DIVSI
Deutsches Institut
für Vertrauen und
Sicherheit im Internet

Vertrauen in Kommunikation im digitalen Zeitalter

www.divsi.de

Vertrauen in Kommunikation im digitalen Zeitalter

Projektbericht

Eine Untersuchung des iRights.Lab im Auftrag des
Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI)

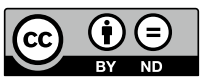
DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet

iRights.Lab

Hamburg, November 2017

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Mittelweg 110 B
20149 Hamburg
www.divsi.de
Matthias Kammer, Direktor
Joanna Schmölz, Wissenschaftliche Leitung
Dr. Dirk Graudenz, Projektleitung

iRights.Lab
Almstadtstr. 9/11, 10119 Berlin
www.irights-lab.de
Philipp Otto, Projektleitung
Dr. Till Kreutzer, Autor
Henning Lahmann, Autor
Unter Mitwirkung von: Valie Djordjevic,
Wiebke Glässer, Eike Gräf, Julia Schrader



INHALTSVERZEICHNIS

Vertrauen in Kommunikation im digitalen Zeitalter

Gleichsam wie ein roter Faden ziehen sich die Begriffe Vertrauen und Sicherheit durch alle Bereiche der grenzenlosen Angebotspalette des Internets. Jeder, der aus welchen Gründen und wo auch immer online geht, erwartet bei einem geöffneten Portal, dass er diesem vertrauen kann, seine Daten dort geschützt sind und es auch bleiben – er sich insgesamt sicher fühlen darf.

Insoweit erleben die uralten Begriffe Vertrauen und Sicherheit gerade seit der Geburt unseres digitalen Zeitalters eine Renaissance. Für mich bilden sie praktisch das Fundament. Die Nutzer müssen darauf bauen können. Je weniger Skepsis bei ihnen vorhanden ist, umso stärker werden sie die unendliche Bandbreite des Internets nutzen. Dieses gilt selbstverständlich nicht nur für Kaufangebote oder andere kommerzielle Spielfelder. Dieses gilt gleichermaßen auch für die zunehmenden Möglichkeiten digitaler Kontakte mit Behörden oder Versorgern.

Der Convenience-Gedanke spielt im zunehmend digitalen Alltag eine große Rolle. Hauptsache bequem, es wird schon nichts Böses passieren, warum soll es gerade mich treffen? Wer will schon hören, dass Cybercrime eine absolut boomende Branche ist und auch Unternehmen immer wieder riesige Datenlecks abdichten müssen.

Vor diesem Hintergrund schien es uns höchste Zeit, nach Wegen zu suchen, die das „Vertrauen in Kommunikation im digitalen Zeitalter" auf eine neue, höhere Ebene heben können. Zwar gehören digitale Kommunikationsmittel für die meisten heute zum Alltag. Eine von uns mit dimap kürzlich realisierte Studie zeigt jedoch, dass eine überwiegende Mehrheit der deutschen Bevölkerung mit dem aktuellen Zustand unzufrieden ist. Dies gilt insbesondere dann, wenn der Einzelne gegenüber Behörden oder Unternehmen eigene, sensible Daten preisgeben soll.

Gerade staatliche Stellen dürften es schwer haben, ihre Angebote einer breiten Öffentlichkeit schmackhaft zu machen, wenn dort kein tiefes Vertrauen vorherrscht. Es verwundert nicht, dass die Menschen mehrheitlich sensible persönliche Nachrichten lieber klassisch-haptisch zugestellt bekommen möchten als über digitale Wege, wie eine weitere DIVSI-Untersuchung gezeigt hat.

Wie also einen Weg finden, den beide Seiten – Nutzer und Anbieter – gemeinsam gehen kön-

Foto: Frederike Heim

Matthias Kammer
Direktor
DIVSI – Deutsches Institut für Vertrauen
und Sicherheit im Internet

nen? Die Untersuchung findet hierfür die folgenden grundsätzliche Überlegungen für eine künftige sichere digitale Kommunikation. Inhaltlich besagen diese:

Rechtliche, technische und organisatorische Aspekte sollten miteinander verbunden werden. Neue Maßnahmen greifen nur in einem übergeordneten Verbund. Dieser so gewährleistete Sicherheitsstandard muss den Menschen gegenüber transparent sein. Gleichzeitig ist darauf zu achten: Ein Plus an Sicherheit darf nicht durch ein Minus an Nutzerfreundlichkeit geschaffen werden.

Ausdrücklich unterstreicht die Untersuchung die unveränderte Bedeutung analoger Kommunikationsmittel. Tatsächlich scheint es mir eine Art von Arroganz zu sein, wenn Internetexperten unterstellen, jeder sei mit der digitalen Kommunikation glücklich und vertraut.

Bereits diese knappe Vorschau auf die grundsätzlichen Gedanken, in die der hier präsentierte Bericht mündet, verdeutlicht die Komplexität der Aufgabe. Skeptiker mögen fragen, ob sich all das tatsächlich in die Praxis umsetzen lässt. Ich meine, sicherlich nicht im Alleingang einzelner Beteiligter. Das notwendige gesteigerte Vertrauen in digitale Kommunikation wird sich nur in einem Zusammenwirken von Staat, Wirtschaft und der Zivilgesellschaft erreichen lassen. Vor allem sollte möglichst rasch ein Anfang gemacht werden. Eine Aufgabe, der sich auch der neu formierte Bundestag nachdrücklich widmen könnte.

Positive Aktivitäten scheinen mir dringend geboten. Diese Untersuchung steuert dazu nicht nur Anregungen bei. Sie bietet darüber hinaus Anstöße, die ein Nachdenken sicherlich lohnen. Ich freue mich über jedes Feedback, natürlich auch und besonders über kritische Ansätze. Denn nur Vielfalt wird uns letzten Endes die erforderlichen Parameter liefern, aus der zum Wohle aller jener Weg gefunden wird, der zum gesteigerten Vertrauen in Kommunikation im digitalen Zeitalter führt.

Parameter für Vertrauen in die digitale Kommunikation

„Durch Schrift wird Kommunikation aufbewahrbar, unabhängig von dem lebenden Gedächtnis von Interaktionsteilnehmern."

Niklas Luhmann, Soziale Systeme, 1984

Kommunikation spielt eine zentrale Rolle im Zusammenleben von Menschen. Wie kaum ein anderes Element durchzieht sie alle gesellschaftlichen Bereiche. Durch ihre Verschriftlichung verändert sich die Dimension von Kommunikation. Die Inhalte werden – wie Luhmann feststellt – gespeichert und festgehalten.

Unsere Kommunikationsmöglichkeiten und -mittel haben sich im historischen Verlauf immer wieder stark gewandelt. Galt Mitte des 19. Jahrhunderts noch das Telegrafenkabel als große Innovation und Beginn der modernen Kommunikation, treten wir heute mit unseren Smartphones ohne Probleme mit Freunden und Familie über Landesgrenzen hinweg in Kontakt und tauschen in Sekundenschnelle Nachrichten oder Fotos aus.

Mit der Digitalisierung haben sich unsere Kommunikationsmöglichkeiten enorm schnell verändert. Diese Dynamik betrifft nicht nur unseren Austausch im privaten Bereich, sondern auch mit Unternehmen wie Banken oder auch Behörden, die zunehmend digitale Kommunikationswege anbieten. Das ist eine große Bereicherung. Wir warten nicht mehr tagelang auf Antworten, die E-Mails von Geschäftspartnern treffen vielmehr innerhalb kürzester Zeit auf unseren Rechnern ein. Gleichzeitig wirft diese Entwicklung auch neue Fragen auf.

Die Rahmenbedingungen und Strukturen, die unsere Kommunikation schützen sollen, sind nicht so schnell mitgewachsen, wie es wünschenswert wäre. Neben allen Vorteilen birgt die Digitalisierung der Kommunikation auch Möglichkeiten des

Foto: Andi Weiland

Philipp Otto
Direktor Think Tank iRights.Lab

Missbrauchs. Die Nutzer und Nutzerinnen sind zunehmend unsicher, wer ihre Kommunikation mitlesen kann, für wen und bei wem sie im Luhmann'schen Sinne aufbewahrt wird. An diesem Punkt setzt diese Publikation an und fragt danach, wie es um unser Vertrauen in die digitale Kommunikation bestellt ist und unter welchen Bedingungen ein Vertrauen überhaupt gerechtfertigt sein kann.

Ohne zu viel vom Ergebnis unserer Ausarbeitungen vorwegzunehmen, ist es offensichtlich, dass es dringend notwendig ist, das Vertrauen in digitale Kommunikationsmittel zu stärken. In der Publikation wird eruiert, welche politischen, technischen, rechtlichen, aber auch gesellschaftlichen Voraussetzungen erfüllt sein müssen, um die Sicherheit und Authentizität der digitalen Kommunikation zu gewährleisten und damit auch das Vertrauen der Nutzerinnen und Nutzer wiederherzustellen beziehungsweise zu stärken.

Sie finden in der Publikation Hintergrundinformationen und Analysen zu diesen Fragen. Wir haben zahlreiche Experten aus Wirtschaft, Politik, Gesellschaft und Wissenschaft befragt und ihre Einschätzungen mit berücksichtigt. Die Publikation liefert Ihnen neue Perspektiven auf ein Thema, das uns als Gesellschaft wichtig sein sollte und bei dem es sich lohnt, gemeinsam mit allen Stakeholdern zu diskutieren und an Lösungen zu arbeiten.

Zusammenfassung

Der vorliegende Bericht zum Projekt „Vertrauen in digitale Kommunikation" befasst sich mit der Frage, wie digitale Kommunikationsmittel, die zunehmend den Alltag bestimmen, im Angesicht von immer wieder auftretenden Sicherheitsbrüchen, Datenschutzvorfällen und Überwachungsskandalen so ausgestaltet werden können, dass Nutzerinnen und Nutzer ihnen das notwendige Vertrauen entgegenbringen können.

Das Projekt geht von der Grundannahme aus, dass ein Bedürfnis nach geschützter und damit vertrauenswürdiger Kommunikation in bestimmten Kommunikationsverhältnissen besteht. Doch obwohl digitale Kommunikationsmittel für die meisten heute zur Selbstverständlichkeit geworden sind, legen die Ergebnisse jüngster Befragungen nahe, dass Nutzerinnen und Nutzer mit dem gegenwärtigen Zustand unzufrieden sind, soweit es darum geht, sensible Informationen mit Unternehmen oder Behörden auf elektronischem Wege auszutauschen. Es fehlt bei vielen an Vertrauen, dass die übermittelten und im Netz gespeicherten persönlichen Informationen ausreichend vor Missbrauch geschützt sind.

Vertrauen in solche Kommunikationsvorgänge erfüllt eine ganz entscheidende Funktion. Sie liegt darin, dass die mitteilende Person mit hinreichender Sicherheit voraussagen kann, was mit den übermittelten Daten und Informationen geschieht und ob und inwieweit sie vor dem Zugriff durch Akteure, die nicht unmittelbar an dem Vorgang beteiligt sind und die nicht legitimiert sind oder die die mitteilende Person nicht legitimiert hat, geschützt sind.

Die Erwartungen der Nutzerinnen und Nutzer in vertrauenswürdige Kommunikation lassen sich wie folgt zusammenfassen:

- Die Daten und Informationen, die sie übermitteln, müssen so weit geschützt sein, dass sie nicht in die Hände Krimineller oder generell unbefugter Dritter geraten;
- die Daten und Informationen dürfen von den Informationsempfängern nicht zum unmittelbaren Nachteil der Nutzerinnen und Nutzer verwendet werden;
- einzelne, sensible Informationen dürfen nicht der allgemeinen Öffentlichkeit zugänglich gemacht werden;
- der Akteur (d.h. die Person bzw. das Unternehmen oder die staatliche Stelle), mit dem kommuniziert wird, muss auch tatsächlich derjenige sein, für den er sich ausgibt;
- die übermittelten Informationen dürfen nicht verfälscht worden sein;
- die versandte Nachricht muss tatsächlich und innerhalb kurzer Zeit den Empfänger erreichen.

Phänomene wie steigende Internetkriminalität, Datenlecks

bei Unternehmen oder staatliche Überwachungstätigkeit im Netz haben in den vergangenen Jahren zu einer Erosion des Vertrauens in digitale Kommunikation geführt. Zugleich lässt sich jedoch beobachten, dass die meisten Menschen trotz mangelnden Vertrauens weiter ständig digitale Kommunikationsmittel für jede Art der Kommunikation, mit sensiblen Inhalten oder ohne, nutzen. Das deutet darauf hin, dass entweder Gleichgültigkeit oder Fatalismus vorherrscht. Umfrageergebnisse zeigen allerdings nichtsdestotrotz, dass der Wunsch nach vertrauenswürdigen digitalen Kommunikationsmitteln weithin besteht.

GRUNDSÄTZE FÜR SICHERE DIGITALE KOMMUNIKATION

1. DIGITALE KOMMUNIKATION MIT SENSIBLEN INHALTEN SOLLTE SICHER UND VERLÄSSLICH SEIN.

Nur wenn ein Kommunikationsmittel als sicher und verlässlich 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 Akteuren 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 dem Akteur stammt, von der sie zu stammen scheint. Verlässlich ist ein Kommunikationsmittel unter anderem dann, wenn die gesendete Nachricht tatsächlich den Empfänger erreicht. Um die so definierte Sicherheit und Verlässlichkeit digitaler Kommunikation zu erreichen, sollten Maßnahmen umgesetzt werden, die rechtliche, technische und organisatorische Aspekte miteinander verbinden.

2. DIE EINGESETZTE TECHNOLOGIE SOLLTE NUTZERFREUNDLICH SEIN.

Digitale Kommunikationsmittel müssen auch nutzerfreundlich sein. Denn werden Kommunikationsmittel, obgleich sicher, mangels Nutzerfreundlichkeit nicht angenommen, können sie das Sicherheitsniveau vertraulicher digitaler Kommunikation nicht steigern. Der Sicherheitsaspekt 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 stets als Einheit gedacht und entsprechend zusammen realisiert werden.

3. DEM NUTZER GEGENÜBER SOLLTE DER GEWÄHRLEISTETE SICHERHEITSSTANDARD KOMMUNIZIERT 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 ihn betreffende sensible Informationen auf digitalem Wege übermittelt werden. Vertrauensfördernde Maßnahmen bieten sich hier insbesondere in Form der Vergabe und Veröffentlichung von anerkannten Gütesiegeln und Zertifikaten an. Die für die Vergabe zuständige Prüfinstanz muss unabhängig sein und selbst offene und transparente Prüfstandards zugrunde legen.

GRUNDSÄTZE FÜR SICHERE DIGITALE KOMMUNIKATION

4. DEM NUTZER SOLLTEN ALTERNATIVE – AUCH ANALOGE – KOMMUNIKATIONSMITTEL ANGEBOTEN WERDEN.

Solange nicht sämtliche Nutzer mit sicheren digitalen Kommunikationsmitteln umgehen können, muss gerade in bedeutenden Kommunikationsverhältnissen darauf geachtet werden, dass bis auf Weiteres 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.

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.

Die wünschenswerte Förderung digitaler Kommunikationsmittel darf nicht mit unmittelbaren Mehrkosten für den Nutzer verbunden sein. Das bedeutet einerseits, dass digitale Angebote nicht kostenpflichtig sein sollten, wenn die entsprechenden analogen Kommunikationswege (bislang) kostenfrei waren. Umgekehrt sollte eine analoge Alternative nicht plötzlich mit finanziellem Aufwand verknüpft sein, wenn sie vor Einführung des digitalen Kommunikationsmittels den Nutzer nichts gekostet hatte. Nutzer haben nur dann tatsächlich Wahlfreiheit des Kommunikationsmittels, wenn keine der Optionen in Bezug auf die Kosten diskriminiert.

Auf die so formulierten fünf Grundsätze für sichere digitale Kommunikation folgt abschließend die Frage, wie diese in die Praxis übertragen werden können. Zu fordern ist in diesem Sinne eine konzertierte Anstrengung von Staat, Wirtschaft und zivilgesellschaftlichen Akteuren mit dem Ziel, die folgenden fünf auf den Grundsätzen aufbauenden Maßnahmen umzusetzen:

- Erhöhung des Sicherheitsniveaus durch Implementierung von Security by Design seitens der Dienstleister im Sinne der jeweils aktuellen Verschlüsselungstechnologien;
- nutzerfreundliches, intuitiv zu handhabendes Design für Sicherheitslösungen;
- Sicherstellung einer diskriminierungsfreien Wahlmöglichkeit zwischen analoger und digitaler Kommunikation;
- Schaffung von Bündelungsmöglichkeiten für digitale Kommunikation mit sensiblen Inhalten, z. B. in Form eines geeigneten Standards zur Sicherstellung von Interoperabilität sowie von Portalen, die diesen Standard umsetzen;
- Auszeichnung teilnehmender Unternehmen durch Siegel oder Zertifikate, die es ermöglichen, dass die Erfüllung der entsprechenden Kriterien als Wettbewerbsvorteil wirkt.

1. Auftakt

Frau Schmidt, 46 Jahre alt, fühlt sich wohl im Internet. Schon längst ist die Nutzung digitaler Technologien für sie zum selbstverständlichen Teil ihres Alltags geworden. Sie sind doch auch so ungemein praktisch: Anstatt wöchentlich zur Bank laufen zu müssen, erledigt sie ihre Kontogeschäfte bequem über ein Online-Portal. Überweisungen tätigen, Kontoauszüge einsehen – alles kein Problem und innerhalb weniger Minuten vom Schreibtisch aus erledigt. So bleibt einfach mehr Zeit für wichtigere Dinge. Auch mit ihrer Krankenkasse kommuniziert Frau Schmidt eigentlich nur noch über das Netz. Wenn sie Fragen zu einer Kassenleistung hat, kann sie direkt auf der Webseite mit einer Kundendienstmitarbeiterin chatten. Mitgliedsbescheinigungen und sonstige Dokumente, die ihren Vertrag mit der Kasse betreffen, werden ihr neuerdings in ein Online-Postfach im Kundenportal der Krankenkasse zugestellt, auf dem sie sich mittels Passwort und einer TAN, die sie per SMS auf ihr Mobiltelefon geschickt bekommt, anmelden kann. Das Design des Portals ist gut gemacht, Frau Schmidt ist mit der intuitiven Handhabung zufrieden. Es bereitet ihr keinerlei Probleme, die wichtigen Dokumente schnell zu finden und mit einem Klick herunterzuladen. Aber nicht nur Geschäfte mit privaten Dienstleistern erledigt sie zunehmend nur noch im Internet. Toll findet sie auch, dass sie sich für immer mehr Behördenangelegenheiten nicht mehr um einen Termin beim Amt kümmern muss. Ihren neuen Personalausweis konnte sie kürzlich über das Online-Bürgeramt ihrer Gemeinde beantragen.

Auch der 73-jährige Herr Schulz findet es im Großen und Ganzen toll, dass er für viele Besorgungen des täglichen Lebens nicht mehr das Haus verlassen muss. Nach ein paar Anfangsschwierigkeiten und mithilfe seiner Enkelkinder hat er inzwischen keinerlei Probleme mehr, Bankgeschäfte online zu erledigen. Auch mit seinen Versicherungen und Energieversorgern kommuniziert er neuerdings fast ausschließlich digital. Als ihm neulich beim Einkaufen auf dem Parkplatz des Supermarktes jemand eine Delle in sein Auto fuhr, konnte Herr Schulz den gesamten Vorgang von der Schadensmeldung bis zur Auszahlung über das Online-Portal seiner Kfz-Versicherung abwickeln. Um seinem Stromversorger den aktuellen Zählerstand zu übermitteln, muss er keine Postkarte mehr ausfüllen und zum Briefkasten bringen, es genügt ein Einloggen in das Kundenportal auf dessen Webseite. Hier kann er die letzten Stromrechnungen einsehen, vergleichen und herunterladen, um sie auf seinem Desktop-PC zu speichern. Und seit seine Tochter ihm erzählt hat, dass auch immer mehr Behörden Dienste über das Internet anbieten, nutzt er zunehmend Angebote des E-Governments. So beantragte er die Baugenehmigung für die neue Garage an seinem Ferienhaus an der Ostsee kürzlich ganz ohne Probleme online von zu Hause aus.

Doch obwohl Herr Schulz und Frau Schmidt die Vorzüge der digitalen Kommunikation mit Behörden, Banken, Versicherungen und anderen Dienstleistern im Alltag sehr wohl zu schätzen wissen, löst die zunehmende Verlagerung der Geschäfte ins Internet bei

beiden gleichzeitig ein diffuses Unbehagen aus. Ihnen ist bewusst, dass sie auf diese Weise immer mehr Spuren im Netz hinterlassen und teils sehr sensible Informationen auf digitalen Wegen übertragen, deren Schwachstellen sie im Einzelnen nicht kennen. Immer wieder hören sie von Datenschutzskandalen, aber was da so genau passiert, wer sich auf welchem Weg Einblick in persönliche Daten verschafft hat und was dann damit gemacht wurde, ist ihnen nicht klar. Bei der Übermittlung von finanziellen Informationen oder solchen über ihre Gesundheit sind sie zunehmend unsicher, und immer häufiger fragen sie sich, ob sie der Kommunikation über das Internet wirklich vertrauen können. Sind ihre persönlichen Informationen geschützt? Herrn Schulz macht vor allem die Überwachung durch staatliche Geheimdienste Sorgen, die 2013 durch die Enthüllungen des ehemaligen US-amerikanischen Geheimdienstmitarbeiters Edward Snowden ans Licht gekommen war.[1] Ist es wirklich so, dass die Regierungen im Internet alles mitlesen und jedenfalls theoretisch jeden seiner digitalen Schritte, von der Kommunikation mit der Autoversicherung bis hin zu E-Mails an seinen Urologen, nachverfolgen und auswerten können? Beim Gedanken daran, was das für Folgen für ihn haben könnte, wird ihm jedenfalls ganz unwohl.

