2. Der Sender, der vom Domaininhaber zur Versendung von E-Mails beauftragt wird, oder ein 3., der unter der Domain des Domaininhabers, E-Mails versendet.
3. Der Internetserviceprovider (im Folgenden Receiver) - z.B. GMX, AOL, Hotmail, Yahoo! etc.
4. Der Report-Empfänger. Das kann sowohl der Domaininhaber als auch der Sender oder eine beauftragte juristische Person sein.
5. Der Empfänger, an den die E-Mail zugestellt werden soll.

[1] https://tools.ietf.org/html/rfc7489
[2] https://tools.ietf.org/html/rfc7489



Der Sender muss zunächst SPF (Sender Policy Framework) Datensätze und den öffentlichen Schlüssel zu DKIM (Domainkeys Identified Mail) für alle zu berücksichtigenden Versand-Domains (die DMARC Policy-Domain) konfigurieren. Hierbei entscheidet der Sender, welche IP-Adressen und welche Signaturen legitimen E-Mailversand ausführen bzw. darstellen.

Beim SPF wird die IP-Adresse des Senders mit einer für diese Domain eingetragenen Liste an IP-Adressen verglichen. Bei DKIM werden E-Mails beim Versand mit einem geheimen Schlüssel kryptografisch signiert, die der Receiver durch Abgleich mit dem öffentlichen Schlüssel auf „Korrektheit" validieren kann. DMARC gewährleistet basierend auf diesen beiden bereits etablierten Technologien die Signaturintegrität.

Mittels DMARC soll dem Domaininhaber nun Einfluss auf den Umgang mit nicht authentifizierten Nachrichten aus den legitimen Domains gegeben werden, indem er neben den oben bereits erwähnten Einträgen, in DMARC Richtlinien festlegt, wie die Receiver im Falle eines Nichtbestehens des DMARC Authentifizierungs-Tests mit den E-Mails verfahren sollen. Eine Nachricht besteht DMARC nicht, wenn sie die SPF und/oder DKIM Prüfung nicht bzw. nur teilweise besteht. Hierzu kann zwischen einer „strict" und „relaxed" Vorgehensweise in Bezug auf die SPF/ DKIM Authentifizierung unterschieden werden.

Ausgangspunkt ist hier, dass DMARC die RFC5322 From Domain nutzt, um authentifizierte Kennzeichnungen zusammenzubinden/zusammenzufügen.[3]

Bei einer „relaxed" Vorgehensweise in Bezug auf DKIM muss die unter DKIM „unterzeichnete" Domain und die RFC5322.From Domain organisatorisch ähnlich sein. Bei einer „strict" Vorgehensweise, müssen diese jedoch exakt übereinstimmen.

Bei einer „relaxed" Vorgehensweise in Bezug auf SPF gilt ähnliches. Die unter SPF authentifizierte RFC53221.MailFrom Domain und RFC5322.From Domain müssen die gleiche organisatorische Domain haben. In der „strict" Vorgehensweise muss dagegen eine exakte DNS Domain Übereinstimmung vorliegen.[4]

Darüber hinaus können sodann Maßnahmen wie z.B. als Spam behandeln (quarantine), ablehnen (reject), oder keine Maßnahmen (none) definiert werden. (Hierbei ist zu beachten, dass der Receiver auch die Ablehnung oder die Behandlung als Spam wählen kann, obwohl die E-Mail den DMARC Authentifizierungs-Test bestanden hat. Ebenso kann der Receiver eine E-Mail akzeptieren, die den DMARC Authentifizierungs-Test nicht bestanden hat, obwohl der Domaininhaber in den Richtlinien die Ablehnung festgelegt hat.)[5]

Diese DMARC Richtlinien werden, neben Reporting-Adressen, auf die nachfolgend näher eingegangen wird, im DNS (Domain Name Service - dem Verzeichnisdienst zu einer Domain; für jedermann zugänglich) als Text Resource Records (TXT RR) veröffentlicht.

Die zuvor erwähnte Reporting-Adresse dient als Feedback-E-Mail-Adresse, an die nun alle (DMARC) teilnehmenden Receiver Informationen über diese DMARC Policy-Domains und zu den E-Mail-Authentifizierungs-Ergebnissen senden.[6] Je nachdem, wer für die Reports durch den Domaininhaber eingetragen wurde, erhält dieser nun Informationen über alle eingehenden E-Mails die vermeintlich von dieser DMARC-Policy Domain versendet wurden. Diese Informationen erfolgen entweder mittels standardisierten „Aggregated Reports" oder „Failure Reports".

