Bernd Lorenz

Datensicherheit von E-Mails

Die Nutzung der E-Mail ist aus dem Alltag kaum noch wegzudenken. Sie dient in vielen Bereichen zur Kommunikation untereinander und enthält oftmals nicht nur die personenbezogenen Daten der Nutzer, sondern häufig auch von Dritten. Nicht immer wird aber bei der Kommunikation per E-Mail eine Verschlüsselung genutzt. Der folgende Beitrag befasst sich mit Fragen der Datensicherheit von E-Mails. Er stellt die geltende Rechtslage dar und eröffnet einen Ausblick auf die DS-GVO.

1 Einleitung

Die E-Mail ist aus dem Alltagsleben nicht mehr wegzudenken. Obwohl längst in der Bevölkerung bekannt ist, dass die herkömmliche unverschlüsselte E-Mail kein sicheres Kommunikationsmittel ist, erfreut sich die E-Mail weiterhin großer Beliebtheit. Das dürfte damit zusammenhängen, dass eine herkömmliche E-Mail schnell und einfach versandt ist, der Versand der E-Mail kostenlos ist und E-Mail-Adressen weit verbreitet sind. Dabei wirft die E-Mail-Kommunikation Fragen der Datensicherheit auf, denen im Folgenden nachgegangen wird.

2 Unverschlüsselte E-Mails

Herkömmliche E-Mails werden unverschlüsselt über das Internet versandt. Die Situation wird oft mit einer Postkarte verglichen.[1] Jeder Postbedienstete, der eine Postkarte befördert, hat die Möglichkeit, die Postkarte zu lesen. Einige Autoren[2] weisen auf einen Unterschied hin: Jede E-Mail wird nämlich beim Versand mittels des Transmission Control Protocols (TCP) in kleine Datenpakete aufgeteilt.[3] Ein Datenpaket kann maximal 64 kB Nutzdaten enthalten.[4] Die E-Mail wird in kleinen Datenpaketen über eine Kette von Rechnern übertragen. Beim Empfänger werden die Datenpakete wieder zusammengesetzt. Eine zufällige Kenntnisnahme durch einen Provider ist nicht ohne Weiteres möglich.

Erforderlich ist vielmehr, dass mit spezieller Software (sog. Packet Sniffer) sämtliche Datenpakete abgefangen und wieder zusammengesetzt werden. Unter einem Packet Sniffer wird eine Software verstanden, die es ermöglicht, die an einem Netzwerkinterface eines Rechners auftretenden Pakete mitzulesen, zu analysieren und darzustellen.[5] Bekannte Programme sind tcpdump und Wireshark (früher: Ethereal).

Ob es damit möglich ist, E-Mails mitzulesen oder nicht, hängt vom Einzelfall ab. Wenn die Daten einer WLAN-Verbindung abgegriffen werden, ist es ohne Weiteres möglich sämtliche Datenpakete abzugreifen. Die Verbindung erfolgt dann über einen bestimmten Router. Wenn die E-Mail dagegen weltweit über verschiedene Server im Internet übertragen wird, ist es möglich, dass die einzelnen Datenpakete ihren Weg über eine unterschiedliche Kette von Rechnern nehmen. Das kann insbesondere dann der Fall sein, wenn einzelne Datenpakete verloren gehen und über eine andere Verbindung neu gesendet werden. In einem solchen Fall würde ein Provider nur einen Teil der E-Mail abgreifen können.

Nichtsdestotrotz ist die unverschlüsselte E-Mail ein unsicheres Kommunikationsmittel. Die E-Mail wird unter Umständen über viele Server weltweit weitergeleitet. Dabei passiert sie unter Umständen auch Server in Ländern, die kein vergleichbares Datenschutzniveau wie Deutschland haben. Es gibt durchaus Länder, in denen die Inhalte von E-Mails abgegriffen und analysiert werden.[6] Es kann nicht ausgeschlossen werden, dass ein Provider eine E-Mail mitliest.

