Wege zur Herstellung von Vertrauen in digitale Kommunikation

von Henning Lahmann und Till Kreutzer, iRights.Lab

Diskussionspapier im Projekt „Braucht Deutschland einen Digitalen Kodex?“

Juli 2017

Inhaltsverzeichnis

1 Ausgangslage

Das vorliegende zweite Themenpapier im Teilprojekt „Vertrauen in Kommunikation im digitalen Zeitalter“ im Rahmen des Projekts „Braucht Deutschland einen Digitalen Kodex?“ untersucht mögliche Ansätze, die dem Ziel dienen, das Vertrauen der Nutzer in digitale Kommunikationsmittel zu stärken und abzusichern. Wie das vorhergehende Themenpapier geht es dabei von der Grundannahme aus, dass es ein Bedürfnis nach geschützter und insofern vertrauenswürdiger Kommunikation gibt, und zwar insbesondere dann, wenn es um die Übermittlung und den Austausch von bestimmten sensiblen Informationen oder Daten geht. Das erste Themenpapier diente in diesem Rahmen einer Bestandsaufnahme. Es stellte zum einen die Frage, wie es gegenwärtig um das Vertrauen in digitale Kommunikation in Deutschland bestellt ist, und beschrieb zum anderen grundsätzliche Ansatzpunkte aus rechtlicher, technischer und organisatorischer Sicht zum Umgang mit diesem Themenkomplex.[1]

Die Untersuchung, gestützt auf aktuelle empirische Erhebungen in Deutschland, gelangte insbesondere zu dem Befund, dass viele Menschen aus durchaus unterschiedlichen Gründen ungenügendes oder kein Vertrauen in digitale Kommunikation haben und deshalb zurückhaltend bei der Nutzung digitaler Kommunikationsmittel sein könnten, um beispielsweise Behördenangelegenheiten zu erledigen oder Geschäfte zu tätigen, die auf die Übermittlung sensibler Daten wie etwa Kontoinformationen angewiesen sind. Da digitale Kommunikation nicht nur allgemein üblich, sondern auch aus verschiedener Hinsicht generell förderungswürdig erscheint, stellt mangelndes Vertrauen ein Problem dar. Vertrauen in die Privatheit, Integrität, Authentizität, Effektivität und Verlässlichkeit von Kommunikation ist in der digitalen Welt wichtiger denn je.

Auch Befragungen, die in jüngerer Zeit in anderen Ländern durchgeführt wurden, stützen die Schlussfolgerungen des ersten Themenpapiers. So zeigte eine umfangreiche Studie in den Vereinigten Staaten – deren Bürger gemeinhin den Ruf haben, weniger um ihre persönlichen Daten besorgt zu sein als Deutsche –, dass ein Zusammenhang zwischen fehlendem Vertrauen in die Sicherheit und Vertraulichkeit privater Informationen und größerer Zurückhaltung bei verschiedenen Online-Aktivitäten auch auf der anderen Seite des Atlantiks sehr nahe liegt und nicht ein rein deutsches Phänomen ist.[2]

An dieser Ausgangslage ansetzend erörtert dieses zweite Themenpapier Rahmenbedingungen für Lösungsmöglichkeiten. Zu diesem Zweck werden anhand einer Zielvorgabe zur Herstellung und Absicherung von Vertrauen fünf inhaltlich miteinander verknüpfte und aufeinander bezogene Leitsätze formuliert und erläutert. Wie bereits im ersten Papier liegt der Fokus dabei auf der Kommunikation zwischen Unternehmen und ihren Kunden (B2C) sowie zwischen staatlichen Stellen und Bürgern (G2C).

[1] “Vertrauen in digitale Kommunikation: Eine Bestandsaufnahme“, DIVSI, Juni 2017.
[2] Rafi Goldberg u.a., Trust in Internet Privacy and Security and Online Activity, NTIA Working Paper, 2016, https://ssrn.com/abstract=2757369; Rafi Goldberg, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, National Telecommunications & Information Administration, 13. Mai 2016, https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

2 Zielvorgabe: Herstellung von Vertrauen in digitale Kommunikation

Es ist von zentraler Bedeutung, dass die Nutzer digitalen Kommunikationsmitteln vertrauen können, mithilfe derer sie mit Unternehmen oder Behörden in Kontakt treten, um bedeutsame oder sensible Inhalte auszutauschen. Um dieses Ziel zu erreichen, erfordern solche Kommunikationsverhältnisse bestimmte Rahmenbedingungen, die durch die im Folgenden formulierte Zielvorgabe unterstützt werden.

So sollte die digitale Kommunikation in erster Linie sowohl sicher als auch nutzerfreundlich sein. Zugleich sollte sie transparent dahingehend sein, dass die Nutzer stets über die eingesetzten Sicherheitsstandards und darüber, wer auf welche Weise Zugriff auf den Inhalt der Kommunikation bekommt, informiert sind. Sie sollte keine erzwungene, alternativlose Übermittlungsmethode sein, sondern vielmehr nur eine gleichberechtigte Option neben anderen, insbesondere analogen, über deren Auswahl der Nutzer frei entscheiden kann. Dabei sollte sie für den Nutzer nicht mit unmittelbaren Mehrkosten verbunden sein.

3 Leitsätze

Aus der so formulierten Vorgabe werden die folgenden fünf Leitsätze abgeleitet, deren Umsetzung das Erreichen des Ziels fördern würde:

1. Digitale Kommunikation mit sensiblen Inhalten sollte sicher sein.
2. Die eingesetzte Technologie sollte nutzerfreundlich sein.
3. Dem Nutzer gegenüber sollte der gewährleistete Sicherheitsstandard transparent gemacht werden.
4. Dem Nutzer sollten alternative – auch analoge –Kommunikationsmittel angeboten werden.
5. Die Wahl des Kommunikationsmittels sollte keine Diskriminierung hinsichtlich der Kosten zur Folge haben.

Die folgenden Kapitel führen diese Sätze der Reihe nach auf und erläutern und erörtern sie jeweils im Detail. Dabei sind die Leitsätze jedoch nicht isoliert voneinander zu betrachten. Vielmehr verweisen sie aufeinander und begrenzen sich dabei zum Teil gegenseitig. Denn jedes der Ziele ist mit widerstreitenden Aspekten abzuwägen und muss insoweit relativiert werden. Dies gilt insbesondere auch für die beiden ersten Leitsätze, die bereits in einem Spannungsverhältnis stehen. Und so offensichtlich die darin formulierten Forderungen nach Sicherheit und Nutzerfreundlichkeit sind: Schon diese beiden scheinbar einfachen Bedingungen besitzen, wie im Folgenden gezeigt wird, für sich genommen im Detail eine durchaus hohe Komplexität.

3.1 Digitale Kommunikation mit sensiblen Inhalten sollte sicher sein.

Wie bereits im ersten Themenpapier herausgearbeitet, ist die Sicherheit digitaler Kommunikation eines der Kernanliegen, um die Herausbildung von Vertrauen bei den Nutzern zu

erreichen. Nur wenn ein Kommunikationsmittel als sicher angesehen ist, wird es auch dazu genutzt werden, um bedeutsame oder sensible Informationen zu übermitteln.

In diesem Sinne ist das Mittel in erster Linie dann als sicher anzusehen, wenn:

- die Inhalte der Kommunikation nur von denjenigen Personen eingesehen werden können, die dazu berechtigt sind;
- die Inhalte nicht verändert oder kompromittiert werden können;
- und für den Empfänger der übermittelten Information gewährleistet ist, dass sie tatsächlich von der Person stammt, von der sie zu stammen scheint.[3]

Um die so definierte Sicherheit digitaler Kommunikation zu erreichen, sollten Maßnahmen umgesetzt werden, die rechtliche, technische und organisatorische Aspekte miteinander verbinden.

3.1.1 Rechtlicher Rahmen

Das Recht bildet den Rahmen, der die einzusetzende Technologie und die organisatorische Implementierung digitaler Kommunikation zu einem gewissen Grad festlegt. Die rechtlichen Grundlagen für die Herstellung und Absicherung von Vertrauen in das System der Kommunikation wurden bereits im ersten Themenpapier dargestellt. Im Folgenden geht es deshalb insbesondere darum, herauszuarbeiten, was die Normen in diesem Zusammenhang im Einzelnen implizieren. Denn aus den rechtlichen Rahmenbedingungen folgen Vorgaben sowohl für die Ausgestaltung der technischen als auch der organisatorischen Absicherung digitaler Kommunikation.

Der rechtliche Rahmen für die Sicherheit digitaler Kommunikation folgt mangels eines einheitlichen IT-Sicherheitsgesetzes aus einer Reihe einzelner Gesetze und Bestimmungen. Zu nennen ist hier zunächst vor allem das Bundesdatenschutzgesetz (BDSG), das sich mit der inhaltlichen Ebene von Kommunikation befasst und dann anzuwenden ist, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Es richtet sich sowohl an öffentliche Stellen auf Bundesebene als auch an privatwirtschaftliche Unternehmen, die mit solchen Daten befasst sind. Das Gesetz basiert auf dem Grundrecht auf informationelle Selbstbestimmung, das im ersten Themenpapier erörtert wurde, und geht von der grundlegenden Annahme aus, dass stets in das Grundrecht eingegriffen wird, wenn persönliche Daten einer betroffenen Person verwendet werden.[4] Dies ist gegeben, wenn digitale Kommunikationsmittel eingesetzt werden, um Informationen zu übermitteln – denn sie werden ja nicht einfach vom Computer des Senders zum Computer des Empfängers durchgeleitet, sondern auf dem Weg auf Servern der beteiligten Dienstleister zumindest vorübergehend gespeichert.

[3] Vgl. Dirk Heckmann u.a., Adäquates Sicherheitsniveau bei der elektronischen Kommunikation: Der Einsatz des E-Postbriefs bei Berufsgeheimnisträgern, Stuttgart 2012, S. 58 f.
[4] Ebd., S. 41.

Ab dem 25. Mai 2018 ist in Deutschland zudem die Datenschutzgrundverordnung (DSGVO) anzuwenden, die am 24. Mai 2016 in Kraft getreten war und als Verordnung der Europäischen Union unmittelbare Geltung entfaltet. Das Bundesdatenschutzgesetz verliert seine Geltung nicht, muss aber den Vorgaben der DSGVO entsprechend angepasst werden.[5] Auch die Verordnung enthält Bestimmungen, die für den Kontext der Sicherheit digitaler Kommunikation von Bedeutung sind.

Für digitale Kommunikation, die mittels elektronischer Signaturen abgesichert werden soll, um die beteiligten Kommunikationspartner sicher identifizieren zu können, sind Signaturgesetz (SigG) sowie Signaturverordnung (SigO) relevant. Sie regeln im Detail, welche technischen Anforderungen elektronische Signaturen allgemein erfüllen müssen, wenn sie für den elektronischen Rechtsverkehr von einer natürlichen Person, einem Unternehmen oder einer staatlichen Stelle verwendet werden. Darüber hinaus bestimmen sie, welche Qualitäts- und Sicherheitsstandards diejenigen Unternehmen zu erfüllen haben, die solche elektronischen Signaturen ausstellen.[6] In diesem Bereich gilt seit dem 1. Juli 2016 zudem die europäische eIDAS-Verordnung, die unter anderem die Regeln in Bezug auf die elektronische Identifizierung europaweit einheitlich und verbindlich regelt. Signaturgesetz und -verordnung behalten allerdings ihre Gültigkeit, soweit sie der eIDAS-Verordnung nicht widersprechen.[7]

3.1.2 Technische Absicherung

Um digitale Kommunikation mit sensiblen Inhalten sicher und damit vertrauenswürdig zu gestalten, spielt die eingesetzte Technik eine zentrale Rolle. Nur wenn die technischen Maßnahmen verhindern können, dass Unbefugte Zugriff auf die Informationen bekommen, die elektronisch übermittelt werden, kann Vertrauen in das System der digitalen Kommunikation überhaupt hergestellt werden. Für diese technische Absicherung sollte auf das Zusammenspiel verschiedener Einzelmaßnahmen zurückgegriffen werden. Zu nennen sind insbesondere Verschlüsselungstechnologien, elektronische Signaturen und elektronische Identifizierungstechnologien, Passwortschutz, Zwei-Faktor-Authentifizierung sowie die Sicherung der Server, Netze und anderer IT-Infrastrukturen. Diese Maßnahmen sind teilweise durch den beschriebenen Rechtsrahmen vorgegeben und werden in den folgenden Abschnitten im Überblick erörtert. Eine Detaillierung zu diesen technischen Maßnahmen findet der interessierte Leser im Anhang.

Verschlüsselung. Wichtigster Faktor für die Absicherung sensibler Inhalte, die via digitale Kommunikation übermittelt werden, ist ihre Verschlüsselung. Darunter wird die Kodierung des Inhaltes einer Nachricht in eine nicht interpretierbare Zeichenfolge mittels eines Algorithmus verstanden, so dass nur Personen, die im Besitz des digitalen Schlüssels sind,

[5] Winfried Veil, Datenschutz in der Mehrebenenfalle, CR-Online, 18. Mai 2017, http://www.cr-online.de/blog/2017/05/18/datenschutz-in-der-mehrebenenfalle/.
[6] Heckmann, S. 42.
[7] Bundesamt für Sicherheit in der Informationstechnik, Elektronische Signaturen, Siegel und Zeitstempel, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/Elektronische_Signaturen_Siegel_und_Zeitstempel/Elektronische_Signaturen_Siegel_und_Zeitstempel_node.html.

den so chiffrierten Inhalt nach Empfang der Nachricht zurück in Klartext umwandeln können.[8] Öffentliche Stellen und privatwirtschaftliche Unternehmen sind aufgrund des geltenden Rechtsrahmens in gewissem Maß verpflichtet, Verschlüsselungstechnologien einzusetzen, wenn sie mit sensiblen Informationen von Bürgern bzw. Kunden umgehen und diese über digitale Kanäle übermitteln.

Digitale Verschlüsselungstechnologien unterscheiden sich dahingehend, an welchem Punkt der Übermittlung die Verschlüsselung ansetzt. Hier kann entweder Ende-zu-Ende-Verschlüsselung oder Punkt-zu-Punkt-Verschlüsselung (letztere wird auch Transport- oder Leitungsverschlüsselung genannt) eingesetzt werden. Bei letzterer werden lediglich die Netzverbindungen zwischen an das Netz angeschlossenen Geräten wie beispielsweise Servern oder den Computern der kommunizierenden Parteien verschlüsselt,[9] was bedeutet, dass der Inhalt der Nachricht per Verschlüsselung zwar vor dem Zugriff unbefugter Dritter geschützt ist, wenn diese von einem Gerät zum anderen übermittelt wird, auf einer Zwischenstation (beispielsweise dem Server des E-Mail-Dienstes des Versenders oder des Empfängers) allerdings unverschlüsselt vorliegt. Im Gegensatz dazu besitzen bei der Ende-zu-Ende-Verschlüsselung lediglich die miteinander kommunizierenden Nutzer die Schlüssel, die notwendig sind, um den Inhalt der Nachricht lesbar zu machen. Die Verschlüsselung erfolgt also durch den Versender auf dessen Endgerät, und die Entschlüsselung kommt erst beim Empfänger zustande. Bei keiner der Zwischenstationen während des Versands liegt die Nachricht also unverschlüsselt vor.[10] Daher gilt die Ende-zu-Ende-Verschlüsselung als wesentlich sicherer als die bloße Punkt-zu-Punkt-Verschlüsselung.