Für den Erhalt dieser Reports ist entscheidend, wer von dem Domaininhaber eingetragen wurde. Dies kann, wie oben erläutert sowohl der Domaininhaber selbst, als auch der Sender sein.

[3] https://tools.ietf.org/html/rfc7489
[4] https://tools.ietf.org/html/rfc7489
[5] https://tools.ietf.org/html/rfc7489
[6] https://tools.ietf.org/html/rfc7489

I. Aggregated Reports

Die Reports sollten nach der Empfehlung von DMARC.org folgendes beinhalten[7]:

- Genügend Informationen für den Report-Empfänger, um analysieren zu können, welche Dispositionen entsprechend der veröffentlichten Richtline getroffen wurden sowie SPF, DKIM Ergebnisse.
- Daten für jede Versender-Subdomain gesonderte From-Mail von der organisatorischen Versender-Domain, auch, wenn keine Richtlinie zu Subdomains angewandt wird.
- versendende und empfangende Domains.
- Die Richtlinie, die vom Domaininhaber veröffentlicht wurde und die Richtlinie, die tatsächlich angewandt wurde, sofern sich diese unterscheiden.
- Die Anzahl der erfolgreichen Authentifizierungen.
- Die Anzahl an Nachrichten, basierend auf allen empfangenen Nachrichten, auch wenn die Zustellung von anderen Filter-Systemen letztlich geblockt wurde.

Bei den „Aggregated Reports" sind 2 Möglichkeiten von Reports zu unterscheiden:

Es gibt zum einen die Möglichkeit

- in regelmäßigen Zeitabständen aggregierte Reports zu den entsprechenden DMARC-Policy Domains zu erhalten, welche laut Spezifikation weder individuelle E-Mail-Adressen noch Zustell-Stati (ob es zugestellt wird, ob es gelöscht wird etc.) beinhalten und zum anderen
- aggregierte Statistik Reports zu IP-Adressen, die E-Mails für die DMARC-Policy Domain versandt haben.[8] Eine IP-Adresse (Internetprotokoll-)Adresse ist eine Zahlenfolge zur Adressierung eines Rechners, die auf dem Internetprotokoll basierend dem Rechner zugeteilt wird. Hierbei kommen im Rahmen der Übermittlung sowohl statische als auch dynamische IP-Adressen in Betracht. Während eine statische IP-Adresse einem bestimmten Anschlussinhaber (genauer: der Netzwerkschnittstelle eines bestimmten Gerätes des Anschlussinhabers) fest zugewiesen wird, wird im Fall der dynamischen Adressierung dem Anschlussinhaber (genauer: der Netzwerkschnittstelle des mit dem Internet kommunizierenden Geräts des Anschlussinhabers) bei jeder neuen Aufnahme der Netzwerkverbindung eine IP-Adresse neu zugewiesen.[9] Die Reports enthalten Informationen sowohl über die Anzahl der zugestellten, als auch über die Anzahl der nicht zugestellten E-Mails. Der erste Report wird übermittelt, sobald ein DMARC Eintrag im DNS veröffentlicht wurde.

[7] https://tools.ietf.org/html/rfc7489
[8] http://dmarc.org/presentations/DMARC_general_overview_20120130.pdf p. 13
[9] 1 BvR 1299/05, Rdnr. 63; Welp, Information und Recht, Band 73, 2009, S.9, 10

Der IP-Report besteht aus einer XML Datei, die folgendes beinhaltet[10]:

- jede IP Adresse, die E-Mails für die DMARC-Policy Domain versandt hat
- die Anzahl an Nachrichten für die DMARC-Policy Domain von jeder dieser IP Adressen
- eine Aussage darüber, wie mit diesen Nachrichten entsprechend der festgelegten DMARC-Richtlinie verfahren wurde
- welche Ergebnisse die Authentifizierung mittels SPF und DKIM ergeben haben.

II. Failure Reports[11]

Die nachrichtenspezifischen Authentifizierungs-Fehler bezogenen Failure Reports können genutzt werden, um etwaige Probleme der Domaininhaber-Infrastruktur zu identifizieren und die Quellen und Gründe herauszufinden, die das Fehlschlagen der Versendung verursacht haben. Sie können ebenfalls dafür verwendet werden, um Untersuchungen hinsichtlich der Quellen und Ziele betrügerischer Nachrichten zu unterstützen. Diese Reports beziehen sich auf individuelle E-Mails, welche die DKIM und/ oder SPF Prüfung nicht bestanden haben.