Frau Schmidt wiederum misstraut vor allem den privaten Unternehmen, vom Sozialen Netzwerk über Suchmaschinen bis zu Banken und Versicherungen, von denen sie sicher ist, dass sie über eine Vielzahl sehr persönlicher Daten von ihr verfügen, selbst wenn sie ihnen diese sogar bewusst anvertraut hat. Gehen sie wirklich sorgfältig mit den sensiblen Informationen um, haben sie diese sicher gespeichert und missbrauchen sie auch nicht? Überdies hat sie in den vergangenen Jahren verschiedentlich in der Zeitung gelesen, dass Kundendaten wie Namen, Adressen, Telefonnummern und sogar Passwörter von Kriminellen abgefischt wurden. So ist ihr bewusst, dass es allein im Jahr 2016 weltweit über 4.000 Datenpannen bei Online-Unternehmen gab und Milliarden von Datenprofilen von Nutzerinnen und Nutzern gestohlen wurden.[2] Warum sollte das gerade denjenigen Unternehmen, denen sie ihre eigenen Daten anvertraut hat, nicht passieren? Würde sie davon überhaupt erfahren? Als sie neulich ihre E-Mail-Adresse beim „Leak-Checker" des Potsdamer Hasso-Plattner-Instituts eingab, um zu erfahren, ob sie selbst schon einmal von einem Online-Datendiebstahl betroffen war[3], musste sie mit Erschrecken feststellen, dass seit 2012 bereits zweimal sowohl ihre Postadresse wie auch ihre Telefonnummer von Hackern auf zwei verschiedenen Online-Diensten abgegriffen worden waren. Diese Erkenntnis hat ihr Vertrauen in digitale Kommunikation nicht gerade gestärkt.

Aber es sind nicht nur Internetkriminalität, Überwachung und Datenschutzskandale, die bei Frau Schmidt und Herrn Schulz ein schwer greifbares Misstrauen auslösen. Hinzu kommt ein stärker werdendes Gefühl der Überforderung. Denn obwohl die Online-Portale der meisten Dienstleister leicht zu bedienen und durchaus sinnvoll und übersichtlich gestaltet sind, ist es ihre schiere Anzahl, die beiden zunehmend Sorge bereitet. Beide sind inzwischen bei Dutzenden Unternehmen im Online-Kundenbereich registriert, wo wichtige Dokumente hinterlegt werden und Geschäftsangelegenheiten zu erledigen sind. Das bedeutet nicht nur, dass sie sich immer mehr Passwörter und Zugangsmethoden merken müssen. So viele Kommunikationskanäle im Auge behalten zu müssen, ist anstrengend und unübersichtlich. Auch stört es vor allem Herrn Schulz, dass sich die Beziehung zwischen den verschiedenen Dienstleistern und ihm schleichend umgekehrt hat. Es liegt nun an ihm, sich auf den Portalen einzuloggen, um die Dokumente beim Anbieter „abzuholen". Was passiert, wenn er eine E-Mail, die ihn darauf hinweist, dass eine wichtige Information für ihn auf einem Kundenportal vorliegt, übersieht? Muss er dann für die negativen Folgen einstehen? In solchen Momenten der Verunsicherung wünscht er sich doch die Zeit zurück, in der er solche Dokumente noch per Post in den Briefkasten neben seiner Haustür zugestellt bekam.

Doch was bleibt Herrn Schulz und Frau Schmidt anderes übrig? Die meisten Unternehmen haben mit mehr oder weniger sanftem Zwang dafür gesorgt,

1 Patrick Beuth, Alles Wichtige zum NSA-Skandal, Zeit Online, 28. Oktober 2013, http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal.
2 Kelly Sheridan, Data Breaches Exposed 4.2 Billion Records in 2016, Dark Reading, 25. Januar 2017, http://www.darkreading.com/attacks-breaches/data-breaches-exposed-42-billion-records-in-2016/d/d-id/1327976.
3 Siehe https://sec.hpi.de/leak-checker/search?.

dass sie inzwischen einen Großteil ihrer Kommunikation mit ihnen auf digitalem Wege erledigen. Frau Schmidts Bank verlangt inzwischen eine Servicegebühr, wenn sie sich ihre Kontoauszüge wie gehabt per Briefpost zuschicken lassen möchte. Der Abruf über das Online-Portal ist hingegen kostenlos. Der Stromanbieter von Herrn Schulz übernimmt nicht mehr das Porto für die Postkarte, auf der er früher den aktuellen Zählerstand eintrug. Stattdessen war ihm nahegelegt worden, online ein Kundenkonto anzulegen, um die Stände künftig direkt dort mitzuteilen. Da er eigentlich nicht bei noch mehr Anbietern im Netz seine persönlichen Informationen hinterlassen wollte und ihm insbesondere diese Umstellung nicht notwendig erschien, wäre er gerne beim analogen Kommunikationsweg geblieben. Fast schon fatalistisch fügte er sich schließlich, und nach kurzer Zeit dachte er auch schon gar nicht mehr weiter darüber nach. Sowohl er als auch Frau Schmidt finden es jedoch nicht gut, dass ihnen zunehmend die Möglichkeit genommen wird, zwischen analoger und digitaler Kommunikation frei wählen zu können.

2. Einleitung

Die beiden Beispiele mit Frau Schmidt und Herrn Schulz zeigen: Digitale Kommunikation ist für die meisten inzwischen zur Selbstverständlichkeit geworden. Gleichzeitig verliert der klassische, „analoge" Brief an Bedeutung. Nicht nur mit Freunden und Familie, sondern auch mit Unternehmen und staatlichen Stellen findet die Kontaktaufnahme mit immer größerer Regelmäßigkeit digital statt. Die Vorteile für Nutzerinnen und Nutzer scheinen auf der Hand zu liegen – sind sie doch schnell, bequem und kostengünstig. Auch Unternehmen können durch die Umstellung auf digitale Kommunikationskanäle und Online-Portale erheblich Ressourcen sparen.

Doch der gut belegte und vielfach veröffentlichte Anstieg an Computerkriminalität sowie die zahlreichen Überwachungs- und Datenschutzskandale, über die in den vergangenen Jahren immer wieder prominent berichtet wurde, haben zur Genüge gezeigt, dass digital gespeicherte und versandte Informationen angreifbar sind. Dies hat dazu geführt, dass das Vertrauen der Nutzerinnen und Nutzer in digitale Kommunikation gelitten hat, insbesondere dann, wenn es um die Übermittlung sensibler Informationen geht.

„Die Menschen haben es fast aufgegeben, ein Vertrauen in die Sicherheit und Verschlossenheit der digitalen Kommunikation zu haben. Man sieht es auch daran, dass allgemein immer offener kommuniziert wird. Das ist eine Veränderung im gesellschaftlichen Verhalten, die auch mit dem fehlenden Vertrauen in die Vertrautheit nichtöffentlicher Kommunikation zu tun hat."

Florian Rötzer, Chefredakteur Telepolis, Konsultation

So zeigen jüngere Umfragen beachtliche Vorbehalte hinsichtlich digitaler Kommunikation über sensible Inhalte mit Unternehmen oder Behörden.[4] Zwar geben einer weiteren Studie zufolge 70 Prozent der Internetnutzer an, ein Online-Postfach auf einem Kundenportal im Internet zu haben, und eine Mehrheit hält diese Postfächer auch für praktisch.[5] Gleichzeitig sind sich zwei Drittel derjenigen, die selbst solche Online-Postfächer nutzen, manchmal unsicher, ob sie dem Anbieter vertrauen können

4 Vgl. z. B. DIVSI, „Elektronische Dokumentenzustellung", repräsentative dimap-Umfrage ab 18 Jahren, 1. und 2. März 2017, https://www.divsi.de/wp-content/uploads/2017/03/2017-03-08_Unterlage_DIVSI-dimap-Umfrage_Dokumentenzustellung.pdf.

5 DIVSI, Digitalisierung – Deutsche fordern mehr Sicherheit. Was bedeutet das für Vertrauen und für Kommunikation? Eine Studie von dimap im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI), Hamburg, August 2017.

oder nicht. Ganze 72 Prozent machen sich Sorgen darüber, dass unbefugte Dritte auf ihr Online-Postfach zugreifen könnten. Lediglich 31 Prozent der Nutzerinnen und Nutzer finden, dass auf diesem Weg ein sicherer Dokumentenaustausch möglich ist. Zwei Drittel wiederum haben nur geringes bis gar kein Vertrauen darauf, dass die Unternehmen sich ausreichend um die Sicherheit ihrer Kunden kümmern.[6]

Selbst dem Staat wird in dieser Hinsicht nur wenig zugetraut. Obwohl 85 Prozent der Befragten der Ansicht sind, der Staat sollte sich stärker um das Thema Sicherheit im Internet kümmern, glauben fast ebenso viele nicht (84 Prozent), dass er dieser Aufgabe überhaupt gerecht werden und die Bürgerinnen und Bürger schützen kann.[7]

Dass digitale Kommunikationswege angesichts dieser Zahlen dennoch zur Selbstverständlichkeit geworden sind, könnte auf Gleichgültigkeit oder aber Fatalismus auf Seiten der Nutzerinnen und Nutzer schließen lassen. Doch ganz so simpel ist es nicht. Wie bereits angedeutet, fühlen sich viele geradezu dazu gedrängt, digital zu kommunizieren. Direkt befragt, kommen andere Präferenzen zum Ausdruck: Nicht weniger als 92 Prozent möchten selbst wählen können, ob Dokumente analog oder digital zugestellt werden. Darüber hinaus fänden es acht von zehn Nutzerinnen und Nutzern besser, wenn ihnen wichtige Dokumente per Briefpost zugeschickt würden und sie diese eben nicht von einem Online-Portal herunterladen müssten.[8]

Diese Zahlen zeigen, dass viele Nutzerinnen und Nutzer mit dem gegenwärtigen Zustand der digitalen Kommunikation mit Unternehmen und Behörden, wenn es um die Übermittlung sensibler Informationen geht, unzufrieden sind. Sie wünschen sich eine Wahlmöglichkeit und sichere digitale Kommunikationsmittel, die Übersichtlichkeit gewährleisten. Von diesem Befund ausgehend, unternimmt der vorliegende Bericht zum Projekt „Vertrauen in digitale Kommunikation" eine Bestandsaufnahme digitaler Kommunikation und erörtert, wie Lösungen für die beschriebenen Probleme und Wünsche der Nutzerinnen und Nutzer gefunden werden können.

6 Alle Zahlen ebd.
7 Ebd.
8 Ebd.

INTERVIEW MIT GIOVANNI BUTTARELLI

„Wir dürfen nicht alle Menschen zu Verdächtigen machen“

? Wann ist digitale Kommunikation vertrauenswürdig? Warum brauchen wir Vertrauen in der digitalen Kommunikation?

Giovanni Buttarelli: Da gibt es zunächst unsere gesetzlichen Regeln. Das Brief- und Postgeheimnis gehört zu den wesentlichen Grundrechten – von der Allgemeinen Erklärung der Menschenrechte der UN über die Europäische Menschenrechtskonvention bis zu den Verfassungen der einzelnen EU-Mitgliedsstaaten. Das Recht auf vertrauliche digitale Kommunikation ist das Äquivalent des traditionellen Briefgeheimnisses.

Aber auch außerhalb des Gesetzes ist die Vertraulichkeit von Kommunikation für das Funktionieren moderner Gesellschaften und Volkswirtschaften wesentlich. Wir müssen uns darauf verlassen können, dass Mitteilungen an die vorgesehenen Empfänger ausgeliefert werden; dass sie unterwegs nicht für andere Zwecke verwendet werden; dass sie nicht an Dritte weitergegeben werden; dass der Inhalt unverändert bleibt und dass die Nachrichten weitergeleitet und die Lieferung nicht verzögert wird. Ohne solche Zusicherungen könnten viele private und geschäftliche Aktivitäten nur von Angesicht zu Angesicht geführt werden.

? Denken Sie, dass in Anbetracht der Datenlecks und Enthüllungen über

Giovanni Buttarelli

Giovanni Buttarelli (geb. 1957) ist seit Dezember 2014 der Europäische Datenschutzbeauftragte. Er wurde auf gemeinsamen Beschluss des Europäischen Parlaments und des Europäischen Rats für fünf Jahre eingesetzt. Zuvor war er von 2009 bis 2014 bereits stellvertretender Europäischer Datenschutzbeauftragter. Von 1997 bis 2009 arbeitete er als Generalsekretär der italienischen Datenschutzbehörde. Er ist Richter am obersten Gerichtshof in Italien und ist an zahlreichen Datenschutzinitiativen und -komitees auch auf internationalem Gebiet beteiligt.

Foto: EDPS

> **Wir befinden uns im Augenblick mitten in der sogenannten vierten industriellen Revolution.** Giovanni Buttarelli

die Massenüberwachung der Geheimdienste in den vergangenen Jahren die gesetzlichen Schutzmaßnahmen ausreichend sind?

GB: Ich glaube, dass die Erwartungen der Bürgerinnen und Bürger zur Datensicherheit zu hoch sind und wir noch viel in Bezug auf Transparenz und Kontrolle tun müssen. Wir befinden uns im Augenblick mitten in der sogenannten vierten industriellen Revolution. Daten werden maschinell zwischen unterschiedlichen Teilnehmern transportiert, als Benutzer verwalten wir unser ganzes Leben mit dem Smartphone, wir bewegen uns von einer Sekunde zur anderen von einer Plattform auf die nächste. Überall hinterlassen wir Datenspuren. Wer was damit macht und wer was über mich weiß, ist dabei den Menschen nicht klar.

Ursprünglich bedeutete Vertraulichkeit der Kommunikation, vorsätzliche Eingriffe und den rechtswidrigen Zugang durch Dritte zu ahnden – dazu gehören auch, aber nicht nur, die Strafverfolgungsbehörden. So ist es immer noch in vielen Mitgliedsstaaten. Aber heute ist Vertraulichkeit der Kommunikation anderer Natur. Wenn Sie im Netz unterwegs sind, fallen automatisch Daten an – niemand muss sich Zugriff verschaffen. Das bedeutet, Sie müssen besser darüber informiert sein, was mit Ihren Daten geschieht. Was sind die Bedingungen für die Nutzung eines Services, eines Sozialen Netzwerks oder eines Messengers? In der Praxis wissen das die wenigsten Menschen.

Nehmen wir WhatsApp als Beispiel: Die App wird von Millionen von Menschen verwendet. Sie ist auf den ersten Blick kostenlos, aber in Wirklichkeit bezahlen Sie mit Ihren Daten, die viel wichtiger sind als Geld. Dadurch kann der Anbieter Profile erstellen, er kann vorhersagen, was Sie tun und was Sie kaufen, relevante Werbung einblenden, die Aktivitäten vorhersagen. Dadurch verwandelt sich der Nutzer in eine Quelle wichtiger Informationen.

? Was können die EU und die Justiz im Allgemeinen tun, um das Vertrauen der Nutzer in die Kommunikation zu erhöhen?

GB: Wir müssen uns bemühen, die kommende Datenschutzrichtlinie der EU vollständig umzusetzen. Damit einher geht die E-Privacy-Richtlinie, die die Integrität und Sicherheit von Datensystemen und Netzwerken erhöhen soll. Außerdem brauchen wir einen neuen Ansatz dafür, Sicherheitsverletzungen von Computersystemen zu erkennen. Zu wissen, was in Netzwerken passiert, ist der Schlüssel, um ihre Zuverlässigkeit zu erhöhen. Systeme und Daten können nie vollständig sicher sein, wir können auf jeden Fall mehr zur Prävention tun.

Dazu gehört auch, die Arbeit der Strafverfolgungsbehörden zu regeln. Die Idee, privatwirtschaftliche Service-Provider zu zwingen, Daten auf Vorrat zu speichern, weil sie möglicherweise irgendwann in der Zukunft von den Strafverfolgungsbehörden verwendet werden könnten, steht im Widerspruch zu den Grundsätzen der Menschenrechtscharta und des Vertrags von Lissabon. Wir dürfen nicht alle Menschen zu Verdächtigen ma-

INTERVIEW MIT GIOVANNI BUTTARELLI

> **Wir sind der Auffassung, dass die Entschlüsselung, das Reverse Engineering oder die Überwachung der durch Verschlüsselung geschützten Kommunikation verboten ist.** Giovanni Buttarelli

chen. Deshalb brauchen wir einen rechtlichen Rahmen, der regelt, wann Menschen gezielt und berechtigt überwacht werden können.

Aus diesem Grund ist der Ansatz einiger Mitgliedsstaaten, weiterhin Vorratsdatenspeicherung zu betreiben, umstritten. 2014 hat der Europäische Gerichtshof entschieden, dass die allgemeine und anlasslose Vorratsdatenspeicherung unzulässig ist. Das Urteil ist auch für die einzelstaatlichen Gesetzesregelungen relevant.

? Es gibt technische Lösungen, um die Vertraulichkeit der Kommunikation zu sichern, zum Beispiel Verschlüsselung. Sollte die EU so etwas stärker unterstützen?

GB: Die Debatte wird oft fälschlicherweise darauf reduziert, dass mehr Privatsphäre der Sicherheit entgegensteht. Das ist aber faktisch nicht so. Die neue Datenschutzrichtlinie verbietet es ausdrücklich, in der digitalen Kommunikationskette eine Soft- oder Hardware-Hintertür einzubauen, die es Dritten erlaubt, Zugang zur Kommunikation zu erlangen. Das betrifft sowohl die Anbieter von Verschlüsselungssoftware, die Service-Provider, die Betriebssystem-Betreiber und so weiter. Nutzer müssen ihre Kommunikation ohne Einschränkungen schützen können. Wir sind der Auffassung, dass die Entschlüsselung, das Reverse Engineering oder die Überwachung der durch Verschlüsselung geschützten Kommunikation verboten ist. Das ist auch der Standpunkt aller nationalen Datenschutzbehörden. Die Nutzung von Ende-zu-Ende-Verschlüsselung sollte nach dem Prinzip von Privacy by Design erfolgen.

Es ist technisch unmöglich, eine solche Hintertür oder Verschlüsselung so zu konstruieren, dass nur die Strafverfolgungsbehörden dazu Zugang haben. Jeder Kriminelle, jeder Terrorist – also diejenigen, die die Ziele der Maßnahmen sind – können diese Sicherheitslücken für ihre Zwecke missbrauchen. Das Einzige, was durch solche Hintertüren erreicht wird, ist, dass unsere Geräte unsicherer werden. Solche Überwachungsmaßnahmen gefährden selbst die Sicherheit unserer Daten und die kritischen Infrastrukturen vieler Mitgliedsstaaten. Deshalb dürfen wir die Datensicherheit nicht schwächen, nur um in einigen Fällen mehr Überwachung zuzulassen.

2.1 Modalitäten der Kommunikation

Bis zur Entwicklung der Telegrafie im 19. Jahrhundert beschränkte sich Distanz-Kommunikation im Wesentlichen – von sehr beschränkten Ausnahmen wie Rauch- oder Lichtzeichen oder dem mündlichen Überbringen von Nachrichten durch Boten abgesehen – auf das Versenden von Briefen. Der Telegraf und wenig später das Telefon machten erstmals den („fernmündlichen") Informationsaustausch in Echtzeit über längere Strecken möglich. Die Erfindung von Telex und Telefax, im Grunde Weiterentwicklungen der Telegrafie, änderten an diesem technologischen Stand bis weit ins 20. Jahrhundert nur wenig.

Erst als sich das in den 60er-Jahren geschaffene Internet zunehmend ausbreitete und spätestens im letzten Jahrzehnt des 20. Jahrhunderts zur selbstverständlich verfügbaren Alltagstechnologie geworden war, änderte sich das Kommunikationsverhalten grundlegend. Seither ist es möglich, sich schnell und unkompliziert, und vor allem ohne relevante Kosten, jederzeit schriftlich auszutauschen. Die E-Mail wurde zum allgegenwärtigen Kommunikationsmittel, sei es für private Zwecke oder für den Austausch zwischen Unternehmen und ihren Kunden sowie Behörden und Bürgern. Die Möglichkeit, auch per Mobiltelefon zu meist bezahlbaren Tarifen auf das Internet zugreifen zu können, hatte noch einmal ein starkes Wachstum des Kommunikationsaufkommens zur Folge. Es wurde zum erwarteten Normalzustand, überall und jederzeit erreichbar zu sein und kommunizieren zu können. Während die Zahl erfolgter Telefongespräche zurückging[9], nahm die schriftliche Kommunikation immer weiter zu[10].

Digitale Kommunikation gibt es in vielen Ausprägungen, z. B. abhängig von den Kommunikationspartnern („wer mit wem"?), dem Zeitverhalten (synchron oder asynchron) oder bestimmten technischen Details (z. B. Ende-zu-Ende oder vermittelt über eine Plattform). Die einfachste Differenzierung dürfte diejenige nach Absender und Adressat sein, auf die im Folgenden zunächst eingegangen wird.

Kommunikation zwischen Personen

Heute kann mit jedem durchschnittlichen Smartphone eine Vielzahl von Apps – also Anwendungsprogrammen für mobile Betriebssysteme – verwendet werden, die es insbesondere ermöglichen, mit anderen in Kontakt zu treten. Neben der E-Mail-Funktion sowie Programmen, die ausschließlich der Kommunikation dienen, wie beispielsweise SMS, iMessage auf Apples iPhone, WhatsApp, Threema, Signal, SIMSme oder Telegram, gibt es eine geradezu unüberschaubare Fülle an Anwendungen, bei denen die Möglichkeit der persönlichen und direkten Kontaktaufnahme mit anderen Nutzerinnen und Nutzern lediglich eine sekundäre Funktion darstellt – so zum Beispiel bei Sozialen Netzwerken wie Twitter, Facebook, LinkedIn oder Instagram. Nicht selten kommt es deshalb vor, dass man sich mit derselben Person wie selbstverständlich auf verschiedenen dieser Kanäle unterhält.

Kommunikation mit Unternehmen

Auch die Kommunikation zwischen Unternehmen und ihren Konsumenten („Business to Customer", B2C) wird mehr und mehr auf digitale Kommunikationsmittel verlagert. So würde es heute kaum eine Firma mehr wagen, keine E-Mail-Adresse zum Zweck der Kontaktaufnahme anzugeben. Mehr noch: Nach dem Telemediengesetz ist eine solche Kontaktmöglichkeit sogar rechtlich vorgeschrieben, wenn das Unternehmen eine Webseite unterhält – was heute auf so gut wie jede Firma zutrifft. Immer häufiger ist es zudem möglich, den Kundenservice nicht nur klassisch per Telefon zu erreichen, sondern auf der Webseite des Unternehmens in Echtzeit mit Mitarbeitern zu chatten. Geht es um die Bereitstellung von Informationen, die sensiblere Daten der Kundinnen und Kunden betreffen – wie zum Beispiel Kontoauszüge oder Krankenkassenunterlagen –, sind Portallösungen weit verbreitet. Hierbei wird der Kunde zumeist per E-Mail lediglich darüber informiert, dass Informationen für ihn vorliegen. Die eigentlichen Informationen werden in einem individuellen Bereich auf dem Server des Anbieters bereitgestellt. Auf diesen kann der Kunde

9 Vgl. https://de.statista.com/statistik/daten/studie/155005/umfrage/volumina-der-in--und-auslandsverbindungen-seit-2005/.
10 Vgl. https://hosting.1und1.de/digitalguide/e-mail/e-mail-marketing/die-e-mail-ist-tot-es-lebe-die-e-mail/.