Im Folgenden wird illustriert, in welcher Form sich digitale Kommunikationsmittel durch den Einsatz von Verschlüsselungsmethoden unterscheiden können.

(a) Messenger-Dienste. Wie bereits im ersten Themenpapier angemerkt, sind in den vergangenen Jahren viele Messenger-Dienste dazu übergegangen, die versendeten Nachrichten mittels Ende-zu-Ende-Verschlüsselung zu sichern. Das trifft unter anderem auf die Anwendungen Threema, Signal, SIMSme, iMessage oder WhatsApp zu. Bei der E-Mail ist sie bislang jedoch nicht Standard.[11] Das liegt daran, dass diese Art der Verschlüsselung bei geschlossenen Kommunikationsplattformen wesentlich einfacher zu realisieren ist als bei einer offenen wie der herkömmlichen E-Mail. So kann WhatsApp beispielsweise nur zur Kommunikation mit anderen WhatsApp-Nutzern verwendet werden. Deshalb kann der Anbieter der Plattform in den vollständig von ihm kontrollierten Applikationen eine Ende-zu-Ende-Verschlüsselung implementieren, ohne dass die Nutzer selbst tätig werden müssten. Daher bekommen sie von dem Einsatz der Technik im Normalfall überhaupt nichts mit

[8] Vgl. Wikipedia, Verschlüsselung, https://de.wikipedia.org/wiki/Verschl%C3%BCsselung.
[9] Vgl. Wikipedia, Leitungsverschlüsselung, https://de.wikipedia.org/wiki/Leitungsverschl%C3%BCsselung.
[10] Andy Greenberg, Hacker Lexicon: What Is End-to-End Encryption?, Wired.com, 25. November 2014, https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.
[11] Wikipedia, End-to-end encryption, https://en.wikipedia.org/wiki/End-to-end_encryption.

und nutzen den Dienst weiter wie zuvor, als die Verschlüsselungsmethode noch nicht zum Einsatz kam.[12]

(b) E-Mail. Das eben genannte Vorgehen bei Messenger-Diensten ist bei der „offenen" E-Mail, mit der man Nachrichten an Nutzer senden kann, die einen anderen Dienstleister nutzen als der Versender selbst (beispielsweise kann eine E-Mail unproblematisch von einem Nutzer mit einem Gmail-Account an einen Nutzer mit einem Account bei GMX geschickt werden), nicht möglich – jedenfalls so lange, wie sich die verschiedenen Anbieter nicht auf einen gemeinsamen Standard einigen, was allerdings schon aufgrund ihrer großen Anzahl sowie der unterschiedlichen geschäftlichen Interessen unwahrscheinlich erscheint.[13] Zwei Standards, die genutzt werden können, um Ende-zu-Ende-Verschlüsselung auch bei E-Mails zu erreichen, sind OpenPGP und S/MIME. Beide Methoden können aber nur eingesetzt werden, wenn ein Nutzer sich seinen öffentlichen Schlüssel vor dem ersten Einsatz beglaubigen lässt. Daraus wird andererseits zugleich deutlich, dass das System der Ende-zu-Ende-Verschlüsselung mittels OpenPGP und S/MIME davon abhängig ist, dass diese Beglaubigung organisatorisch sichergestellt ist. Zudem müssen beide Kommunikationspartner denselben Standard einsetzen.

(c) Geschlossene Mail-Systeme: De-Mail und E-Postbrief. Geschlossene Systeme zur Erhöhung der Sicherheit sind auch der von der Deutschen Post 2010 eingeführte E-Postbrief[14] sowie die sogenannten De-Mail-Dienste. Letztere sind Anbieter von E-Mail-Diensten, die besonderen Anforderungen an die Sicherheit, Vertraulichkeit und Integrität genügen, wie sie das im Mai 2011 in Kraft getretene De-Mail-Gesetz vorgibt. Erfüllt ein Diensteanbieter die angeführten Kriterien, kann er sich beim Bundesamt für Sicherheit in der Informationstechnik, das für die Aufsicht zuständig ist, als De-Mail-Anbieter akkreditieren lassen.[15] In § 5 Absatz 3 bestimmt das Gesetz, dass der Anbieter Vertraulichkeit, Integrität und Authentizität der mit dem Dienst an einen anderen akkreditierten Diensteanbieter versendeten Nachrichten dadurch zu gewährleisten hat, dass eine Transportverschlüsselung eingesetzt wird und dass der Inhalt der Nachricht während der Übermittlung verschlüsselt sein muss. Eine Ende-zu-Ende-Verschlüsselung ist hingegen nicht vorgeschrieben. Nach entsprechender Kritik kündigten die akkreditierten De-Mail-Anbieter im

[12] WhatsApp hat die Ende-zu-Ende-Verschlüsselung für alle Nutzer im April 2016 eingeführt, vgl. Spiegel Online, WhatsApp verschlüsselt Kommunikation vollständig, 6. April 2016, http://www.spiegel.de/netzwelt/apps/whatsapp-messenger-fuehrt-ende-zu-ende-verschluesselung-ein-a-1085636.html.

[13] So beruhte z.B. das Geschäftsmodell von Gmail bis vor Kurzem darauf, dass der Inhalt von E-Mails gescannt wird, damit dem Nutzer passende Werbung angezeigt werden kann. Ende-zu-Ende-Verschlüsselung würde dies vereiteln; vgl. Florian Rötzer, Bei jeder Mail wird mitgelesen, Telepolis, 2. April 2004, https://www.heise.de/tp/features/Bei-jeder-Mail-wird-mitgelesen-3434025.html.

[14] E-Post, Ist ein E-Postbrief auch ohne Ende-zu-Ende-Verschlüsselung sicher?, https://www.epost.de/privatkunden/hilfe/brief-fax/sicher-digital-kommunizieren/ist-ein-epostbrief-auch-ohne-ende-zu-ende-verschluesselung-sicher.html.

[15] Siehe die Liste akkreditierter Anbieter unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/Akkreditierte_DMDA/Akkreditierte_DMDA.html.

März 2015 jedoch an, künftig eine auf PGP basierende Ende-zu-Ende-Verschlüsselung als Option für alle Nutzer anzubieten.[16]

Auch der E-Postbrief-Dienst der Deutschen Post setzt grundsätzlich nicht auf eine Ende-zu-Ende-Verschlüsselung beim Versand der Nachrichten. Im Normalfall werden sie allerdings während des Transports verschlüsselt. Darüber hinaus wird zugesichert, dass die E-Postbriefe auch verschlüsselt im Posteingang des Nutzers, also auf dem entsprechenden Server, abgelegt werden.[17] Überdies wurde 2013 auch beim E-Postbrief die Möglichkeit der Ende-zu-Ende-Verschlüsselung mit dem ausdrücklichen Ziel eingeführt, damit den gesetzlichen Anforderungen an vertrauliche Kommunikation mit Berufsgeheimnisträgern wie beispielsweise Ärzten oder Anwälten genüge zu tragen. Diese sollten mit dieser Option in die Lage versetzt werden, elektronische Kommunikationsmittel in der geschäftlichen Korrespondenz zu nutzen, ohne gegen ihre Verschwiegenheitspflicht nach § 203 des Strafgesetzbuches zu verstoßen.[18]

(d) Portallösungen. Immer mehr Unternehmen wie beispielsweise Banken, Versicherungen oder auch Stromanbieter verzichten hingegen darauf, vertrauliche Dokumente mittels E-Mail oder verwandter Kommunikationsmittel an ihre Kunden zu verschicken, sondern setzen stattdessen auf sogenannte Portallösungen. Diese kommen auch in der öffentlichen Verwaltung im Kontakt zu den Bürgern immer häufiger zur Anwendung.[19] Dokumente wie Rechnungen, Kontoauszüge oder Baugenehmigungen werden auf den Servern des Unternehmens bzw. der Behörde gespeichert. Der Nutzer bekommt im Normalfall eine E-Mail zugesandt, mittels der er darüber informiert wird, dass ein neues wichtiges Dokument zur Einsicht oder zum Abruf über das Webportal des Anbieters vorliegt. Zumeist enthält die Nachricht selbst auch den entsprechenden Link zum Portal, auf der sich der Nutzer anmelden kann, um gesicherten Zugriff zum Dokument zu erhalten. Ob die Dokumente auf dem Server des Anbieters selbst ebenfalls verschlüsselt gespeichert sind, hängt vom Unternehmen bzw. der Behörde und im Zweifel auch von der Sensibilität der in dem Dokument enthaltenen Informationen ab.

Elektronische Signatur und elektronischer Identitätsnachweis. Nicht um den Inhalt digitaler Kommunikation selbst vor dem Zugriff unbefugter Dritter zu schützen, sondern um die Identität des Urhebers einer Nachricht nachvollziehen zu können und um ihre Integrität zu verifizieren, wird auf elektronische Signaturen und damit zusammenhängend auf einen elektronischen Identitätsnachweis zurückgegriffen. Unter elektronischen Signaturen versteht man solche Daten, die anderen elektronischen Daten beigefügt oder mit ihnen verknüpft sind (§ 2 Nr. 1 SigG). Sie dienen der Authentifizierung des Urhebers der Nachricht

[16] Spiegel Online, De-Mail bekommt durchgehende Verschlüsselung, 9. März 2015, http://www.spiegel.de/netzwelt/netzpolitik/de-mail-bekommt-ende-zu-ende-verschluesselung-a-1022472.html.
[17] Siehe E-Post, Ist ein E-Postbrief auch ohne Ende-zu-Ende-Verschlüsselung sicher?, https://www.epost.de/privatkunden/hilfe/brief-fax/sicher-digital-kommunizieren/ist-ein-epostbrief-auch-ohne-ende-zu-ende-verschluesselung-sicher.html.
[18] Jürgen Seeger, Ende-zu-Ende-Verschlüsselung für E-Postbrief, Heise Online, 2. März 2013, https://www.heise.de/newsticker/meldung/Ende-zu-Ende-Verschluesselung-fuer-E-Postbrief-1815160.html.
[19] Vgl. z.B. den am 1. Januar 2017 in Kraft getretenen § 41 Absatz 2a des Verwaltungsverfahrensgesetzes, der die Bekanntgabe von Verwaltungsakten über öffentlich zugängliche Netze regelt.

bzw. des übermittelten Dokuments und garantieren dessen Unverfälschtheit, indem sie nachträgliche Veränderungen erkennbar machen.[20] Damit verfolgen sie den Zweck, die Rechtssicherheit sowohl bei der digitalen Kommunikation mit Unternehmen im Bereich des E-Commerce als auch mit öffentlichen Stellen im E-Government zu erhöhen.

Passwortschutz und Zwei-Faktor-Anmeldung. Für die Absicherung digitaler Kommunikation darf die Bedeutung des Passwortschutzes nicht unterschätzt werden. Denn Passwörter schützen unmittelbar vor dem Zugriff unbefugter Dritter auf die Inhalte von Kommunikation, sei es, weil diese auf den Servern von E-Mail-Diensten oder sonstigen Dienstleistern gespeichert sind, oder auf der Festplatte des Nutzers. Zusätzlich zum reinen Passwortschutz setzen immer mehr Online-Dienste auf die sogenannte Zwei-Faktor-Anmeldung, um E-Mail-Postfächer oder andere Webportale, auf denen sensible Informationen der Nutzer gespeichert sind, vor Fremdzugriffen zu schützen. Bei diesen Verfahren wird zusätzlich zum Passwort eine weitere Abfrage, z.B. nach einer TAN[21] durchgeführt.

Sicherung der informationstechnischen Systeme. Um sichere digitale Kommunikation zu ermöglichen, müssen insbesondere die Anbieter der Kommunikationsmittel – seien es private Unternehmen wie E-Mail-Dienste oder aber öffentliche Stellen, die mit Bürgern auf elektronischem Wege kommunizieren – dafür Sorge tragen, dass die eingesetzte IT-Infrastruktur vor Angriffen durch Hacker geschützt ist. Das gilt insbesondere für die Server, auf denen die sensiblen Informationen entweder kurzzeitig oder über einen längeren Zeitraum gespeichert sind, und ist dann umso entscheidender, wenn die Kommunikationsinhalte dort unverschlüsselt abgelegt werden. Zu den technischen Sicherheitsmaßnahmen gehören zum Beispiel die Verwendung von Antiviren-Software, Firewalls und sogenannten Intrusion Detection Systems. Zudem sollten die installierten Software- und Hardwarekomponenten stets auf dem aktuellen Stand gehalten werden.[22]

3.1.3 Organisatorische Absicherung

Neben die erörterten technischen Lösungen zur Absicherung digitaler Kommunikation treten organisatorische Maßnahmen, die die Umsetzung der technischen Sicherheitsvorkehrungen unterstützen. Es handelt sich um solche Schutzinstrumente, die durch Handlungsanweisung oder durch Verfahrens- und Vorgehensweisen umgesetzt werden.[23] Sie können dabei entweder darauf abzielen, bereits implementierte Maßnahmen zu überprüfen und zu verifizieren, oder die Vorgehensweise der Akteure auf dem Gebiet digitaler Kommunikation im Hinblick auf die Einhaltung von Vorgaben zur technischen Absicherung auf fortlaufender Basis zu überwachen. Solche Maßnahmen der Überwachung und Überprüfung können von hoheitlicher Seite vorgenommen werden, oder auch der Selbstkontrolle obliegen.

---

[20] Heckmann, S. 42.
[21] TAN: transaction authentification number, Transaktionsnummer.
[22] Für einen Überblick über zu treffende Maßnahmen siehe Wikipedia, Informationssicherheit, https://de.wikipedia.org/wiki/Informationssicherheit.
[23] Datenschutz-Wiki, Technische und organisatorische Maßnahmen, https://www.datenschutz-wiki.de/Technische_und_organisatorische_Ma%C3%9Fnahmen.

Zuständig für die organisatorische Stützung der technischen Sicherungsmaßnahmen sind zunächst einmal die Akteure selbst, also einerseits diejenigen öffentlichen Stellen und Unternehmen, die auf digitalem Wege mit Bürgern und Kunden kommunizieren, und andererseits diejenigen Instanzen, die wie beispielsweise Zertifizierungsdienste an der Absicherung vertraulicher Kommunikation beteiligt sind. Zum Teil folgt die organisatorische Ausgestaltung dabei wiederum aus den Vorgaben der rechtlichen Rahmenbedingungen. So enthalten die oben aufgeführten Gesetze und Verordnungen – insbesondere das Bundesdatenschutzgesetz, die Datenschutzgrundverordnung, die Signaturverordnung und das De-Mail-Gesetz – für ihren jeweiligen Anwendungsbereich Maßnahmenkataloge, die die innere Organisation der Akteure betreffen.