Für den Versand von Failure Reports geht aus dem AFRF Format hervor, welche Daten reported werden. Es handelt sich hierbei u.a. um die folgenden Daten:

- Die IP-Adresse
- Die Ausgangs-E-Mail Adresse
- Die Empfänger-E-Mail Adresse
- Der Betreff der E-Mail
- Der E-Mail-Body

Es ist zu beachten, dass die DMARC Authentifizierung sich allein auf die DNS Domain bezieht und nicht den lokalen Teil einer in der Nachricht gefundenen E-Mail Adress-Kennzeichnung/Identifikation authentifiziert.[12]

[10] http://dmarc.org/faq.html
[11] https://tools.ietf.org/html/rfc7489
[12] https://tools.ietf.org/html/rfc7489

B. Rechtliche Würdigung

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

Hierbei sind sowohl datenschutzrechtliche als auch strafrechtliche Aspekte zu berücksichtigen.

I. Datenschutz, insbesondere TKG (Telekommunikationsgesetz)

1. Personenbezogene Daten

Fraglich ist, ob durch die beiden Arten von Reports („Aggregated", „Failure"), personenbezogene Daten erhoben, verarbeitet oder genutzt werden, wobei hier in Ermangelung eigenständiger Definitionen im TKG, die Begriffsbestimmungen des BDSG zum Tragen kommen. Unter Erhebung ist gemäß § 3 III BDSG „das Beschaffen von Daten über den Betroffenen" zu verstehen. Unter Verarbeitung fällt gemäß § 3 IV BDSG „das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten". Nutzen meint gemäß § 3 V BDSG „jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt". Durch die Reports werden u.U., neben den IP-Adressen des Senders, auch die oben angesprochenen Daten erhoben und verarbeitet, indem diese Reports an den jeweiligen Reportempfänger übermittelt werden.

Da das TKG für den Begriff „personenbezogene Daten" ebenfalls keine eigene Definition enthält, ist insoweit auf die allgemeine Definition des BDSG zurückzugreifen. Gemäß § 3 I BDSG sind personenbezogene Daten, „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". 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.

Bei Verwendung von DMARC sind zunächst unterschiedliche Fallkonstellationen zu differenzieren:

1. Der Domaininhaber ist eine juristische Person und gleichzeitig der Sender, der als Reportempfänger eingetragen ist. Er erhält vom Receiver den Report über die entsprechenden IP-Adressen.
2. Der Domaininhaber ist eine juristische Person und bedient sich einer oder mehrerer juristischen Personen als Sender. Der Domaininhaber ist als Reportempfänger eingetragen. Er erhält vom Receiver den Report über die entsprechenden IP-Adressen der Sender.
3. Der Domaininhaber bedient sich einer oder mehrerer juristischen Personen als Sender. Einer (oder mehrere)der Sender ist als Reportempfänger eingetragen. Er erhält vom Receiver den Report mit den in Betracht kommenden IP-Adressen.
4. Eine Person versendet unter Verwendung der Domain des legitimen Inhabers, E-Mails (Phishing)

Im Hinblick auf die IP-Adressen, die in den Reports übermittelt werden, ist wie oben bereits erörtert, zwischen statischen und dynamischen IP-Adressen zu unterscheiden. Hierbei ist zu beachten, dass Sender im Rahmen der best practice grundsätzlich keine dynamischen IP-Adressen zur E-Mailversendung verwenden, da von E-Mail Servern mit dynamisch vergebenen IP-Adressen überwiegend Spam versendet wird.[13] Dennoch ist nicht auszuschließen, dass auch und gerade im Fall von Phishing (Fall 1.4.) dynamische IP-Adressen durch die Reports übermittelt werden. Jedenfalls lässt sich dies aus den DMARC Richtlinien nicht eindeutig feststellen oder verneinen.[14]

a) statische IP-Adresse

Die statische IP-Adresse wird einhellig als personenbezogenes Datum qualifiziert, da für jedermann eine Zuordnung zu ihrem tatsächlichen Inhaber möglich ist.[15]

b) dynamische IP-Adresse

Ob dynamische IP-Adressen als personenbezogenes Datum qualifiziert werden können, ist dagegen streitig, da eine Zuordnung, wie im Falle der statischen IP-Adresse nicht besteht. Ausgangspunkt des Meinungsstreits ist das Tatbestandsmerkmal der „Bestimmbarkeit" iSd § 3 I BDSG. Die Zuordnung zu einer dynamischen IP-Adresse erfolgt durch den Internetzugangs-Anbieter (Accessprovider) lediglich temporär. Hierbei wird eine Anonymität der Internet-Nutzer gewährleistet. Auch, wenn die IP-Adresse von Server Betreibern ausgelesen werden kann, ist eine längerfristige Verbindung der Adresse mit einem Namen, infolgedessen der Nutzer bekannt werden würde, nicht möglich.[16] Aus der IP-Adresse als solcher, ergibt sich unmittelbar kein Bezug zu einer bestimmten Person, sodass dieser zunächst hergestellt werden muss.[17]