über einen Login auf seinen Account, seinen persönlichen Zugang, zugreifen, für den er sich mit einem Benutzernamen oder einer Kundennummer und einem Passwort anmelden muss. Diese einfachste Form der Authentifizierung wurde von einigen Anbietern inzwischen vor dem Hintergrund von Phishing-Angriffen[11] durch die sichereren sogenannten Zwei-Faktor-Verfahren ersetzt. Eine andere Form von Portallösungen besteht darin, dass Nutzer mit Unternehmen durch das Ausfüllen von Formularen auf deren Webseiten Kontakt aufnehmen können. Für den Kunden besteht ein Nachteil darin, dass er in vielen Fällen keine Kopie seiner Nachricht erhält und somit auch nicht glaubhaft machen kann, dass er sie abgesandt hat.

Kommunikation mit Behörden

Neben Unternehmen der Privatwirtschaft etablieren inzwischen auch immer mehr Behörden und andere staatliche Stellen digitale Kommunikationskanäle mit den Bürgerinnen und Bürgern („Government to Citizen", G2C). Dass man heute per E-Mail mit der jeweils zuständigen Behörde in Kontakt treten kann, um bestimmte Informationen zu erlangen, versteht sich dabei fast von selbst. Auch Termine mit zum Beispiel Bürgerämtern oder Kfz-Zulassungsstellen können im Normalfall über die entsprechenden Webseiten vereinbart werden. Sogar Verwaltungsentscheidungen mit unmittelbarer rechtlicher Wirkung wie beispielsweise Baugenehmigungen werden mitunter auf elektronischem Wege zugestellt.[12] Dies geschieht im Regelfall durch den Einsatz von Online-Postfächern, also Portallösungen.[13]

Kommunikationsformen

Das Projekt „Vertrauen in Kommunikation im digitalen Zeitalter" konzentriert sich in erster Linie auf die Kommunikation B2C und G2C. Soweit dabei von „digitaler Kommunikation" gesprochen wird, liegt der Fokus auf verschiedenen Varianten der E-Mail sowie auf den genannten Portallösungen. Auch hybride Formen, die sich zugleich analoger und digitaler Techniken bedienen – wie beispielsweise der E-Postbrief der Deutschen Post, Neopost oder Pixelletter –, fallen unter diese weiter gefasste Definition digitaler Kommunikation. Andere digitale Kommunikationsformen wie Messenger-Dienste werden nur genannt, soweit dies für das Verständnis einzelner Punkte notwendig erscheint. Die digitalen Kommunikationsmittel werden insbesondere dem Brief als derjenigen analogen Form der Kommunikation gegenübergestellt, die auch im digitalen Zeitalter insofern weiterhin bedeutsam ist, als viele Behörden noch vorwiegend wie auch zahlreiche Unternehmen auf diese Weise kommunizieren.

> **„Vertrauen in die digitale Kommunikation ist ein Thema, das man gar nicht überbewerten kann. Es ist enorm wichtig, und es müssen Anstrengungen unternommen werden, um Vertrauen aufzubauen und so dem Digitalisierungsprozess mit offenen Augen zu begegnen. Dafür muss sich langfristig auch eine Kultur entwickeln."**
>
> **Prof. Dr. Norbert Pohlmann,** Professor für Informationssicherheit an der Westfälischen Hochschule und Geschäftsführender Direktor des Instituts für Internet-Sicherheit if(is), Konsultation

Auswirkungen

Als Folge des Umstands, dass wir heute zunehmend auf digitalem Wege miteinander sowie mit Behörden und Unternehmen kommunizieren, sind mehr und mehr Informationen und persönliche Daten über jede

11 Phishing: Versuch, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetnutzers zu gelangen und damit Identitätsdiebstahl zu begehen (Quelle: https://de.wikipedia.org/wiki/Phishing).

12 Siehe zum Beispiel für Berlin das Webportal https://www.berlin.de/ebg/, über das das gesamte Baugenehmigungsverfahren elektronisch abgewickelt werden kann.

13 Rechtliche Grundlage hierfür ist der zum 1. Januar 2017 in Kraft getretene § 41 Abs. 2a des Verwaltungsverfahrensgesetzes, der die Bekanntgabe von Verwaltungsakten über „öffentlich zugängliche Netze" regelt. Die Abwicklung des Verwaltungsverfahrens in dieser Form ist von der vorherigen Einwilligung des Bürgers abhängig. Vgl. dazu im Detail Alexander Schmid und Claudia Heudecker, Der vollständig automatisierte Erlass eines Verwaltungsakts (§ 35a VwVfG) sowie die Bekanntgabe eines Verwaltungsakts über öffentlich zugängliche Netze (§ 41 Abs. 2a VwVfG) (Teil 2), jurisPR-ITR 8/2017, http://bit.ly/2qaOKqG.

Person im Datenstrom des Internets unterwegs oder auf Servern im Netz gespeichert.[14] Denn bei der digitalen Kommunikation sind neben den eigentlichen Kommunikationsteilnehmerinnen und -teilnehmern zumeist auch Dritte involviert. Diese – insbesondere Kommunikationsdienstleister wie zum Beispiel E-Mail-Provider – transportieren die Kommunikation nicht nur auf digitalem Wege, sondern speichern diese auch auf ihren Servern, zumindest vorübergehend. Dadurch steigt die Gefahr von Missbrauch.

Das über das herkömmliche Telefon geführte Gespräch ist flüchtig – jedenfalls solange es niemand mitschneidet, was eine seltene Ausnahme und nicht die Regel ist. Elektronisch übermittelte Daten müssen jedoch gespeichert werden, bevor sie von den Kommunikationsteilnehmerinnen und -teilnehmern abgerufen oder ihnen zugestellt werden können. Die dadurch entstehenden Kopien der Daten können in einer Weise automatisiert gescannt und analysiert werden, die bei rein analoger Übermittlung von Informationen so nicht oder nur mit hohem Aufwand möglich ist – Briefe beispielsweise kamen und kommen im Normalfall ungeöffnet und damit ungelesen bei den Empfängern an. Zudem gilt, dass jedenfalls für technische Laien oft überhaupt nicht nachzuvollziehen ist, wo diese Speicherung erfolgt – ob im Inland oder Ausland, ob auf Servern des Unternehmens, mit dem in Kontakt getreten wird, oder auf denen eines ansonsten unbeteiligten Dritten. Wer außer dem Versender und dem Adressaten der E-Mail theoretisch noch Zugriff auf ihren Inhalt hat, bleibt für Anwender, die nicht über spezielle EDV-Kenntnisse verfügen, für gewöhnlich im Dunkeln.

> **„In der digitalen Kommunikation verhält sich der Mensch wie in vielen anderen Lebensbereichen. Auch wenn er gewisse Zweifel an der Datensicherheit hat, handelt er pragmatisch und nimmt Risiken in Kauf."**
>
> **Peter Schaar,** Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID), Konsultation

Die zunehmende Hinwendung zur Portallösung, die bei Unternehmen wie insbesondere Stromanbietern oder Banken zu beobachten und infolge der genannten Gesetzesänderung künftig auch bei der Kommunikation mit Behörden zu erwarten ist, bringt zudem einen grundsätzlicheren Wandel des Kommunikationsverhaltens mit sich. Bedeuteten die Nutzung sowohl von analogen Briefen als auch von E-Mails, dass die Unternehmen oder Behörden die Informationen den Kunden bzw. Bürgern überbrachten, wird von diesen bei der Portallösung erwartet, dass sie die Informationen selbst aktiv abrufen. Die Kommunikation zwischen den Akteuren wandelt sich so von einer Bring- zu einer Holschuld. Der Nutzer ist damit nicht nur in der Verantwortung, sich selbst darum zu kümmern, dass die Informationen zu ihm gelangen[15]; er hat, jedenfalls teilweise, zudem dafür zu sorgen, dass die Informationsübertragung beim Abruf sicher ist.[16] Das kann sich dann als problematisch erweisen, wenn er nur wenig über die technischen Abläufe während des Kommunikationsvorgangs weiß. Diese Verlagerung könnte einen Paradigmenwechsel für solche Kommunikationsverhältnisse auslösen.

14 Andrea Voßhoff, Vertrauen und Kommunikation in einer digitalisierten Welt aus Sicht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Vortrag, 17. November 2014, https://www.bfdi.bund.de/DE/Infothek/Reden_Interviews/2014/VertrauenundKommunikation_Muenster171114.html?nn=5217192.

15 Was zumindest bei der Kommunikation mit Behörden noch davon abhängig gemacht wird, dass der Bürger dieser Form der Informationsmitteilung vorher zugestimmt hatte.

16 Z. B. darf der Nutzer Warnungen nicht ignorieren, dass Zertifikate, die zur Absicherung einer Verbindung genutzt werden, nicht gültig sind.

INTERVIEW MIT HARALD LEMKE

Vertrauen ist kontextabhängig

? Herr Lemke, was bedeutet Vertrauen in digitale Kommunikation für Sie? Welchen Stellenwert hat dieses Vertrauen für unsere Gesellschaft?

Harald Lemke: Mein Vertrauen in Kommunikation ist zunächst einmal davon abhängig, in welchem Zusammenhang ich mich bewege. Ich muss das Gefühl haben, dass ich ohne Vorbehalte kommunizieren kann. Vertrauen entsteht nicht erst nach einer Analyse aller Sicherheitsanforderungen, sondern schon vorher als reines Bauchgefühl. Ich muss also entweder ein gutes Gefühl oder wenigstens kein Störgefühl haben, wenn ich mich mit jemandem über bestimmte Inhalte austausche.

Es macht dabei einen Unterschied, ob ich Ihnen ein Interview gebe, ob ich in einem Projekt mit dem Bundeskriminalamt vertrauliche Informationen austausche oder ob ich im höchst privaten Bereich über intime Probleme rede. Ich halte Vertrauen in die Kommunikation gesellschaftlich für außerordentlich wichtig, weil ich glaube, dass eine Gesellschaft nur dann ein subjektives und objektives Gefühl von Freiheit entwickeln

Harald Lemke

Harald Lemke ist seit Juli 2010 Sonderbeauftragter für E-Government und E-Justice bei der Deutsche Post AG.

Er gehörte der Enquetekommission Internet und digitale Gesellschaft an, ist Vorstandvorsitzender im Verein zur Selbstregulierung der Internetwirtschaft (SRIW e.V.), Mitglied im Verein Nationales E-Government Kompetenzzentrum (NEGZ e.V.) sowie Mitglied des Beirats des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI).

Von 2003 bis 2008 arbeitete er im Range eines Staatssekretärs als CIO für Hessen. Zwischenzeitlich war Lemke Berater für McKinsey & Company. 2002/2003 arbeitete er als IT-Direktor des BKA in Wiesbaden und war dort u. a. zuständig für die Einführung von INPOL-neu.

Foto: Deutsche Post AG

> **Wir haben ein Telekommunikationsgesetz, das verbietet, dass meine Kommunikation aufgezeichnet und analysiert wird.** Harald Lemke

kann, wenn die Unbeschwertheit, die mit dem Vertrauen kommt, gegeben ist.

? Es gibt Umfragen, die besagen, dass Nutzer kein Vertrauen in digitale Kommunikation haben. Unter welchen Umständen kann denn dieses Gefühl von Vertrauen in der Kommunikation zwischen Staat und Bürger oder Unternehmen und Verbraucher entstehen?

HL: Aus meiner ganz persönlichen Sicht kann ich dieses „kein Vertrauen" nicht unterschreiben. Bei meiner Kommunikation im geschäftlichen Kontext – als Kunde oder als Endverbraucher mit Unternehmen – habe ich zunächst keine hohe Erwartungshaltung, was Vertraulichkeit und Integrität angeht.

Ich gehe zum Beispiel bei Online-Händlern immer davon aus, dass sie versuchen, den Preis hochzutreiben und das meiste herauszuschlagen. Sie sammeln Daten und kaufen Profile und wissen daher vielleicht, dass sie von mir mehr verlangen können als von einem anderen Kunden, weil ich mehr Geld zu haben scheine. Ich vertraue ihnen zwar nicht, aber ich kann trotzdem mit ihnen Geschäfte machen – weil es zum Beispiel vertragliche Regelungen gibt, an die wir beide uns halten.

? Wenn wir einen anderen Kontext wählen – sagen wir mal, Sie wollen medizinische Produkte kaufen.

HL: Darauf kommt es eben an. In dem Moment, wo es um einen Sachverhalt geht, bei dem es auf Vertraulichkeit ankommt, würde ich keinen Online-Händler wählen. Dann würde ich vor Ort in einem Geschäft einkaufen. Nehmen wir ein Medikament, das nahelegen würde, dass ich an einer gesellschaftlich stigmatisierten Krankheit leide. In diesem Fall würde ich in den Nachbarort fahren, um es dort in der Apotheke zu kaufen. Andere Medikamente, bei denen es nicht so sensitiv ist, würde ich auch in einer Internetapotheke kaufen, wenn es sinnvoll ist. Immer wenn es um ein Geheimnis geht, das ich bewahrt haben möchte, würde ich keinem Online-Dienst vertrauen.

? Das heißt, Sie wollen in gewissen Kontexten keine digitalen Kommunikationskanäle nutzen, auch wenn Sie dadurch einen höheren Aufwand haben?

HL: Das liegt nicht am Kommunikationskanal, sondern an denjenigen, die dort tätig sind. Im konkreten Beispiel den Internetversandhändlern. Ich traue ihnen heute keine Integrität mehr zu.

? Aber wieso trauen Sie der Infrastruktur?

HL: Ich glaube nicht, dass Internet-Service-Provider wie die Telekom oder Vodafone meine Kommunikation mitschneiden und daraus Erkenntnisse gewinnen. Wir haben ein Telekommunikationsgesetz, das verbietet, dass meine Kommunikation aufgezeichnet und analysiert wird. Der Schaden, den eine Telekom hätte, wenn herauskommen würde, dass sie das trotzdem macht, wäre unendlich. Deshalb kann ich mir nicht vorstellen, dass ein Unternehmen an dieser Stelle systematisch Recht bricht. Es gibt natürlich immer die Gefahr, dass irgendein Systemadministrator

INTERVIEW MIT HARALD LEMKE

> **Mein Vertrauen in die digitalen Dienste würde erheblich steigen, wenn wir alle etwas mehr Sorgfalt und Geld für digitale Sicherheit aufwenden würden.** Harald Lemke

Unfug treibt, aber das ist vergleichbar mit dem Risiko, dass jemand bei mir einbricht und meine Privatunterlagen stiehlt.

? Das sind also zwei Faktoren, die Ihnen das Vertrauen geben: einmal das Gesetz und einmal die Reputation des Unternehmens.

HL: Genau.

? Wie bewerten Sie Gütesiegel und Zertifikate, die anzeigen, dass Kommunikation gewissen Sicherheitsstandards entspricht? Können sie zusätzliches Vertrauen schaffen?

HL: Ich bewerte sie relativ hoch. Ich weiß als Ingenieur, Informatiker und informierter Mensch, dass hundertprozentige Sicherheit ein Wunschtraum ist. Es kann sie nie geben. Also geht es darum, sicherzustellen, dass der Aufwand, die Sicherheitsvorkehrungen zu brechen, möglichst hoch ist. Trotzdem bleibt ein Risiko: Wer genug Geld, Ressourcen und Zeit hat, kann diese Mechanismen überwinden.

Mit Qualitätsanforderungen kann dieser Aufwand so hoch getrieben werden, dass zumindest kriminelles Verhalten von Einzelpersonen oder sogar Organisationen so erschwert wird, dass sie sich lohnendere Ziele suchen. Organisationen, bei denen Geld keine Rolle spielt oder die aufgrund ihrer Rahmenbedingungen keinen echten Verfolgungsdruck haben – also zum Beispiel Nachrichtendienste –, sind natürlich trotzdem in der Lage, die Sicherheitsbarrieren zu überwinden. Mit dieser Vorstellung habe ich meinen Frieden gemacht, sonst würde ich paranoid werden. Das ist zwar nichts, was mich glücklich macht, aber ich habe mich arrangiert.

? Brauchen wir höhere verpflichtende Standards und eine Haftung, wenn ein gewisses Mindestmaß an Sicherheitsstandards nicht eingehalten wird?

HL: Wir haben mit den europäischen Auflagen wie beispielsweise der eIDAS-Verordnung schon einen Satz an Normen an der Hand, mit denen man Kommunikationssysteme entwickeln und betreiben kann, die ein hinreichendes Maß an technischer und organisatorischer Sicherheit bieten. Es wird sich über die nächsten Jahre erweisen: Gibt es dafür eine ausreichende Zahlungsbereitschaft? Eins muss jedem klar sein: Sicherheit muss ich bezahlen, entweder mit Aufwand, mit Geld oder in der Regel mit beidem.

Das führt dann zur Frage, ob es überhaupt einen Markt für Vertrauen und Sicherheit gibt. Ich bin da nicht mehr ganz so sicher. Viele Verbraucher sparen sich krank und verkaufen ihre Seele, wenn sie dabei ein paar Cent sparen können. Im Übrigen verkauft jeder meiner Bekannten, der sich WhatsApp installiert, auch ungefragt meine Kontaktdaten. Diese Bedenkenlosigkeit macht mich schon manchmal zornig. Ob Standards wie eIDAS in dieser Welt erfolgreich sind, hängt deshalb sehr davon ab, ob es genügend Bereitschaft gibt, für sie zu bezahlen. Mein Vertrauen in die digitalen Dienste würde erheblich steigen, wenn wir alle etwas mehr Sorgfalt und Geld für digitale Sicherheit aufwenden würden.

2.2 Warum Digitalisierung der Kommunikation?

Es wäre falsch, sich bei dem anhaltenden Phänomen der zunehmenden Digitalisierung von Kommunikation nur auf die negativen und risikobehafteten Aspekte zu konzentrieren. Im Gegenteil: Die Vorteile der Umstellung von analogen Kommunikationsmitteln zu digitalen liegen auf der Hand. Sie sind im Vergleich zur Briefpost schneller, bequem und insbesondere auch kostengünstig verfügbar. Dienste des E-Governments können darüber hinaus die Verwaltung erheblich vereinfachen und entlasten, was zu signifikanten Effizienzgewinnen führen würde. Dadurch können Zeit und Geld eingespart werden, gerade auch auf Seiten des Bürgers. Entsprechendes gilt für geschäftliche Interaktionen mit Unternehmen.

Zu diesem Thema haben sich die Meinungen der Internetnutzer in den vergangenen Jahren entwickelt. So ergibt sich aus der jüngsten Studie, die von dimap im Auftrag von DIVSI durchgeführt wurde, dass die Digitalisierung laut sieben von zehn Befragten ihnen viele Vorteile biete. Insgesamt findet jeder Zweite, es sei komfortabler, Dokumente elektronisch zu verwalten und nicht in Form von Papierdokumenten. Schließlich spielt auch der Umweltschutz eine beachtliche Rolle: 79 Prozent der Nutzerinnen und Nutzer sagen, Online-Postfächer seien umweltschonender, da durch sie weniger Papier benötigt würde.[17]

2.3 Das Projekt und der Projektverlauf

Wie bereits in der Einleitung ausgeführt, geht das Projekt „Vertrauen in Kommunikation im digitalen Zeitalter" von der durch Umfragen gestützten Grundannahme aus, dass ein Bedürfnis nach geschützter und damit vertrauenswürdiger Kommunikation in sensiblen Kommunikationsverhältnissen besteht. Zu diesem Zweck wurde der Frage nachgegangen, wie solche Kommunikationsverhältnisse ausgestaltet sein könnten, damit das Bedürfnis nachhaltig befriedigt wird. Ein erstes im Projekt entstandenes Themenpapier diente der Bestandsaufnahme. Es untersuchte, wie es gegenwärtig um das Vertrauen in digitale Kommunikation bestellt ist. Ein daran anschließendes zweites Papier erörterte darauf aufbauend mögliche Lösungsansätze zur Herstellung und Stärkung von Vertrauen und stellte zu diesem Zweck fünf Grundsätze für sichere digitale Kommunikation auf. Die beiden Themenpapiere wurden schließlich ergänzt durch umfangreiche Interviews und Konsultationen mit Vertreterinnen und Vertretern aus Politik, Wirtschaft und Wissenschaft sowie weiteren Stakeholdern aus dem Feld der digitalen Kommunikation.

2.4 Aufbau des Dokuments

Das vorliegende Dokument orientiert sich im weiteren Verlauf an den Linien der beiden Themenpapiere. Auf die Analyse der Funktion von Vertrauen für gesellschaftliche Verhältnisse und der daran anschließenden Darstellung des gegenwärtigen Zustandes des Vertrauens in digitale Kommunikation folgt die Aufstellung der fünf Grundsätze für sichere digitale Kommunikation. Ihre umfassende Erläuterung wird zum Abschluss in einem Epilog durch konkrete Forderungen für ihre Umsetzung ergänzt. Die Ausführungen werden durch die erwähnten Interviews und Zitate aus den Konsultationen vervollständigt. Ein Annex geht zum vertieften Verständnis im Detail auf einige technische Details der Absicherung digitaler Kommunikation ein.

17 DIVSI, Digitalisierung – Deutsche fordern mehr Sicherheit. Was bedeutet das für Vertrauen und für Kommunikation?, August 2017.

3. Vertrauen in Kommunikation

Die im letzten Abschnitt aufgezählten technischen Umstände elektronischer Kommunikation erfordern beinahe selbstverständlich Vertrauen – Vertrauen der Kommunikationsteilnehmerinnen und -teilnehmer darauf, dass der Inhalt von den in welcher Funktion auch immer am Vorgang Beteiligten (also z. B. auch von den technischen Dienstleistern) sorgfältig und vertraulich behandelt wird. In diesem Zusammenhang ist allerdings zunächst einmal genauer zu erörtern, welche gesellschaftliche Funktion Vertrauen überhaupt erfüllt.