Die Erkenntnisse über die Überwachung des Internets durch die Geheimdienste führen zu einer Verschärfung in der Beurteilung der Unsicherheit von unverschlüsselten E-Mails. Der Internetverkehr wird in großem Umfang durch die Geheimdienste

1 Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften vom 8.11.2010, BT-Drs. 17/3630, 1; *Berger,* NJW 2001, 1530, 1535; *Bergt,* CR 2014, 726, 727; *Fuhrberg,* K&R 1999, 20, 23; *Horst,* MDR 2000, 1293, 1299; *Jungk,* AnwBl. 2001, 170, 172; *Kess,* DSB 2014, 218, 218; *Kubach/Gutsche,* K&R 2015, 86, 87; *Lapp,* BRAK-Mitt. 1997, 106, 107; *Pohlmann*, in: Jäger, Handbuch Sicherheitsgefahren, 2015, S. 239, 242; *Roßnagel/Pfitzmann,* NJW 2003, 1209, 1212; *Schrödel*, Ich glaube, es hackt!, 4. Aufl. 2016, S. 233 ff.; *Wagner/Lerch,* NJW-CoR 1996, 380, 384; a. A. *Härting*, MDR 2001, 61, 62; *Härting,* NJW 2005, 1248, 1248; *Koch,* DuD 2014, 691, 691.

2 *Axmann/Degen*, NJW 2006, 1457, 1457 f.; *Degen,* VBlBW 2005, 329, 336; *Härting,* MDR 2001, 61, 61; Hartung/Scharmer/*Hartung*, Berufs- und Fachanwaltsordnung, 6. Aufl. 2016, § 2 BORA Rn. 89; *v. Lewinski,* BRAK-Mitt. 2004, 12, 13; *Schöttle*, Anwaltliche Rechtsberatung via Internet, 2004, S. 43 ff.

RA Dr. Bernd Lorenz

Fachanwalt für IT-Recht, Urheber- und Medienrecht, sowie für gewerblichen Rechtsschutz. Betrieblicher Datenschutzbeauftragter bei Schulz Sozien in Essen

E-Mail: Lorenz@st-sozien.de

3 *Kurose/Ross*, Computernetzwerke, 6. Aufl. 2014, S. 257 f.; *Tanenbaum/Wetherall*, Computernetzwerke, 5. Aufl. 2012, S. 628, 632 f.; *Zisler*, Computer-Netzwerke, 4. Aufl. 2016, S. 197 ff.

4 *Baun*, Computernetzwerke kompakt, 3. Aufl. 2015, S. 152; *Tanenbaum/Wetherall*, s. o. Fn. 3., S. 628.

5 *Kappes*, Netzwerk- und Datensicherheit, 2. Aufl. 2013, S. 137.

6 *Pohlmann*, s. o. Fn. 1, S. 239, 242.

überwacht und aufgezeichnet.[7] Dies geschieht aber auch im Hinblick auf andere Kommunikationsmittel. So werden auch Telefongespräche in großem Umfang von den Geheimdiensten abgehört.[8] Trotz der Überwachung von Telefongesprächen käme aber niemand auf die Idee, das Telefon als nicht datenschutzkonformes Kommunikationsmittel zu bezeichnen. Die Möglichkeit der Überwachung durch die Geheimdienste besteht im Prinzip bei allen Kommunikationsmitteln. Selbst Briefe können durch Geheimdienste geöffnet werden, wenn dies wohl auch nur in geringem Maße geschieht. Selbst verschlüsselte Nachrichten können in bestimmten Fällen von den Geheimdiensten entschlüsselt und mitgelesen werden.[9] Kein Kommunikationsmittel gewährt folglich eine absolute Sicherheit. Wenn aber sowieso bei praktisch jedem Kommunikationsmittel das Risiko besteht, dass es von Geheimdiensten abgehört wird, kann dieses Risiko nicht dazu führen ein Kommunikationsmittel generell als nicht datenschutzkonform einzustufen und diese Kommunikationsform generell zu untersagen.