Die Anlage zum bereits erwähnten § 9 des Bundesdatenschutzgesetzes führt zum Beispiel in abstrakten Begriffen einige Maßnahmen auf, die öffentliche Stellen und private Unternehmen, die mit der Verarbeitung personenbezogener Daten befasst sind, vorbehaltlich ihrer Verhältnismäßigkeit umsetzen sollen, um das von § 9 Satz 1 geforderte Niveau des Schutzes der personenbezogenen Daten der Bürger bzw. Kunden zu gewährleisten. Die Vorgaben gehen von dem Leitsatz aus, dass „die innerbehördliche oder innerbetriebliche Organisation so zu gestalten [ist], dass sie den besonderen Anforderungen des Datenschutzes entspricht“ (Satz 1 der Anlage). Das bedeutet, dass die Behörde bzw. das Unternehmen selbst dafür Sorge zu tragen hat, die Abläufe so zu gestalten, dass diejenigen im letzten Abschnitt genannten technischen Maßnahmen zur Kommunikationssicherheit auch umgesetzt werden. Dabei muss im Auge behalten werden, dass es stets auf den Einzelfall ankommt und nicht jeder Anbieter alle Maßnahmen im gleichen Maße durchzuführen hat. Entscheidend ist unter anderem stets, wie sensibel die Informationen sind, die erhoben und verarbeitet werden.[24]

Eine zentrale Verpflichtung für öffentliche Stellen und Unternehmen, die mit personenbezogenen Daten umgehen, ist es insoweit, einen Beauftragten für den Datenschutz zu benennen. Dieser ist in erster Linie dafür zuständig, dafür zu sorgen, dass die von § 9 BDSG geforderten Maßnahmen auch umgesetzt und eingehalten werden.[25] Darüber hinaus zu treffende Maßnahmen sind beispielsweise das Vier-Augen-Prinzip,[26] Überwachung und Kontrolle der Datenverarbeitungsvorgänge durch entsprechend geschultes und eingeteiltes Personal,[27] Identitätskontrollen wie z.B. durch Chipkarten in sensiblen Bereichen des Betriebs,[28] der Erlass von Arbeitsrichtlinien etwa über den sicheren Umgang mit Datenträgern[29] oder die regelmäßige Erstellung von Backups und Sicherungskopien.[30] Auch gele-

[24] Plath, S. 358.
[25] Ebd., S. 351.
[26] Siehe Wikipedia, Vier-Augen-Prinzip, https://de.wikipedia.org/wiki/Vier-Augen-Prinzip: Es „besagt, dass wichtige Entscheidungen nicht von einer einzelnen Person getroffen werden oder kritische Tätigkeiten nicht von einer einzelnen Person durchgeführt werden sollen oder dürfen. Ziel ist es, das Risiko von Fehlern und Missbrauch zu reduzieren“.
[27] Plath, S. 353.
[28] Ebd., S. 359.
[29] Ebd., S. 361.
[30] Ebd., S. 364.

gentliche, unangekündigte Überprüfungen der Maßnahmen zum Schutz der gespeicherten und verarbeiteten Inhalte dienen der Erhöhung des Schutzniveaus.[31]

Ähnliche Vorgaben existieren für Zertifizierungsdiensteanbieter nach der Signaturverordnung (§ 2) und für Vertrauensdiensteanbieter gemäß der eIDAS-Verordnung (Artikel 19 Absatz 1). Auch für Anbieter des De-Mail-Dienstes ist gesetzlich vorgeschrieben, dass sie nur dann akkreditiert werden können, wenn sie technisch und organisatorisch nach dem jeweils aktuellen Stand der Technik so aufgestellt sind, dass sie die Vorgaben des De-Mail-Gesetzes zur sicheren und zuverlässigen Erbringung der Dienste einzuhalten in der Lage sind (§ 18 Absatz 1 Nr. 3 und Absatz 2 Satz 1 De-Mail-Gesetz). Die Einhaltung der gesetzlichen Bestimmungen wird durch die jeweils zuständige Aufsichtsbehörde überprüft und laufend überwacht. Für Zertifizierungsdiensteanbieter ist das die Bundesnetzagentur, bei Vertrauensdiensteanbietern und De-Mail-Anbietern das Bundesamt für Sicherheit in der Informationstechnik.

In Bezug auf De-Mail-Dienste hat das BSI darüber hinaus technische Richtlinien zu formulieren und zu veröffentlichen, die die technischen und organisatorischen Anforderungen an die Anbieter genau spezifizieren.[32] Führt eine Überprüfungsmaßnahme des BSI zu dem Ergebnis, dass der Anbieter gegen die gesetzlichen Vorgaben verstößt, so kann es Bußgelder erheben, den Betrieb vorläufig untersagen und in letzter Konsequenz sogar die Akkreditierung entziehen.

Im Gegensatz zu diesem strikten Modell der Überprüfung und Überwachung durch staatliche Stellen ist der Gesetzgeber beim Bundesdatenschutzgesetz den Weg der regulierten Selbstregulierung gegangen. So sieht der § 9a BDSG die nicht verpflichtende Möglichkeit eines Datenschutzaudits vor. Unternehmen und öffentliche Stellen können ihr Datenschutzkonzept und ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen. Der Anreiz, von dieser Möglichkeit auch tatsächlich Gebrauch zu machen, soll dadurch geschaffen werden, dass das Ergebnis im Anschluss veröffentlicht werden kann. Gerade weil es in den vergangenen Jahren wiederholt zu Datenschutzskandalen gekommen ist, was zu einer erhöhten Skepsis seitens der Nutzer im Hinblick auf die Sicherheit und Vertraulichkeit ihrer Daten geführt hat, geht das Gesetz bestimmt nicht völlig zu Unrecht von der Annahme aus, dass ein als tauglich und vertrauenswürdig bestätigtes Datenschutzkonzept für die geprüfte Stelle ein Asset darstellen kann, das positive Auswirkungen auf die Wettbewerbsfähigkeit zur Folge hat.[33] Allerdings sieht § 9a Satz 2 BDSG ausdrücklich vor, dass die näheren Anforderungen an den Pro-

[31] Vgl. Datenschutz-Wiki, Checkliste Technische und organisatorische Maßnahmen, https://www.datenschutz-wiki.de/Checkliste_Technische_und_organisatorische_Ma%C3%9Fnahmen.
[32] Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/TechnischeRichtlinien/TechnRichtlinien_node.html.
[33] Vgl. Plath. S. 366 f.

zess des Audits in einem Spezialgesetz näher ausformuliert werden sollen. Dies ist jedoch bis heute nicht geschehen.[34]

Auch die Datenschutzgrundverordnung setzt eher auf Selbstregulierung bzw. die sogenannte Ko-Regulierung als auf strikte staatliche Aufsicht, um die Einhaltung datenschutzrechtlicher Bestimmungen zu erreichen. So bestimmt Artikel 40 Absatz 2 lit. h), dass Branchen- und Berufsverbände, die Unternehmen und anderen Stellen vertreten, die mit der Verarbeitung personenbezogener Daten befasst sind, Verhaltensregeln über Maßnahmen und Verfahren ausarbeiten können, die die Sicherheit der Datenverarbeitung betreffen. Nach Artikel 40 Absatz 4 und Artikel 41 soll zudem eine private Stelle eingerichtet werden, die die Einhaltung der so formulierten Verhaltensregeln überwacht. Diese Stelle ist durch die jeweils zuständige staatliche Aufsichtsstelle zu akkreditieren, wenn sie ausreichende Expertise aufweisen kann, unabhängig ist, keinen Interessenkonflikten unterliegt, einem angemessenen Beschwerdeverfahren folgt und bei Verstößen Sanktionen verhängen kann.[35]

Ein Beispiel für eine solche Vereinigung in Deutschland, die zum Zweck der Selbstregulierung im Bereich des Datenschutzes geschaffen worden ist, ist die Selbstregulierung Datenschutz e.V. (SRIW), die vom Bitkom und Unternehmen der digitalen Wirtschaft gegründet wurde.[36] Gemäß seiner Selbstbeschreibung setzt er es sich zum Ziel, „das Vertrauen der Nutzer in digitale Produkte und Dienste zu verbessern und zu erhalten“, und verpflichtet seine Mitglieder deshalb, Selbstverpflichtungen wie Kodizes oder vergleichbare Selbstregulierungsmaßnahmen einzuhalten.[37]

Schließlich können sich Unternehmen und Behörden, die mit dem Umgang mit sensiblen Informationen ihrer Kunden und Bürger befasst sind, auch ihr Konzept im Hinblick auf die Sicherung der eingesetzten informationstechnischen Systeme von einer öffentlichen Stelle überprüfen und anschließend zertifizieren lassen. Hierfür hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den „IT-Grundschutz“ formuliert, dessen Einhaltung nach einem Audit anhand einer Zertifizierung bestätigt wird, die die geprüfte Stelle veröffentlichen kann.[38] Ziel dieses Grundschutzes ist es, ein angemessenes und ausreichendes Schutzniveau für die Systeme zu erreichen. Dazu empfehlen die vom BSI herausgegebenen IT-Grundschutz-Kataloge technische Sicherheitsmaßnahmen sowie infrastrukturelle, organisatorische und personelle Schutzmaßnahmen.[39]

---

[34] Ebd., S. 367.
[35] Ebd., S. 1196.
[36] https://sriw.de/.
[37] https://sriw.de/index.php/der-sriw.
[38] Es handelt sich um die sogenannte ISO 27001 Zertifizierung, vgl. https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html.
[39] Vgl. Wikipedia, IT-Grundschutz, https://de.wikipedia.org/wiki/IT-Grundschutz.

3.1.4 Bewertung

Im Hinblick auf den formulierten Leitsatz, dass Vertrauen der Nutzer in digitale Kommunikation in erster Linie dadurch hergestellt werden sollte, dass übermittelte sensible Daten geschützt werden, lassen sich aus den vorangegangenen Ausführungen die folgenden Schlüsse ziehen: Zunächst einmal zeigen die umfangreichen rechtlichen Rahmenbedingungen, dass die Sicherheit von und das Vertrauen in Kommunikationsmittel, die für (u. a.) sensible Kommunikationsvorgänge genutzt werden, bedeutend sind. Dies ist vom Gesetzgeber entsprechend auch so erkannt worden. Die von ihm geschaffenen gesetzlichen Grundlagen sind heterogen und über eine Vielzahl an Einzelgesetzen verstreut, davon abgesehen aber grundsätzlich als geeignet anzusehen, Sicherheit zu schaffen und damit Vertrauen zu stärken. Die genannten Gesetze, die verschiedene Aspekte der Sicherheit adressieren, machen eine Reihe von Vorgaben, die öffentliche Stellen und Unternehmen immer dann umzusetzen haben, wenn sie mit persönlichen Informationen von Nutzern umgehen. Zentral ist dabei das Gebot, Verschlüsselungsverfahren zur Sicherung der Inhalte selbst einzusetzen. Allerdings geht diese Pflicht ausdrücklich nur so weit, wie sie auch als verhältnismäßig zu bewerten ist. Sobald die Implementierung einer bestimmten Verschlüsselungstechnologie mit einem unangemessenen Kostenaufwand verbunden ist, ist die datenverarbeitende Stelle dem Gesetz nach nicht gezwungen, diese auch einzusetzen. Darüber hinaus macht der rechtliche Rahmen bewusst keine Vorgaben dahingehend, welche Art von Verschlüsselung zum Einsatz kommen soll. Den Behörden und Unternehmen verbleibt also stets ein erheblicher Spielraum, um die Sicherungsmaßnahmen den individuellen betrieblichen Umständen bzw. der jeweiligen Kommunikationssituation anzupassen. Vorgeschrieben ist damit lediglich, dass Kommunikation mit sensiblen Inhalten generell zu sichern ist. Dieser Vorgabe genügen im Grundsatz Sicherungsmaßnahmen jeder Art, also nicht nur Verschlüsselung, sondern auch beispielsweise Passwortschutz, Zwei-Faktor-Anmeldung sowie, im Bedarfsfall, das Vorsehen digitaler Signaturen. Daneben sind organisatorische Vorkehrungen zu treffen, anhand derer die technischen umgesetzt und überprüft werden.

Die angeführten Beispiele haben gezeigt, dass die meisten Anbieter sich innerhalb dieses Spielraums nicht dafür entscheiden, die Maßnahmen mit dem höchsten Sicherheitsniveau einzusetzen. Die Gründe hierfür werden unterschiedlich sein. Bei manchen Dienstleistern ist der Grund vermutlich darin zu suchen, dass eine vollständige Ende-zu-Ende-Verschlüsselung mit den Geschäftsinteressen des Unternehmens in Konflikt stehen würde, die darin bestehen, E-Mails zum Zwecke der zielgerichteten Werbung zu scannen.[40] Doch selbst De-Mail-Dienste sowie der E-Postbrief der Deutschen Post, deren zentrales Geschäftsmodell gerade das hohe Datensicherheitsniveau darstellt, setzen nicht oder je-

[40] Dies war bislang Teil des Geschäftsmodells von Googles E-Mail-Dienst Gmail. Allerdings kündigte das Unternehmen im Juni 2017 an, von dieser Praxis künftig Abstand zu nehmen, vgl. Mark Bergen, Google Will Stop Reading Your Emails for Gmail Ads, Bloomberg, 23. Juni 2017, https://www.bloomberg.com/news/articles/2017-06-23/google-will-stop-reading-your-emails-for-gmail-ads; Anfang 2017 war zudem die Möglichkeit veröffentlicht worden, PGP bei Gmail einzusetzen, vgl. Fabian A. Scherschel, E2EMail: Google veröffentlicht PGP für GMail als Open-Source-Projekt, Heise Online, 28. Februar 2017, https://www.heise.de/security/meldung/E2EMail-Google-veroeffentlicht-PGP-fuer-GMail-als-Open-Source-Projekt-3638073.html.

denfalls nicht standardmäßig auf die höchste erreichbare Sicherheitsstufe. Das liegt nicht zuletzt daran, dass ein höheres Verschlüsselungsniveau noch immer eine langsamere Verarbeitungszeit bedeutet und vor allem mit erheblich größerem Aufwand für die Kommunizierenden verbunden ist.

Einem allgemein hohen Sicherheitsniveau in der digitalen Individualkommunikation abträglich ist zudem das Nutzerverhalten, das in gewisser Hinsicht paradox ist. Zwar äußern viele Nutzer Bedenken, wenn nach der Vertrauenswürdigkeit digitaler Kommunikation gefragt wird, was unter anderem auf die verschiedenen Datenschutzskandale der vergangenen Jahre zurückzuführen ist.[41] Auffällig ist jedoch, dass der Großteil der Nutzer trotz dieses Bewusstseins um staatliche Überwachungstätigkeiten und kompromittierende Handlungen durch Kriminelle sich nicht selbst darum bemüht, Dienste zu nutzen, die eine höhere Sicherheit gewährleisten.[42] Auch hierfür gibt es eine Vielzahl von Gründen. So scheint es vielen Nutzern einerseits trotz der genannten Bedenken geradezu gleichgültig zu sein, ob ihre Daten von unbefugten Dritten abgefangen und eingesehen werden.[43] Andererseits ist vielen die Einrichtung sicherer Technologien entweder zu aufwändig, oder sie wissen schlicht gar nicht, dass und wie sie selbst – etwa durch Nutzung technisch besser abgesicherter Systeme als unverschlüsselten E-Mails – für die Sicherheit ihrer Kommunikation sorgen können.[44]

Ein wesentlicher Aspekt, der die Nutzer von der Verwendung von Kommunikationsdiensten mit einem höheren Sicherheitsniveau abhält, wird zudem darin liegen, dass mehr Sicherheit zumeist mehr Aufwand und weniger Nutzerfreundlichkeit bedeutet. Dieser Aspekt spiegelt auf Nutzerseite das Problem der Anbieter wider: sichere Verschlüsselungstechnologien sind nicht nur schwierig zu implementieren, sondern bislang oft auch nur umständlich zu nutzen, was viele potentielle Nutzer, zumal wenn sie technisch weniger versiert sind, abschreckt. Solche Schwierigkeiten bestehen nicht nur bei verschlüsselter Kommunikation. Auch die Nutzung einer optionalen Zwei-Faktor-Anmeldung oder das Merken komplexer Passwörter vergrößern den Aufwand für die Kommunikation. Da Nutzerfreundlichkeit und einfache Bedienung gerade in der Individualkommunikation mit Endnutzern stets gegen die Sicherheit streiten werden, liegt in diesen Faktoren eine weitere ganz wesentliche Anforderung, um digitale Kommunikation letztlich sicherer zu machen und das Vertrauen hierin nachhaltig zu steigern.