Da allein der Accessprovider die Zuteilung der IP-Adresse vornimmt und daher der Personenbezug für ihn ohne erheblichen Aufwand möglich ist, sind die oben beschriebenen Fälle streitig, bei denen andere Personen, wie hier der Mailbox-Anbieter, dynamische IP-Adressen erheben und übermitteln.

[13] http://postmaster.1und1.de/de/fehlermeldungen/; http://postmaster.gmx.de/de/e- mail-policy/
[14] https://tools.ietf.org/html/rfc7489
[15] https://www.datenschutzzentrum.de/ip-adressen/; Härting, Internetrecht 4. Auflage 2010, Rdnr 91
[16] Nietsch, CR 11/2011, S. 764
[17] Anmerkung zu BGH III ZR 146/10, jurisPR- ITR 15/2011 S.4

aa) Relativität des Personenbezugs

Eine Auffassung[18] geht von der Relativität des Personenbezugs aus und stellt für die Bewertung der Bestimmbarkeit iSd § 3 I BDSG darauf ab, ob die verantwortliche Stelle mit den ihr normalerweise zur Verfügung stehenden Mitteln und ohne unverhältnismäßigen Aufwand den Bezug zu einer natürlichen Person herstellen kann. Es wird insbesondere danach differenziert, ob die Deanonymisierung mit verhältnismäßigem Aufwand möglich ist. Dies sei jedoch nur dem Access Provider möglich.[19] Ein Dritter (hier der Mailbox-Anbieter) könnte den Nutzer hinter der IP-Adresse nur mit Hilfe des Access Providers ermitteln, der aber mangels Rechtsgrundlage Dritten diese Angaben nicht zur Verfügung stellen darf. Die theoretische Möglichkeit einer Identifikation des Nutzers kann der vorgenannten Definition der Bestimmbarkeit nicht entsprechen.[20]

bb) Objektivität des Personenbezugs

Nach dieser Auffassung ist es nicht relevant, ob ein unverhältnismäßiger Aufwand erforderlich ist, um die IP-Adresse zu deanonymisieren. Ausreichend ist allein, dass die theoretische Möglichkeit der Verknüpfung der IP-Adresse mit einer natürlichen Person in irgendeiner Form besteht.[21] Darauf, dass eine Bestimmbarkeit der Person im Rechtssinne nur gegeben sei, wenn die Person mit legalen Mitteln identifiziert werden könne, komme es nicht an. Das Datenschutzrecht solle gerade vor dem Missbrauch von Daten schützen, sodass eine derartige Einschränkung des Begriffs der Bestimmbarkeit nicht gerechtfertigt erscheine.[22] Die Objektivität des Personenbezugs lässt sich auch auf Erwägungsgrund 26 der Datenschutz-Richtlinie 95/46/EG stützen.[23] Auch die Art 29 Gruppe geht von dem absoluten Begriff aus. In Erwägung Nr. 26 zur EU-Datenschutzrichtlinie 95/46/EG wird eindeutig festgelegt, dass alle Mittel zu berücksichtigen sind, die von dem für die Verarbeitung Verantwortlichen oder von jeder anderen Person nach vernünftiger Einschätzung zur Identifizierung der betreffenden Person genutzt werden können, um festzustellen, ob eine Person bestimmbar ist.[24]

Da nicht ausgeschlossen werden kann, dass Dritte über das zur Herstellung des Personenbezugs erforderliche Zusatzwissen verfügen, kommt es für den Personenbezug nur auf die faktisch zu beurteilende Wahrscheinlichkeit einer möglichen Identifizierung an.[25] Auch bei dynamischen IP-Adressen können diese durch Dritte mit Hilfe der Logfiles des Internet Service Providers (ISP) einzelnen Anschlüssen und damit ggf. einzelnen Personen zugeordnet werden. Daher muss