3 Einwilligung bei unverschlüsselten E-Mails

3.1 Geltende Rechtslage

Die Frage, ob das Versenden unverschlüsselter oder nicht ausreichend verschlüsselter E-Mails zulässig ist, ist umstritten. Während eine Auffassung hierin keine Verletzung des Datenschutzes, der Verschwiegenheitsplicht[10] oder einer vertraglichen Geheimhaltungspflicht sieht, macht die zutreffende Auffassung die Verletzung des Datenschutzes[11], der Verschwiegenheitspflicht[12] oder einer vertraglichen Geheimhaltungspflicht[13] davon abhängig, ob der Betroffene in die Kommunikation per E-Mail eingewilligt hat oder nicht. Eine vermittelnde Ansicht meint, dass eine Einwilligung in die Kommunikation per E-Mail nur bei erhöhtem Vertraulichkeitsrisiko erforderlich ist.[14] Dies soll z. B. bei Vertretung von politisch Verfolgten oder Wirtschaftsspionage der Fall sein.

Da es keine Rechtsvorschrift gibt, die die Offenbarung von personenbezogenen Daten durch das Versenden von unverschlüsselten E-Mails erlaubt, kann nach § 4 Abs. 1 BDSG nur eine Einwilligung zur Zulässigkeit eines solchen Verhaltens führen. Öffentliche und nicht-öffentliche Stellen, die nach § 1 Abs. 2 BDSG in den Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) oder in den Anwendungsbereich der Landesdatenschutzgesetze fallen, können die unverschlüsselte E-Mail nur dann als Kommunikationsmittel verwenden, wenn der Empfänger und andere betroffene Personen eingewilligt haben.

Betroffener ist dabei jeder, dessen personenbezogene Daten in der E-Mail enthalten sind. Betroffener ist nicht nur der Empfänger der E-Mail, sondern unter Umständen auch ein Dritter, über den Absender und Empfänger der E-Mail personenbezogene Daten austauschen. Insofern sind Fallkonstellationen denkbar, in denen die Einwilligung des Absenders und des Empfängers nicht ausreichen, sondern auch eine Einwilligung von Personen erfordern, die am Kommunikationsprozess selbst nicht beteiligt sind.

Die Einwilligung bedarf nach § 4a S. 3 BDSG grundsätzlich der Schriftform i. S. d. §§ 126 f. BGB[15]. Ausnahmsweise kann auch eine andere Form ausreichen, wenn wegen besonderer Umstände eine andere Form angemessen ist. Dies ist in diesem Zusammenhang regelmäßig der Fall. Wollen zwei Personen daher per E-Mail kommunizieren, genügt eine mündliche oder eine per E-Mail abgegebene Einwilligungserklärung.

Die Einwilligung kann grundsätzlich auch konkludent erteilt werden,[16] indem der Empfänger der E-Mail dem Absender seine E-Mail-Adresse mitteilt.[17] So kann z. B. in der Angabe der E-Mail-Adresse auf dem Briefkopf oder in der Übergabe einer Visitenkarte mit der E-Mail-Adresse eine konkludente Einwilligung liegen.[18] Auch die Veröffentlichung einer E-Mail-Adresse auf der eigenen Website[19] oder in sozialen Medien kann eine konkludente Einwilligung darstellen. Durch solche Handlungen bringt der Empfänger der E-Mail zum Ausdruck, dass er damit einverstanden ist, per E-Mail zu kommunizieren. Veröffentlicht jemand die E-Mail-Adresse nur zur ersten Kontaktaufnahme, weil sie eine Pflichtangabe nach § 5 Abs. 1 Nr. 2 TMG darstellt, muss er dies durch einen zusätzlichen Hinweis zum Ausdruck bringen.

3.2 Rechtslage nach DS-GVO

Ab dem 25.5.2018 findet gemäß Art. 99 Abs. 2 DS-GVO die Datenschutz-Grundverordnung (DS-GVO)[20] Anwendung. Sie wird erhebliche Erleichterungen im Hinblick auf die nach Art. 6 Abs. 1 S. 1 lit. a DS-GVO erforderliche Einwilligung bringen. Es gibt nämlich keinen Grundsatz der Schriftform wie in § 4a Abs.