---

[41] Nur 4,4 Prozent der Befragten einer repräsentativen Umfrage von Convios Consulting gehen davon aus, dass ihre E-Mails nicht von Hackern, Geheimdiensten oder ihrem E-Mail-Provider mitgelesen werden, siehe Thomas Heuzeroth, Misstrauen gegen Amerikaner nutzt Web.de und T-Online, Welt Online, 21. Mai 2017, https://www.welt.de/wirtschaft/webwelt/article164778604/Misstrauen-gegen-Amerikaner-nutzt-Web-de-und-T-Online.html.

[42] So nutzten im März 2017 nur 16,1 Prozent der Deutschen E-Mail-Dienste mit Verschlüsselung, siehe Convios Consulting, Datenschutz und Verschlüsselung, Repräsentative Umfrage im Auftrag von Web.de und GMX, März 2017, S. 8, https://www.slideshare.net/WEBDE_DEUTSCHLAND/der-trumpeffekt-das-digitale-misstrauen-wchst%20.

[43] Vgl. Patrick Bernau, Daten gehackt? Mir doch egal!, Fazit – das Wirtschaftsblog, 10. September 2015, http://blogs.faz.net/fazit/2015/09/10/experiment-zu-datenschutz-und-datensicherheit-6470/; das dort zitierte Experiment zeigte jedoch auch, dass Nutzer empfindlicher auf Datenschutzverstöße reagierten, je sensibler die Daten waren.

[44] Vgl. die Umfrage der Convios Consulting, S. 7.

3.2 Die eingesetzte Technologie sollte nutzerfreundlich sein.

Für das Vertrauen in digitale Kommunikation ist es damit nicht ausreichend, dass die eingesetzten Kommunikationsmittel sicher sind. Vielmehr müssen sie auch nutzerfreundlich sein. Denn werden Kommunikationsmittel, obgleich sicher, mangels Nutzerfreundlichkeit nicht angenommen, können sie das Sicherheitsniveau vertraulicher digitaler Kommunikation nicht steigern. Der Sicherheitsaspekt solcher Technologien läuft leer, wenn Nutzer auf leichter zu handhabende, dabei aber unsicherere Kommunikationswege zurückgreifen. Deshalb ist es entscheidend, dass Sicherheit nicht auf Kosten der Nutzerfreundlichkeit erreicht wird. Beide Aspekte müssen vielmehr, soweit möglich, stets als Einheit gedacht und entsprechend zusammengebracht werden.

Wie beschrieben ist die gewöhnliche E-Mail, deren Inhalt lediglich mittels einer Transportverschlüsselung bei der Übermittlung zwischen Client und Server und zwischen den Servern der beteiligten Dienstleister vor dem Zugriff unbefugter Dritter geschützt ist, nicht als besonders sicher anzusehen. Ihr großer Vorteil besteht jedoch darin, dass sie sehr einfach zu nutzen und in den vergangenen zwei Jahrzehnten vor allem zum absoluten Standard digitaler Kommunikation geworden ist. Das bedeutet, dass sich jede Lösung, die ein höheres Sicherheitsniveau gewährleisten soll, an dem Bedienkomfort der E-Mail orientieren muss, um Nutzer dauerhaft überzeugen zu können.

In dieser Hinsicht stehen Messenger-Dienste wie WhatsApp, Threema und Co. der E-Mail in Hinblick auf die bloße Bedienbarkeit in nichts nach. Um diese Anwendungen zu nutzen, ist kein weiteres technisches Verständnis vonnöten. Allerdings handelt es sich um geschlossene Systeme – sie sind untereinander und insbesondere auch nicht mit E-Mail-Diensten kompatibel. Die Verwendung von Messenger-Diensten erhöht somit die Anzahl von Kommunikationskanälen, was im Zweifel dazu führen kann, dass der Nutzer die Übersicht verliert. Zudem eignen sich die gängigen Dienste nur schlecht für die Übermittlung von Dokumenten in Form von Anhängen und sind damit oft nicht für die Kommunikation zwischen Behörde und Bürger bzw. Unternehmen und Kunde zu gebrauchen. Ein wesentlicher Grund für diesen Umstand ist darin zu finden, dass sie anders als E-Mail-Dienste vor allem dazu dienen, synchrone Kommunikation wie beispielsweise das Chatten zu ermöglichen. Sie sind konzeptionell damit Varianten der Sprachkommunikation wie vor allem dem Telefongespräch enger verwandt als asynchronen Kommunikationsmitteln wie z. B. der Briefpost.

Dies ist bei De-Mail-Diensten und beim E-Postbrief anders. Diese Anwendungen sind gerade darauf ausgelegt, auch Dokumente mit sensiblen Inhalten sicher zu übermitteln und sind zudem eher als Pendant zur klassischen, analogen Kommunikation mittels Brief konzipiert. Allerdings handelt es sich auch bei ihnen um geschlossene Systeme, die dadurch zwar eine gesteigerte Absicherung aufweisen, aber nicht mit anderen digitalen Kommunikationsmitteln kompatibel sind.[45] Insbesondere sind die De-Mail-Dienste auf Deutschland

[45] Da es sich beim E-Postbrief um einen hybriden Dienst handelt, folgt aus diesem Umstand allerdings nicht, dass die Nachricht den Empfänger nicht erreicht, sollte dieser selbst kein Nutzer des Dienstes sein; vielmehr wird die Nachricht in

beschränkt. Mit nicht-deutschen Nutzern im Ausland kann nicht kommuniziert werden, da eine Registrierung nur möglich ist, wenn man entweder deutscher Staatsbürger ist oder in Deutschland ansässig.[46] Hinzu kommen weitere Faktoren, die zum Zweck eines höheren Schutzniveaus implementiert sind, die Nutzung aber umständlicher machen. So ist für die erstmalige Registrierung eines De-Mail-Kontos erforderlich, dass sich der Nutzer beim Anbieter identifizieren lässt, beispielsweise indem er seinen Personalausweis vorlegt. Zieht er um und bekommt so eine neue Meldeadresse, muss er sich erneut registrieren. Um sich anschließend sicher bei seinem Konto anzumelden – was für die meisten De-Mail-Dienstleistungen Voraussetzung ist – sind zwei voneinander unabhängige Sicherungsmittel erforderlich, also beispielsweise die Eingabe eines Passwortes und die Nutzung der eID-Funktion des elektronischen Personalausweises. Hierfür ist es wiederum nötig, extra Hardware anzuschaffen und bereitzuhalten, damit der Chip des Ausweises vom Computer gelesen werden kann.[47]

Auch für die Registrierung zum E-Postbrief muss der Ausweis bei einer Postfiliale vorgelegt werden. Daneben muss der Hauptwohnsitz des Nutzers durch eine Kombination einer „HandyTAN“, die per Mobiltelefon übermittelt wird, und einer „AdressTAN“, die per Brief zugestellt wird und anschließend im Webportal des E-Postbriefes eingegeben wird, bestätigt werden. Diese Verfahren sind jedenfalls mit der vergleichsweise umstandslosen Registrierung eines neuen Kontos bei einem normalen E-Mail-Dienstleisters an Aufwand nicht zu vergleichen. Auch die Anmeldung beim Webportal des Dienstes ist für gewöhnlich mit einem einfachen, selbstgewählten Passwort zu erledigen. Soweit zusätzlich eine Zwei-Faktor-Anmeldung beispielsweise mittels einer auf das Mobiltelefon gesendeten TAN angeboten wird, ist diese zusätzliche Sicherheitsstufe jedenfalls optional und steht damit zur Disposition des Nutzers. Dieser kann selbst entscheiden, ob er ein wenig Bedienkomfort aufgeben will, um den Schutz seines E-Mail-Kontos zu erhöhen.

Wünscht der Nutzer eines normalen E-Mail-Dienstes, dass seine Nachrichten mittels Ende-zu-Ende-Verschlüsselung gegen den Zugriff unbefugter Dritter abgesichert sind – wie beispielsweise durch Verwendung von OpenPGP oder S/MIME – so ist seine Mitwirkung vonnöten, was bei der bloßen Transportverschlüsselung nicht der Fall ist.[48] Das Problem ist hierbei allerdings, dass der Einsatz der genannten Verschlüsselungstechnologien bislang kaum laientauglich ist. Neuere Browser-Plugins wie beispielsweise Mailvelope sind zwar benutzerfreundlicher, stehen bislang aber nur für wenige E-Mail-Dienste zur Verfügung.[49] Darüber hinaus besteht bei dieser asymmetrischen Verschlüsselungsmethode[50] die zusätzliche Gefahr, dass der Nutzer seinen privaten, geheimen Schlüssel vergisst. Ist dies geschehen und hat der Nutzer nicht die Vorsichtsmaßnahme der Anfertigung einer

---

diesem Fall ausgedruckt, kuvertiert, frankiert und an den Empfänger per Postbote ausgeliefert, siehe https://www.epost.de/privatkunden/brief-und-fax/briefe-online-versenden.html.

[46] Anna Biselli, De-Mail: Das tote Pferd wird weitergeritten, wie viel das kostet, soll geheim bleiben, Netzpolitik.org, 9. Juli 2015, https://netzpolitik.org/2015/de-mail-das-tote-pferd-wird-weitergeritten-wieviel-das-kostet-soll-geheim-bleiben/.

[47] Vgl. Wikipedia, De-Mail, https://de.wikipedia.org/wiki/De-Mail#De-Mail-Nutzerkonten_und_-Adressen.

[48] Heckmann, S. 68.

[49] Michael Herfert, Annika Selzer und Ulrich Waldmann, Laientaugliche Schlüsselgenerierung für die Ende-zu-Ende-Verschlüsselung, DuD 2016, S. 290, 291.

[50] Zur Erläuterung des Begriffs “asymmetrische Verschlüsselungsmethode” siehe den Anhang.

Sicherheitskopie des betreffenden Zertifikats ergriffen, so hat er keinen Zugriff mehr auf die verschlüsselten Informationen. Angesichts der Vielzahl an Passwörtern für webbasierte Dienste und andere Anwendungen, die sich Nutzer digitaler Technologien heutzutage merken müssen, sind es viele Menschen gewohnt, ein vergessenes Passwort zurücksetzen zu lassen und mithilfe des eigenen E-Mail-Accounts ein neues zu generieren. Dies ist bei dieser Art der Verschlüsselung jedoch gerade nicht möglich. Ist der Schlüssel verloren, so sind es auch die verschlüsselten Informationen.[51]

Angesichts der aufgeführten Probleme im Hinblick auf die Nutzerfreundlichkeit besonders sicherer digitaler Kommunikationsmittel versuchen Anbieter wie ProtonMail, insoweit einen Kompromiss anzubieten.[52] Die Dienste geben es jedenfalls zum Ziel aus, die oben beschriebenen Sicherungsmaßnahmen wie Ende-zu-Ende-Verschlüsselung und die verschlüsselte Ablage der Nachrichten im Postfach des Nutzers mit einer einfachen Handhabbarkeit zum Ausgleich zu bringen und dabei gleichzeitig mit anderen E-Mail-Anwendungen kompatibel zu bleiben.

Die Benutzungsfreundlichkeit von Portallösungen hängt stark von der konkreten Ausgestaltung des jeweiligen Portals ab. Wird hierbei Zwei-Faktor-Authentifizierung eingesetzt, mag dies zwar etwas umständlich sein, ist generell aber intuitiv und damit einfach zu bedienen. Umstände bereiten Portallösungen weniger aufgrund ihrer Ausgestaltung, sondern weil sie zu einem Paradigmenwechsel führen. Diesen könnte man als Übergang von einer Bring- zur Holschuld bei der Kommunikation mit Behörden und Unternehmen umschreiben. Anders ausgedrückt: Statt die jeweilige Information direkt übermittelt zu bekommen – wie bei E-Mail oder Messengern – muss der Nutzer sie sich bei der Kommunikation über Online-Postfächer aktiv beschaffen. Dies hat in vielerlei Hinsicht Auswirkungen auf den Nutzer. Zum einen trägt er, indem ihm eine erhöhte Mitwirkungspflicht übertragen wird, eine größere Verantwortung. Für den Zugang der Information ist nunmehr nicht mehr nur der Sender, sondern auch der Empfänger verantwortlich. Dies kann vor allem dann problematisch werden, wenn Portallösungen von einer Vielzahl wichtiger Kommunikatoren eingesetzt werden. Denn die Portale sind per se nicht miteinander verbunden, sondern jedes Unternehmen, jede Behörde verwendet ein eigenes System, für das man jeweils einen eigenen Zugang benötigt. Eine Vielzahl voneinander isolierter Portale von Behörden, Banken, Versicherungen etc. dauerhaft im Blick zu halten, für alle Zugänge Login-Daten zu erzeugen und zu merken usw. kann den Nutzer schnell überfordern. Gerade die dadurch steigende Anzahl an Passwörtern für die verschiedenen Portale macht diese Verfahren nicht nur nutzerunfreundlich, sondern stellt potentiell sogar ein Sicherheitsrisiko dar. Denn Nutzer werden versucht sein, die Passwörter entweder an einem unsicheren Ort abzulegen (etwa als Textdokument auf der Festplatte) oder stets das gleiche, leicht zu merkende, Passwort zu verwenden. Bei einem Hackerangriff auf einen der Dienste, bei dem es zum Diebstahl von Kundendaten inklusive Passwörtern kommt, würden so alle Logins, die

[51] Heckmann, S. 68.
[52] https://protonmail.com. Alternativen zu ProtonMail sind beispielsweise unseen.is (https://unseen.is/), Tutanota (https://tutanota.com/#!home) oder ScryptMail (https://scryptmail.com/login), die nach ähnlichen Prinzipien funktionieren.

mit diesem Passwort gesichert wurden, gleichzeitig kompromittiert, sofern der Dienst die Passwörter nicht ausreichend gesichert hat.[53]

Um diese Unübersichtlichkeit zu vermeiden, könnte es sich anbieten, einzelne Portale zusammenzuführen bzw. zu zentralisieren. So gibt es beispielsweise Anwendungen, mit der sich mehrere Konten bei verschiedenen Banken verwalten lassen.[54] Als Vorbild für ein solches zentralisiertes Portal bietet sich ein Blick nach Estland an. Hat man sich mit seinem elektronischen Personalausweis oder über sein Bankkonto bei dem estnischen E-Government-Portal angemeldet, kann man nicht nur Behördengänge erledigen, sondern auch seine eigenen Gesundheitsdaten an Ärzte übermitteln oder private Geschäfte erledigen.[55] Dabei sollte zugleich aber natürlich nicht vergessen werden, dass eine solche Zentralisierung auch Risiken birgt. Denn wird dieser eine Zugang kompromittiert, sind auf einen Schlag wiederum alle sensiblen Daten und Inhalte gleichzeitig gefährdet. Auch hierbei muss daher sorgfältig zwischen Nutzerfreundlichkeit und Sicherheit abgewogen werden.