3.1 Die gesellschaftliche Funktion von Vertrauen

Der Begriff „Vertrauen" entzieht sich einer einfachen, für alle denkbaren Situationen angemessenen Definition. In seiner grundlegendsten Form bezeichnet „Vertrauen" einen psychischen Zustand, der sich auf ein Gegenüber bezieht und Erwartungen an dessen (künftiges) Verhalten formuliert. Wer einer anderen Person vertraut, der verlässt sich darauf, dass sich diese entweder so verhalten wird, wie es vereinbart worden ist, oder wie es den (berechtigten) Erwartungen der vertrauenden Person entspricht. Dies impliziert zugleich ein Moment der Unsicherheit. Wäre es gesichert, wie sich die andere Person verhält, so wäre Vertrauen weniger wichtig oder gar unnötig. Deshalb ist es auch immer mit einem gewissen Risiko verbunden, der anderen Person Vertrauen zu schenken: Die Erwartung an deren Verhalten kann trotz Vertrauens stets enttäuscht werden. Auf der anderen Seite setzt Vertrauen ein Mindestmaß an Wissen über die andere Person voraus. Bei völliger Unkenntnis über die Eigenschaften des Gegenübers kann nur auf ein erwünschtes künftiges Verhalten gehofft, jedoch nicht darauf vertraut werden.[18]

In der immer komplexer und unübersichtlicher werdenden modernen Gesellschaft, so der Soziologe Niklas Luhmann, reicht dieses interpersonale Vertrauen allein allerdings nicht mehr aus. Denn täglich

18 Walter Bamberger, Interpersonal Trust – Attempt of a Definition, 2010, http://www.ldv.ei.tum.de/en/research/fidens/interpersonal-trust/.

kommt es zu Interaktionen mit Personen und anderen Akteuren wie Unternehmen oder Behörden, zu denen keine persönliche Beziehung besteht und über die der Kommunizierende so gut wie nichts wissen kann, denen er aber trotzdem ein gewisses Vertrauen entgegenbringen muss, damit die Interaktion in der jeweils angezeigten Weise erfolgreich sein kann. Interpersonales Vertrauen muss daher durch das sogenannte Systemvertrauen ersetzt bzw. ergänzt werden. Die Erwartungen an das Funktionieren des Systems, dessen Teil der Einzelne ist, wird dadurch stabilisiert, dass darauf vertraut werden kann, dass sich die Mitglieder des Systems den ihnen zugewiesenen Rollen entsprechend verhalten.[19]

Ist dieses Systemvertrauen gegeben, so Luhmann, dann kann Vertrauen seine zentrale gesellschaftliche Funktion erfüllen und als entscheidender Mechanismus dienen, die Komplexität unserer Interaktionen mit anderen innerhalb der modernen Gesellschaft zu reduzieren. Auf diese Weise macht es Vertrauen möglich, mit den Unsicherheiten und Unwägbarkeiten, die der heutigen Gesellschaft inhärent sind, zurechtzukommen. Systemvertrauen macht diese Unsicherheit tolerierbar und versetzt den Einzelnen somit in die Lage, trotz der undurchschaubaren Komplexität, die sichere Voraussagen über die Zukunft verhindert, Entscheidungen zu treffen und so überhaupt handlungsfähig zu bleiben.[20]

3.2 Bezugspunkte des Vertrauens in der digitalen Welt

Eine sich hieran anschließende Frage ist, was Vertrauen angesichts seiner Funktion für die Kommunikation in der modernen Gesellschaft bedeutet. So ist einerseits zu fragen, worauf sich Vertrauen in der digitalen Welt bezieht, um dann zu eruieren, ob es seine Funktion erfüllen kann. Mit anderen Worten: Zu erörtern ist, wann davon gesprochen werden kann, dass digital übermittelte Kommunikation überhaupt vertrauenswürdig ist.

„Vertrauen in die digitale Kommunikation hängt davon ab, dass Menschen selbst entscheiden können, welche Information öffentlich wird und welche vertraulich bleiben soll. Das ist letztendlich eine große Herausforderung für jeden Kommunikationsweg, also auch für die Post und das Telefon. Bei der digitalen Kommunikation sehen die Menschen am ehesten ihr Vertrauen herausgefordert, weil man bei den verschiedenen Plattformen, die man nutzt, schwerer selbst entscheiden kann, in welcher Weise man in die Öffentlichkeit tritt."

Marion Grether, Direktorin des Museums für Kommunikation Nürnberg, Konsultation

Vertrauen in die Kommunikationsmittel kommt gerade in der digitalen Welt, in einer Informations- und Kommunikationsgesellschaft, eine wichtige Rolle zu. Zwar wurde von einigen Anhängern der sogenannten Post-Privacy-Bewegung[21] behauptet, dass es eines solchen Vertrauens nicht mehr bedürfe. Die Teilnehmerinnen und Teilnehmer digitaler Kommunikation sollen hiernach an der Vertraulichkeit von Informationen und Kommunikationsinhalten gar nicht mehr interessiert sein, was – wenn man hiervon tatsächlich ausgehen könnte – Vertrauen in ihren Schutz naturgemäß entbehrlich machen würde. Vor allem aufgrund der Verbreitung von Sozialen Netzwerken wie Facebook, Twitter, Instagram, aber auch Xing oder LinkedIn, ist wiederholt die Behauptung aufgestellt worden, der Begriff von Privatheit und damit auch der Inhalt dessen, was jeder Einzelne als privat oder intim anderen vorenthalten möchte, habe sich in der digitalen Gesellschaft grundlegend gewandelt und sei mittlerweile aufgeweicht. Da es ohnehin unmöglich sei, im Internet volle Kontrolle über die eigenen Daten zu behalten, müsse ein grundlegend anderer Umgang mit persönlichen Informationen gefunden werden.

19 Niklas Luhmann, Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität, 3. Aufl. Stuttgart 1989, Kapitel 7.
20 Bamberger, ebd.
21 Vgl. Christian Heller, Post Privacy: Prima leben ohne Privatsphäre, München 2011; Gary Younge, Social Media and the Post-Privacy Society, Guardian, 2. April 2012, https://www.theguardian.com/commentisfree/cifamerica/2012/apr/02/social-media-and-post-privacy-society; Nova Spivack, The Post-Privacy World, Wired, Juli 2013, https://www.wired.com/insights/2013/07/the-post-privacy-world/.

Unter anderem habe der traditionelle Datenschutz in seiner Funktion ausgedient.[22]

Die Vertreter von Post-Privacy repräsentieren aber mit ihren Ansichten weder die Mehrheit der Bevölkerung[23], noch behaupten selbst sie, dass es in der digitalen Welt keinerlei Privatsphäre oder Geheimhaltung/Datenschutz von sensiblen Informationen mehr geben sollte. Vielmehr ist sicherlich unbestritten, dass auch heute noch hochsensible Daten existieren, deren Sicherheit einem objektiven Schutzinteresse unterliegt und die vor dem unkontrollierten Zugriff durch Dritte geschützt werden müssen. Zu denken wäre an sensible Gesundheitsdaten oder auch Kreditkarteninformationen, Kontostände oder sonstige Daten, die die eigene finanzielle Sphäre betreffen.[24] Gelangen solche Daten in falsche Hände, werden kompromittiert oder missbraucht, können den Betroffenen erhebliche Schäden entstehen. Auch die persönliche Reputation kann beeinträchtigt sein, was im Einzelfall für Opfer existenzbedrohende Konsequenzen nach sich ziehen kann. Das gilt umso mehr in einer zunehmend digitalisierten Welt, in der Daten die Identität der Menschen prägen und repräsentieren. Die häufigen Fälle von Identitätsdiebstahl zeigen eindrücklich die Bedeutung einer nichtmanipulierten und authentischen Identität im digitalen Raum.

Auch wenn viele Menschen heute über Soziale Netzwerke einer oft nicht bestimmbaren Anzahl von Dritten einen beachtlichen Einblick in ihr Leben gewähren, kann nicht gefolgert werden, dass für sie die Privatheit bestimmter Informationen nachrangig ist. Wer eine E-Mail an eine gute Freundin schreibt, um von den Ergebnissen der letzten Vorsorgeuntersuchung zu berichten, wird darauf vertrauen wollen, dass außer der Freundin niemand mitliest. Wer seine Kontoauszüge auf dem Online-Portal seiner Bank abruft, wird darauf vertrauen, dass bei der Übertragung niemand die Daten abfängt und kopiert – den meisten wird klar sein, dass diese Daten sehr leicht zum finanziellen Nachteil des Betroffenen missbraucht werden können, sollten sie in falsche, kriminelle Hände geraten. Mehr noch, die Person wird darauf vertrauen, dass sie nach der Eingabe der Webadresse der Bank im Browserfenster auch tatsächlich auf die Seite der Bank geleitet wird und nicht auf die eines Dritten, die nur genauso aussieht. Wer in einer E-Mail, die von der eigenen Bank zu stammen vorgibt, einen Link zum Webportal anklickt, um beispielsweise den aktuellen Kontoauszug herunterzuladen, wird jedenfalls darauf hoffen, dass die Nachricht keine Fälschung ist und der Link nicht in betrügerischer Absicht zur Seite eines Kriminellen führt.[25] Und auch wenn jedem bewusst sein dürfte, dass alle Nutzerinnen und Nutzer ständig Datenspuren im Netz hinterlassen, die für interessierte Stakeholder Rückschlüsse auf unser Verhalten und unsere Vorlieben zulassen, werden die meisten dennoch zumindest darauf vertrauen wollen, dass diese Daten nicht gegen sie, also zu ihrem unmittelbaren Nachteil, verwendet werden.

> **„Vertrauen im Internet ist eine kostbare Ware, weil die Kommunikation nicht direkt stattfindet, sondern vermittelt wird."**
>
> **Peter Schaar,** Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID), Konsultation

> **„Es sollte nicht darum gehen, das Vertrauen in die digitale Kommunikation zu fördern, sondern ein angemessenes Risikowissen zu generieren und auf dieser Grundlage vernünftige Entscheidungen treffen zu können."**
>
> **Prof. Dr. Wolfgang Schulz,** Direktor am Hans-Bredow-Institut für Medienforschung an der Universität Hamburg, Konsultation

22 Jan Rähm, Wissenschaftler plädieren für einen neuen Datenschutz, Deutschlandfunk, 9. Juli 2016, http://www.deutschlandfunk.de/also-doch-post-privacy-wissenschaftler-plaedieren-fuer.684.de.html?dram:article_id=359646.

23 Siehe hierzu weiter unten, Kapitel 3.3.

24 Stephan Dörner, Die Deutschen sind erschreckend uninformiert, Welt.de, 27. Juli 2015, https://www.welt.de/wirtschaft/webwelt/article144508313/Die-Deutschen-sind-erschreckend-uninformiert.html.

25 Wobei in diesem Zusammenhang darauf hinzuweisen ist, dass das Phänomen des Phishings (siehe unten 3.4.1) inzwischen zu einem so großen Problem geworden ist, dass ein Vertrauen auf die Authentizität eines Links in einer E-Mail nicht mehr empfohlen werden kann.

ERWARTUNGEN VON NUTZERN AN VERTRAUENSWÜRDIGE KOMMUNIKATION

Es lässt sich also festhalten, dass Nutzerinnen und Nutzer von vertrauenswürdiger Kommunikation – ob digital oder analog – erwarten, dass:

- die Daten und Informationen, die sie übermitteln, geschützt sind und nicht in die Hände Krimineller oder generell unbefugter Dritter geraten;
- die Daten und Informationen von den Informationsempfängern nicht zum unmittelbaren Nachteil der Nutzerinnen und Nutzer verwendet werden;
- einzelne, sensible Informationen nicht der allgemeinen Öffentlichkeit zugänglich gemacht werden;
- der Akteur, d.h. die Person bzw. das Unternehmen oder die staatliche Stelle, mit dem kommuniziert wird, auch tatsächlich derjenige ist, für den er sich ausgibt;
- die Informationen nicht verfälscht worden sind;
- die versandte Nachricht tatsächlich und innerhalb kurzer Zeit den Empfänger erreicht.

Vertrauen in Kommunikationsvorgänge erfüllt eine ganz wesentliche Funktion. Sie liegt darin, dass die mitteilende Person mit hinreichender Sicherheit vorhersagen kann, was mit den übermittelten Daten und Informationen geschieht. Der Absender weiß auch nicht, ob und inwieweit die Nachricht vor dem Zugriff durch Akteure, die nicht unmittelbar an dem Vorgang beteiligt sind und die nicht legitimiert sind oder die die mitteilende Person nicht legitimiert hat, geschützt ist. Dies gilt für jede, zumindest jede durch Technik vermittelte, Individualkommunikation, unabhängig von den verwendeten Kommunikationsmitteln.

Vergleichbare Anforderungen kann auch der Empfänger stellen, beispielsweise möchte er in der Regel sicherstellen, dass der Absender auch derjenige ist, als der er sich ausgibt, und er hat auch ein Interesse an unverfälschten Nachrichten. Vertrauenswürdige Kommunikation hat also beidseitig hohe Ansprüche an Privatheit und Integrität der Inhalte, Authentizität von Sender und Empfänger und an Effektivität und Verlässlichkeit der Zustellung.

3.3 Mangelndes Vertrauen in der digitalen Welt

Wie die vorstehenden Ausführungen gezeigt haben, kommt Vertrauen in Kommunikation in der digitalen Welt besondere Bedeutung zu. Zugleich ist aber festzustellen, dass es besonderen Herausforderungen ausgesetzt ist. So wies die damalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger bereits im Juli 2013 in einem Interview mit der *Süddeutschen Zeitung* darauf hin, dass das Vertrauen in die digitale Kommunikation aufgrund der Datenschutz- und Überwachungsskandale der vergangenen Jahre beeinträchtigt ist.[26]

Auch die Bundestagsfraktion der Grünen konstatierte in einem Antrag an die Bundesregierung im Sommer 2016, mit dem sie etwas gegen den „Stillstand beim E-Government"[27] in Deutschland unternehmen wollte, dass die geringe Akzeptanz vorhandener Angebote im Netz jedenfalls „auch auf ein mangelndes Vertrauen der Bürgerinnen und Bürger

26 Wolfgang Janisch und Heribert Prantl, Interview mit Justizministerin Leutheusser-Schnarrenberger, Vertrauen in digitale Kommunikation ist beeinträchtigt, Süddeutsche Zeitung, 6. Juli 2013, http://www.sueddeutsche.de/politik/justizministerin-leutheusser-schnarrenberger-vertrauen-in-digitale-kommunikation-ist-beeintraechtigt-1.1714126.

27 E-Government wird insoweit ganz allgemein als der digitale Austausch zwischen Bürgern und Unternehmen auf der einen und staatlichen Einrichtungen auf der anderen Seite verstanden.

INTERVIEW MIT PROF. DR. SARA HOFMANN

„Vor allem muss es darum gehen, Hürden abzubauen“

? Was bedeutet Vertrauen in digitale Kommunikation?

Sara Hofmann: Eine gute Frage – sie wird in der Wissenschaft gerade ziemlich heiß diskutiert. Wir würden typischerweise unterscheiden zwischen Vertrauen in eine Technik – also in das Internet als Kommunikationskanal zum Beispiel oder in Facebook als Plattform – und Vertrauen in den potenziellen Kommunikationspartner. Das können Organisationen oder Verwaltungen sein, aber auch Privatpersonen.

? Wenn wir es eingrenzen auf die Frage des Vertrauens zwischen Bürgern oder Kunden auf der einen Seite und staatlichen Stellen oder Unternehmen auf der anderen Seite: Was sind die Bedingungen, damit Vertrauen in Kommunikation gerechtfertigt ist? Wann ist es gestört?

SH: Vertrauen ist ja eine Art unbegründete Erwartung, dass sich mein Gegenüber in einer bestimmten Art und Weise verhält. Es ist unglaublich schwierig, so etwas nachzuprüfen, gerade wenn es um digital vermittelte Kommunikation geht. Bei digitaler Kommunikation geht es typischerweise darum,

Prof. Dr. Sara Hofmann

Sara Hofmann ist seit Januar 2016 Juniorprofessorin für Digitale Medien im öffentlichen Sektor an der Universität Bremen und Wissenschaftlerin am Institut für Informationsmanagement Bremen GmbH (ifib). Nach dem Studium der Wirtschaftsinformatik promovierte sie 2014 am Lehrstuhl für Wirtschaftsinformatik und Informationsmanagement an der Westfälischen Wilhelms-Universität Münster und war dort bis zu ihrem Wechsel nach Bremen Postdoktorandin. In ihrer Forschung beschäftigt sie sich u. a. mit der Nutzung von E-Government-Technologien durch Bürger*innen und Verwaltungen, der Anwendung Sozialer Medien im öffentlichen Sektor sowie mit Prozessen der IT-Nutzung und -Akzeptanz im Allgemeinen.

Foto: Imago Photoatelier

> **Nutzer machen in solchen Fällen Abstriche bezüglich der Erwartung, wie ihre Daten behandelt werden.** Prof. Dr. Sara Hofmann

dass mit meinen Daten oder Informationen nichts passiert, was ich nicht möchte. Das nachzuweisen – oder wenigstens glaubhaft zu versichern – ist nicht einfach. Es lässt sich nur im Nachhinein feststellen, dass meine übermittelten Informationen tatsächlich so verwendet wurden, wie ich das erwartete. Dann war mein Vertrauen gerechtfertigt.

? DIVSI hat eine Erhebung dazu gemacht. Sie ergab, dass das Vertrauen in digitale Kommunikationsmittel und in ihre technische Sicherheit eher gering ist. Wie schätzen Sie das ein? Welchen Stellenwert hat das Vertrauen in die eigenen Kommunikationsmittel? Wo ist die Abwesenheit von Vertrauen problematisch?

SH: Wenn man sich Dienste wie Facebook oder WhatsApp anschaut, würden wahrscheinlich sehr viele Menschen sagen, sie sind mit den Datenschutzrichtlinien nicht einverstanden. Aber trotzdem werden diese Dienste von unglaublich vielen Menschen genutzt. Das liegt daran, dass der persönliche Nutzen überwiegt und einen viel höheren Stellenwert hat als das Vertrauen in die Technologie. Nutzer machen in solchen Fällen Abstriche bezüglich der Erwartung, wie ihre Daten behandelt werden. Sie vergleichen das mit den Möglichkeiten, die sie dadurch haben: dass sie mühelos mit ihren Freunden kommunizieren und Kontakt halten können mit der ganzen Welt.

Problematisch wird das im Bereich E-Government, also Informationstechnologie in der Verwaltung. Dort haben wir ein ziemlich großes Problem beim Vertrauen. Es gibt eine unbegründete Angst, dass der Staat den Bürger überwacht nach dem Motto „Der Staat hat meine Daten, und ich werde ein gläserner Bürger." Sehr viele Dienste werden nicht genutzt, die aber eigentlich einen sehr großen Nutzen haben würden. Aus einer Forscherperspektive ist dieses Misstrauen an dieser Stelle selten angebracht, sondern sollte eher woanders stattfinden.

? Welche Erklärung haben Sie, woran das liegen könnte?

SH: Typischerweise hat man nicht so viele Verwaltungskontakte pro Jahr. Wenn ich meine Steuererklärung einmal im Jahr per Papier einreiche, ist der Aufwand für mich eigentlich nicht so viel höher, als wenn ich das elektronisch mache. Bei Facebook aber gehen mir Möglichkeiten komplett verloren, wenn ich den Dienst nicht nutze.

? Wie kann man die Menschen davon überzeugen und das Vertrauen stärken?

SH: Das ist ein schwieriges Thema im öffentlichen Sektor. Der Staat, oder besser gesagt, die Verwaltung, müsste sehr viel mehr Mittel und Zeit investieren, um uns Bürgerinnen und Bürgern bestimmte Dienste zu erklären, sodass wir ein Verständnis dafür entwickeln, was geht und was nicht geht. Vertrauen muss häufig fehlendes Wissen ersetzen. Wenn ich nicht weiß, wie Dinge funktionieren, dann muss ich darauf vertrauen, dass es schon irgendwie gut gehen wird. Wenn ich aber als Bürgerin weiß, wie bestimmte Dienste ablaufen, dann brauche ich gar nicht mehr so viel Vertrauen.

INTERVIEW MIT PROF. DR. SARA HOFMANN

> **Vertrauen spielt zwar eine große Rolle, aber vor allem muss es darum gehen, Hürden abzubauen und es einfacher zu machen, Dienste zu nutzen.** Prof. Dr. Sara Hofmann

Es würde möglicherweise helfen, wenn der Staat sich andere Akteure mit ins Boot holt, die mehr Vertrauenswürdigkeit genießen. Bei Themen wie E-Government könnten das kritische Organisationen wie der Chaos Computer Club sein. Damit signalisiert man: „Uns ist die Sicherheit sehr wichtig. Dazu arbeiten wir mit Vertretern der Zivilgesellschaft zusammen." Das könnte das Vertrauen stärken.

? Brauchen wir für bestimmte Kommunikationsfälle auch technische Sicherheitsmaßnahmen, also zum Beispiel eine verpflichtende Ende-zu-Ende-Verschlüsselung?

SH: Das sollte auf jeden Fall verpflichtend sein. Es ist aber schwierig, hier Standards durchzusetzen. Auf staatlicher Seite kann man das machen, aber wenn es um die privaten Geräte der Bürgerinnen und Bürger geht, wird das komplizierter.

? Aber wenn eine staatliche Seite nur eine Ende-zu-Ende verschlüsselte Kommunikationslösung anbietet, dann könnte ja auch nur jemand mit seinem Gerät dieses wahrnehmen, wenn er auch verschlüsselt. Wäre das eine Lösung?

SH: Wenn man bestimmte Technologien vorgibt, die genutzt werden müssen, und anders geht es nicht, kann man das natürlich durchsetzen. Das sehen wir zum Beispiel beim Personalausweis. Die Daten dort sind sicher verschlüsselt, aber ohne Weiteres nicht zugänglich. Um ihn auslesen zu können, braucht man spezielle Lesegeräte. Die kann man sich zwar besorgen, aber es schafft eine unglaubliche Hürde. Der Ausweis ist zwar sicherer, aber auf Kosten der Nutzbarkeit. Die meisten Leute sind nicht bereit, diesen Aufwand in Kauf zu nehmen.

? Immer mehr Kommunikation findet digital statt, auch zwischen Staat und Bürger. Aber manche Menschen möchten ihre Behördengänge weiterhin analog erledigen – und das wird eine gewisse Zeit lang auch so bleiben. Wie kann man diesen Übergang vernünftig gestalten?