[18] Eckhardt, CR 2011/5 (S. 342 mit weiteren Verweisen); Härting, Internetrecht, 4. Aufl. 2010, S. 23 Rdnr. 94
[19] LG München 7 O 1310/11, Rdnr. 120
[20] AG München 133 C 5677/08, Rdnr. 22-24; Eckhardt CR 5/2011S. 342
[21] Härting, Internetrecht 4. Auflage Rdnr. 93
[22] AG Berlin Mitte 5 C 314/06 Rdnr.13, 14
[23] WP 136 (01248/07/DE der Artikel 29 Datenschutzgruppe, S. 21 ff.; WP 148 (00737/DE) der Artikel 29 Datenschutzgruppe, S.9; Stiemerling/Hartung CR 1/ 2012, S. 64
[24] WP 136 (01248/07/DE der Artikel 29 Datenschutzgruppe S. 17 ff.
[25] Welp, Informstion und Recht, Band 73, 2009 S. 206

zumindest von einer Personenbeziehbarkeit der dynamischen IP-Adresse und damit der Anwendung der Datenschutzgesetze ausgegangen werden.[26]

cc) Zwischenergebnis:

Nach hiesiger Ansicht sprechen die besseren Gründe für die Objektivität des Personenbezugs, jedenfalls ist für den übergeordneten Zweck, nämlich dem Schutz vor Phishing und Spam im Zweifel davon auszugehen, dass dynamische IP-Adressen ein personenbezogenes Datum darstellen. Da nicht ausgeschlossen werden kann, dass Dritte über das zur Herstellung des Personenbezugs erforderliche Zusatzwissen verfügen, kommt es für den Personenbezug daher auf die tatsächlich zu beurteilende Möglichkeit einer möglichen Identifizierung an.

c) Domains und andere Daten

Domains sind Folgen aus Buchstaben und Zeichen, die einer (oder mehrerer) IP-Adresse(n) zugeordnet sind. [27] Auch Domains können demnach einen Personenbezug aufweisen, insbesondere wenn z.B. der Name einer natürlichen Person enthalten ist. Da nicht auszuschließen ist, dass mittels der Failure Reports auch E-Mail Adressen, oder sonstige personenbezogene Daten übermittelt werden, ist dem Grunde nach die datenschutzrechtliche Relevanz zu bejahen.

2. Erlaubnistatbestand/ Rechtfertigung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur dann zulässig, wenn sie durch Gesetz oder andere Rechtsvorschriften erlaubt ist oder der Betroffene einwilligt.

a) Einwilligung

Für die Fälle, in denen der Domaininhaber, gleichzeitig Sender ist und/oder der Sender selbst als Reportempfänger eingetragen worden ist, ist von einer Einwilligung auszugehen.

1. Gesetzlicher Erlaubnistatbestand

a. §§ 91, 88 TKG

Bei den oben genannten Beispielen (I.1. 1.-3.) ist das Tatbestandsmerkmal der natürlichen Person nicht erfüllt, da der Inhaber der statischen IP-Adresse eine juristische Person ist und der Bezug zu einer natürlichen Person nicht hergestellt werden kann.[28]

Zu beachten ist jedoch, dass das TKG in § 91 I 2 TKG den Schutzbereich auf juristische Personen erweitert. Der Schutz erstreckt sich allerdings nur dann auf die juristische Person, soweit Daten

[26] https://www.datenschutzzentrum.de/ip-adressen/
[27] Fetzer, TKG Kommentar, 2008, § 3 Nr.13 Rdnr. 67
[28] Anm. zu BGH III ZR 146/10, JurisPR- ITR 15/2011 Anm.2, S. 4; Härting, Internetrecht, 4. Auflage 2010, S. 23 Rdnr. 94

betroffen sind, die dem Fernmeldegeheimnis gemäß § 88 I TKG unterliegen. [29] Dem Fernmeldegeheimnis unterfallen gem. § 88 I TKG der „Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war". 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. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

Unter den Schutzbereich der §§ 91 ff TKG unterfallen damit auch Verbindungsdaten juristischer Personen.[30]

Geschützt werden die Daten von Teilnehmern und Nutzern. Teilnehmer sind gemäß § 3 Nr. 20 TKG natürliche oder juristische Personen, die mit dem Anbieter der Telekommunikation einen Vertrag über die Erbringung des Dienstes haben. Nutzer iSd § 91 TKG ist gemäß § 3 Nr. 14 TKG jede natürliche Person, die Telekommunikationsdienste tatsächlich in Anspruch nimmt. Da hier weder ein Vertragsverhältnis zwischen Domaininhaber/Sender und Receiver besteht, noch das Tatbestandsmerkmal des Nutzers einschlägig ist, ist § 91 TKG schlussendlich nicht anwendbar, soweit Domaininhaber und Sender juristische Personen sind.