Der vorausgegangene Abschnitt hat gezeigt, dass eine technische und organisatorische Absicherung für sich genommen nicht ausreichend ist, um digitale Kommunikation mit sensiblen Inhalten tatsächlich zu schützen. Denn die Motivationen und das daraus resultierende Verhalten der Nutzer sollte nicht unterschätzt werden. Nur wenn sich die eingesetzte Technologie auch hinreichend intuitiv und einfach bedienen lässt, wird sie genutzt werden. Darüber hinaus erscheint es notwendig, dass die Nutzer sich über die eingesetzten Sicherungsmaßnahmen beim jeweiligen Dienst im Klaren sind und sich hierauf verlassen können. Auch das Wissen um Sicherheitstechnologien erhöht das Bewusstsein für den Schutz sensibler Daten und kann auf diese Weise mit dazu beitragen, dass Nutzer geneigt sind, sich für Anbieter zu entscheiden, die auf höhere Sicherheitsstandards setzen.

3.3 Dem Nutzer gegenüber sollte der gewährleistete Sicherheitsstandard gegenüber transparent gemacht werden.

Transparenz fördert das Vertrauen in digitale Kommunikation. Wenn der Nutzer leicht erkennen kann, welches Sicherheitsniveau beim jeweiligen Kommunikationsvorgang gewährleistet ist, so ist es ihm besser möglich abzuschätzen, welches Risiko er eingeht, wenn ihm betreffende sensible Informationen auf digitalem Wege übermittelt werden. Auf dem Gebiet der digitalen Kommunikationssicherheit stellt sich das Problem, dass detaillierte Informationen hierüber die meisten Nutzer überfordern werden. Verstehen sie die Informationen nicht, die eigentlich ihrer Aufklärung dienen sollen, wird keine Transparenz

[53] Dieses Resultat wird im Falle einer Zwei-Faktor-Anmeldung selbstverständlich verhindert; zudem kann (und sollte) der Diensteanbieter natürlich Vorkehrungen treffen, um die Passwörter der Nutzer sicher zu speichern, z.B. durch die Erzeugung sogenannter salted hashes, vgl. Wikipedia, Salt (Kryptologie), https://de.wikipedia.org/wiki/Salt_(Kryptologie).
[54] Ein Beispiel für eine solche Smartphone-App ist Centralway Numbrs, die allerdings wegen Sicherheitsrisiken in der Kritik stand; vgl. Christian Siedenbiedel, Die neuen Apps fürs Online-Banking, FAZ.net, 12. Mai 2014, http://www.faz.net/aktuell/finanzen/meine-finanzen/sparen-und-geld-anlegen/konten-bei-unterschiedlichen-banken-mit-einer-app-verwalten-das-geht-jetzt-aber-ist-es-auch-sicher-12933595.html.
[55] Sabine Adler, E-Government macht das Leben leichter, Deutschlandfunk, 24. Mai 2016, http://www.deutschlandfunk.de/estland-e-government-macht-das-leben-leichter.1766.de.html?dram:article_id=355026.

erreicht. Wie auch auf anderen Gebieten, in denen Verbraucherinformationen über die Spezifika des Produkts aus diesem Grund sinnlos sind, bieten sich hier vertrauensfördernde Maßnahmen insbesondere in Form der Vergabe und Veröffentlichung von Gütesiegeln und Zertifikaten an. Diese können solchen Unternehmen und öffentlichen Stellen verliehen werden, die großes Vertrauen genießen und durch ihr spezielles Know-How sicherstellen können, dass für die jeweilige Konstellation angemessene Kommunikationssicherheit gewährleistet ist. Dabei ist zu gewährleisten, dass die Prüfinstanz unabhängig ist und selbst offene und transparente Prüfstandards zugrunde legt.[56]

Dass zum Beispiel die Verbindung zwischen dem eigenen Computer (Client) und dem Webserver, auf dem die gerade abgerufene Webseite gespeichert ist, mittels TLS[57] verschlüsselt ist, kann man in den neueren Versionen aller gängigen Webbrowser daran erkennen, dass neben der Adresszeile ein Schloss abgebildet ist. Ein noch höheres Sicherheitsniveau wird gewährleistet, wenn die Adresszeile zusätzlich (teilweise) grün hinterlegt ist. Dies ist dann der Fall, wenn der Dienst, mit dem die Kommunikationsverbindung zum Datenaustausch aufgebaut wurde, ein sogenanntes Extended-Validation-Zertifikat vorweisen kann.[58] Ein solches Zertifikat bestätigt die Identität des Dienstes und soll so insbesondere Phishing-Angriffe verhindern, da der Nutzer leichter erkennen kann, ob er sich zum Beispiel tatsächlich auf der Webseite seiner Bank befindet und nicht auf einer gefälschten Webseite, die sich als die Webseite seiner Bank ausgibt und auf diese Weise die Login-Daten des Nutzers abzufischen versucht. Die Extended-Validation-Zertifikate für Webseiten werden nach Prüfung der Vergabekriterien der eIDAS-Verordnung gemäß durch die Vertrauensdiensteanbieter herausgegeben, welche in Deutschland wiederum unter der Aufsicht des BSI stehen. Erfüllt der Anbieter sogar die erhöhten Anforderungen an sogenannte qualifizierte Dienste nach der eIDAS-Verordnung, dann ist er berechtigt, seine Dienste mit dem „EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter“ zu bewerben.[59] Dieses Siegel ist zwar nur mittelbar für den Endnutzer interessant, da es hier um das Verhältnis zwischen Vertrauensdiensteanbieter und Webdienst bei der Vergabe der Zertifikate geht, aber sie stellen dennoch einen weiteren Baustein zur Herstellung von Vertrauen in digitale Kommunikation dar.

Auch die datenverarbeitenden öffentlichen Stellen und privatwirtschaftlichen Unternehmen, die ein Datenschutzaudit nach § 9a des Bundesdatenschutzgesetzes durchführen lassen, sollen nach dem bekundeten Willen des Gesetzgebers nach der erfolgreichen Durchführung ein Gütesiegel vergeben bekommen, anhand dessen sie den Nutzern ihrer Dienste anzeigen können, dass sie mit den sensiblen Daten den gesetzlichen Vorgaben

[56] Günter Krings und Lars Mammen, Zertifizierungen und Verhaltensregeln – Bausteine eines modernen Datenschutzes für die Industrie 4.0, RDV 2015, S. 231, 232.
[57] Siehe dazu den Anhang.
[58] Vgl. Wikipedia, Extended Validation Zertifikat, https://de.wikipedia.org/wiki/Extended-Validation-Zertifikat; ist nur ein Schloss abgebildet, ist die Verbindung mittels TLS gesichert, aber das Zertifikat ist weniger vertrauenswürdig als ein Extended-Validation-Zertifikat.
[59] Bundesamt für Sicherheit in der Informationstechnik, Qualifizierung als Vertrauensdiensteanbieter, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/VDA_Qualifizierung/VDA_Qualifizierung.html;jsessionid=B21144B59BCAB5E28A7567AFA8ED035E.2_cid351.

entsprechend sorgfältig umgehen.[60] Da es wie bereits erwähnt allerdings bislang an einer spezialgesetzlichen Ausgestaltung des Audits fehlt, können auch noch keine Siegel erlangt werden. Es existieren davon unabhängig aber bereits Beispiele für ähnliche Zertifikate. So vergibt das unabhängige Landesdatenschutzzentrum Schleswig-Holstein ein Datenschutz-Gütesiegel.[61] Es bestätigt, dass eine Dienstleistung den datenschutzrechtlichen Vorgaben entspricht und dass dies in einem förmlichen Prüfverfahren festgestellt wurde. Die Datensicherheit ist einer der Schwerpunkte während des Audits.[62] Eine entsprechende Funktion erfüllt auch das europaweit vergebene European Privacy Seal.[63]

Die neue europäische Datenschutzgrundverordnung sieht in Artikel 42 ebenfalls Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen vor, um die Transparenz gegenüber Nutzern im Hinblick auf die Einhaltung von Datenschutzstandards zu verbessern. Die Nutzer sollen anhand dieser Zertifikate schnell und einfach erkennen können, welches Datenschutzniveau bei einem bestimmten Produkt oder einer Dienstleistung erreicht wird.[64]

Auch wenn die Audits nicht verpflichtend sind, sondern auf freiwilliger Basis erfolgen, sollte darauf hingearbeitet werden, dass diese Möglichkeit von den öffentlichen Stellen und Unternehmen, die sensible Inhalte auf digitalem Wege an Nutzer übermitteln, eingesetzt wird. Gerade weil digitale Kommunikation immer mehr zum Normalfall wird und damit das Vertrauen der Nutzer in digitale Kommunikationsmittel immer größere Bedeutung gewinnt, ist es entscheidend, dass sie in die Lage versetzt werden, selbst einschätzen zu können, in welchen Kontexten sie einem Dienst vertrauen können und wann nicht. Denn dem Großteil der Nutzer fehlt es sowohl an eigenem Verständnis als auch an geeigneten Mitteln, um selbst das Sicherheitsniveau des jeweiligen Kommunikationsmittels überprüfen zu können.

3.4 Dem Nutzer sollten alternative – auch analoge – Kommunikationsmittel angeboten werden.

Wie bereits im ersten Themenpapier ausgeführt, bietet digitale Kommunikation gegenüber analoger eine Reihe von Vorteilen. Ihre Ausweitung sowohl im Verhältnis Unternehmen zu Kunde als auch von Staat zu Bürger zu fördern, erscheint daher sinnvoll.

Die Nutzung digitaler Kommunikationsmittel allerdings nicht lediglich voranzubringen, sondern darüber hinaus wie beispielsweise in Estland[65] oder Dänemark[66] auch verpflichtend zu machen, stößt in Deutschland bis auf weiteres noch auf Probleme und steht bislang auch noch nicht auf der Agenda des Gesetzgebers. So ist zum einen die Gruppe derer, die im Umgang mit dem Internet allgemein und digitaler Kommunikation im Speziellen weder geschult noch geübt sind, beachtlich und daher keinesfalls zu vernachlässigen. Vor

[60] Plath, S. 369.
[61] Siehe https://www.datenschutzzentrum.de/guetesiegel/.
[62] https://www.datenschutzzentrum.de/guetesiegel/faq/.
[63] https://www.european-privacy-seal.eu/EPS-en/Home.
[64] So Erwägungsgrund 100 der Datenschutzgrundverordnung.
[65] Leonid Bershidsky, Envying Estonia's Digital Government, Bloomberg, 4. März 2015, https://www.bloomberg.com/view/articles/2015-03-04/envying-estonia-s-digital-government.
[66] Danish Agency for Digitisation, Campaigning for Mandatory Digital Communication, 3. Dezember 2013, https://www.digst.dk/servicemenu/english/news/campaigning-for-mandatory-digital-communication.

allem, wenn es um essentielle Dienste wie Angebote der Daseinsvorsorge oder der Kommunikation zum Beispiel mit der Krankenkasse geht, darf die Förderung der Digitalisierung nicht dazu führen, dass dieser Teil der Bevölkerung ausgeschlossen wird. Darüber hinaus sind strukturelle Merkmale wie vor allem die Größe der Bundesrepublik zu berücksichtigen. Flächendeckende Lösungen für digitale Kommunikation mit dem Staat oder der Privatwirtschaft zu finden, ist in Staaten mit 1,3 Millionen (Estland) bzw. 5,7 Millionen (Dänemark) Einwohnern selbstverständlich ungleich einfacher als in einem Land mit mehr als 82 Millionen. Geht es um Kommunikation mit öffentlichen Stellen, so tritt als Hindernis die stark ausgeprägte föderale Struktur Deutschlands hinzu, die bundesweite Regelungen in dieser Hinsicht unwahrscheinlich macht oder zumindest immens erschwert.[67] Zugleich bedeutet die Größe allein natürlich nicht, dass das Vorhaben von vornherein zum Scheitern verurteilt wäre. Mit regional oder auf einzelne Bundesländer begrenzten Feldversuchen könnten (und sollten) in dieser Hinsicht Möglichkeiten ausgelotet werden.

Solange nicht sämtliche Bürger mit sicheren digitalen Kommunikationsmitteln umgehen können, muss gerade in bedeutenden Kommunikationsverhältnissen (wie vor allem G2C, aber auch beispielsweise bei Bankdienstleistungen, Energieversorgung und Diensten des Gesundheitssektors) darauf geachtet werden, dass Alternativen angeboten werden. Das bedeutet, dass sowohl staatliche Stellen als auch privatwirtschaftliche Unternehmen den Bürgern und Kunden neben dem digitalen Weg stets auch alternative, analoge Kommunikationsmittel anbieten sollten, wenn es um den Versand sensibler Inhalte geht.

Für die öffentliche Verwaltung ist dies sogar gesetzlich vorgeschrieben. So regelt der § 3a des Verwaltungsverfahrensgesetzes die Möglichkeit der Übermittlung elektronischer Dokumente an den Bürger. Diese ist aber nur zulässig, wenn der Bürger einen Zugang hierfür eröffnet. Es ist also ihm überlassen, ob er das tut oder nicht. Entsprechend ist die Bekanntgabe von Verwaltungsakten mittels eines Webportals, auf das der adressierte Bürger zugreifen muss, von dessen ausdrücklicher Einwilligung abhängig.[68]

Dem gleichen Prinzip folgt auch die elektronische Steuererklärung ELSTER. Zwar hat die Bundesregierung 2015 beschlossen, darauf hinzuarbeiten, dass nach und nach fast alle Steuererklärungen online ausgefüllt werden, um sie automatisiert prüfen zu können, am Freiwilligkeitsprinzip selbst soll jedoch nicht gerüttelt werden.[69] Dementsprechend sind

---

[67] Ein Versuch, dieses Problem zu lösen, ist der sogenannte Portalverbund, der die verschiedenen Online-Portale von Bund, Ländern und Kommunen so verknüpft, dass Nutzer die gesuchte öffentliche Dienstleistung schnell, direkt und sicher erreichen können, egal, über welches Verwaltungsportal sie eingestiegen sind; vgl. IT-Planungsrat, Projektsteckbrief Portalverbund, 4. August 2016, http://www.it-planungs-rat.de/SharedDocs/Downloads/DE/Entscheidungen/21_Sitzung/6_Anlage1_Portalverbund.pdf?__blob=publicationFile&v=2.

[68] § 41 Absatz 2a Verwaltungsverfahrensgesetz. Siehe dazu Alexander Schmidt und Claudia Heudecker, Der vollständig automatisierte Erlass eines Verwaltungsakts (§ 35a VwVfG) sowie die Bekanntgabe eines Verwaltungsakts über öffentlich zugängliche Netze (§ 41 Abs. 2a VwVfG), Juris, 21. April 2017, https://www.juris.de/jportal/portal/page/homerl.psml?nid=jpr-NLITADG000217&cmsuri=/juris/de/nachrichten/zeigenachricht.jsp.