SH: Der Staat hat die Verpflichtung, jeden Bürger zu bedienen. Daher muss es für Menschen, die aus welchen Gründen auch immer nicht online sind, immer die Möglichkeit geben, ihre Interaktionen mit dem Staat analog abzuwickeln. Es sollte also immer irgendwie Offline-Kontaktpunkte geben. Das gilt auch für die digitale Generation: Vertrauen spielt zwar eine große Rolle, aber vor allem muss es darum gehen, Hürden abzubauen und es einfacher zu machen, Dienste zu nutzen.

in Datensicherheit und Datenschutz" zurückzuführen ist.[28]

> **„Die Datenschutzskandale der letzten Jahre haben das Vertrauen in die digitale Kommunikation stark beschädigt. Nutzerinnen und Nutzer agieren dadurch allerdings nicht unbedingt achtsamer, sondern haben vielmehr keine großen Erwartungen an die Vertraulichkeit.**
>
> **Frederick Richter,** Vorstand der Stiftung Datenschutz, Konsultation

Neben der in der Einleitung zitierten jüngsten repräsentativen Studie, die dimap im Auftrag von DIVSI durchgeführt hat, stützen auch andere aktuelle Befragungen die These, dass Misstrauen gegenüber den Kommunikationswegen im digitalen Zeitalter in der Bevölkerung verbreitet ist. Dies gilt sowohl in Bezug auf das Verhältnis zu staatlichen Angeboten als auch gegenüber der Kommunikation mit privatwirtschaftlichen Unternehmen.

So kam eine weitere dimap-Umfrage von Anfang März 2017 zu dem Ergebnis, dass es die Mehrheit der Bürger (55 Prozent) „eher schlecht" oder „sehr schlecht" findet, wenn Unternehmen oder Behörden wichtige Dokumente und Informationen ihren Kunden bzw. Bürgern per E-Mail zustellen oder in einem Online-Postfach zum Abruf hinterlegen.[29] Es sind dabei deutliche Unterschiede zwischen den einzelnen Altersgruppen festzustellen. Befragte unter 35 haben deutlich weniger Berührungsängste in dieser Hinsicht: 58 Prozent der Befragten in dieser Altersgruppe finden die elektronische Zustellung von Dokumenten und Informationen gut. Die entgegengesetzte Einstellung ist bei den über 65-Jährigen zu beobachten, von ihnen sind zwei Drittel skeptisch.

Noch auffälliger als die Skepsis gegenüber der Übermittlung oder Bereitstellung von Informationen durch Unternehmen oder Behörden auf digitalem Wege ist die in der gleichen Befragung zum Ausdruck gekommene Sorge, dass die persönlichen Daten der Kunden bzw. Bürger auf digitalen Kommunikationskanälen nicht sicher sind. Ganze 64 Prozent, also beinahe zwei Drittel aller Teilnehmerinnen und Teilnehmer, gaben an, in dieser Hinsicht „eher besorgt" oder „sehr besorgt" zu sein. Dieser Umstand impliziert einen Mangel an Vertrauen gegenüber digitalen Kommunikationsmitteln, wenn es darum geht, dass Unternehmen oder Behörden sensible Informationen an Kunden bzw. Bürger übermitteln. Nutzer sind sich unsicher, ob an diesem entscheidenden Punkt ein hinreichender Schutz gewährleistet werden kann.

Der eGovernment MONITOR, der jährlich vom Institute for Public Information Management gemeinsam mit der Initiative D21 durchgeführt wird, kommt für das Jahr 2016 zu dem Ergebnis, dass die Nutzung von E-Government-Angeboten in Deutschland leicht steigt, allerdings noch immer nicht einmal jeder zweite deutsche Onliner auf diese zurückgreift (45 Prozent).[30] Dieser Studie zufolge gaben im Jahr 2014 noch zwei Drittel der Befragten in Deutschland an, dass Bedenken bezüglich Sicherheit und Schutz sensibler persönlicher Daten sie von der Nutzung der Angebote abhielten. Dieser Wert ist zwar für 2016 auf nur noch etwas mehr als ein Drittel (34 Prozent) gesunken[31], zeigt aber dennoch die Bedeutung dieser Themen für einen signifikanten Teil der Nutzer.

Von denjenigen Befragten, die Sorgen bezüglich Sicherheit und Schutz sensibler Daten äußerten, waren für jeweils die Hälfte Angst vor Datendiebstahl sowie ein Mangel an Information darüber, was mit den Daten passiert, die gewichtigsten Gründe für das fehlende Vertrauen. Als weitere Faktoren wurden die Sorge vor mangelnder Sicherheit bei der Datenübertragung (48 Prozent), vor dem möglichen Zusammenführen von Daten in einer zentralen Datenbank („gläserner Bürger", 48 Prozent) und Bedenken hinsichtlich der Sorgfalt im Umgang mit den Daten von Seiten der Behörden (46 Prozent) genannt.[32]

28 Antrag der Fraktion Bündnis 90/Die Grünen, Stillstand beim E-Government beheben – Für einen innovativen Staat und eine moderne Verwaltung, BT-Drucksache 18/9056, 6. Juli 2016, S. 2, http://dip21.bundestag.de/dip21/btd/18/090/1809056.pdf.
29 DIVSI, „Elektronische Dokumentenzustellung", repräsentative dimap-Umfrage ab 18 Jahren, 1. und 2. März 2017, https://www.divsi.de/wp-content/uploads/2017/03/2017-03-08_Unterlage_DIVSI-dimap-Umfrage_Dokumentenzustellung.pdf.
30 IPIMA und Initiative D21, eGovernment MONITOR 2016 – Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, September 2016, S. 6, http://initiatived21.de/app/uploads/2016/12/egovmon2016_web.pdf.
31 Ebd., S. 7.
32 Ebd., S. 17.

Diese Befunde sind nicht auf Deutschland oder Europa beschränkt. Auch in anderen Ländern durchgeführte Befragungen kommen zu Ergebnissen, die ein verbreitetes Misstrauen gegenüber digitalen Kommunikationsangeboten zeigen. 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 naheliegt und eben kein rein deutsches Phänomen ist.[33]

Aus all diesen Zahlen wird trotz ihrer Unschärfe jedenfalls deutlich, dass die Mehrheit der Nutzerinnen und Nutzer eben nicht in einer Zeit leben will, die den Schutz der Privatsphäre als tragendes Prinzip des gesellschaftlichen Zusammenlebens aufgegeben hat. Im Gegenteil, Datenschutz und Vertrauen in sensible Kommunikation bleibt für sie von entscheidender Bedeutung. Wer digital kommuniziert, wird daher auch weiterhin zumindest darauf vertrauen wollen, dass sensible Daten ein Mindestmaß an Schutz vor dem Zugriff Dritter genießen.

> **„Unsere Erfahrung zeigt, dass immer weniger Nutzer bereit sind, nicht vertrauliche Dienste zu verwenden. Unsere Nutzerzahlen steigen konstant. Die breite Masse hat sich allerdings noch nicht von datenschutzrechtlich problematischen Diensten abgewendet. Bei vielen Menschen ist das Bewusstsein für Datenschutz und Privatsphäre noch wenig ausgeprägt. Das hängt sicher auch damit zusammen, dass die Thematik nicht so leicht greifbar und verständlich ist wie andere gesellschaftsrelevante Themen. Bequemlichkeit spielt sicherlich auch eine Rolle. Trotzdem ist der Trend positiv."**
>
> **Roman Flepp,** Pressesprecher, Threema GmbH, Konsultation

3.4 Gründe für mangelndes Vertrauen in der digitalen Welt

Der Feststellung, dass ein Misstrauen in Kommunikationswege in der digitalen Welt weit verbreitet ist, schließt sich die Frage nach den Gründen an. Dazu ist zunächst festzuhalten, dass die Entstehung von Vertrauen von einer Reihe von Faktoren abhängig ist. Individuell vertrauen wir anderen Personen, wenn wir ihr künftiges Verhalten zumindest zu einem bestimmten Grad voraussehen können, es also eine gewisse Konsistenz aufweist. Der primäre Gradmesser hierfür ist ihr Verhalten in der Vergangenheit.[34] Wird die so geformte Erwartungshaltung durch eine Handlung, die die Konsistenz durchbricht, enttäuscht, so geht Vertrauen verloren. Daneben spielen andere Aspekte eine Rolle, wenn Vertrauen gebildet werden soll, wie bestimmte als vertrauenswürdig akzeptierte Eigenschaften, zum Beispiel Ehrlichkeit, Loyalität oder Besonnenheit.[35]

Vertrauen in ein System ist ebenfalls davon abhängig, dass es sich als stabil erweist, also in einem Mindestmaß konsistent ist, so dass die Erwartungen des Einzelnen an das Verhalten des Systems nur im Ausnahmefall enttäuscht werden. Stabilität wird insbesondere dann erreicht, wenn sich die Akteure, die an dem System beteiligt sind, ihren (beruflichen oder institutionellen) Rollen entsprechend verhalten.[36] Repräsentanten des Systems Kommunikation sind beispielsweise Briefträger oder E-Mail-Serviceprovider.

33 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.
34 Nissenbaum, S. 159.
35 Ebd.
36 Bamberger, ebenda.

3.4.1 Ursachen für systemisches Misstrauen gegenüber Kommunikation in der digitalen Welt

In der digitalen Sphäre wird die Herausbildung von Vertrauen dadurch erschwert, dass an jedem Kommunikationsvorgang neben dem unmittelbaren Kommunikationspartner eine Vielzahl mittelbarer weiterer Teilnehmer beteiligt ist – so zum Beispiel die E-Mail-Dienstleister. Da die kommunizierenden Personen deshalb oft gar nicht wissen können, wer alles von den Inhalten des Vorgangs Kenntnis nehmen kann, ist das Vertrauen in den Kommunikationsweg von vornherein erheblich erschwert. Durch diese Komplexität kommt dem Systemvertrauen in der digitalen Welt eine noch einmal erhöhte Bedeutung zu. Es ist für die Kommunikationsteilnehmerinnen und -teilnehmer schwieriger, überhaupt Vertrauen aufzubauen. Zugleich ist es leichter zu enttäuschen und zu unterminieren. Kommt es dadurch abhanden, so kann es seine Funktion nicht mehr erfüllen. In dem Fall steigt das inhärente Risiko für die kommunizierende Person. Dies reduziert ihre Handlungsfähigkeit und führt im Extremfall dazu, dass die Kommunikation ganz abgebrochen oder von vornherein unterlassen wird. In den vergangenen Jahren hat eine Vielzahl unterschiedlicher Vorkommnisse dazu geführt, dass das Systemvertrauen in digitale Kommunikationsmittel erheblich Schaden genommen hat.[37]

So ist beispielsweise Internetkriminalität, die ihren Ausgangspunkt zumeist in der Manipulation oder Störung von Kommunikationsvorgängen nimmt, heute ein großes Problem. Sogenannte Phishing-Attacken, die den Zweck verfolgen, die Identität des Opfers zu stehlen oder sensible Daten wie Bank- oder Kreditkarteninformationen abzugreifen, gehören zu den häufigsten Formen der Kriminalität im Netz. Die Angriffe werden dabei immer raffinierter und bedienen sich immer häufiger des sogenannten Social Engineering, also der manipulierenden Beeinflussung von Zielpersonen, um sie zu bestimmten kompromittierenden Handlungen zu verleiten. Durchgeführt werden diese im Regelfall mittels einer E-Mail, die entweder von einer Person zu kommen scheint, der der Empfänger der Nachricht vertraut, oder die sonst einen auf ihn zugeschnittenen persönlichen und vertrauenerweckenden Inhalt aufweist.[38] Ist man erst einmal Opfer einer solchen Straftat geworden, so wird man der Kommunikation über Online-Kanäle künftig nur noch wenig Vertrauen entgegenbringen. Doch schon die durchaus erschreckenden Statistiken und regelmäßigen Medienberichte über groß angelegte Phishing-Attacken allein können potenziell zu einem Vertrauensverlust in der Bevölkerung beitragen.[39]

Auch staatliche Stellen haben in den vergangenen Jahren ihren Anteil daran gehabt, dass Vertrauen in digitale Kommunikation verloren gegangen ist.[40] Es ist zu einer ganzen Reihe von sich häufig sogar wiederholenden Ereignissen gekommen, die das Vertrauen in die Kommunikation der Bürgerinnen und Bürger mit Behörden und Unternehmen erschüttert haben. Um nur das prominenteste Beispiel zu nennen: Im Jahr 2013 enthüllte der NSA-Whistleblower Edward Snowden, dass die Geheimdienste vor allem der Vereinigten Staaten und des Vereinigten Königreichs jahrelang massenhaft die digitale Kommunikation von Nutzerinnen und Nutzern weltweit überwacht hatten und bis heute überwachen.[41] In Deutschland wiederum plant die Bundesregierung, eine „Zentralstelle für Informationstechnik im Sicherheitsbereich" zu errichten, zu deren Aufgaben es unter anderem gehören soll, Methoden zu entwickeln, Verschlüsselungen von Kommunikationsdiensten zu brechen.[42] Durch solche Maßnahmen wird die Vertraulichkeit des Inhalts von digitaler Kommunikation jedes Einzelnen potenziell kompromittiert.

37 Vodafone Institut, Auf dem Weg zum digitalen Staat: Erfolgsbedingungen von E-Government-Strategien am Beispiel Estlands, 2014, S. 5, http://www.vodafone-institut.de/wp-content/uploads/2015/09/VFI_eGovEra_DE.pdf.

38 Bundeskriminalamt, Internet-Kriminalität/Cybercrime, https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html.

39 Vgl. Bitkom, Jeder zweite Internet-Nutzer Opfer von Cybercrime, 13. Oktober 2016, https://www.bitkom.org/Presse/Presseinformation/Jeder-zweite-Internetnutzer-Opfer-von-Cybercrime.html.

40 Vgl. Bitkom, Vertrauen in Datensicherheit im Internet schwindet weiter, 9. Dezember 2013, https://www.bitkom.org/Presse/Presseinformation/Vertrauen-in-Datensicherheit-im-Internet-schwindet-weiter.html.

41 Siehe z. B. Oslo University Library, Global Surveillance, An Annotated and Categorized Overview of the Revelations Following the Leaks by the Whistleblower Edward Snowden, http://www.ub.uio.no/fag/informatikk-matematikk/informatikk/faglig/bibliografier/no21984.html.

42 Georg Mascolo, Neue Behörde soll für Regierung verschlüsselte Kommunikation knacken, sueddeutsche.de, 23. Juni 2016, http://www.sueddeutsche.de/digital/sicherheitspolitik-neue-behoerde-soll-fuer-regierung-verschluesselte-kommunikation-knacken-1.3047884.

„Das Vertrauen, dass die Politik digitale Kommunikationsstrukturen rechtlich und technisch schützt, ist durch die Geheimdienstskandale massiv erschüttert worden."

Florian Rötzer, Chefredakteur Telepolis, Konsultation

„Durch die Snowden-Enthüllungen haben sowohl staatliche Stellen als auch Unternehmen an Vertrauen eingebüßt. Bei Letzteren hat dies zu einer Bewegung geführt, sich auf Seiten der Kunden zu stellen und deren Grundrechte gegenüber dem Staat zu verteidigen. Unternehmen achten seitdem deutlich mehr darauf, als vertrauenswürdig wahrgenommen zu werden."

Susanne Dehmel, Mitglied der Geschäftsleitung Recht & Sicherheit, Bitkom e.V., Konsultation

3.4.2 Vertrauensverlust trotz Sicherheit

Das Systemvertrauen in digitale Kommunikation wird nicht nur durch unbefugte Eingriffe von Dritten, durch Sicherheitslücken oder illegale Handlungen erschwert.[43] Vielmehr veranlasst auch im Grunde sichere Kommunikation, bei der sich Unbefugte oder Unbeteiligte (rechtswidrig) Zugang zum Kommunikationsvorgang verschaffen können, zunehmend systemisches Misstrauen.

So legen die zitierten Studien nahe, dass das Vertrauen in die Kommunikation in der digitalen Welt nicht nur dadurch untergraben wird, dass die Vorgänge nicht sicher sind bzw. als nicht sicher empfunden werden. Sicherheit impliziert in diesem Zusammenhang eine Abwehr nach außen, also den Schutz der sensiblen Daten und Informationen vor dem Zugriff durch Dritte, die nicht legitimiert wurden, an dem Kommunikationsvorgang teilzunehmen. Das können, wie ausgeführt, Kriminelle oder Geheimdienste sein.

„IT-Sicherheit wird bei der Entwicklung von Anwendungen oder Tools häufig erst zu einem späten Zeitpunkt berücksichtigt. Dies ist auch in anderen Bereichen der Fall. Zum Beispiel wurden Sicherheitssysteme wie Gurte oder Airbags erst Jahrzehnte nach der Erfindung des Automobils eingeführt, um die Sicherheit der Insassen zu erhöhen."

Patrick Franitza, stellv. Pressesprecher der secunet Security Networks AG, Konsultation

Gerade in der Online-Welt wird das Vertrauen darüber hinaus häufig bereits durch diejenigen beeinträchtigt, die vom Nutzer im Grunde befugt wurden, Einsicht in den Kommunikationsvorgang zu nehmen bzw. an diesem teilzunehmen. Viele Anwendungen zur digitalen Kommunikation können heute gar nicht mehr gestartet werden, ohne dass sich der Nutzer zuvor über die Zustimmung zu den allgemeinen Vertragsbedingungen – die im Normalfall gar keine oder jedenfalls kaum Beachtung finden – dazu bereit erklärt hat, den Anbieter bis zu einem gewissen Grad „mitlesen" zu lassen bzw. das Abgreifen von Daten zuzulassen. So warnten Datenschutzexperten bei der Einführung von Googles E-Mail-Dienst Gmail im Jahr 2004 davor, dass das Scannen der Inhalte der E-Mails durch den Anbieter mit dem Zweck, kontextbasierte und damit gezieltere Werbung anzeigen zu können, das implizite systemische Vertrauen der Verbraucher in E-Mail-Dienstleister beeinträchtigen würde.[44] Auch Plattformbetreiber wie Social-Media-Unternehmen sammeln zumeist Daten über ihre registrierten Nutzerinnen und Nutzer, gerade auch wenn diese über die Dienste miteinander kommunizieren, und lassen sich dazu über die allgemeinen Vertragsbedingungen von den Nutzerinnen und Nutzern die Genehmigung erteilen. Über die Einzelheiten solcher Handlungen und deren Regeln herrscht bei den Nutzerinnen und Nutzern häufig Unsicherheit und Unkenntnis. Gründe hierfür sind, unter anderem, die Komplexität von Nutzungsbedingungen und Rechtsgrundlagen und die Aufdeckung unwahrer Behauptungen der Diensteanbieter.

43 Vgl. Nissenbaum, S. 166ff.

44 Privacy Rights Clearinghouse, Thirty-One Privacy and Civil Liberties Organizations Urge Google to Suspend Gmail, 6. April 2004, https://www.privacyrights.org/blog/thirty-one-privacy-and-civil-liberties-organizations-urge-google-suspend-gmail.

„Mehr Impulse für eine sichere digitale Kommunikation aus der Wirtschaft wären wünschenswert."

Matthias Gärtner, Pressesprecher beim Bundesamt für Sicherheit und Informationstechnik, Konsultation

Hinzu kommt das Problem der Spam-Mails, also unerwünschter E-Mails, die zumeist Werbung enthalten. Spam basiert nicht, jedenfalls nicht in erster Linie, auf mangelnder Sicherheit, sondern schlicht auf dem Phänomen, dass der Versand einer E-Mail (anders als bei physischer Post) kaum Kosten verursacht. Spam hat dazu geführt, dass E-Mail als Kommunikationsform erheblich an Vertrauen eingebüßt hat.

Schließlich ist zu erwägen, ob und inwieweit sich der beschriebene Paradigmenwechsel von der Bring- zur Holschuld negativ auf das Vertrauen der Nutzerinnen und Nutzer in digitale Kommunikation auswirken könnte. Auch hier geht es weniger um das Problem, dass die von Unternehmen oder Behörden bereitgestellten Portallösungen nicht sicher sind – es kann wohl davon ausgegangen werden, dass Kommunikationsverbindungen zu diesen Portalen im Normalfall den gängigen Verschlüsselungsstandards genügen. Ein Faktor, der das Vertrauen mindert, könnte jedoch beispielsweise sein, dass es durch die Verschiebung zur Holschuld zunehmend den Nutzerinnen und Nutzern aufgebürdet wird, die Übersicht darüber zu behalten, bei welchen Portalen relevante Dokumente oder Informationen regelmäßig abzurufen sind. Zwar werden Nutzerinnen und Nutzer für gewöhnlich per E-Mail (die zumeist auch einen entsprechenden Link direkt zum jeweiligen Portal enthalten) darüber informiert, dass diese zum Abruf bereitstehen. Dennoch ist mit dieser Art der Kommunikation eine Verantwortungsverlagerung verbunden. Es ist deshalb jedenfalls durchaus denkbar, dass eine solche Unübersichtlichkeit zu einem Gefühl der Unsicherheit im Netz beiträgt.

INTERVIEW MIT DR. KONSTANTIN VON NOTZ

Der Staat hat sich dafür entschieden, die IT-Infrastruktur grundsätzlich zu gefährden

? Was bedeutet Vertrauen in digitale Kommunikation? Welchen Stellenwert hat dieses Vertrauen für unsere Gesellschaft?

Konstantin von Notz: Vertraulichkeit in der Kommunikation ist eine wichtige Säule der Rechtsstaatlichkeit – für den einzelnen Bürger, aber auch für die Wirtschaft. Wenn man sich anschaut, was Rechtsstaaten von Unrechtsstaaten unterscheidet, dann ist die Vertraulichkeit von Kommunikation ein ganz zentrales Merkmal – gerade mit Blick auf eine immer digitalisiertere Welt. Denn diese Entwicklung erleichtert zwar die Kommunikation zwischen immer mehr Menschen – aber damit auch deren Überwachung.

? Wann ist denn Vertrauen in digitale Kommunikation gerechtfertigt und wann nicht?

KvN: Jeder rechtschaffene Mensch muss darauf vertrauen können, dass seine Privatsphäre – und damit seine Menschenwürde – vom Rechtsstaat geschützt wird. Er muss technische Kommunikati-

Dr. Konstantin von Notz

Dr. Konstantin von Notz, stellvertretender Vorsitzender und Sprecher für Netzpolitik der Bundestagsfraktion der Grünen.

Der Jurist und Bundestagsabgeordnete aus Schleswig-Holstein koordiniert als stellvertretender Vorsitzender die Innen-, Rechts- und Gesellschaftspolitik der Bundestagsfraktion der Grünen. Als Obmann im NSA-Untersuchungsausschuss war er an der parlamentarischen Aufklärung des internationalen Überwachungsskandals beteiligt. Der netzpolitische Sprecher setzt sich für die aktive Gestaltung des digitalen Wandels ein: Vor staatlichen und kommerziellen Interessen müssen die Bürger- und Verbraucherrechte sowie die Chancen auf gesellschaftliche Teilhabe im Mittelpunkt einer verantwortungsvollen Digitalpolitik stehen.