Für den Sender als natürliche Person, sowie den oben genannten 4. Fall des Phishings ist der Personenbezug dagegen zu bejahen, insbesondere hinsichtlich der Failure Reports, da hierbei, wie bereits erörtert, ein Ausschluss der Übermittlung personenbezogener Daten derzeit nicht möglich ist.

Fraglich ist jedoch die Reichweite des Fernmeldegeheimnisses.

Gemäß § 88 III TKG dürfen Diensteanbieter über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderliche Maß hinaus, weder sich noch anderen Kenntnis von Fernmeldegeheimnissen iSv § 88 I TKG verschaffen. Neben dem „sich verschaffen" ist Diensteanbietern auch die Weitergabe von Fernmeldegeheimnissen an Dritte untersagt.[31] Eine Ausnahme gilt hier jedoch, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht.

b. Erheben und Verwenden von Verkehrsdaten, § 100 TKG iVm §96 TKG

Ein Erlaubnistatbestand könnte sich aus § 100 TKG iVm § 96 TKG ergeben.

Gemäß § 100 TKG darf der Diensteanbieter, soweit erforderlich, zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden.

[29] Fetzer , TKG Kommentar 2008, § 91 TKG Rdnr. 11
[30] Fetzer , TKG Kommentar 2008, § 91 TKG Rdnr. 11
[31] Ellinghaus, TKG Kommentar 2008, § 88 Rdnr. 28

Diensteanbieter ist gemäß § 3 Nr. 6 TKG „jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt." Dies ist bei Sendern der Fall. IP-Adressen müssten als Verkehrsdaten zu qualifizieren sein. Verkehrsdaten sind gemäß § 3 Nr. 30 TKG „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet und genutzt werden". Verkehrsdaten beziehen sich dabei auf einen konkreten Telekommunikationsvorgang.

In der Rechtsprechung werden IP-Adressen als Verkehrsdaten qualifiziert.[32] Nach § 96 I Nr. 1 TKG fallen IP-Adressen unter den Begriff der Verbindungsdaten, soweit sie zum Aufbau, zur Aufrechterhaltung der Telekommunikation oder zur Entgeltabrechnung notwendig sind.[33] Die Erhebung von IP-Adressen ist grundsätzlich erforderlich, weil sie für die Aufrechterhaltung einer Internetverbindung benötigt werden.

Der Begriff der Störung ist umfassend zu verstehen als jede vom Diensteanbieter nicht gewollte Veränderung der von ihm für sein Telekommunikationsangebot genutzten technischen Einrichtungen.[34] Unter den Begriff der Verwendung kann auch die Übermittlung an Dritte fallen, soweit dies zur Störungsbeseitigung erforderlich ist.[35]

Zu beachten ist, dass unter Berücksichtigung des Fernmeldegeheimnisses (Art. 10 I GG, § 88 TKG) und des Grundrechts auf informationelle Selbstbestimmung (Art. 1 I, Art.2 I GG) nicht vorausgesetzt wird, dass im Einzelfall bereits Anhaltspunkte für eine Störung oder einen Fehler an den Telekommunikationsanlagen vorliegen. Es genügt vielmehr, dass die in Rede stehende Datenerhebung und –verwendung geeignet, erforderlich und im engeren Sinn verhältnismäßig ist, um abstrakten Gefahren für die Funktionstüchtigkeit des Telekommunikationsbetriebs entgegenzuwirken.[36]

Zwar greift § 100 TKG in die vorgenannten Rechte ein; diese können und müssen aber mit den berechtigten Belangen der Telekommunikationsunternehmen, öffentlichen Interessen und den übrigen Interessen der Empfänger abgewogen werden, wobei der Verhältnismäßigkeitsgrundsatz zu wahren ist.

Schutzgüter sind unter anderem die Telekommunikationsinfrastruktur.