[69] Albert Funk, Steuererklärung ohne Stift und Papier, Tagesspiegel Online, 8. Dezember 2015, http://www.tagesspiegel.de/wirtschaft/einfuehrung-ab-2017-steuererklaerung-ohne-stift-und-papier/12692584.html.

bislang nur wenige Gruppen von Steuerpflichtigen wie beispielsweise Unternehmen verpflichtet, die Steuererklärung elektronisch zu erledigen.[70]

Einen anderen Weg mit der – kleiner werdenden[71] – Gruppe der „digital Ausgeschlossenen“ umzugehen, verfolgt Dänemark. Dort ist, wie beschrieben, die digitale Abwicklung sämtlicher Kommunikationsvorgänge zwischen Bürgern und öffentlichen Stellen seit 2015 verpflichtend. Und tatsächlich wurde in jenem Jahr bereits 80 Prozent der G2C-Kommunikation auf elektronischem Wege erledigt.[72] Von dieser Verpflichtung gibt es aber wichtige Ausnahmen. So sind die Behörden einerseits gesetzlich verpflichtet, den „digital Ausgeschlossenen“ in den örtlichen Gemeindezentren Hilfe bereit zu stellen, damit auch sie ihre Angelegenheiten mit dem Staat digital durchführen können. Ist ein Bürger darüber hinaus aus bestimmten Gründen überhaupt nicht in der Lage, die digitalen Kommunikationsmittel zu nutzen, so bleibt der dänische Staat weiterhin verpflichtet, alternative Mittel zur Verfügung zu stellen.[73] Wenn man sich in Deutschland in der Zukunft dafür entscheiden sollte, vom Freiwilligkeitsprinzip Abstand zu nehmen, dann böte sich ein solcher Ansatz trotz eines möglicherweise beträchtlichen finanziellen Aufwandes, den die Umstellung auf eine solche hybride Struktur nach sich ziehen könnte, jedenfalls dem Grundsatz nach auch für die Bundesrepublik an.

3.5 Die Wahl des Kommunikationsmittels sollte für den Nutzer nicht mit unmittelbaren Mehrkosten verbunden sein bzw. in dieser Hinsicht nicht zwischen analoger und digitaler Kommunikation unterscheiden.

Trotz der erwarteten Effizienzgewinne ist die Umstellung auf Infrastrukturen, die die digitale Kommunikation zwischen öffentlichen Stellen und Bürgern bzw. Unternehmen und Kunden ermöglichen, zunächst mit erheblichen Kosten verbunden. Jedenfalls soweit dabei öffentliche Haushalte belastet werden, werden diese Mittel auch von den Steuerzahlern aufgebracht werden.[74]

Davon abgesehen aber sollte die Förderung digitaler Kommunikation nicht mit unmittelbaren Mehrkosten für den Nutzer verbunden sein. Das bedeutet einerseits, dass digitale Angebote nicht gebührenpflichtig sein sollten, wenn die entsprechenden analogen Kommuni-

[70] Portal der Finanzämter in Baden-Württemberg, Wann bin ich verpflichtet, ELSTER zu nutzen?, http://www.fa-baden-wuerttemberg.de/pb/,Lde/Startseite/ELSTER/Wann+bin+ich+verpflichtet_++ELSTER+zu+nutzen_.
[71] Im Jahr 2016 gaben nur noch 16 Prozent der Befragten einer repräsentativen Studie in Deutschland an, das Internet nie zu benutzen, vgl. DIVSI, DIVSI Internet-Milieus 2016: Die digitalisierte Gesellschaft in Bewegung, Hamburg, Juni 2016, S. 12, https://www.divsi.de/wp-content/uploads/2016/06/DIVSI-Internet-Milieus-2016.pdf; zugleich steigt bei internetfernen Bevölkerungsgruppen das Phänomen der sogenannten Passiv-Onliner, also Personen, die das Internet selbst nicht nutzen, sich dessen Vorteilen aber bewusst sind und sich deshalb im Bedarfsfall Hilfe holen oder konkrete Aufgaben an Nutzer delegieren, vgl. DIVSI, DIVSI Ü60-Studie: Die digitalen Lebenswelten der über 60-Jährigen in Deutschland, Hamburg, Oktober 2016, S. 76, https://www.divsi.de/wp-content/uploads/2016/10/DIVSI-UE60-Studie.pdf.
[72] Danish Agency for Digitisation, The Danish Public Sector Reaches Ambitious Digital Milestone, https://www.digst.dk/Servicemenu/English/Policy-and-Strategy/eGOV-strategy/The-Danish-public-sector-reaches-ambitious-digital-milestone.
[73] Danish Agency for Digitisation, We Are Working to Make E-Government in Denmark More User-Friendly, 12. Februar 2014, https://www.digst.dk/Servicemenu/English/News/We-are-working-to-make-egovernment.
[74] Siehe z.B. für die Einführung der De-Mail Anna Biselli, De-Mail: Das tote Pferd wird weitergeritten, wie viel das kostet, soll geheim bleiben, Netzpolitik.org, 9. Juli 2015, https://netzpolitik.org/2015/de-mail-das-tote-pferd-wird-weitergeritten-wieviel-das-kostet-soll-geheim-bleiben/.

kationswege (bislang) kostenfrei waren. Umgekehrt sollte eine analoge Alternative nicht plötzlich mit Gebühren verknüpft sein, wenn sie vor Einführung des digitalen Kommunikationsmittels den Nutzer nichts gekostet hatte. Diese Grundsätze sind eine Folge des Prinzips der Freiwilligkeit bei der Wahl des Kommunikationsmittels. Denn die Entscheidung ist für den Nutzer nur dann wirklich frei, wenn keine der Optionen in Bezug auf die Kosten diskriminiert.

Wenn also beispielsweise eine Bank ihren Kunden bislang Kontoauszüge und andere Dokumente kostenlos per (analoger) Post zustellte, dann sollte die eingeführte Möglichkeit, auf reines Online-Banking umzustellen, nicht dazu führen, dass für den analogen Service künftig Gebühren fällig werden – jedenfalls dann nicht, wenn der Abruf der Dokumente über das Webportal der Bank oder gegebenenfalls die Zustellung per E-Mail kostenfrei ist. Das sollte selbst dann gelten, wenn die Geschäftsbedingungen des Unternehmens vorsehen sollten, dass es zu einer Zustellung auf Papier kommt, wenn der Kunde es über einen längeren Zeitraum versäumt, die Dokumente online einzusehen oder herunterzuladen.[75]

Für Services hingegen, die auch in analoger Form nicht kostenfrei sind oder waren, kann anders herum selbstverständlich auch digital ein Preis aufgerufen werden. So ist für das Versenden von Briefen an Unternehmen oder Behörden – im Regelfall – das normale Briefporto zu zahlen. Es spricht daher aus Erwägungen der Gleichbehandlung nichts dagegen, diese Dienstleistung auch bei digitaler Zustellung kostenpflichtig zu gestalten, jedenfalls dann, wenn der Service vergleichbar ist – was in diesem Fall insbesondere bedeutet, dass das Schutzniveau hinsichtlich des Inhaltes der Kommunikation genauso hoch sein sollte wie beim analogen Brief.[76]

Die Vermeidung von Mehrkosten muss umgekehrt auch für den Fall gelten, dass einem Nutzer, der den digitalen Weg nicht wählen kann oder möchte, keine Mehrkosten bei Nutzung eines alternativen Kommunikationsmittels (im Sinne des vierten Leitsatzes) entstehen.

4 Zusammenfassende Erwägungen

Das vorliegende zweite Themenpapier im Projekt „Vertrauen in Kommunikation im digitalen Zeitalter“ zeigt Wege auf, wie das Vertrauen der Nutzer in digitale Kommunikationsmittel, die bei der Übermittlung sensibler Inhalte durch Unternehmen und Verwaltung eingesetzt werden, gestärkt werden kann. Zu diesem Zweck wurden fünf Leitsätze aufgestellt. Die Ausführungen zum Rechtsrahmen im Kontext des ersten Leitsatzes zeigen, dass dieser vorrangig auf den Aspekt der Sicherheit der Kommunikation fokussiert. Relativiert wird dieser Fokus allenfalls in Bezug auf etwaige Kostenfolgen – und deren Angemessenheit – für die kommunizierenden Stellen.

[75] Vgl. insoweit die „Sonderbedingungen zur Nutzung des Online-Banking Postfachs“ der Deutschen Bank, Stand: Oktober 2016, Punkt 3, https://www.deutsche-bank.de/pfb/data/docs/ser-DB-Sonderbedingungen-Nutzung-Postfach-PBC.pdf.
[76] Vgl. insoweit die Preise für die elektronische Zustellung des E-Postbriefes: https://www.epost.de/privatkunden/hilfe.html#/faq/brief-fax/sicher-digital-kommunizieren/wie-viel-kostet-der-e-postbrief-mit-elektronischer-zustellung-.

Wenig Konkretes lässt sich dem Recht indes in Bezug auf andere Faktoren entnehmen, die im Hinblick auf das Gesamtziel erhöhter Kommunikationssicherheit und verstärktem Vertrauen in digitale Kommunikation zu berücksichtigen sind und die mitunter gebieten, von der Maxime maximal möglicher Sicherheit Abstriche zu machen. Die Sicherheit digitaler Kommunikation ist auf diesem Weg nur ein Faktor unter mehreren. Sichere Kommunikationsmittel, die von den designierten Zielgruppen nicht bedient werden können oder durch einfacher benutzbare, aber unsicherere Alternativen ersetzt werden, verfehlen ihre Funktion, da sie nicht verwendet werden. Sie werden sich am Markt nicht durchsetzen, so dass der angebotene Sicherheitsstandard wirkungslos bleibt. Ein optimales Maß an Sicherheit ist daher nur zu erreichen, wenn die Aspekte Sicherheit und Nutzerfreundlichkeit als einheitliches Ganzes und somit, soweit möglich, effektiv zusammengebracht werden. Daraus folgt als Handlungsanleitung, dass Diensteanbieter stets darauf hinarbeiten sollten, Sicherheitstechnologien auf eine Weise in ihren Produkten zu implementieren, dass die Nutzerfreundlichkeit darunter nicht leidet. Die Ausführungen haben dahingehend gezeigt, dass es nach dem derzeitigen Stand der Technik kaum realistisch scheint, gleichzeitig größtmögliche Sicherheit und größtmögliche Nutzerfreundlichkeit zu erreichen. Es müssen daher an einem der beiden zentralen Faktoren Abstriche gemacht werden – es geht darum, diese möglichst klein zu halten und ein Produkt zu schaffen, das sinnvoll als sowohl sicher als auch nutzerfreundlich bezeichnet werden kann, also auch von Laien einfach zu benutzen und dabei gegen die weitaus meisten realistischen Angriffsszenarien ausreichend geschützt ist.

Alternativ könnte man erwägen, die Entscheidung in einem begrenzten Rahmen den Nutzern selbst zu überlassen. So wäre auch denkbar, dass Diensteanbieter, falls sie einen sehr sicheren, dabei aber vergleichsweise komplizierten Dienst anbieten, gleichzeitig eine einfacher zu bedienende, entsprechend aber nicht ganz so gut abgesicherte Alternative im Angebot haben. In einem solchen Fall wäre die klare, in leicht verständlicher Sprache verfasste Aufklärung von entscheidender Bedeutung. Nur wenn ein Nutzer sofort nachvollziehen kann, was das jeweilige Produkt im Hinblick auf den Sicherheitsaspekt bietet, kann er eine informierte Entscheidung treffen und die gegebenenfalls auf ihn übertragene Verantwortung für die Vertraulichkeit der übermittelten Inhalte übernehmen.

Um das Vertrauen in die Kommunikationsmittel – und deren Sicherheit – zu stärken, sollten zudem Reputationssysteme wie Gütesiegel und Zertifikate eingesetzt werden. Auch solche werden nachhaltig dazu führen, dass die Nutzer die sicheren Varianten moderner Kommunikationsmittel insbesondere bei sensibler Kommunikation annehmen und verwenden.

Schließlich kann Vertrauen in die Sicherheit digitaler Kommunikation nur dann gestärkt und erhalten werden, wenn die herausgearbeiteten Gebote auch durchgesetzt werden. Wie bereits im ersten Themenpapier angeführt, werden insbesondere Verstöße gegen den Datenschutz bislang nur unzureichend verfolgt. Wenn auf Übertretungen jedoch keine Sanktionen folgen, wird das Vertrauen der Nutzer in die Sicherheit ihrer sensiblen Informationen untergraben. Zu diesem Zweck könnte über Ansätze der Selbst- und Ko-

Regulierung nachgedacht werden. Solche Modelle würden es den beteiligten Akteuren im Zusammenspiel mit dem Gesetzgeber und staatlicher Aufsicht ermöglichen, im Rahmen einer freiwilligen Selbstkontrolle effektive Maßnahmen zur Durchsetzung der Schutzbestimmungen umzusetzen.[77]

Die fünf Leitsätze lassen sich, etwas verkürzt, auf die Begriffe Sicherheit, Nutzerfreundlichkeit, Transparenz, Angebot von Alternativen und ökonomische Nichtdiskriminierung bringen. Diese Begriffe stehen in verschiedenen Abhängigkeiten, die zum Abschluss dieses Themenpapiers noch kurz herausgearbeitet werden sollen.

Sicherheit und Nutzerfreundlichkeit stehen in einem direkten Spannungsverhältnis. Die Erfahrung hat gezeigt, dass eine erhöhte Sicherheit im digitalen Raum in der Regel mit einer geringeren Nutzerfreundlichkeit erkauft wird. Eine Ausnahme sind abgeschlossene digitale Ökosysteme (z.B. Plattformen), die Sicherheit auch bei hoher Nutzerfreundlichkeit herstellen können.

Transparenz ist eine Eigenschaft, die direkt auf Sicherheit einzahlt, weil sie Nutzern die Risiken, die sie ggf. eingehen, bzw. die Sicherheit, die sie gewinnen, ersichtlich macht. Transparenz kann damit auch dazu führen, dass Nutzer Lösungen mit geringerer Nutzerfreundlichkeit akzeptieren, um eine höhere Sicherheit bei der Kommunikation zu haben.

Das Angebot von Alternativen ist nur bei ökonomischer Nichtdiskriminierung dieser Alternativen glaubwürdig und tragfähig. Die Verfügbarkeit alternativer Kommunikationsmittel trägt weiterhin zur Sicherheit bei, weil Nutzer, die sich beispielsweise sicheren, aber komplexen digitalen Werkzeugen nicht gewachsen fühlen, nicht den einfachen Weg eines unsicheren Kommunikationskanals wählen. In diesem Zusammenhang ist wiederum Transparenz wichtig, damit Nutzerfreundlichkeit nicht das führende Kriterium bei der Auswahl des Kommunikationswegs ist.

Im Verhältnis zur Unterstützung von Vertrauen in Kommunikation ist Sicherheit der wesentliche Faktor, ohne den Vertrauen substanziell nicht hergestellt werden kann. Nutzerfreundlichkeit und Transparenz sind unterstützende Hilfsmittel, die überhaupt erst die Nutzung sicherer Lösungen für einen Großteil der Nutzer ermöglichen bzw. sie von der Nutzung derselben überzeugen. Das Angebot von Alternativen und die ökonomische Nichtdiskriminierung schließlich öffnen Wege für vertrauensvolle Kommunikation auch für diejenigen Nutzer, denen aus verschiedenen Gründen der Einsatz der üblichen digitalen Wege verschlossen bleibt.

[77] Vgl. Selbstregulierung Informationswirtschaft e.V., Chancen und Voraussetzungen effektiver Selbst- und Ko-Regulierung zur Förderung des Verbraucherschutzes und des Datenschutzes in der digitalen Welt, Positionspapier, Mai 2014, S. 4, https://sriw.de/images/pdf/Broschueren/140521_SRIW_Positionspapier_Selbst-_und_Ko-Regulierung_v03.pdf.