> **Deutschland ist das einzige Land, das sich derart systematisch mit den Snowden-Veröffentlichungen auseinandergesetzt hat.**
>
> Dr. Konstantin von Notz

onsmittel nutzen können, ohne dass jemand Unbefugtes diese Kommunikation mitschneidet und auswertet. Edward Snowden hat vor vier Jahren enthüllt, dass Staaten massenhafte und anlasslose Datenerfassung betreiben. Es gab zwar vorher schon Verdachtsmomente, er hat aber belegt, dass es tatsächlich passiert. Nicht nur Staaten wie China, Nordkorea und andere, die wir als rechtsstaatlich problematisch beurteilen, sondern auch rechtsstaatliche Demokratien erfassen massenhaft Daten von Menschen.

Foto: von-notz.de

? Sie haben sich im NSA-Untersuchungsausschuss sehr viel mit den Snowden-Enthüllungen beschäftigt. Was sind die Folgen vier Jahre später?

KvN: Wir hätten rechtliche Maßnahmen ergreifen müssen, um diese Rechtsverstöße systematisch zu verfolgen und sie zu stoppen. Das ist nicht erfolgt. Deutschland ist das einzige Land, das sich derart systematisch mit den Snowden-Veröffentlichungen auseinandergesetzt hat. Wir konnten Erkenntnisse und konkrete Belege dafür gewinnen, dass Verbindungsdaten automatisiert ausgelesen, gespeichert und gerastert werden und zusätzlich Millionen von Suchmerkmalen eingesetzt werden, um alle Inhalte zu erfassen. All diese Praktiken laufen aber weiter. Wir haben zwar ein Problembewusstsein entwickelt, nicht nur bei Bürgerrechtlern, die sich mit dem Thema befassen, sondern auch in einer größeren Öffentlichkeit – übrigens insbesondere auch in weiten Teilen der Wirtschaft. Aber die Große Koalition und die Sicherheitsbehörden verweigern sich schlichtweg, ernsthafte Konsequenzen zu ziehen und die Überwachung zu stoppen. Die Große Koalition hat ganz im Gegenteil versucht, die Praktiken ex post einfach zu legalisieren, was unserer Auffassung nach ein klarer Verfassungsbruch ist – und auch mit Blick auf die Sicherheit von uns allen im Digitalen setzt man damit auf eine völlig verquere Strategie.

? Wie kann in dieser Situation trotzdem das Vertrauen in digitale Kommunikation gestärkt werden? Was kann etwa die Wirtschaft tun, um vertrau-

INTERVIEW MIT DR. KONSTANTIN VON NOTZ

> **Aber wenn der Staat in dieser fundamentalen rechtsstaatlichen Frage der Vertraulichkeit der Kommunikation unklar ist, wird man am Ende kein nachhaltiges Vertrauen erhalten können.** Dr. Konstantin von Notz

enswürdige Kommunikation zu gewährleisten?

KvN: Die Wirtschaft muss sich viel entschlossener gegen diese illegalen Praktiken von staatlicher Seite wehren. Sie sind Einfallstore für Schadsoftware und Datendiebstahl. Ganz konkret kauft der Staat mit Steuergeldern auf dem Schwarzmarkt Sicherheitslücken an, die er offen hält, um damit Terrorverdächtige oder andere Straftäter zu überwachen. Das sind nachher die Lücken, durch die ganz normale Wirtschaftsunternehmen und die IT-Infrastruktur insgesamt angegriffen werden.

Wir brauchen hier neben klaren Standards auch Anreize für die Wirtschaft. So braucht es für Initiativen für mehr Verschlüsselung das Engagement von wirtschaftlicher Seite. Aber wenn der Staat in dieser fundamentalen rechtsstaatlichen Frage der Vertraulichkeit der Kommunikation unklar ist, wird man am Ende kein nachhaltiges Vertrauen erhalten können. Ich garantiere: Die nächsten Skandale sind vorprogrammiert. Es wird zu Abgriffen von Informationen und Daten kommen. Informationen werden eingesetzt, um Leute zu diskreditieren oder wirtschaftliche Vorteile zu erlangen.

? Was halten Sie von Zertifizierungen und Gütesiegeln, um den Bürgern Orientierung zu geben, dass gewisse Sicherheitsstandards eingehalten werden?

KvN: Solche Initiativen sind auf keinen Fall schädlich – vor allem, wenn sie im Rahmen eines umfassenderen Ansatzes aus verbindlichen Sicherheitsstandards und Haftungsregeln den Verbrauchern transparent und verlässlich einen Überblick verschaffen. Doch die beste Verbraucherprävention nützt nichts, wenn der Staat nicht strukturell für Sicherheit sorgt: Es gibt kein richtiges Leben im falschen. Artikel 10 des Grundgesetzes, das Briefgeheimnis und das Post- und Fernmeldegeheimnis, ist eine fundamentale Säule des Vertrauens und der Rechtsstaatlichkeit – auch vor dem Hintergrund der deutschen Geschichte. Staatliche Gewalt muss sich an die Verfassung halten. Wenn aber der Staat mit seiner staatlichen Gewalt und seinen finanziellen Ressourcen daran arbeitet, die Sicherheit der Kommunikation aufzubohren, dann wird man das durch noch so schöne privatwirtschaftliche Initiativen nicht verändern können.

Das können Sie wunderbar am BSI, dem Bundesamt für Sicherheit in der Informationstechnik, beobachten. Das ist eine gute Institution mit fachkundigen Leuten,

die wichtige Arbeit machen. Sie versuchen, Sicherheitslücken zu schließen. Gleichzeitig kaufen das Innenministerium, das Bundesamt für Verfassungsschutz und der Bundesnachrichtendienst Sicherheitslücken an und halten sie offen. Deshalb wirkt jede BSI-Initiative abgeschmackt.

? Halten Sie es für sinnvoll, dass für bestimmte Kommunikationskonstellationen des Staates höhere Standards eingeführt werden? Sollte zum Beispiel die Kommunikation mit meiner lokalen Behörde – ob für die Steuererklärung oder andere Dienstleistungen – immer Ende-zu-Ende verschlüsselt laufen?

KvN: Es ist immer gut, Sicherheitsstandards zu erhöhen. Dadurch können zum Beispiel einfache kriminelle Angriffe verhindert werden, und das kann man durch eine starke Ende-zu-Ende-Verschlüsselung. Doch was passiert hinter den beiden Enden? Ich bleibe aber dabei, dass dadurch das Grundproblem nicht aus der Welt geschafft ist. Man darf den Leuten nichts vormachen. Wenn ein Staat sich entscheidet, die Infrastruktur grundsätzlich zu gefährden, dann können weder der Endverbraucher noch wirtschaftliche Initiativen das fundamentale Sicherheitsproblem aus der Welt schaffen.

? Könnten nicht zum Beispiel verschiedene große E-Mail-Anbieter sich entscheiden, gemeinsam eine Ende-zu-Ende-Verschlüsselung einzuführen? Staatliche Sicherheitsapparate hätten dann tatsächlich Schwierigkeiten, diese Kommunikation abzufragen. Welche Anreize bräuchte es, damit die Anbieter so ein Produkt entwickeln?

KvN: In der Vergangenheit argumentierten viele Unternehmen, dass sie keine Ende-zu-Ende-Verschlüsselung anbieten würden, weil es ihnen zu teuer war. Das ist nach den Snowden-Enthüllungen vielen IT-Anbietern auf die Füße gefallen. Diejenigen, die sagen konnten, wir sind vertrauenswürdig und verschlüsseln die Kommunikation, hatten einen steigenden Vertrauensvorschuss. Das kann also ein Verkaufsargument sein. Aber wir dürfen den Staat nicht aus der Verantwortung entlassen und einfach so hinnehmen, was da läuft. Frei und sicher im Netz kommunizieren zu können, ist die Grundsatzfrage für Rechtsstaatlichkeit und Teilhabe im digitalen Zeitalter.

> **Diejenigen, die sagen konnten, wir sind vertrauenswürdig und verschlüsseln die Kommunikation, hatten einen steigenden Vertrauensvorschuss.** Dr. Konstantin von Notz

3.5 Zwischenfazit

Die vorstehenden Ausführungen haben gezeigt, dass viele Menschen der digitalen Kommunikation aus verschiedenen Gründen nicht vertrauen. Vertrauen in die Integrität, Authentizität und Vertraulichkeit von Individualkommunikation ist in der digitalen Welt jedoch wichtiger denn je. Trotz mangelnden Vertrauens benutzen die meisten Menschen ständig digitale Kommunikationsmittel für jede Art der Kommunikation, gleich welchen Inhalts, sensibel oder nicht.

Ein unmittelbarer Zusammenhang zwischen dem weitverbreiteten Misstrauen und dem Kommunikationsverhalten ist insofern nicht ersichtlich. Letztlich hat diese „Ignoranz des Misstrauens" zwar große Vorteile, denn hielte das Misstrauen von digitaler Kommunikation ab, würde der Fortschritt verweigert und aufgehalten, und von den erheblichen Vorteilen digitaler Kommunikation würde kein oder nur unzureichend Gebrauch gemacht.

Somit ist ein gravierender Missstand zu statuieren: Kommunikation spielt in der digitalen Welt eine herausragende Rolle für das soziale, berufliche und private Leben der Menschen. Um diesem Bedürfnis nachzukommen, benutzen die Menschen – bewusst oder unbewusst, wohl oder übel – ständig Kommunikationsmittel, die nicht sicher sind und denen sie ganz häufig nicht vertrauen. Das wiederum bereitet vielen offensichtlich Sorgen und führt zu Effizienz- und Systemvertrauensverlusten.

Auf diesem Befund aufbauend, geht es im Folgenden darum, Ansätze auszuloten, die dem Ziel dienen, das Vertrauen der Nutzerinnen und Nutzer in digitale Kommunikationsmittel zu stärken und abzusichern. Zu diesem Zweck werden fünf inhaltlich miteinander verknüpfte und aufeinander bezogene Grundsätze für sichere digitale Kommunikation formuliert und erläutert.

4. Fünf Grundsätze für sichere digitale Kommunikation

Es ist von zentraler Bedeutung, dass die Nutzer digitalen Kommunikationsmitteln vertrauen können, mithilfe derer sie (u. a.) mit Unternehmen oder Behörden in Kontakt treten, um bedeutsame oder sensible Inhalte auszutauschen. Aufgrund der Komplexität kann Vertrauen in digitale Kommunikation praktisch nur als Systemvertrauen aufgebaut und aufrechterhalten werden. Es ist deshalb zu erörtern, wie es hergestellt, bestärkt und gewährleistet werden kann. Dazu erfordern solche Kommunikationsverhältnisse bestimmte Rahmenbedingungen, die durch die im Folgenden formulierten Grundsätze unterstützt werden.

Die folgenden Kapitel führen diese Sätze der Reihe nach auf und erläutern und erörtern sie jeweils im Detail. Dabei sind die Leitsätze nicht isoliert voneinander zu betrachten. Vielmehr verweisen sie aufeinander und begrenzen sich dabei zum Teil gegenseitig – jedes der Ziele ist mit widerstreitenden Aspekten abzuwägen. Dies gilt insbesondere auch für die beiden

GRUNDSÄTZE FÜR SICHERE DIGITALE KOMMUNIKATION

1. DIGITALE KOMMUNIKATION MIT SENSIBLEN INHALTEN SOLLTE SICHER UND VERLÄSSLICH SEIN.

2. DIE EINGESETZTE TECHNOLOGIE SOLLTE NUTZERFREUNDLICH SEIN.

3. DEM NUTZER GEGENÜBER SOLLTE DER GEWÄHRLEISTETE SICHERHEITSSTANDARD KOMMUNIZIERT WERDEN.

4. DEM NUTZER SOLLTEN ALTERNATIVE – AUCH ANALOGE – KOMMUNIKATIONSMITTEL ANGEBOTEN WERDEN.

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.

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.

4.1 Digitale Kommunikation mit digitalen Inhalten sollte sicher und verlässlich sein

Sicherheit und Verlässlichkeit digitaler Kommunikation ist 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 und verlässlich 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;
- für den Empfänger der übermittelten Information gewährleistet ist, dass sie tatsächlich von der Person stammt, von der sie zu stammen scheint;
- und die Nachricht tatsächlich zugestellt wird.[45]

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

4.1.1 Der rechtliche Rahmen

Rechtliche Vorschriften dienen als zentraler Baustein für die Absicherung analoger und digitaler Kommunikation und damit zur Herstellung und Stärkung von Systemvertrauen. Schützt das Recht nicht davor, die Integrität, Authentizität und Vertraulichkeit von Individualkommunikation zu verletzen, kann sich Vertrauen in das System der Kommunikation nur schwer entwickeln oder leicht nachhaltig beschädigt werden. Als ein Beispiel, in diesem Fall aus der „analogen Zeit", sei die Praxis der Abteilung M des Ministeriums für Staatssicherheit in der Deutschen Demokratischen Republik genannt, Briefe mittels spezieller technischer Vorrichtungen zu öffnen und wieder zu schließen und dabei kaum sichtbare Spuren am Briefumschlag zu hinterlassen.[46] Solche Maßnahmen schädigen die Privatheit der Kommunikation. Werden sie bekannt (was letztlich bei derlei gravierenden Verletzungen fast immer geschieht), untergraben sie das Vertrauen in das Kommunikationssystem als solches. Es wird in der Folge nicht mehr für vertrauliche Kommunikation genutzt werden.

> **„Der Staat muss den Rahmen für eine sichere digitale Kommunikation setzen. Das beginnt im rechtlichen Bereich, geht über die technische Richtliniensetzung bis hin zur Einführung von Gütesiegeln, wo der Staat unterstützen kann."**
>
> **Matthias Gärtner,** Pressesprecher beim Bundesamt für Sicherheit und Informationstechnik, Konsultation

Insofern erklärt es sich, dass die Nachrichtenübermittlung per Brief schon mit Beginn der Neuzeit rechtlich abgesichert wurde, um das Vertrauen der Bürgerinnen und Bürger in das System zu stützen. Die Allgemeine Preußische Postordnung von 1712 sanktionierte Postbeamte mit Entlassung und Bestrafung wegen Meineids. In Frankreich drohte hierfür ab 1742 gar die Todesstrafe.[47]

Grundrechtliche Garantien

In Deutschland wird das Brief- und Postgeheimnis seit 1949 durch Artikel 10 des Grundgesetzes als

45 Vgl. Dirk Heckmann u. a., Adäquates Sicherheitsniveau bei der elektronischen Kommunikation: Der Einsatz des E-Postbriefs bei Berufsgeheimnisträgern, Stuttgart 2012, S. 58f.

46 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.

47 Vgl. Wikipedia, Briefgeheimnis, https://de.wikipedia.org/wiki/Briefgeheimnis.

INTERVIEW MIT PROF. DR. UDO HELMBRECHT

Software- und Hardware-Produkthaftung ist notwendig

? Das Vertrauen in die digitale Infrastruktur ist in Deutschland relativ gering – das war das Ergebnis einer kürzlich durchgeführten DIVSI-Erhebung. Viele Menschen haben eine pragmatisch-fatalistische Haltung im Sinne von „Nichts ist sicher". Sie halten die Kommunikationsmittel nicht für vertrauenswürdig, benutzen sie aber trotzdem. Wie bewerten Sie das?

Udo Helmbrecht: Es gibt eine übertriebene Erwartungshaltung, dass es so etwas wie hundertprozentige Sicherheit im IT-Bereich gibt. Wenn man Auto fährt, fährt man auch nicht mit 150 Stundenkilometern auf einer Landstraße. Man weiß: Ich kann leicht ins Schleudern kommen und hänge dann am Baum. Trotzdem sagt niemand, dass er kein ABS oder keinen Sicherheitsgurt braucht.

Foto: Privat

Prof. Dr. Udo Helmbrecht

Prof. Dr. Udo Helmbrecht hat mehr als 40 Jahre Berufserfahrung im IT-Sektor.

1955 in Castrop-Rauxel/Nordrhein-Westfalen geboren, studierte er Physik, Mathematik und Computerwissenschaften an der Ruhr-Universität in Bochum und promovierte dort 1984 in theoretischer Physik. Seit 2010 hat Udo Helmbrecht eine Honorarprofessur an der Universität der Bundeswehr in München inne.

Seine Erfahrung auf dem Gebiet der Informationssicherheit sammelte er durch die Leitung diverser Projekte der Technik- und Versicherungswirtschaft sowie im Bereich Luft- und Raumfahrt. Von 2003 bis 2009 war er der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Seit dem 16. Oktober 2009 ist Helmbrecht geschäftsführender Direktor (engl. Executive Director) der European Network and Information Security Agency (ENISA) mit Sitz in Heraklion auf Kreta.

INTERVIEW MIT PROF. DR. UDO HELMBRECHT

> **Die Frage ist, wie wir vernünftiges Risikobewusstsein bei den Endnutzern entwickeln können, damit sie nicht fatalistisch im Netz unterwegs sind.** Prof. Dr. Udo Helmbrecht

Bei der ganzen Diskussion vermischen sich viele Kontexte, die nichts miteinander zu tun haben. Um bei dem Bild vom Auto zu bleiben: Wenn Sie mit Ihrem Auto auf einer nassen Straße fahren, dann reden Sie nicht darüber, dass Geheimdienste versuchen, Ihr Auto zu manipulieren. Aber wenn Sie Präsident oder Kanzlerin sind, kann schon jemand Interesse daran haben.

Sie müssen einen Umgang mit Sicherheit finden, der für Sie adäquat ist. Dann ignorieren Sie vielleicht die Geheimdienste oder Terroristen, aber schützen sich gegen Identitätsdiebstahl und andere Cyberkriminalität. Die Frage ist, wie wir vernünftiges Risikobewusstsein bei den Endnutzern entwickeln können, damit sie nicht fatalistisch im Netz unterwegs sind. Sie sollen sagen, genauso wie ich im realen Leben Fahrrad fahre, Auto fahre, zur Bank oder zur Post gehe und dabei bestimmte Regeln beachte, gehe ich in der virtuellen Welt digital zur Bank oder zur Post. Und dabei halte ich mich auch an bestimmte Sicherheitsmaßnahmen.

Wie kann Ihrer Meinung nach das Vertrauen in digitale Kommunikation gestärkt werden?

UH: Das eine ist sicherlich Aufklärung. Die Menschen müssen sich bewusst werden, wann sie was und auf welche Weise kommunizieren. Ein einfaches Beispiel: Eine E-Mail ist wie eine mit Bleistift geschriebene Postkarte, das heißt, jeder kann sie lesen und verändern. Genau so, wie ich nicht möchte, dass der Postbote meine Briefpost lesen kann, so will ich auch in der virtuellen Welt nicht, dass andere meine E-Mails lesen können.

Die Anbieter müssen aber auch mehr für ihre Produkte werben. Sie müssen den Menschen besser kommunizieren: „Bei uns kannst du dich darauf verlassen, dass nach menschlichem Ermessen keine Dritten deine Kommunikation unberechtigterweise mithören."

Können Zertifizierungen und Gütesiegel den Verbrauchern helfen, vertrauenswürdige Angebote zu identifizieren?

UH: So etwas könnte sicherlich weiterhelfen. Beim Auto gibt es zum Beispiel den TÜV, der die staatlichen Vorgaben überprüft. Dann gibt es Produkttests wie bei der Stiftung Warentest. Andere Gütesiegel funktionieren auf Basis von Selbstverpflichtung, etwa das CE-Gütesiegel. Wir brauchen eine Mischung von Standards, Selbstverpflichtung, Produktinformation – und an den Stellen, wo es nicht gleich funktioniert, vielleicht sogar ein wenig Druck vom Staat.

Wie stehen Sie in der Diskussion um Produkthaftung bei IT-Anwendungen? Sind Sie für solche Maßnahmen?

UH: Die Diskussion über Softwarehaftung begann in Deutschland in großem Stil im Anschluss an die Botnet-Attacke von Telekom-Routern im November 2016. Plötzlich begann man darüber zu reden, ob man Hersteller verpflichten sollte, für bestimmte kri-

tische Geräte wie Router Aktualisierungen bereitzuhalten.

Ich bin für Software- und Hardware-Produkthaftung. Man muss nur sorgfältig in kleinen Schritten vorgehen, weil es heute noch keine ausreichenden Standards gibt. Die vorhandenen kommen aus dem Hochsicherheitsbereich und sind zu teuer und aufwendig für Endnutzer-Angebote. Deshalb sollten wir uns langsam annähern.

? Brauchen wir mehr geförderte Angebote, um die Bürger darüber zu informieren, wie sichere Kommunikation funktioniert? Oder ist es sinnvoller, mehr darin zu investieren, um nutzerfreundlichere und sichere Angebote zu schaffen?

UH: Beides sollte gemacht werden. Die Sicherheitsfeatures, die wir heute in den Autos haben, waren auch nicht von Anfang an da. Wir haben sie in den letzten 30 Jahren nach und nach entwickelt und eingebaut. Dieser Prozess ist in der Informationstechnologie ganz am Anfang. Wir haben heute praktisch keine Haftung für IT-Anwendungen, aber fangen langsam an, das zu diskutieren. Wie schon gesagt, das muss in kleinen Schritten geschehen. Auf der anderen Seite kann man den Wettbewerb fördern und den Nutzern sagen, es gibt bestimmte Provider, die besser sind als andere, weil sie höhere Sicherheitsstandards haben.

Leider werden die IT-Medien, also Magazine und Zeitschriften, noch nicht so flächendeckend gelesen wie andere Produktinformationen, zum Beispiel wie das ADAC-Magazin beim Auto. Es gibt zwar *Computer Bild* oder *Heise*, aber sie werden immer noch als Nischenmedien wahrgenommen.

? Wer sollte Ihrer Meinung nach solche Informationskampagnen anstoßen?

UH: Wir haben das im Beirat für „Deutschland sicher im Netz" schon einige Male diskutiert. Leider fiel uns kein Patentrezept dafür ein. Wir haben einige Ideen, aber wir schaffen es nicht, diese so zu skalieren, dass sie die Masse der Menschen erreichen. Es gibt eigentlich eine Menge Initiativen, sowohl staatliche als auch von der Wirtschaft und sogar auf EU-Ebene, wie etwa den Cyber Security Month, den die EU-Mitgliedsstaaten jährlich im Oktober veranstalten. Trotzdem ist die Reichweite gering. Das Bundesamt für Sicherheit in der Informationstechnik hat eine Webseite mit Informationen für Bürger, in der viel Arbeit drinsteckt. Aber auch sie kriegen damit nicht die Skalierung und die Flächendeckung hin, die notwendig ist.