Hierin könnte die Rechtfertigung der Erhebung und Übermittlung der IP-Adressen liegen, da der E-Mailverkehr von Phishing und Spam E-Mails freigehalten werden soll und die Reports dazu dienen 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. Soweit

[32] BGH III ZR 146/10, Rdnr. 23; 1 BvR 256/08, Rdnr.44 ff.. , OLG Frankfurt 13 U 105/07, Rdnr. 104; BT- Drucks 15/2316, S. 90
[33] TKG Kommentar 2008, Fetzer, § 96 Rdnr. 6
[34] BGH III ZR 146/10 Rdnr. 24
[35] TKG Kommentar 2008, Fetzer § 100 Rdnr 3
[36] BGH III ZR 146/10 Rdnr. 25

die IP-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 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 kann. Der damit verbundene Eingriff ist im Hinblick auf den Schutz der Funktions- und Leistungsfähigkeit der Telekommunikationsinfrastruktur einerseits und dem Schutz der sensiblen personenbezogenen Daten, die Schäden in größerem Umfang für die Betroffenen von Phishing verursachen können andererseits, vergleichsweise gering und überwiegt die legitimen, teilweise ebenfalls grundrechtlich abgesicherten Interessen der nicht legitimen Versender und der Empfänger sowie die öffentlichen Interessen an der Funktionstüchtigkeit und Leistungsfähigkeit der Telekommunikationsinfrastruktur nicht.[37] Insbesondere hinsichtlich der Übermittlung der IP-Adresse ist zu beachten, dass die Identität des jeweiligen Nutzers aus der IP-Nummer selbst nicht erkennbar ist und erst durch die Zusammenführung mit weiteren Angaben ermittelbar wird.

c. Einwilligung nach § 28 BDSG

Falls Daten übermittelt werden, die nicht dem Fernmeldegeheimnis unterliegen und damit das TKG nicht zur Anwendung kommt, könnte das Erheben und Verwenden der personenbezogenen Daten unter § 28 I 1 Nr. 2 bzw. II BDSG gerechtfertigt sein.

Danach ist die Übermittlung oder Nutzung zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Bei dieser Interessenabwägung kommt es auf einen Zweck an, dessen Verfolgung vom gesunden Rechtsempfinden gebilligt wird. Die Erhebung und Verwendung der Daten muss zur Wahrung der berechtigten Interessen nicht nur dienlich, sondern erforderlich sein.[38]

Hier kann auf die oben bereits vollzogene Argumentation verwiesen werden.

Fazit und Zwischenergebnis:

Die Reports sind datenschutzrechtlich grundsätzlich zulässig und gerechtfertigt. Zu beachten ist jedoch stets der Verhältnismäßigkeitsgrundsatz.

[37] BGH III ZR 146/10 Rdnr. 31
[38] Gola, Klug, Körffer, BDSG Kommentar, 10. Aufl.2010, § 28 Rdnr. 25

II. Strafrecht

Einschlägige Strafvorschriften sind §§ 206 II Nr. 2 sowie 303 a I StGB.

1. §206 StGB

Sofern der Receiver eine Nachricht nicht zustellt, könnte er sich nach § 206 II 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-Maildienste anbietet, erfüllt.

b) Geschäftsmäßiges Erbringen von Telekommunikation ist gemäß § 3 Nr. 10 TKG 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 II Nr. 2 StGB ist jede Form der dem Fernmeldegeheimnis unterliegenden Telekommunikation. Die E-Mail ist geeignetes Tatobjekt iSd § 206 II Nr. 2 StGB. Der Begriff der Sendung erstreckt sich auch auf unkörperliche Gegenstände, da § 206 II Nr. 2 StGB nicht, wie § 206 II Nr. 1 StGB auf verschlossene Sendungen beschränkt ist.[39] 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 Phishingmails 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.[40] Dies ist hier der Fall, da die E-Mails beim Receiver eingehen und dann bestimmt wird, wie mit diesen E-Mails verfahren wird.

[39] OLG Karlsruhe 1 Ws 152/04 Rdnr.21; Fischer, 58. Aufl. § 206 StGB Rdnr. 13
[40] OLG Karlsruhe 1 Ws 152/04 Rdnr.21

d) 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. [41] Insbesondere ist der E-Mailverkehr von diesem Schutzbereich umfasst.[42]

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 [43] 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 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 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 I iVm 1 I GG (informationelle Selbstbestimmung) folgt vielmehr, dass der Empfänger in der Regel selbst entscheiden möchte, wie er mit solchen E-Mails verfahren will, dh. ob er Kenntnis von ihr

[41] OLG Karlsruhe 1 Ws 152/04 Rdnr.22
[42] Fischer, 58. Aufl. § 206 Rdnr. 15
[43] OLG Karlsruhe 1 Ws 152/04 Rdnr. 23; Fischer, 58. Auflage, § 206 Rdnr. 9

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.[44] 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, § 88 III 3 TKG.