Anhang: Details zur technischen Absicherung von Kommunikation

In diesem Anhang finden sich in Ergänzung zu Kapitel 3.1.2 weitere Details zum Thema der technischen Absicherung von Kommunikation.

Rechtsrahmen für den Einsatz von Verschlüsselungsverfahren

Öffentliche Stellen und privatwirtschaftliche Unternehmen sind aufgrund des geltenden Rechtsrahmens in gewissem Maß verpflichtet, Verschlüsselungstechnologien einzusetzen, wenn sie mit sensiblen Informationen von Bürgern bzw. Kunden umgehen und diese über digitale Kanäle übermitteln. So ist im Bundesdatenschutzgesetz bestimmt, dass sie „dem Stand der Technik entsprechende Verschlüsselungsverfahren“ verwenden sollten, um „zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“.[78] Auch die Datenschutzgrundverordnung verpflichtet nach Art. 24 Absatz 1 diejenigen Personen, die für die Verarbeitung personenbezogener Daten verantwortlich sind, entsprechende Verschlüsselungstechnologien einzusetzen.[79] Da § 9 Satz 2 BDSG allerdings zugleich einschränkt, dass nur solche Maßnahmen umgesetzt werden müssen, deren Aufwand „in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht“, kann aus der Vorschrift selbst keine absolute gesetzliche Pflicht abgeleitet werden, digitale Kommunikation stets zu verschlüsseln, selbst wenn der Einsatz von Verschlüsselungstechnologien heutzutage keine große technische Herausforderung mehr darstellt.[80] Insbesondere macht das Gesetz auch keine Vorgabe dahingehend, welche Art Verschlüsselung zu verwenden ist und in welchen Phasen der Übermittlung die Inhalte der Kommunikation zu verschlüsseln sind.

Symmetrische und asymmetrische Verschlüsselungsverfahren

Inhalte digitaler Kommunikation können entweder mittels symmetrischer oder asymmetrischer Verfahren verschlüsselt werden. Welche Methode gewählt wird, hat Konsequenzen für das Sicherheitsniveau und die Geschwindigkeit des Prozesses. Bei symmetrischer Verschlüsselung existiert nur ein kryptographischer Schlüssel. Mit diesem wird die Nachricht vor dem Versand verschlüsselt und anschließend vom Empfänger wieder entschlüsselt. Das bedeutet, dass die Kommunikationspartner einen Weg finden müssen, den Schlüssel auf eine sichere Weise auszutauschen, da er beiden bekannt sein muss. Gelangt ein Dritter in Besitz des Schlüssels, zum Beispiel indem er den Vorgang des Schlüsselaustauschs kompromittiert, so kann auch er den Inhalt der Nachricht entschlüsseln und einsehen. Der zentrale Vorteil symmetrischer Verschlüsselungsverfahren ist deren hohe Geschwindigkeit.[81] Ein Beispiel für diese Methode ist der Advanced Encryption Standard (AES), der in seinen komplexeren Varianten als sehr sicher gilt und aus diesem Grund

[78] Siehe Satz 2 Nr. 4 und Satz 3 der Anlage zu § 9 Satz 1 BDSG.
[79] Kai-Uwe Plath (Hrsg.), Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. Auflage 2016, S. 117 f.
[80] Ebd., S. 365.
[81] Vgl. Kryptowissen.de, Symmetrische Verschlüsselung, http://www.kryptowissen.de/symmetrische-verschluesselung.html.

unter anderem in den Vereinigten Staaten zur Verschlüsselung staatlicher Dokumente der höchsten Geheimhaltungsstufe zugelassen ist.[82] Eine grundsätzliche Herausforderung beim Einsatz von Verschlüsselungssystemen ist die sichere Aufbewahrung der Schlüssel. Die Deutsche Post beispielsweise setzt für die Transportverschlüsselung auf AES. Die dazu notwendigen Schlüssel sind laut Angaben des Unternehmens dadurch vor unberechtigten Zugriffen geschützt, dass sie in einem zertifizierten Hardware-Security-Module hinterlegt sind.[83]

Asymmetrische Verschlüsselung hingegen funktioniert, ohne dass die miteinander kommunizierenden Personen einen gemeinsamen geheimen Schlüssel austauschen müssen. Es erzeugt vielmehr jeder Nutzer zwei einander zugeordnete Schlüssel, einen geheimen, privaten Schlüssel und einen öffentlichen, der nicht geheim gehalten wird. Der private Schlüssel verbleibt beim Nutzer, der nicht geheime wird hingegen anderen Kommunikationspartnern mitgeteilt. Wollen diese eine Nachricht mit sensiblen Inhalten an den Nutzer schicken, so verschlüsseln sie die Nachricht mit dessen öffentlichem Schlüssel und senden sie an ihn. Hat der Nutzer die Nachricht erhalten, kann er sie mit dem privaten Schlüssel, der sich auf seinem eigenen System befindet, entschlüsseln und lesen.[84] Die Methode ist sehr sicher, da kein geheimer Schlüssel ausgetauscht werden muss und da aus der Kenntnis des öffentlichen Schlüssels der zugehörige private Schlüssel nicht effizient berechnet werden kann.[85] Außerdem muss der Nutzer nur dafür Sorge tragen, dass niemand an den privaten Schlüssel gelangt (bei symmetrischer Verschlüsselung müssen hingegen sämtliche Schlüssel, die zur Geheimhaltung aller ausgetauschten Nachrichten eingesetzt wurden, sicher aufbewahrt werden[86]). Darüber hinaus muss sichergestellt sein, dass der öffentliche Schlüssel des Empfängers, der für die Verschlüsselung der Nachricht eingesetzt wird, nicht von einem Angreifer ausgetauscht, d.h. kompromittiert worden ist (z.B. im Fall sogenannter Man-in-the-Middle-Angriffe). Denn wäre dies der Fall, könnte der Angreifer erreichen, dass er die für einen Anderen bestimmte Nachricht lesen könnte, sofern es ihm gelänge, die verschlüsselte Nachricht abzufangen. Auch im Fall asymmetrischer Verschlüsselungen muss also eine gewisse Sorgfalt walten. In der Praxis lässt sich dies im Vergleich zu symmetrischen Verschlüsselungsverfahren allerdings einfacher organisieren.

Ein Hauptproblem dieser Verschlüsselungsmethode ist, dass asymmetrische Algorithmen im Vergleich zu symmetrischen komplexer sind, deshalb deutlich mehr Rechenleistung benötigen und somit nur sehr langsam ausgeführt werden können. Aus diesem Grund werden die beiden Verfahren häufig miteinander kombiniert: Bei der sogenannten hybriden Verschlüsselung wird die eigentliche Nachricht mittels eines schnellen symmetrischen Ver-

[82] CNSS Policy No. 15, Fact Sheet No. 1, National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, Juni 2003, http://csrc.nist.gov/groups/ST/toolkit/documents/aes/CNSS15FS.pdf.
[83] Siehe E-Post, Datenschutz und Datensicherheit, Hohe Sicherheits- und Datenschutzstandards sowie moderne Verschlüsselungstechniken, https://www.epost.de/privatkunden/sicherheit.html#sicherheit-und-verschluesselungstechniken.
[84] Vgl. Wikipedia, Asymmetrisches Kryptosystem, https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem.
[85] Heckmann, S. 66.
[86] Vgl. Wikipedia, Asymmetrisches Kryptosystem, https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem.

fahrens verschlüsselt. Anschließend wird lediglich der symmetrische Schlüssel selbst asymmetrisch verschlüsselt und kann so sicher übermittelt werden.[87]

Bei der Verschlüsselung eingesetzte technische Protokolle

Die gängigste Form der Transportverschlüsselung im Internet ist das hybride Verschlüsselungsprotokoll Transport Layer Security (TLS, Transportschichtsicherheit), die Weiterentwicklung des Secure-Sockets-Layer-Protokolls (SSL). Es wird vor allem eingesetzt, um Daten zu verschlüsseln, die über das Hypertext Transfer Protocol (HTTP, Hypertext-Übertragungsprotokoll) von einem Webserver im World Wide Web zum Webbrowser (auch als Client bezeichnet) des Endnutzers übermittelt werden. Ist das Übertragungsprotokoll auf diese Weise abgesichert, wird es als HTTPS (Hypertext Transfer Protocol Secure, sicheres Hypertext-Übertragungsprotokoll) in der Adresszeile des Browsers gekennzeichnet. TLS dient aber darüber hinaus auch der Verschlüsselung anderer digitaler Kommunikationswege, so insbesondere bei der Übertragung von Daten zwischen einem E-Mail-Server und dem E-Mail-Client des Nutzers (zum Beispiel mittels POP3, der zurzeit standardmäßigen dritten Version des Post Office Protocol; die Verschlüsselung via TLS wird als POP3S gekennzeichnet). TLS kommt zum Tragen, wenn der Client (z.B. der Webbrowser) des Nutzers eine Verbindung zu einem Server (z.B. dem Webserver) aufbaut. Der Server identifiziert sich gegenüber dem Client mit einem Zertifikat, welches vom Client auf Vertrauenswürdigkeit überprüft wird. Geprüft wird auch, ob der Name des Servers und der im Zertifikat angegebene Name identisch sind. Ist dies der Fall, wird mittels eines asymmetrischen Verfahrens ein kryptographischer Schlüssel erstellt und ausgetauscht. Anhand dieses Schlüssels wird im Anschluss die gesamte Kommunikation zwischen Client und Server mit einem symmetrischen Verfahren verschlüsselt.[88] Die notwendigen (Webseiten-)Zertifikate (sogenannte TLS-Zertifikate) werden durch sogenannte Vertrauensdiensteanbieter ausgegeben, für deren Aufsicht nach der europäischen eIDAS-Verordnung seit dem 1. Juli 2016 in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig ist.[89]

Angriffe auf Verschlüsselungsverfahren

Selbst Ende-zu-Ende-Verschlüsselung kann von sich aus keine hundertprozentige Sicherheit garantieren. Zum einen müssen natürlich die Endgeräte der an der Kommunikation beteiligten Personen ausreichend gegenüber Angriffen durch Hacker gesichert sein. Gelingt es Dritten, sich hier Zugang zu verschaffen, so können sie die privaten, geheimen Schlüssel abgreifen und damit die Verschlüsselung der Kommunikation unterminieren. Darüber hinaus können sie die Inhalte der versendeten Nachrichten einsehen, sofern sie nach Abschluss des Kommunikationsvorgangs unverschlüsselt auf der Festplatte des Nutzers gespeichert sind. Zum anderen besteht beim Einsatz asymmetrischer oder hybrider

[87] Ebd.
[88] Vgl. Wikipedia, Transport Layer Security (TLS), https://de.wikipedia.org/wiki/Transport_Layer_Security.
[89] Bundesamt für Sicherheit in der Informationstechnik, Qualifizierung als Vertrauensdiensteanbieter, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/VDA_Qualifizierung/VDA_Qualifizierung_node.html.

Verschlüsselung die Gefahr sogenannter Man-in-the-Middle-Angriffe. Darunter versteht man Angriffe, bei denen ein Dritter sich als der Empfänger der Nachricht ausgibt – indem er den öffentlichen Schlüssel des eigentlich vorgesehenen Empfängers durch seinen eigenen ersetzt – so dass die Nachricht mittels eines Schlüssels verschlüsselt wird, der dem Dritten bekannt ist. Nachdem dieser die Nachricht auf diese Weise lesbar gemacht und verwertet hat, kann er sie mit dem öffentlichen Schlüssel des eigentlichen Empfängers verschlüsseln und an diesen weiterleiten, so dass der Angriff unentdeckt bleiben kann.[90] Um dies zu verhindern, erzeugen manche Verschlüsselungsprogramme einzigartige und einmalige Zeichenfolgen, die auf den öffentlichen Schlüsseln der Kommunikationspartner basieren. Vor Beginn der verschlüsselten Kommunikation können Sender und Empfänger die Zeichenfolge über einen zweiten Kanal vergleichen. Stimmt sie überein, können sie mit hoher Wahrscheinlichkeit davon ausgehen, dass es keinen „Man in the Middle" gibt.[91]

Ein weiteres Problem bei der Verschlüsselung von digitaler Kommunikation sind sogenannte Backdoors: bewusst in den Programmcode geschriebene Sicherheitslücken, die dafür sorgen, dass beispielsweise Strafverfolgungsbehörden oder Geheimdienste im Bedarfsfall auf die Inhalte der Kommunikation mit bzw. zwischen Verdächtigen oder aus anderen Gründen zu überwachenden Personen zugreifen können.[92] Solche Maßnahmen werden insbesondere nach terroristischen Anschlägen immer wieder gefordert, weil viele Terrororganisationen bevorzugt auf solche Messenger-Anwendungen zurückgreifen, die Ende-zu-Ende-Verschlüsselung anbieten.[93] Experten warnen allerdings seit Längerem, dass solche Backdoors praktisch nicht in dem Sinne „sicher" implementiert werden können, dass sie nicht zugleich auch von weiteren Akteuren ausgenutzt werden können, um die Sicherheit des digitalen Kommunikationsmittels zu kompromittieren. Dadurch werde die staatliche Maßnahme zu einem Sicherheitsrisiko für sämtliche Nutzer.[94]

Standards für die Verschlüsselung von E-Mails

Die beiden Standards OpenPGP und S/MIME für eine Ende-zu-Ende-Verschlüsselung bei E-Mails setzen auf eine hybride Verschlüsselung, um sowohl sicher als auch ausreichend schnell zu sein. Ein Nutzer, der diese Verschlüsselung zum ersten Mal einsetzen will, muss sich seinen öffentlichen Schlüssel beglaubigen lassen, damit dieser ihm zur Erschwerung von Man-in-the-Middle-Angriffen eindeutig zugeordnet werden kann. Bei S/MIME übernimmt dies für gewöhnlich eine Zertifizierungsstelle,[95] während bei OpenPGP

[90] Das analoge Äquivalent hierzu ist das Abfangen, spurlose Öffnen und anschließende Wiederverschließen eines Briefes, wie es beispielsweise das Ministerium für Staatssicherheit der DDR praktizierte; vgl. Hanna Labrenz-Weiß, Abteilung M, MfS-Handbuch, Berlin 2005, S. 28, http://www.bstu.bund.de/DE/Wissen/Publikationen/Publikationen/handbuch_abt-m_labrenz-weiss.pdf?__blob=publicationFile.
[91] Andy Greenberg, Hacker Lexicon: What Is End-to-End Encryption?, Wired.com, 25. November 2014, https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.Greenberg.
[92] Bruce Schneier u.a., A Worldwide Survey of Encryption Products, The Berkman Center for Internet & Society at Harvard University, Research Publication No. 2016-2, 11. Februar 2016, S. 6, http://ssrn.com/abstract=2731160.
[93] Siehe jüngst z.B. in Bezug auf Telegram: Rebecca Tan, Terrorists' Love for Telegram, Explained, Vox, 30. Juni 2017, https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter.
[94] Harold Abelson u.a., Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, Journal of Cybersecurity, 2015, S. 1.
[95] Siehe Wikipedia, E-Mail-Verschlüsselung, https://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung.

diese Funktion durch „Web of Trust“ realisiert wird. Das bedeutet, dass jeder Teilnehmer den öffentlichen Schlüssel eines anderen Teilnehmers verifizieren kann. Diese gegenseitigen Bestätigungen sollen dafür sorgen, dass die Echtheit der öffentlichen Schlüssel aller Teilnehmer garantiert ist.[96]

Kombination von geschlossenen Systemen und E-Mail

Einige Anbieter von E-Mail-Diensten versuchen, das Dilemma zwischen der leichteren Implementierung eines höheren Verschlüsselungsstandards bei geschlossenen Systemen und der Notwendigkeit, weiterhin Nachrichten an Nutzer schicken zu können, die einen anderen E-Mail-Dienst verwenden, durch eine Kombination der Verfahren zu lösen.