? Vielleicht brauchen wir einfach noch mehr Zeit?

UH: Leider haben wir diese Zeit nicht. Die Sicherheitsvorfälle nehmen mit der Nutzung zu: Die Ransomware-Attacken, WannaCry oder Botnet-Angriffe, die wir in den letzten Monaten erlebt haben, werden sicherlich nicht die letzten sein. Die nächsten Cyberattacken könnten vor der Tür stehen. Wir müssen die Kommunikationssicherheit kurzfristig erhöhen, z. B. durch die Einführung verbindlicher Zertifizierungsmaßnahmen oder Produkthaftung, um auf zukünftige Sicherheitsvorfälle vorbereitet zu sein.

> **„Wir haben heute praktisch keine Haftung für IT-Anwendungen, aber fangen langsam an, das zu diskutieren.** Prof. Dr. Udo Helmbrecht

Grundrecht geschützt. In erster Linie adressiert es wie alle Grundrechte den Staat: Es verbietet, dass staatliche Bedienstete selbst Briefe öffnen. Darüber hinaus entfaltet es aber auch eine Drittwirkung insofern, dass es den Staat zudem verpflichtet, mittels gesetzlicher Regeln dafür Sorge zu tragen, dass auch im Postwesen tätige private Dienstleistungsunternehmen und sonstige Dritte die Vertraulichkeit des Inhalts von Briefen nicht verletzen.[48] Zu diesen gesetzlichen Regeln gehört unter anderem das Strafrecht. Hierdurch wird jede Person strafrechtlich sanktioniert, die das Briefgeheimnis (§ 202 Strafgesetzbuch) oder das Post- oder Fernmeldegeheimnis (§ 206) verletzt.

Auch digitale Kommunikationsvorgänge werden neben den genannten technischen Schutzmaßnahmen durch rechtliche Garantien flankiert, die den Zweck verfolgen, das Vertrauen in das System abzusichern. In erster Linie handelt es sich hierbei wiederum um grundrechtliche Garantien.

So umfasst der Artikel 10 des Grundgesetzes zunächst einmal nicht nur das Brief- und Postgeheimnis, sondern schützt als Fernmeldegeheimnis genauso Inhalte und Umstände individueller Kommunikationsvorgänge, die drahtlos oder drahtgebunden mittels elektromagnetischer Signale erfolgen. Da es auf die konkrete Übermittlungsart hierbei nicht ankommt, erstreckt sich der Schutz auf die Kommunikation via Internet.[49] Auch hier richtet sich das Grundrecht nicht nur an den Staat selbst, um dessen eigene Handlungsmöglichkeiten zu beschränken; er hat im Sinne einer Drittwirkung des Grundrechts auch dafür zu sorgen, dass private Kommunikationsdienstleister das Recht nicht verletzen. Entscheidend ist allerdings, dass die Nachrichten nur dann und so lange von Artikel 10 geschützt sind, wie sie zwischen Absender und Empfänger unterwegs sind – was ein Speichern auf den Servern des E-Mail-Dienstleisters mit einschließt, wie das Bundesverfassungsgericht im Jahr 2009 mit Hinweis auf den Schutzzweck des Grundrechts entschied.[50] Befinden sich die Informationen noch auf dem Computer des Ersteren oder sind bereits angekommen und beim Empfänger gespeichert, greift der Schutzbereich des Grundrechts nicht mehr.[51]

Daten, die sich auf dem Computer einer Person selbst befinden und Auskunft über diese erteilen können, werden nicht durch das Fernmeldegeheimnis, sondern allgemein durch datenschutzrechtliche Regelungen geschützt. Grundrechtlich unterfüttert werden diese durch das Recht auf informationelle Selbstbestimmung, welches durch das Bundesverfassungsgericht im sogenannten Volkszählungsurteil als Ausprägung des allgemeinen Persönlichkeitsrechts herausgebildet worden war.[52] Es definiert die Befugnis jeder Person, im Grundsatz stets selbst darüber bestimmen zu können, ob ihre persönlichen Daten preisgegeben und wie und wofür sie verwendet werden.[53] Weil aber das Recht auf informationelle Selbstbestimmung nach der Konzeption des Bundesverfassungsgerichts notwendig darauf beschränkt ist, vor gezielten und punktuellen Datenerhebungen durch den Staat zu schützen, greift es dann nicht, wenn staatliche Stellen beispielsweise den gesamten Computer eines Bürgers ausspähen oder überwachen. Um diese Schutzlücke zu schließen, entwickelte das Gericht in einer weitreichenden Entscheidung von 2008 das sogenannte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das verfassungsrechtlichen Schutz vor Online-Durchsuchungen gewährt.[54] Sobald digitale Kommunikationsvorgänge also abgeschlossen und die sensiblen Informationen auf dem Rechner des Empfängers gespeichert sind, wird deren Vertraulichkeit nicht mehr durch das Fernmeldegeheimnis, sondern je nach Kontext durch eines der beiden vorgenannten Rechte geschützt. Auch diese beiden Grundrechte richten sich wiederum in zweierlei Hinsicht an den Staat. So ist er einerseits angehalten, sie nicht durch eigene, nicht gerechtfertigte Maßnahmen zu verletzen.[55] Zum an-

48 Bodo Pieroth und Bernhard Schlink, Grundrechte – Staatsrecht II, 23. Auflage, Heidelberg 2007, S. 191.
49 Ebd., S. 193.
50 Bundesverfassungsgericht, Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers nicht verfassungswidrig, Pressemitteilung Nr. 79/2009, 15. Juli 2009, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-079.html.
51 Entscheidung des Bundesverfassungsgerichts im Fall „Kommunikationsdaten", 2. März 2006, http://www.servat.unibe.ch/dfr/bv115166.html.
52 Entscheidung des Bundesverfassungsgerichts im Fall „Volkszählung", 15. Dezember 1983, http://www.servat.unibe.ch/dfr/bv065001.html.
53 Claudio Franzius, Das Recht auf informationelle Selbstbestimmung, Zeitschrift für das juristische Studium 3/2015, S. 259.
54 Ebd., S. 262f.
55 Nicht gerechtfertigt sind solche Maßnahmen insbesondere dann, wenn sie ohne gesetzliche Grundlage vorgenommen werden und/oder nicht verhältnismäßig sind.

deren hat er durch einfachgesetzliche Vorgaben dafür zu sorgen, dass auch private Akteure den Datenschutz achten.

Einfachgesetzliche Absicherungen und Vorgaben

Der weitere rechtliche Rahmen für die Sicherheit digitaler Kommunikation, aus dem Vorgaben sowohl für die Ausgestaltung der technischen als auch der organisatorischen Absicherung folgen, findet sich in 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 oben erläuterten Grundrecht auf informationelle Selbstbestimmung und geht von der grundlegenden Annahme aus, dass stets in das Grundrecht eingegriffen wird, wenn persönliche Daten einer betroffenen Person verwendet werden.[56] 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.

Die oben genannten Grundrechte sowie die Datenschutzgesetze werden durch strafrechtliche Vorschriften ergänzt. So stellt der § 202a des Strafgesetzbuchs das Ausspähen von Daten unter Strafe, die gespeichert und gegen unberechtigten Zugriff gesichert sind, während § 202b Strafgesetzbuch es sanktioniert, wenn jemand Daten, die nicht für ihn bestimmt sind, während einer nicht öffentlichen Datenübermittlung abfängt. Da der § 206 Strafgesetzbuch zudem ausdrücklich auch Verletzungen des Fernmeldegeheimnisses umfasst, sind damit sämtliche Phasen digitaler Kommunikationsvorgänge gegenüber unberechtigten Dritten strafrechtlich abgesichert. Darüber hinaus ist mit dem § 203 StGB allgemein die Verletzung von Privatgeheimnissen durch sogenannte Berufsgeheimnisträger wie Anwälte, Ärzte, Psychologen und weitere Berufsgruppen strafbewehrt. Auch das Bundesdatenschutzgesetz selbst umfasst Vorschriften, die Verstöße entweder mit Bußgeld oder sogar mit Strafe sanktionieren.[57]

Ab dem 25. Mai 2018 ist in Deutschland zudem die Datenschutzgrundverordnung (DSGVO) anzuwenden, die am 24. Mai 2016 in Kraft getreten ist und als Verordnung der Europäischen Union unmittelbare Geltung entfaltet. Das Bundesdatenschutzgesetz verliert seine Geltung nicht, muss aber den Vorgaben der DSGVO entsprechend angepasst werden.[58] 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 (SigV) 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.[59] 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.[60]

56 Ebd., S. 41.
57 Siehe §§ 43, 44 Bundesdatenschutzgesetz; die Gesetze der Länder enthalten entsprechende Bestimmungen.
58 Winfried Veil, Datenschutz in der Mehrebenenfalle, CR-Online, 18. Mai 2017, http://www.cr-online.de/blog/2017/05/18/datenschutz-in-der-mehrebenenfalle/.
59 Heckmann, S. 42.
60 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.

Das Problem der Durchsetzung

Rechtliche Absicherungen sind nur dann in der Lage, Systemvertrauen herzustellen bzw. abzusichern, wenn das Recht auch durchgesetzt wird. Dies ist in der digitalen Welt insbesondere im Hinblick auf die Drittwirkung der genannten Grundrechte und damit auf das Handeln privater Akteure wie beispielsweise von E-Mail-Dienstleistern nicht immer unproblematisch. So bemängeln Datenschutzbeauftragte, dass Verstöße gegen datenschutzrechtliche Bestimmungen kaum sanktioniert werden.[61] Dies kann mitunter auch eine Folge des Umstands sein, dass (noch) nicht immer klar ist, wie sich bestimmte rechtliche Konstruktionen auf digitale Kommunikationsvorgänge übertragen lassen. So beharrt Google beispielsweise auf dem Standpunkt, das Fernmeldegeheimnis sei auf die Praxis des Scannens von E-Mails, die auf den Servern des Unternehmens (zwischen)gespeichert sind, nicht anwendbar, da es sich um automatisierte, also nicht unmittelbar durch Menschen gesteuerte Prozesse handelt.[62]

> **„Es gibt ja auch in anderen Bereichen klare rechtliche Bestimmungen, an die sich Unternehmen halten müssen. Dies kann durchaus auch ein Wettbewerbsvorteil sein und das Vertrauen stärken. Daher wäre es eine gute Idee, höhere Sicherheitsstandards für digitale Kommunikation auch gesetzlich durchzusetzen."**
>
> **Prof. Dr. Bernd Blöbaum,** Institut für Kommunikationswissenschaft der Universität Münster; Sprecher des DFG-Graduiertenkollegs „Vertrauen und Kommunikation in einer digitalisierten Welt", Konsultation

4.1.2 Technische Absicherung

Die aufgezählten Rechtsvorschriften geben den Rahmen vor, innerhalb dessen sich die Sicherung digitaler Kommunikation zu bewegen hat. Schon die genannten Durchsetzungsschwierigkeiten allerdings zeigen, dass gesetzliche Garantien und Verbote allein nicht dafür sorgen können, dass Kommunikation als sicher und damit vertrauenswürdig angesehen werden kann. Dazu ist es vielmehr notwendig, die Vorgaben insbesondere durch technische Maßnahmen zu flankieren. Dies ist für sich genommen keineswegs neu: Schon analoge Kommunikation mittels Briefverkehrs setzte stets auf konkrete technische Vorkehrungen, um den Inhalt zu schützen.

Technische Absicherung von Vertrauen in analoge Kommunikation

Denn auch wer einen Brief verschickt, muss nicht nur darauf vertrauen können, dass der mit der Versendung beauftragte Dienst den Brief auch wie vereinbart zum Adressaten liefert. Schon seit Jahrhunderten ist dieses Vertrauen in die Integrität des Kuriers als nicht hinreichend erachtet worden – selbst wenn er den ihm übergebenen Brief stets verlässlich bei der richtigen Person abgeliefert hat. Dieser Umstand genügte gerade nicht, um ein solides Vertrauen dahingehend zu erzeugen, dass der Brief auch ungeöffnet und damit ungelesen beim Empfänger ankam. Die räumliche Distanz zwischen Versender und Empfänger machte Briefe in besonderem Maße gefährdet für Zugriffe durch Dritte und damit die Verletzung der Privatheit des Inhalts. Schon frühzeitig wurde das Vertrauen in das System der Briefzustellung deshalb durch technische Methoden abgesichert. Mithilfe von Siegeln wurden Briefe so verschlossen, dass niemand den Brief öffnen konnte, ohne das Siegel zu zerstören und somit die Handlung zu offenbaren. Noch heute werden

61 Christiane Schulzki-Haddouti, Datenschutz-Verstöße werden sehr selten sanktioniert, Der Datenschutz-Blog, 4. April 2016, https://www.datenschutzbeauftragter-online.de/datenschutz-verstoesse-werden-sehr-selten-sanktioniert/9536/.

62 Bei Einführung von Googles E-Mail-Dienst Gmail im Jahr 2004 hatten Beauftragte für den Datenschutz verschiedener Länder die Ansicht vertreten, die Praxis, E-Mails zu Werbezwecken routinemäßig automatisiert zu scannen, verstoße gegen das Briefgeheimnis und das Recht auf Privatsphäre, vgl. RP Online, Staatsanwalt soll Google-Mail überprüfen, 18. Mai 2004, https://www.datenschutzbeauftragter-online.de/datenschutz-verstoesse-werden-sehr-selten-sanktioniert/9536/; in einem Gerichtsprozess im kalifornischen San José im Jahr 2013 führte Google hingegen explizit aus, automatisierte Verarbeitung der E-Mails könne keine Verletzung der Rechte darstellen. Mehr noch: "Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their communications are processed by the recipient's ECS [electronic communications service] provider in the course of delivery." Dominic Rushe, Google: Don't Expect Privacy When Sending to Gmail, The Guardian, 15. August 2013, https://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit.

INTERVIEW MIT PROF. DR. CLAUDIA ECKERT

Sichere Kommunikationskanäle sind oft zu kompliziert

? Was bedeutet Vertrauen in digitale Kommunikation für Sie?

Claudia Eckert: Es bedeutet, dass die Kommunikation nur denen zugänglich ist, mit denen ich wirklich kommunizieren möchte. Dass sie nicht abgehört wird, ohne dass ich es mitbekomme; dass sie nicht geändert wird; dass nicht etwas hineingeschnitten wird, was ich nicht gesagt habe – das sind die Dinge, die ich mit Vertrauen in die digitale Kommunikation verbinde.

? Welchen Stellenwert hat dieses Vertrauen für unsere Gesellschaft?

CE: Einen extrem hohen Stellenwert. Wir sind abhängig davon, dass Kommunikation und die Kommunikationsinfrastrukturen funktionieren. In der vernetzten digitalen Welt, in der wir leben, geht es immer um Kommunikation. Das Internet of Things, vernetzte Geräte, beruht auf dem Austausch von Daten. Wenn ich dem nicht mehr

Foto: Fraunhofer AISEC

Prof. Dr. Claudia Eckert

Prof. Dr. Claudia Eckert ist Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit AISEC in München und Professorin der Technischen Universität München, wo sie den Lehrstuhl für IT-Sicherheit in der Fakultät für Informatik innehat.

Zu ihren Forschungsschwerpunkten zählen die Entwicklung von Technologien zur Erhöhung der System- und Anwendungssicherheit, die Sicherheit eingebetteter Systeme und die Erforschung neuer Techniken zur Erhöhung der Resilienz und Robustheit von Systemen gegen Angriffe. Ihre Forschungsergebnisse wurden in über 160 begutachteten Fachbeiträgen veröffentlicht.

Als Mitglied verschiedener nationaler und internationaler industrieller Beiräte und wissenschaftlicher Gremien berät sie Unternehmen, Wirtschaftsverbände sowie die öffentliche Hand in allen Fragen der IT-Sicherheit. In Fachgremien wirkt sie mit an der Gestaltung der technischen und wissenschaftlichen Rahmenbedingungen in Deutschland sowie an der Ausgestaltung von wissenschaftlichen Förderprogrammen auf EU-Ebene.

INTERVIEW MIT PROF. DR. CLAUDIA ECKERT

> **Man muss Sicherheitstechniken so einbauen, dass die Nutzer möglichst wenig Arbeit damit haben.** Prof. Dr. Claudia Eckert

vertrauen kann und den Verdacht habe, dass die Kommunikation unterwandert ist, dann bricht mir ganz viel weg.

? Wie vertrauenswürdig würden Sie unsere aktuellen digitalen Kommunikationsmittel – etwa E-Mail, Messenger – bewerten?

CE: Da muss man unterscheiden: So, wie sie wirklich genutzt werden, oder welches Potenzial sie überhaupt bieten, sie sicher zu nutzen? Man kann E-Mails so nutzen, dass sie vom Absender verschlüsselt und signiert und erst beim Empfänger entschlüsselt werden. Dieser holt sie wie aus einem Briefumschlag wieder heraus. Alle Vermittlungsstellen dazwischen haben keinen Einblick, was versendet wurde. Das Potenzial ist also da.

Die Praxis sieht aber so aus: Nur ein Bruchteil der Menschen benutzt diese Sicherheitsmechanismen, die im Prinzip verfügbar sind. Eine E-Mail ist in der Form, wie sie die meisten Menschen verwenden, mit Sicherheit nicht vertrauenswürdig. Wir bekommen Informationen von Personen, die ihre Absenderadressen verschleiern, Inhalte werden verfälscht, E-Mails werden abgefangen und mitgelesen, Nachrichten werden umgeleitet. Das ist der Stand der Dinge, das geschieht jeden Tag. Die sicheren Verfahren werden nicht verwendet. Sie sind zu kompliziert, und die Menschen sind überfordert. Die Technologie ist da, aber sie ist nicht nutzbar.

Messenger-Dienste sind einen Schritt weiter, weil manche grundlegenden Sicherheitsfeatures schon integriert sind. Viele Messenger verschlüsseln automatisiert die Nachrichten – WhatsApp, der Messenger, der in Deutschland wahrscheinlich am meisten genutzt wird, hat das inzwischen eingeführt. Es gibt aber auch andere Anbieter, wie Threema, Signal oder Wire, die das machen. Die Nutzer merken davon nichts. Deshalb funktioniert das in diesem Bereich. Man muss Sicherheitstechniken so einbauen, dass die Nutzer möglichst wenig Arbeit damit haben.

? Brauchen wir einen neuen Standard zur Verschlüsselung, wenn die Technik zu kompliziert ist? Am besten in einer konzertierten Aktion von mehreren Marktakteuren?

CE: Einen neuen Standard brauchen wir nicht. Wir haben ja mehrere funktionierende Standards. Wir brauchen eher praktikable Lösungen, die es erlauben, zwischen all den Standards hin und her wechseln zu können. Beispiel: Ich habe in meinem Mailprogramm sowohl die Erweiterungen für die S/MIME-Verschlüsselung als auch für die PGP-Verschlüsselung installiert. Aber die beiden sind untereinander nicht kompatibel. Ich muss immer verschiedene Wege wählen, je nachdem, was mein Gegenüber benutzt. Ich bräuchte eigentlich eine Art Adapter, eine Art Zwischenschicht, die diesen Austausch umsetzt. Ich frage mich immer, wieso bei der E-Mail diese Interoperabilität fehlt. Beim Mobilfunk gibt es Roaming. Da werden Sie von Zelle zu Zelle und Netz zu Netz weitergereicht, ohne dass Sie als Benutzer irgendetwas tun müssen oder es überhaupt merken. Wieso schaffen wir das bei E-Mails nicht?

? Wie könnte man die Anreize setzen, um das zu erreichen? Brauchen wir höhere Sicherheitsstandards, die verpflichtend sind?

CE: Es gibt ja schon verpflichtende Sicherheitsstandards, zwar nicht für Normalbürger, aber für Unternehmen. Es ist aber schwierig, Menschen durch Regularien dazu zu bekommen, sich auf eine bestimmte Weise zu verhalten. Das funktioniert besser durch Anreiz- und Belohnungssysteme. Das heißt, der Kunde oder die Kundin bekommt einen Teil des Preises zurückerstattet, wenn er oder sie etwas tut. Oder hat Zugang zu einem sonst verschlossenen Bereich. Einfach etwas verbieten – und die Einhaltung dieses Verbots überwachen – ist im IT-Umfeld schwierig und eher nicht sinnvoll.

Die Frage ist also: Sind Belohnungssysteme vorstellbar, wenn jemand konsequent Sicherheitsdienste einsetzt? Das Konzept kennen wir zu einem gewissen Grad aus der Versicherungswirtschaft. Wer entsprechend Vorsorge treibt, sein Risiko eindämmt und Maßnahmen ergreift, um keinen Schaden zu erleiden, wird in seiner Versicherungspolice heruntergestuft oder bekommt Rabatte. Könnte man sich auf dieser Basis Businessmodelle überlegen, die es schaffen, dass sowohl Anbieter als auch Endkunden konsequent Security einsetzen? Das wäre eine Überlegung wert.

? Wie bewerten Sie Gütesiegel und Zertifikate, um das Vertrauen in die digitale Kommunikation zu stärken oder überhaupt entstehen zu lassen?

CE: In Deutschland schauen wir durchaus stark auf Gütesiegel. TÜV-Plaketten strahlen eine Art Verlässlichkeit aus. Da hat jemand nach gewissen Standards auf ein Produkt geschaut, hat sein Siegel darunter gesetzt, und damit kann ich sicher sein: Das hat eine gewisse grundlegende Qualität. Es würde gerade in Deutschland einen Mehrwert darstellen, solche Gütesiegel zu vergeben, wenn es klar wäre, nach welchen Regeln die Siegel verliehen werden. Was wird eigentlich zertifiziert? Einfach nur, dass die Weboberfläche gut gestaltet ist? Oder ob ein Programm wirklich kein Schindluder treibt?

Wenn das eine vernünftige Sicherheitsanalyse ist, in der die Gerätschaften nach dem Stand der Technik durchleuchtet werden, dann hat es einen gewissen Sinn. Dadurch würde das Vertrauen schon steigen. Das wäre vor allem wichtig bei Technologien wie dem Internet of Things, bei dem Geräte aus aller Herren Länder eingebaut werden und miteinander kommunizieren, ohne dass ich nur die leiseste Ahnung habe, was sie wirklich tun. Das könnte eine gewisse Basisqualität herstellen, die das Siegel bestätigt. ⊡

> **Es würde gerade in Deutschland einen Mehrwert darstellen, solche Gütesiegel zu vergeben, wenn es klar wäre, nach welchen Regeln die Siegel verliehen werden.**
>
> Prof. Dr. Claudia Eckert

Briefumschläge so verschlossen, dass ihr Inhalt im Normalfall nicht unbemerkt von jemand anderem als dem bezweckten Adressaten gesichtet werden kann. Zugespitzt könnte man sagen, dass der Briefverkehr viele Merkmale einer digitalen Ende-zu-Ende-Verschlüsselung aufweist: Der Versender verschließt die Nachricht oder versiegelt sie gar, und erst der vorgesehene Empfänger öffnet den Umschlag und erhält somit Zugriff auf den Inhalt.