7 *Rosenbach/Stark*, Der NSA Komplex, 2015, S. 120 ff.; *Schaar*, Überwachung total, 2014, S. 7 ff.; *Schneier*, Data und Goliath, 2015, S. 74 ff.

8 *Rosenbach/Stark*, s. o. Fn. 7, S. 186; *Schaar*, s. o. Fn. 7, S. 28 f.

9 *Schneier*, s. o. Fn. 7, S. 164 ff.

10 *Axmann/Degen,* NJW 2006, 1457, 1458; Dombek/Ottersbach/Schulze zur Wiesche/*v. Lewinski*, Die Anwaltssozietät, 2. Aufl. 2015, § 4 Rn. 110; *Härting,* MDR 2001, 61, 62; Hartung/Scharmer/*Hartung*, s. o.s. o. Fn. 2, § 2 BORA Rn. 89; Henssler/Prütting/*Henssler*, Bundesrechtsanwaltsordnung, 4. Aufl. 2014, § 43a Rn. 68; *Kleine-Cosack*, Bundesrechtsanwaltsordnung, 7. Aufl. 2015, § 43a Rn. 80; *Koch,* DuD 2014, 691, 694; *Makoski,* K&R 2007, 246, 248; *Sassenberg,* AnwBl 2006, 196, 196; *Schöttle*, s. o. Fn. 2, S. 68, 72.

11 *Stellpflug/Haase,* MedR 2016, 603, 605.

12 Arndt/Lerch/*Sandkühler*, Bundesnotarordnung, 8. Aufl. 2016, § 18 Rn. 19; *Backu,* ITRB 2003, 251, 252; *Berger*, NJW 2001, 1530, 1535; Feuerich/Weyland/*Träger*, Bundesrechtsanwaltsordnung, 9. Aufl. 2016, § 43a BRAO Rn. 25b; *Koch,* AnwBl. 1997, 421, 428; *Sassenberg/Bamberg,* DStR 2006, 2052, 2053; *Stellpflug/Haase,* MedR 2016, 603, 605; *Wagner-Lerch,* NJW-CoR 1996, 380, 385.

13 *Backu,* ITRB 2003, 251, 252.

14 *Degen,* VBlBW 2005, 329, 337; *Degen,* NJW 2008, 1473, 1479; *Degen/Emmert*, Elektronischer Rechtsverkehr, 2016, § 8 Rn. 446; *v. Lewinski,* BRAK-Mitt. 2004, 12, 16.

15 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 52. Ergl. 3/2017, § 4a BDSG Rn. 84; *Däubler*/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 5. Aufl. 2016, § 4a Rn. 11; *Kühling/Seidel/Sivridis*, Datenschutzrecht, 3. Aufl. 2015, Rn. 325; *Lorenz,* ZD 2012, 367, 370; *Riesenhuber,* RdA 2011, 257, 259; Simitis/*Simitis*, Bundesdatenschutzgesetz, 8. Aufl. 2014, § 4a Rn. 33, 36; Spindler/Schuster/*Spindler/Nink*, Recht der elektronischen Medien, 3. Aufl. 2015, § 4a BDSG Rn. 10.

16 *Bergmann/Möhrle/Herb*, s. o.s. o. Fn. 15, § 4a BDSG Rn. 85; *Däubler*/Klebe/Wedde/Weichert, s. o.s. o. Fn. 15, § 4a Rn. 16; *Kühling/Seidel/Sivridis*, s. o.s. o. Fn. 15, Rn. 326; *Lorenz,* ZD 2012, 367, 368; Taeger/Gabel/*Taeger*, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Aufl. 2013, § 4a Rn. 41; a. A. Simitis/*Simitis*, s. o. Fn. 15, § 4a Rn. 44.

17 Arndt/Lerch/*Sandkühler*, s. o. Fn. 12, § 18 Rn. 19; *Sassenberg/Bamberg,* DStR 2006, 2052, 2053; *Sassenberg,* AnwBl 2006, 196, 196.

18 *Hoffmann/Luch/Schulz/Tallich/Tischer*, Der E-POSTBRIEF in der öffentlichen Verwaltung, Einsatzoptionen im Sozial- und Steuerverfahren sowie für Berufsgeheimnisträger (2. Gutachten), 2011, S. 128 f.