Eines der bekannteren Beispiele hierfür ist der schweizerische Dienst ProtonMail, der auf der PGP-Architektur aufbaut.[97] Sendet ein ProtonMail-Nutzer eine Nachricht an einen Empfänger, der ebenfalls diesen Dienst verwendet, so ist die E-Mail automatisch via asymmetrische Verschlüsselung auf dem gesamten Weg, also Ende-zu-Ende, verschlüsselt. Von den Verschlüsselungsprozessen bekommen die Nutzer nichts mit, sie laufen unsichtbar im Hintergrund ab.[98] Zwischen ProtonMail-Nutzern funktioniert der Dienst im Hinblick auf die Verschlüsselung also ganz ähnlich wie die geschlossenen Messenger-Dienste. Damit handelt es sich bei dieser Anwendung um ein Beispiel für sogenannte Security by Design, also eine Software, bei deren Entwicklung der Sicherheitsaspekt von vornherein einen integralen Bestandteil darstellte.[99]

Soll hingegen eine E-Mail an einen Nutzer gesendet werden, der nicht ProtonMail benutzt, sondern einen anderen E-Mail-Dienst wie zum Beispiel GMX, Yahoo oder Gmail, kann die asymmetrische Verschlüsselung nicht zum Einsatz kommen. Will der Nutzer eine gewöhnliche E-Mail ohne besonders sensible Inhalte verschicken, dann kann er ProtonMail nutzen wie jeden anderen Dienst auch – das heißt, die Nachricht wird auf normalem Wege vom ProtonMail-Server zum Server des Dienstes des Empfängers verschickt und mittels Transportverschlüsselung abgesichert. Handelt es sich hingegen um eine E-Mail mit sensiblen Inhalten, besteht die Option, auf ein symmetrisches Verschlüsselungsverfahren zurückzugreifen, um eine Ende-zu-Ende-Verschlüsselung zu erreichen. Dazu verschlüsselt der ProtonMail-Nutzer die von ihm verfasste E-Mail vor dem Versand mittels einer entsprechenden Funktion im E-Mail-Programm des Dienstes und legt ein Passwort fest. Wie bei symmetrischer Verschlüsselung üblich, muss dieses Passwort dem Empfänger auf einem sicheren Wege mitgeteilt werden. Zugleich erhält dieser eine E-Mail, die einen Link zu der Webseite von ProtonMail enthält. Klickt er auf diesen Link, gelangt er zu einer Eingabemaske, in der er das zuvor erhaltene Passwort eingeben muss. Ist dieser Vorgang

[96] Wikipedia, Web of Trust, https://de.wikipedia.org/wiki/Web_of_Trust.
[97] Swati Khandelwal, The Best Way to Send and Receive End-to-End Encrypted Emails, The Hacker News, 18. März 2016, http://thehackernews.com/2016/03/the-best-way-to-send-and-receive-end-to.html.
[98] ProtonMail, What Is End-to-End Encryption?, 4. Mai 2015, https://protonmail.com/blog/what-is-end-to-end-encryption/.
[99] Vgl. Niklaus Schild, Sichere Softwareentwicklung nach dem „Security by Design“-Prinzip, Heise Online, 19. August 2009, https://www.heise.de/developer/artikel/Sichere-Softwareentwicklung-nach-dem-Security-by-Design-Prinzip-403663.html.

erfolgreich, wird der Inhalt der E-Mail anschließend lokal auf dem Endgerät des Empfängers entschlüsselt.[100] Hinzu kommt schließlich, dass E-Mails, die der ProtonMail-Nutzer von Nutzern anderer Dienste empfängt, beim Eingang auf dem Server automatisch mittels des öffentlichen Schlüssels des Nutzers verschlüsselt und so gespeichert werden.

Online-Dokumentenablage

Das De-Mail-Gesetz sieht für akkreditierte Diensteanbieter ausdrücklich die Möglichkeit vor, auch als Online-Dokumentenablage zu fungieren. Wenn dieser Dienst angeboten wird, dann hat der Anbieter nach § 8 Satz 3 des Gesetzes alle eingestellten Dokumente verschlüsselt abzulegen. Obwohl bislang noch keiner der vom BSI akkreditierten De-Mail-Dienste die Möglichkeit, einen solchen „De-Safe“ anzulegen, anbietet,[101] kann aus dieser Vorschrift doch zumindest in der Tendenz eine gesetzgeberische Wertung herausgelesen werden, dass Dokumente mit sensiblen Informationen über Bürger bzw. Kunden, die auf Servern gespeichert werden, verschlüsselt werden sollten.

Signaturen: technische und rechtliche Details

Signaturen werden für gewöhnlich mittels asymmetrischer Verschlüsselungsverfahren erstellt. Dazu wird ein sogenannter Hashwert (Prüfsumme) aus der zu sendenden Nachricht gebildet und anschließend mit dem privaten Schlüssel des Versenders signiert. Nachricht und Signatur werden zusammen verschickt. Der Empfänger prüft die Signatur des Hashwerts mittels des öffentlichen Schlüssels des Versenders und ist somit in der Lage, die Signatur zu verifizieren. Ist dies erfolgreich, so kann der Empfänger davon ausgehen, dass die Nachricht tatsächlich vom Sender, also dem Besitzer des privaten Schlüssels, stammt, und dass sie während der Übermittlung nicht verändert wurde.[102] Die beiden bereits genannten asymmetrischen Verschlüsselungsstandards OpenPGP und S/MIME unterstützen diese Methode der Erzeugung elektronischer Signaturen.

Das Signaturgesetz definiert verschiedene Arten von elektronischen Signaturen. Den höchsten Sicherheitsstandard weisen die sogenannten qualifizierten elektronischen Signaturen (QES) auf, die auf qualifizierten Zertifikaten beruhen. Diese Zertifikate dienen dazu, die Gültigkeit der verwendeten Signaturprüfschlüssel zu bestätigen und sie eindeutig einer natürlichen Person und ihrer Identität zuzuordnen. Sie werden durch Zertifizierungsdiensteanbieter vergeben, die wiederum bestimmte, nach Signaturgesetz und -verordnung vorgegebene Anforderungen erfüllen müssen. Die Anbieter unterliegen der Aufsicht der Bundesnetzagentur und können sich bei dieser akkreditieren lassen, um öffentlich bestätigt zu bekommen, dass sie die gesetzlichen Anforderungen erfüllen.[103]

---

[100] Ebd.
[101] Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/Akkreditierte_DMDA/Akkreditierte_DMDA.html.
[102] Vgl. Wikipedia, Asymmetrisches Kryptosystem, https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem.
[103] Vgl. Wikipedia, Signaturgesetz (Deutschland), https://de.wikipedia.org/wiki/Signaturgesetz_(Deutschland).

Neben der reinen Ausweisfunktion im Internet hat der neue deutsche Personalausweis auch eine elektronische Unterschriftsfunktion. Um diese nutzen zu können, muss der Besitzer ein Signaturzertifikat bei einem der Vertrauensdienste erwerben und auf die Ausweiskarte laden. Zusätzlich wird ein Lesegerät benötigt, das an den eigenen Computer angeschlossen wird.[104] Während in Deutschland die Nutzung der elektronischen Funktionen des neuen Personalausweises auch wegen Datenschutzbedenken nach Angaben des Bundesinnenministeriums bislang eher die Ausnahme darstellt,[105] sind vergleichbare Mechanismen beispielsweise in Estland gesetzlich verpflichtend und werden von den Bürgern angenommen.[106] Über das dort entwickelte „X-Road"-System, das den sicheren, verschlüsselten Datenaustausch zwischen den estnischen Bürgern und öffentlichen Stellen, aber auch privatwirtschaftlichen Unternehmen ermöglicht, können nicht nur Behördenangelegenheiten, sondern gerade auch private Geschäfte abgewickelt werden. Um das System zu nutzen, melden sich die Bürger mittels ihres elektronischen Personalausweises an und verwenden zur Erledigung von Geschäften seine Signaturfunktion.[107]

Die Anmeldefunktion für Internetdienste ist auch in Deutschland für den elektronischen Personalausweis vorgesehen. So ist es beispielsweise möglich, sich bei De-Mail-Diensten online mit der eID-Funktion des Personalausweises auszuweisen. Das gilt sowohl für die erstmalige Registrierung, die zwingend eine eindeutige Identifikation des Nutzers voraussetzt, als auch für den anschließenden gewöhnlichen Login am De-Mail-Konto. Dadurch wird eine Anmeldung mit „hohem Sicherheitsniveau" gewährleistet, was für die Nutzung vieler der besonderen Dienste von De-Mail Voraussetzung ist.[108]

Sicherheit von Passwörtern und Zwei-Faktor-Anmeldung

Viele Experten vertreten inzwischen die Ansicht, Passwörter sollten aufgrund ihrer inhärenten Unsicherheit mittelfristig der Vergangenheit angehören.[109] Trotzdem sind sie bislang noch immer weit verbreitet und oft sogar der einzige Schutzwall. Es wird heute allgemein empfohlen, lange, komplexe und einzigartige Passwörter auszuwählen. Das Bundesamt für Sicherheit in der Informationstechnik hat diesbezüglich eine Handreichung ver-

[104] Bundesministerium des Innern, Die elektronischen Funktionen des Personalausweises, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Funktionen/funktionen_node.html.
[105] Ingo Dachwitz, Im Gesetz zum elektronischen Personalausweis versteckt sich ein automatisierter Abruf für Geheimdienste, Netzpolitik.org, 24. April 2017, https://netzpolitik.org/2017/im-gesetz-zum-elektronischen-personalausweis-versteckt-sich-ein-automatisierter-abruf-fuer-geheimdienste/.
[106] Sabine Adler, E-Government macht das Leben leichter, Deutschlandfunk, 24. Mai 2016, http://www.deutschlandfunk.de/estland-e-government-macht-das-leben-leichter.1766.de.html?dram:article_id=355026; allerdings ist in diesem Zusammenhang darauf hinzuweisen, dass eine solche Implementierung in Estland unter anderem dadurch deutlich vereinfacht waren, dass das Land nur 1,3 Millionen Einwohner hat und zudem seine gesamte Verwaltungsinfrastruktur nach der Unabhängigkeit 1990 neu aufbauen musste und somit frühzeitig auf Digitalstrategien setzen konnte. Diese Bedingungen lassen sich in Deutschland so nicht abbilden.
[107] Eric Jaffe, How Estonia Became a Global Model for E-Government, Sidewalk Talk, 20. April 2016, https://medium.com/sidewalk-talk/how-estonia-became-a-global-model-for-e-government-c12e5002d818.
[108] Bundesministerium des Innern, Gute Kombination für mehr Sicherheit im Internet, http://www.personalausweisportal.de/DE/Wirtschaft/Anwendungsbeispiele/De-Mail/De-Mail_node.html.
[109] Hakan Tanriverdi, Warum Passwörter abgeschafft werden müssen, Sueddeutsche.de, 9. Juni 2016, http://www.sueddeutsche.de/digital/it-sicherheit-warum-passwoerter-abgeschafft-werden-muessen-1.3026987.

öffentlicht, die eine Reihe von Tipps für ein gutes Passwort aufführt.[110] Manche Anbieter digitaler Kommunikationsmittel sind aus diesem Grund dazu übergegangen, es mit technischen Mitteln zu verhindern, dass Nutzer zu einfache Passwörter bei der Anmeldung zum Dienst einstellen.[111]

Und während einige Experten inzwischen nicht mehr dazu raten, die verwendeten Passwörter regelmäßig zu ändern, sollte dies unverzüglich geschehen, wenn es einen erfolgreichen Hacker-Angriff auf den genutzten Dienst gegeben hat, da es den kriminellen Akteuren bei solchen Sicherheitsvorfällen zumeist darum geht, Kundendaten einschließlich der Passwörter abzufischen.[112] Im Fall der Passwörter ist es in diesem Zusammenhang entscheidend, wie das betroffene Unternehmen mit den Passwörtern intern umgegangen ist, ob diese also im Klartext oder im Sinne einer guten Praxis beispielsweise als Hash[113] gespeichert worden sind.

Das Verfahren der Zwei-Faktor-Anmeldung gilt als wesentlich sicherer, erfordert aber seitens des Nutzers auch einen größeren Aufwand. Neben der Eingabe eines Passworts als erster Faktor der Absicherung erfolgt eine weitere Abfrage. Zumeist geschieht diese mittels SMS an das Mobiltelefon des Nutzers, die eine einmalige Session-TAN enthält (TAN: transaction authentification number, Transaktionsnummer). Diese Nummer ist ebenfalls einzugeben, bevor der Nutzer auf das Postfach oder Portal zugreifen kann. Mitunter wird die TAN über einen anderen Weg gesendet, beispielsweise per E-Mail oder an eine App des Mobiltelefons. Auch bei einem Fingerabdruckscanner, der nach der Passworteingabe zum Einsatz kommt (und nicht bloß an dessen Stelle), handelt es sich um einen solchen zweiten Faktor.[114] Höhere Sicherheit entsteht dadurch, dass es für Hacker oder sonstige unbefugte Dritte nicht ausreicht, an das Passwort für den Zugang zu gelangen. Ohne einen physischen Zugriff auf das Mobiltelefon oder das sonstige Gerät, das für die Zwei-Faktor-Anmeldung verwendet wird, bleibt das Postfach oder Portal geschützt. Inzwischen bieten immer mehr E-Mail-Dienste dieses Verfahren an, allerdings stets nur als Option für die Nutzer, nicht verpflichtend.[115]

---

[110] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html.
[111] Siehe z.B. beim E-Postbrief der Deutschen Post, https://www.epost.de/privatkunden/sicherheit.html#sicherheit-und-verschluesselungstechniken.
[112] Simon Hurtz, Warum es falsch ist, Passwörter regelmäßig zu ändern, Sueddeutsche.de, 20. Januar 2017, http://www.sueddeutsche.de/digital/it-sicherheit-warum-es-falsch-ist-passwoerter-regelmaessig-zu-aendern-1.3106648.
[113] Sogenannte Hashfunktionen sind Abbildungen, die eine große Eingabemenge (die Schlüssel, in diesem Fall die Passwörter) auf eine kleinere Zielmenge abbildet; letztere sind die sogenannten Hashwerte. Passwörter können gehasht werden, um sie sicher zu speichern; vgl. Wikipedia, Hashfunktion, https://de.wikipedia.org/wiki/Hashfunktion.
[114] Morten Luchtmann, So sichern Sie Ihre Konten bei Facebook, Amazon und Google, Sueddeutsche.de, 29. Juni 2016, http://www.sueddeutsche.de/digital/passwort-sicherheit-so-sichern-sie-ihre-konten-bei-facebook-amazon-und-google-1.3055333.
[115] Siehe z.B. bei Yahoo Mail, https://de.hilfe.yahoo.com/kb/SLN5013.html.