Hier kommen jedenfalls die Vorschriften der StPO in Betracht. Die Übermittlung von Kommunikationsinhalten an Strafverfolgungsbehörden kann aufgrund eines wirksamen Beschlusses gem. §§ 99, 100, 100a, 100b, 100g , 100 h, 100 i, 101 StPO erfolgen.[45]

Ob daneben auch allgemeine Rechtfertigungsgründe, wie § 34 StGB eingreifen können, ist umstritten.[46] Nach Ansicht des OLG Karlsruhe, der auch hier gefolgt wird, gelten dann, wenn besondere Fallgestaltungen vorliegen, die den Rahmen des 88 Abs.3 Satz 3 TKG sprengen, auch die allgemeinen Rechtfertigungsgründe.[47] 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.[48]

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

[44] OLG Karlsruhe 1 Ws 152/04 Rdnr. 23
[45] Fischer, 58. Auflage, § 206 Rdnr. 9
[46] Fischer, 58. Auflage, § 206 Rdnr. 9
[47] Fischer, 58. Auflage, § 206 Rdnr. 9
[48] OLG Karlsruhe 1 Ws 152/04 Rdnr.25

2. Datenveränderung, §303a StGB

Eine Strafbarkeit könnte sich ferner nach § 303a 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.[49]

Eine Rechtfertigung kann aber auch hier durch eine mutmaßliche Einwilligung geschehen[50], 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.

[49] Fischer, 58. Auflage, § 303 a StGB, Rdnr. 10
[50] Fischer, 58. Auflage, § 303 a StGB, Rdnr. 13

C. Gesamtergebnis und Empfehlungen

1. Die Implementierung von DMARC ist vereinbar mit deutschem Recht unter Beachtung von teilweise erheblichen Einschränkungen.

Während die rechtmäßige Umsetzung von Aggregated Reports einfacher zu realisieren ist, begegnet hingegen die zweckmäßige Implementierung von Failure Reports erheblichen datenschutzrechtlichen Bedenken.

Im Einzelnen:

a) Bei Aggregated Reports:

Die Übermittlung von Aggregated Reports ist aus datenschutzrechtlichen Gesichtspunkten bedenklich: Die in den Reports enthaltenen Versand-IPs sind juristisch betrachtet als personenbezogene Daten einzuordnen und unterliegen mithin den Anforderungen des Bundesdatenschutzgesetzes.

Für die Anwendung von Aggregated Reports im Rahmen des DMARC Verfahrens bedeutet dies somit, dass die dort enthaltenen Reportdaten zwar grundsätzlich übermittelt werden dürfen, die Übermittlung darf jedoch lediglich im Rahmen des gesetzlichen Erlaubnistatbestandes, d.h. zur Erkennung und Eingrenzung von Spam und Phishing sowie zum Schutz der Telekommunikationsanlagen und unter Wahrung des Verhältnismäßigkeitsgrundsatzes erfolgen.

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

b) Bei Failure Reports:

Im Vergleich zu Aggregated Reports enthalten Failure Reports eine Vielzahl von personenbezogenen Daten, die für den effektiven Einsatz von DMARC jedoch nicht unbedingt erforderlich sind.

Aufgrund des Datensparsamkeitsgrundatzes wird dringend empfohlen auf Redacting zurückzugreifen, um zu vermeiden, dass personenbezogene Daten des Empfängers einer betrügerischen Mail übermittelt werden. Zu diesen Daten zählen zwingend Subject und Body der betreffenden E-Mail sowie die E-Mail Adresse des Empfängers.

2. Schlussendlich sind noch einige Empfehlungen auszusprechen:

a) Um den Missbrauch im Hinblick auf den Reportempfang auszuschließen, ist gemäß RFC 7489 Kapitel 7.1 ein Authentifizierungs- und Verifizierungssystem umzusetzen[51], sodass gewährleistet wird, dass der konkrete Reportempfänger tatsächlich befugt und gewillt ist die Daten zu erhalten. Bei externen Report-Adressen ist es empfehlenswert, wenn möglich, die Reports an die DMARC-Policy Domain zustellen zu lassen und anschliessend an die externe Report-Adresse weiterzuleiten.

b) Darüber hinaus sollte der Empfänger in Kenntnis über die alternative Verfahrensweise von E-Mails gesetzt und ihm die Entscheidungsbefugnis gewährt werden, insbesondere im Hinblick auf Spam-Mails. Jedenfalls muss ein Verfahren hinsichtlich der Dispositionsbefugnis ausgearbeitet werden. Dies kann in den AGB des ISPs oder DMARC Richtlinien erfolgen.

[51] https://tools.ietf.org/html/rfc7489#section-7.1