19 *Hoffmann/Luch/Schulz/Tallich/Tischer*, s. o. Fn. 18, S. 128 f.

20 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119, S. 1.

1 S. 3 BDSG mehr für die Einwilligungserklärung.[21] Dies folgt aus Art. 7 DS-GVO, der die Bedingungen für die Einwilligung nennt. Die Schriftform ist danach keine Bedingung. Nach Art. 7 Abs. 1 DS-GVO trifft den Verantwortlichen zwar die Beweislast für die Einwilligung. Dies kann aber nicht mit dem Schriftformerfordernis gleichsetzt werden. Der Beweis der Einwilligung kann z. B. auch durch Zeugenbeweis erbracht werden. Auch spricht Erwägungsgrund 32 S. 1, 2 davon, dass die Einwilligung elektronisch, mündlich oder durch andere Erklärungen oder Verhaltensweisen geschehen kann, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigen Verarbeitung ihrer personenbezogenen Daten signalisiert.

Andere Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO werden für eine unverschlüsselte E-Mail-Kommunikation regelmäßig nicht in Betracht kommen. Insbesondere dient die unverschlüsselte Kommunikation nicht der Wahrung eines berechtigten Interesses des Absenders nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO. Zwar kommt als berechtigtes Interesse grundsätzlich jedes von der Rechtsordnung gebilligte rechtliche, tatsächliche, wirtschaftliche oder ideelle Interesse in Betracht.[22] Insofern könnte auch die Ersparung von Kosten, die eine verschlüsselte Kommunikation verursacht, ein berechtigtes Interesse darstellen. Die unverschlüsselte Kommunikation ist aber nicht zur Wahrung der Kostenersparnis erforderlich, denn die Kosten für eine verschlüsselte Kommunikation sind nicht derart hoch, dass sie den am Kommunikationsprozess beteiligten Personen wirtschaftlich nicht zumutbar wären. So ist z. B. das Programm GnuPG als freie Software kostenlos verfügbar.[23] Die Kosten für eine De-Mail bzw. einen E-Postbrief liegen für Geschäftskunden unter den Portkosten eines herkömmlichen Briefes.[24] Auch der Aufwand für die ggf. selber vorzunehmende Verschlüsselung ist derart gering, dass die Personalkosten vernachlässigt werden können. Außerdem überwiegen die Interessen der betroffenen Person am Datenschutz.

4 Verschlüsselte E-Mails

Verschlüsselte E-Mails dürfen auch ohne Einwilligung des Betroffenen versandt werden.[25] Bei ausreichend verschlüsselten E-Mails werden keine personenbezogenen Daten gegenüber Dritten offenbart. Voraussetzung ist, dass eine ausreichende Verschlüsselung vorgenommen wird. Es gibt verschiedene Verschlüsselungsverfahren, -programme und –initiativen, bei denen grundsätzlich davon ausgegangen werden kann, dass E-Mails ohne Einwilligung des Betroffenen versandt werden können.

Bei der **E-Mail Made in Germany**[26] handelt es sich um einen Zusammenschluss deutscher Provider. E-Mails zwischen diesen Providern werden nur verschlüsselt übertragen. Es erfolgt eine Verschlüsselung zwischen den E-Mail-Servern der Provider. Darüber hinaus erfolgt außerdem eine Verschlüsselung zwischen dem Endgerät und dem E-Mail-Server.

Unter dem Stichwort „**Volksverschlüsselung**“[27] hat die Deutsche Telekom im Jahre 2016 eine Initiative zur Ende-zu-Ende-Verschlüsselung von E-Mails gestartet.

Bei **Pretty Good Privacy (PGP)** handelt es sich um ein Programm, das E-Mails zuverlässig verschlüsselt und signiert.[28] PGP gilt als sicher gegenüber Brute-Force-Attacken.[29] OpenPGP ist ein standardisiertes Datenformat, das auf PGP basiert.[30] Der **GNU Privacy Guard (GnuPG oder GPG)** ist ein freies Kryptographiesystem, das den OpenPGP-Standard implementiert.[31]

Secure / Multipurpose Internet Mail Extensions (S/MIME) ist ein Standard für die Verschlüsselung und das Signieren von MIME-gekapselter E-Mail durch ein hybrides Kryptosystem.[32] Allerdings wird durch *Ziegler* auf gewisse Schwächen von S/MIME hingewiesen.[33] Stellen, die die Zertifikate ausstellen, hätten sich in der Vergangenheit nicht gerade als besonders vertrauenswürdig erwiesen.

Die **De-Mail** bietet gemäß § 4 Abs. 3 DeMailG eine verschlüsselte Kommunikation zwischen dem Nutzer und seinem De-Mail-Konto. Weiterhin erfolgt gemäß § 5 Abs. 3 S. 2 DeMailG eine Transportverschlüsselung. Eine Ende-zu-Ende-Verschlüsselung ist dagegen gemäß § 5 Abs. 3 S. 3 DeMailG nicht zwingend vorgeschrieben.[34] Unter einer Ende-zu-Ende-Verschlüsselung wird eine Verschlüsselung über alle Übertragungsstationen hinweg verstanden,[35] indem die Inhalte der E-Mail beim Absender verschlüsselt und erst beim Empfänger wieder entschlüsselt werden. Kritiker sehen in der kurzfristigen Entschlüsselung der Nachrichten beim Provider ein nicht erforderliches Sicherheitsrisiko der De-Mail.[36] Dieses Sicherheitsrisiko führt jedoch nicht dazu, die De-Mail als nicht datenschutzkonform anzusehen, denn der De-Mail-Diensteanbieter muss im Akkreditierungsverfahren

21 Ehmann/Selmayr/*Heckmann/Paschke*, Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 22; *Gola/Jaspers/Müthlein/Schwartmann*, Datenschutz-Grundverordnung im Überblick, 2. Aufl. 2017, S. 13, 36; *Härting*, Datenschutz-Grundverordnung, 2016, Rn. 357; *Kremer/Garsztecki* AnwZert ITR 18/2016 Anm. 2 B. II. 2.; *Krohm*, ZD 2016, 368, 370; Kühling/Buchner/*Buchner/Kühling*, Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 27; *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016, § 2 Rn. 5; *Lorenz* K&R 2016, 450, 454; Plath/*Plath*, BDSG/DSGVO, 2. Aufl. 2016, Art. 7 DSGVO Rn. 6; *Schantz*, NJW 2016, 1841, 1844; *Schneider*, Datenschutz nach der EU-Datenschutz-Grundverordnung, 2017, S. 156.

22 Vgl. Gola/*Schulz*, Datenschutz-Grundverordnung, 2017, Art. 6 Rn. 51; Kühling/Buchner/*Buchner/Petri*, s. o. Fn. 21, Art. 6 Rn. 146; *Härting*, s. o. Fn. 21, Rn. 429; *Laue/Nink/Kremer*, s. o. Fn. 21, § 2 Rn. 35.

23 URL: https://www.gnupg.org (Abruf 8.10.2017).

24 URLs: https://www.epost.de/geschaeftskunden/preise.html (Abruf 8.10.2017); https://geschaeftskunden.telekom.de/blobCache/umn/uti/328588_1463996896000/blobBinary/tarifdetails-de-mail-web.pdf (Abruf 8.10.2017).

25 *Stellpflug/Haase*, MedR 2016, 603, 604.

26 URL: http://www.e-mail-made-in-germany.de (Abruf 8.10.2017).

27 URL: https://www.volksverschluesselung.de (Abruf 8.10.2017).

28 *Poguntke*, Basiswissen IT-Sicherheit, 3. Aufl. 2013, S. 237.

29 *Eckert*, IT-Sicherheit. 9. Aufl. 2014, S. 845.

30 Wikipedia, Stichwort „OpenPGP“; URL: https://de.wikipedia.org/wiki/OpenPGP (Abruf 22.5.2017).

31 Wikipedia, Stichwort „GNU Privacy Guard“, URL: https://de.wikipedia.org/wiki/GNU_Privacy_Guard (Abruf 22.5.2017).

32 Wikipedia, Stichwort, „S/MIME“, URL: https://de.wikipedia.org/wiki/S/MIME (Abruf 22.5.2017).

33 *Ziegler*, Sicher in sozialen Netzwerken, 2016, S. 303.

34 Unterrichtung durch die Bundesregierung zum Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften vom 8.12.2010, BT-Drs. 17/4145, S. 9; *Spindler*, CR 2011, 309, 314.

35 Wikipedia, Stichwort „Ende-zu-Ende-Verschlüsselung“, URL: https://de.wikipedia.org/wiki/Ende-zu-Ende-Verschl%C3%BCsselung (Abruf 22.5.2017).

36 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16.4.2009, DuD 2009, 424; Arndt/Lerch/*Sandkühler*, s. o. Fn. 12, § 18 Rn. 20; *Lapp*, jurisPR-ITR 25/2010 Anm. 2 G; *Lechtenbörger*, DuD 2011, 268; *Neumann*, Stellungnahme zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften vom 20.3.2013; *Neumann*, Stellungnahme Elektronischer Rechtsverkehr vom 14.4.2013, URL: http://ccc.de/system/uploads/128/original/demail_april2013.pdf; URL: http://ccc.de/system/uploads/126/original/stellungnahme-demail2013.pdf (Abruf 8.10.2017); *Stollhof*, DuD 2003, 691, 694 f.

nachweisen, dass er Sicherheit und Datenschutz gewährleistet.[37] Seit April 2015 bieten die De-Mail-Diensteanbieter sogar zusätzlich die Möglichkeit einer Ende-zu-Ende-Verschlüsselung mittels PGP an.[38] Problem der Ende-zu-Ende-Verschlüsselung ist allerdings, dass die E-Mails von den De-Mail-Diensteanbietern nicht mehr automatisiert auf Schadsoftware geprüft werden können. Der Empfänger der De-Mail muss diese nach der Entschlüsselung selber auf Schadsoftware prüfen.

Der **E-Postbrief** der Deutschen Post (kurz E-Brief) ist ein Hybridpostdienst mit angeschlossener Website für den Austausch elektronischer Nachrichten über das Internet.[39] Bei dem E-Postbrief mit klassischer Zustellung wird die versandte E-Mail durch die Deutsche Post ausgedruckt, kuvertiert, frankiert und dem Empfänger per Briefpost zugestellt.[40] Bei dem E-Postbrief mit elektronischer Zustellung erfolgt eine verschlüsselte Übermittelung der E-Mail über das Internet. Der Absender übermittelt dem Provider die E-Mail über ein vor Zugriffen von außen abgesichertes Gateway oder über eine gesicherte Internet-Verbindung. Der Provider verschlüsselt die E-Mail, die dann über eine gesicherte Tunnelverbindung an den Empfängerprovider übermittelt wird, dort entschlüsselt und wiederum über eine gesicherte Verbindung dem Empfänger übergeben wird.[41] Wie bei der De-Mail kann der E-Postbrief kurzzeitig in unverschlüsselter Form beim Provider vorliegen. Dies ist aus datenschutzrechtlicher Sicht unerheblich, denn auch die Deutsche Post als E-Postbrief-Provider hat die Erfüllung bestimmter Sicherheitsstandards nachgewiesen.[42] Optional wird auch eine Ende-zu-Ende-Verschlüsselung angeboten. Aber auch ohne die Option der Ende-zu-Ende-Verschlüsselung gilt der E-Postbrief als sicher.[43] Entscheidend ist, dass die E-Mail auf dem Transportweg verschlüsselt wird.

Das besondere elektronische Anwaltspostfach (beA), das **Elektronische Gerichts- und Verwaltungspostfach (EGVP)**, das besondere elektronische Behördenpostfach (beBPo) und das besondere elektronische Notarpostfach – Sichere Beteiligtenkommunikation (beN-SBK) bieten durch Verschlüsselung und Signatur eine sichere elektronische Kommunikation zwischen Behörden, Gerichten, Rechtsanwälten und Notaren.[44] Es erfolgt eine Ende-zu-Ende-Verschlüsselung.[45] Verschlüsselt wird die Nachricht nicht nur beim Transport, sondern auch der Inhalt der Nachricht wird verschlüsselt (doppelte Verschlüsselung).[46] Die Verschlüsselung beruht auf dem Protokollstandard OSCI-Transport (Online Services Computer Interface[47]).

ZIP- und PDF-Programme bieten die Möglichkeit an, Dokumente zu verschlüsseln. Dazu sind ein hoher Verschlüsselungsgrad und ein sicheres Passwort[48] auszuwählen. Der Empfänger kann das Dokument nur öffnen, wenn er das individuelle Passwort für das Dokument kennt. Das Passwort muss dem Empfänger auf einem zweiten sicheren Weg, z. B. per Telefon oder Briefpost, übermittelt werden.[49] Das Passwort darf nicht per unverschlüsselter E-Mail übersandt werden.

5 Fazit

Es gibt inzwischen vielfältige Möglichkeiten E-Mails zu verschlüsseln. Diese Möglichkeiten sollten auch genutzt werden, denn das Versenden einer unverschlüsselten E-Mail ist nur zulässig, wenn sämtliche Betroffene in die unverschlüsselte Kommunikation eingewilligt haben. Dies sicherzustellen ist aber nicht immer einfach, insbesondere wenn die personenbezogenen Daten Dritter betroffen sind.

37 Unterrichtung durch die Bundesregierung vom 8.12.2010, BT-Drs. 17/4145, S. 9.

38 heise online vom 22.4.2015, URL: http://www.heise.de/security/meldung/De-Mail-Ende-zu-Ende-Verschluesselung-mit-PGP-gestartet-2616388.html (Abruf 8.10.2017); *Brosch/Lummel/Sandkühler/Freiheit*, Elektronischer Rechtsverkehr mit dem beA, 2017, Rn. 92; *Degen/Emmert*, s. o. Fn. 14, Rn. 233.

39 Wikipedia, Stichwort „E-Postbrief", URL: https://de.wikipedia.org/wiki/E-Postbrief (Abruf 22.5.2017).

40 *Hoffmann/Luch/Schulz/Tallich/Tischer/Warnecke*, Der E-POSTBRIEF in der öffentlichen Verwaltung, Chancen, Einsatzoptionen, rechtliche Handlungsspielräume (1. Gutachten), 2011, S. 8; *Hoffmann/Tallich/Warnecke,* MMR 2011, 775, 775; *Luch/Tischer,* DÖV 2011, 598, 599; *Luch/Schulz,* innovative Verwaltung 4/2011, 32, 32; *Schulz,* DuD 2011, 263, 263.

41 *Hoffmann/Luch/Schulz/Tallich/Tischer*, s. o. Fn. 18, S. 64.

42 *Hoffmann/Luch/Schulz/Tallich/Tischer*, s. o. Fn. 18, S. 64.

43 *Hoffmann/Luch/Schulz/Tallich/Tischer*, s. o. Fn. 18, S. 65 ff.

44 *Kulow,* BRAK Magazin 4/2016, 4.

45 *Brosch/Sandkühler,* NJW 2015, 2760, 2762 f.; *Brosch/Lummel/Sandkühler/Freiheit*, s. o. Fn. 38, Rn. 262, 355, 364; *Jungbauer/Jungbauer*, Das besondere elektronische Anwaltspostfach (beA) und der ERV, 2. Aufl. 2017, § 3 Rn. 30.

46 *Brosch/Lummel/Sandkühler/Freiheit*, s. o. Fn. 38, Rn. 262, 266.

47 Wikipedia, Stichwort „Online Services Computer Interface", URL: https://de.wikipedia.org/wiki/Online_Services_Computer_Interface (Abruf 22.5.2017).

48 Dazu *Lorenz,* DuD 2013, 220, 223.

49 *Fischer/Heyde,* WPK Magazin 2/2014, 42, 44; *Sorge,* NJW-Beil. 2016, 100, 101 f.