Technische Unterstützung von Systemvertrauen in Kommunikation in der digitalen Welt

Die spezifischen Eigenschaften der digitalen Sphäre erschweren die Vertrauensbildung in die Kommunikation erheblich. Einige der Faktoren, die eine zentrale Rolle spielen, wenn sich Vertrauen zwischen Kommunikationsteilnehmerinnen und -teilnehmern herausbilden soll, lassen sich nur schwer oder gar nicht im Internet abbilden. Aspekte wie erleichterte Anonymität, flexible Identitäten, Entkörperlichung oder nur schwer durchschaubare Kontexte, vor deren Hintergrund Kommunikation stattfindet, unterminieren interpersonales Vertrauen.[63] Hinzu kommt, dass viele vormals sichtbare Vorgänge, die im Zusammenhang mit Kommunikation nun digital erfolgen, im Verborgenen stattfinden und jedenfalls für den technisch durchschnittlich informierten Bürger kaum nachvollziehbar sind, was es zusätzlich erschwert, den Prozess als vertrauenswürdig zu empfinden.

Da interpersonales Vertrauen aus diesen Gründen insofern noch schwerer zu realisieren ist als bei Kommunikation, die auf analogen Wegen erfolgt, liegt es nahe, bei digitaler Übermittlung von Informationen das Vertrauen in das System noch stärker durch technische Maßnahmen abzusichern bzw. zu unterstützen. Hierbei geht es neben dem Schutz des Inhalts der Kommunikation auch um die Authentizität; also darum, dass die Identität des Absenders verifiziert werden kann und sichergestellt ist, dass die Nachricht tatsächlich von dem Absender stammt, von dem sie zu stammen scheint. Obwohl es selbstverständlich schon im analogen Zeitalter möglich war, Schriftstücke zu fälschen, ist dies durch digitale Hilfsmittel um ein Vielfaches einfacher geworden.

Um die so umrissene technische Absicherung zu erreichen, 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 Annex.

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, sodass nur Personen, die im Besitz des digitalen Schlüssels sind, den so chiffrierten Inhalt nach Empfang der Nachricht zurück in Klartext umwandeln können.[64] Öffentliche Stellen und privatwirtschaftliche Unternehmen sind aufgrund des geltenden Rechtsrahmens in gewissem Maße 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 (diese 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[65], was bedeutet, dass der Inhalt der

63 Helen Nissenbaum, Will Security Enhance Trust Online, or Supplant It?, in: R. Kramer und K. Cook (Hg.), Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions, New York 2004, S. 155, 161f.
64 Vgl. Wikipedia, Verschlüsselung, https://de.wikipedia.org/wiki/Verschl%C3%BCsselung.
65 Vgl. Wikipedia, Leitungsverschlüsselung, https://de.wikipedia.org/wiki/Leitungsverschl%C3%BCsselung.

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.[66] Daher gilt die Ende-zu-Ende-Verschlüsselung als wesentlich sicherer als die bloße Punkt-zu-Punkt-Verschlüsselung.

> **„Ende-zu-Ende-Verschlüsselung ist technisch möglich und könnte auch flächendeckend bei E-Mails durchgesetzt werden. Die Frage ist nur, wer diese Aufgabe übernimmt und hier die nötigen Ressourcen investiert."**
>
> **Prof. Dr. Norbert Pohlmann,** Professor für Informationssicherheit an der Westfälischen Hochschule und Geschäftsführender Direktor des Instituts für Internet-Sicherheit if(is), Konsultation

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

(a) Messenger-Dienste. In den vergangenen Jahren sind 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.[67] Das liegt daran, dass diese Art der Verschlüsselung bei geschlossenen Kommunikationsplattformen wesentlich einfacher zu realisieren ist als bei einer nicht geschlossenen wie der „offenen" 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 und nutzen den Dienst weiter wie zuvor, als die Verschlüsselungsmethode noch nicht zum Einsatz kam.[68]

(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 zur Verschlüsselung einigen, was allerdings schon aufgrund ihrer großen Anzahl sowie der unterschiedlichen geschäftlichen Interessen unwahrscheinlich erscheint.[69] 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. Das Fraunhofer-Institut für Sichere Informationstechnologie hat basierend auf dem Verschlüsselungsstandard S/MIME unter dem Namen „Volksverschlüsselung" eine Infrastruktur und eine Software zur sicheren Ende-zu-Ende-Verschlüs-

66 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/.
67 Wikipedia, End-to-end encryption, https://en.wikipedia.org/wiki/End-to-end_encryption.
68 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.
69 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.

selung entwickelt.[70] Dieses Verfahren setzt insbesondere auf Benutzerfreundlichkeit.

(c) Verschlüsselnde Mail-Systeme: De-Mail und E-Postbrief. Systeme zur Erhöhung der Sicherheit sind auch der von der Deutschen Post 2010 eingeführte E-Postbrief[71] sowie die sogenannten De-Mail-Dienste. Beide Systeme sind plattformbasiert. Sicherheit wird dadurch hergestellt, dass auf den Übermittlungswegen konsequent Transportverschlüsselung eingesetzt wird.

De-Mail-Dienste werden von Anbietern von E-Mail-Diensten bereitgestellt, 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.[72] 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 März 2015 jedoch an, künftig eine auf PGP basierende Ende-zu-Ende-Verschlüsselung als Option für alle Nutzer anzubieten.[73]

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.[74] 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 leisten. 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.[75]

Sowohl De-Mail-Dienste als auch der E-Postbrief sind geschlossene Systeme.

(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.[76] 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, mit 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 dem 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.

70 Vgl. https://volksverschluesselung.de.
71 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.
72 Siehe die Liste akkreditierter Anbieter unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/Akkreditierte_DMDA/Akkreditierte_DMDA.html.
73 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.
74 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.
75 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.
76 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.

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 bzw. des übermittelten Dokuments und garantieren dessen Unverfälschtheit, indem sie nachträgliche Veränderungen erkennbar machen.[77] 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[78], durchgeführt.

Sicherung der informationstechnischen Systeme. Um sichere digitale Kommunikation zu ermöglichen, müssen 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 gehört 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.[79]

> **„Als Laie ist es nicht notwendig, alle technischen Details der Verschlüsselung zu verstehen. Dies ist ja auch in anderen Bereichen wie etwa beim Fliegen oder Bahnfahren nicht der Fall. Viel mehr zählt die intuitive Checkliste zum Vertrauen, die etwa danach fragt, wie kompetent ist der Anbieter, welche Motive hat er, wie ist seine Reputation."**
>
> **Prof. Dr. Bernd Blöbaum,** Institut für Kommunikationswissenschaft der Universität Münster; Sprecher des DFG-Graduiertenkollegs „Vertrauen und Kommunikation in einer digitalisierten Welt", Konsultation

> **„Was ich schade fände, ist, wenn der Nutzer meint, er könne nichts tun. Am Ende ist es wie bei jedem Konsumgut: Wenn man etwas nicht mehr nutzt, reagiert der Markt darauf und muss dann etwas ändern. Die Menschen sollten auch ein bisschen mehr darauf achten, welche digitalen Kommunikationsdienste sie nutzen. Man nimmt ja an dem ganzen System teil, und daher glaube ich, wenn auch vom Nutzer selbst gefordert werden würde, dass digitale Kommunikationsmittel transparenter und einfacher handhabbar sein müssen, die Internetsicherheit auch zunehmen würde."**
>
> **Marion Grether,** Direktorin des Museums für Kommunikation Nürnberg, Konsultation

77 Heckmann, S. 42.
78 TAN: transaction authentification number, Transaktionsnummer.
79 Für einen Überblick über zu treffende Maßnahmen siehe Wikipedia, Informationssicherheit, https://de.wikipedia.org/wiki/Informationssicherheit.

4.1.3 Organisatorische Absicherung

Neben der technischen und der rechtlichen kann auch eine organisatorische Absicherung zur Stärkung von Vertrauen führen. Infrage kommen Maßnahmen vielfältiger Art. Organisation als Merkmal erfordert als Träger in der Regel eine Institution, und diese kann beispielsweise durch prozess- oder regelbasiertes Arbeiten, durch die Einführung geeigneter Rollen, durch Selbstverpflichtungen, durch Zertifizierungen oder durch eine lange Tradition verlässlichen Handelns vertrauensstiftend wirken. Erst dies ermöglicht es, dass Recht in zielgerichtetes Verhalten, gerade auch technischer Natur, umgesetzt wird. Damit dient sie als ein wichtiger Transmissionsmechanismus, der den rechtlichen Rahmen wirksam und die technischen Maßnahmen umsetzbar macht.

Organisatorische Maßnahmen sind Schutzinstrumente, die entweder darauf abzielen können, 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.

Zuständig für die organisatorische Stützung von 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 vorhergehenden Kapitel 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 in gleichem Maße durchzuführen hat. Entscheidend ist unter anderem stets, wie sensibel die Informationen sind, die erhoben und verarbeitet werden.[80]

Eine zentrale Verpflichtung für öffentliche Stellen und Unternehmen, die mit personenbezogenen Daten umgehen, ist es, 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.[81] Darüber hinaus zu treffende Maßnahmen sind beispielsweise das Vier-Augen-Prinzip[82], Überwachung und Kontrolle der Datenverarbeitungsvorgänge durch entsprechend geschultes und eingeteiltes Personal[83], Identitätskontrollen wie z. B. durch Chipkarten in sensiblen Bereichen des Betriebs[84], der Erlass von

80 Kai-Uwe Plath (Hrsg.), Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. Auflage 2016, S. 358.
81 Ebd., S. 351.
82 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."
83 Plath, S. 353.
84 Ebd., S. 359.

Arbeitsrichtlinien etwa über den sicheren Umgang mit Datenträgern[85] oder die regelmäßige Erstellung von Sicherungskopien.[86] Auch gelegentliche unangekündigte Überprüfungen der Maßnahmen zum Schutz der gespeicherten und verarbeiteten Inhalte dienen dazu, das Schutzniveau zu erhöhen.[87]

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.[88] 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 einen Wettbewerbsvorteil bewirken kann.[89] Allerdings sieht § 9a Satz 2 BDSG ausdrücklich vor, dass die näheren Anforderungen an den Prozess des Audits in einem Spezialgesetz näher ausformuliert werden sollen. Dies ist jedoch bis heute nicht geschehen.[90]

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 andere 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.[91]

85 Ebd., S. 361.
86 Ebd., S. 364.
87 Vgl. Datenschutz-Wiki, Checkliste Technische und organisatorische Maßnahmen, https://www.datenschutz-wiki.de/Checkliste_Technische_und_organisatorische_Ma%C3%9Fnahmen.
88 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/TechnischeRichtlinien/TechnRichtlinien_node.html.
89 Vgl. Plath. S. 366f.
90 Ebd., S. 367.
91 Ebd., S. 1196.

Ein Beispiel für eine solche Vereinigung in Deutschland, die zum Zweck der Selbstregulierung im Bereich des Datenschutzes geschaffen worden ist, ist der Selbstregulierung Informationswirtschaft e.V. (SRIW), der von Bitkom und Unternehmen der digitalen Wirtschaft gegründet wurde.[92] 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.[93]

> **„Gütesiegel sind vielfach nur ein Marketinginstrument und hängen schnell den technologischen Entwicklungen hinterher. Daher sind Gütesiegel grundsätzlich kritisch zu hinterfragen. Ich würde den Markt spielen lassen und nur dort eingreifen, wo der Nutzer in seiner Entscheidungskraft ausgehebelt wird."**
>
> **Roman Flepp,** Pressesprecher, Threema GmbH, Konsultation

Schließlich können Unternehmen und Behörden, die mit sensiblen Informationen ihrer Kunden und Bürger umgehen, 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.[94] 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.[95]

> **„Im Hinblick auf IT-Sicherheit nehmen Behörden in Deutschland eine besondere Position ein. Sie genießen einen großen Vertrauensvorschuss – daher liegt ihnen viel an der Vertrauenswürdigkeit der bereitgestellten Systeme, und IT-Sicherheit spielt bei deren Entwicklung eine entscheidende Rolle."**
>
> **Patrick Franitza,** stellv. Pressesprecher der secunet Security Networks AG, Konsultation

4.1.4 Bewertung

Im Hinblick auf den formulierten Grundsatz, 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

92 https://sriw.de/.
93 https://sriw.de/index.php/der-sriw.
94 Es handelt sich um die sogenannte ISO 27001-Zertifizierung, vgl. https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html.
95 Vgl. Wikipedia, IT-Grundschutz, https://de.wikipedia.org/wiki/IT-Grundschutz.

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.[96] Doch selbst De-Mail-Dienste sowie der E-Postbrief der Deutschen Post, deren zentrales Geschäftsmodell gerade das hohe Datensicherheitsniveau darstellt, setzen nicht oder jedenfalls nicht standardmäßig auf die höchste erreichbare Sicherheitsstufe. Das liegt nicht zuletzt daran, dass ein höheres Verschlüsselungsniveau noch immer eine längere Verarbeitungszeit bedeutet und vor allem mit erheblich größerem Aufwand für die Kommunizierenden verbunden ist. Zudem kann es schwierig sein, bestimmte Funktionen im Rahmen einer Ende-zu-Ende-Verschlüsselung abzubilden.

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.[97] 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.[98] 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.[99] Andererseits ist vielen die Einrichtung sicherer Technologien entweder zu aufwendig, oder sie wissen schlicht gar nicht, dass und wie sie selbst – etwa durch Nutzung technisch besser abgesicherter Systeme als unverschlüsselter E-Mails – für die Sicherheit ihrer Kommunikation sorgen können.[100]

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 potenzielle Nutzer, zumal, wenn sie technisch weniger

96 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.

97 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.

98 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.

99 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.

100 Vgl. die Umfrage der Convios Consulting, S. 7.

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.

4.2 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 offene 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. Es handelt sich um geschlossene Systeme – sie sind nicht 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. Es handelt sich bei ihnen um geschlossene Systeme, die dadurch zwar eine gesteigerte Absicherung bei hoher Benutzerfreundlichkeit aufweisen können, in Konsequenz aber nicht mit anderen digitalen Kommunikationsmitteln kompatibel sind.[101] Einige Faktoren bei der Nutzung sind für ein höheres Schutzniveau notwendig, erfordern allerdings im Vorfeld einen höheren Aufwand seitens des Nutzers. 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

101 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 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.

INTERVIEW MIT TIM TAUBERT

Verbraucher interessieren sich für sichere Kommunikation

? Was bedeutet Vertrauen in digitale Kommunikation für Sie?

Tim Taubert: Vertrauen heißt, dass ich den Produkten, die ich kaufe und zur Kommunikation benutze, aber auch den Netzwerken, die diese Produkte wiederum benutzen, aus welchem Grund auch immer vertraue. Ob ich ihnen vertraue, weil sie gute Werbung machen, weil ich informiert bin, weil der Quelltext frei verfügbar (Open Source) ist oder weil mir Freunde gesagt haben, das wäre ein guter Dienst, ist nicht entscheidend. Vertrauen ist ja immer auf eine Art blind.

? Und warum würden Sie das als blindes Vertrauen bezeichnen? Die Menschen haben sich doch informiert und bewusst eine Kommunikationsmethode gewählt, die sie für vertrauenswürdig halten.

TT: Aus ihrer Sicht mag das stimmen, aber aus meiner Sicht – jemand, der sich den ganzen Tag mit Kryptografie, Sicherheit und Software beschäftigt – ist das trotzdem ein blindes Vertrauen. Selbst für mich ist es aufwendig, herauszufinden, ob ein Produkt vertrauenswürdig ist oder nicht. Selbst ich muss mich auf Meinungen aus der Sicherheits-Community verlassen. Ich kann zwar selbst Nachforschungen anstellen, um zu prüfen, ob die Verschlüsselung sicher ist,

Foto: Andreas Prietzel

Tim Taubert

Tim Taubert ist IT-Sicherheitsexperte und spricht hier ausschließlich für sich selbst. Er arbeitet derzeit bei Mozilla, wo er hauptsächlich für sichere und verschlüsselte Kommunikation des Firefox-Browsers verantwortlich ist. Seine Arbeitsgebiete sind unter anderem Verschlüsselungsprotokolle, angewandte Kryptografie und formale Verifikation von kryptografischen Algorithmen. Er bloggt auf timtaubert.de und twittert unter @ttaubert.

INTERVIEW MIT TIM TAUBERT

> **Ich bin unsicher, inwiefern Zertifizierungen für Software überhaupt sinnvoll sind.**
>
> Tim Taubert

ob sie gut implementiert ist, ob der Dienst vertrauenswürdig ist – das ist aber sehr langwierig. Es ist zwar gut, wenn Nutzer sich informieren und bewusst dafür entscheiden, ein verschlüsseltes Produkt zu verwenden. Das heißt aber nicht unbedingt, dass sie die Fähigkeiten haben, zu beurteilen, ob das Produkt wirklich das tut, was es sagt. Sie müssen den Aussagen anderer vertrauen.

? Was würden Sie als Experte sagen: Unter welchen Umständen ist Vertrauen in digitale Kommunikationsmittel gerechtfertigt und wann nicht?

TT: Vertrauen ist etwas, das sich über die Zeit und die Nutzerzahlen definiert. Wenn ein Produkt vor fünf Jahren auf den Markt gekommen ist und seitdem nur gute Bewertungen bekommt und die Leute, die sich auskennen, der Meinung sind, dass es sicher ist, weil sie noch besser informierten Leuten vertrauen, dann entsteht eine Art Kette, der man wahrscheinlich vertrauen kann. Ich glaube nicht, dass man sich alleine informiert entscheiden kann, weil das wie gesagt selbst für Experten schwer ist.

? Eine solche Kette, über Reputation Vertrauen zu gewinnen und zu stärken, ist eine sehr langwierige Sache. Wie kann ein Unternehmen oder eine Organisation versuchen, schneller bei den Nutzern Vertrauen zu generieren?

TT: Es würde schon helfen, wenn der Gesetzgeber nicht der Meinung wäre, er müsse in der Lage sein, jegliche Kommunikation abzuhören. Und dann so etwas wie die Entschlüsselungsbehörde ZITiS (Zentrale Stelle für Informationstechnik im Sicherheitsbereich) aufbaut, in dem Wunsch, das durchzuführen. Wenn der Bundesinnenminister Thomas de Maizière behauptet, er könnte WhatsApp-Nachrichten abhören, dann zerstört das das Vertrauen der Nutzer. Dabei spielt es keine Rolle, ob er es wirklich kann. Schon die Behauptung untergräbt das Vertrauen in digitale Kommunikation.

? Was halten Sie dann von staatlichen Zertifizierungen und Gütesiegeln?

TT: Natürlich könnte der Staat mit dem Bundesamt für Sicherheit in der Informationstechnologie (BSI) zusammenarbeiten – oder das BSI könnte das alleine tun – und bestimmte Richtlinien aufstellen. Die sind aber davon abhängig, wie sehr man dem Staat zutraut, sinnvolle Richtlinien für diese komplexe Problematik zu erlassen.

Ich bin unsicher, inwiefern Zertifizierungen für Software überhaupt sinnvoll sind. Viele der vorhandenen Richtlinien sind sehr exotisch und nicht mehr zeitgemäß. Der Prozess, in dem Zertifizierungen entstehen, ist recht langwierig und konservativ. Sie haben für Software für den Massenmarkt nur einen begrenzten Sinn, weil sie bisher nur dafür sorgen, dass die Software für den staatlichen Einsatz geeignet ist. Das hat nichts damit zu tun, was wir mit Sicherheit für normale Nutzer meinen.

? Hier eine andere Idee: Brauchen wir höhere Sicherheitsstandards, die

gesetzlich durchgesetzt werden? Zum Beispiel, dass Anbieter regelmäßige Sicherheits-Updates anbieten müssen – und wenn sie das nicht tun, müssen sie haften.

TT: Ich bin auf jeden Fall gegen eine solche Pflicht, weil ich nicht daran glaube, dass der Gesetzgeber in der Lage wäre, das ordentlich zu formulieren. Die Software-Welt bewegt sich so schnell, dass ein Gesetz schon kompletter Unsinn wäre, sobald es verabschiedet würde.

Ich glaube zwar sonst nicht so sehr an den freien Markt, aber in dem Fall würde ich den Verbrauchern ein bisschen Macht zugestehen, dass sie sich für die technisch fortgeschrittenere Lösung entscheiden. Heutzutage ist ein Browser, der sich nicht automatisch aktualisiert, völlig obsolet. Nutzer erwarten, dass Updates im Hintergrund geladen werden. Vor fünf, sechs Jahren war das noch nicht so. Heutzutage ist es auch völlig normal, dass ein Messenger die Nachrichten Ende-zu-Ende verschlüsselt. Ob die Verschlüsselung ordentlich implementiert ist oder nicht, ist eine andere Frage. Aber zumindest ist das ein Begriff, mit dem Verbraucher etwas anfangen können und worauf sie achten.

Die Software- und Sicherheitsindustrie hat noch einen sehr weiten Weg vor sich und muss noch viel verbessern. Aber ich glaube, sie ist selbst daran interessiert, vor allen Dingen, weil die Verbraucher immer mehr Wert darauf legen. Sie wollen einen sicheren Browser. Sie wollen, dass ihre Nachrichten verschlüsselt werden. Die Gesetzgebung kann hier nicht das einzige Mittel der Wahl sein.

? Wir hatten ja schon gesagt, dass die meisten Menschen sich nicht unbedingt gut auskennen mit digitalen Produkten. Brauchen wir geförderte Angebote, wo man zum Beispiel lernt, wie Verschlüsselung funktioniert?

TT: Ich wäre sehr begeistert davon, wenn es solche Angebote gäbe. Wir selbst haben zum Beispiel beim Girl's Day – das ist ein Tag, an dem Schülerinnen sich sogenannte Männerberufe anschauen – versucht, den Mädchen näherzubringen, was wir tun. Das Thema war Snapchat, weil das viele Jugendliche nutzen. Wir haben über Fragen geredet wie: Was passiert, wenn man Snapchat verwendet? Wie läuft die Kommunikation ab, ist sie sicher? Was denken sie, was mit den Fotos auf den Snapchat-Servern passiert? Wenn das Foto auf dem Handy ihrer Freundin nach zehn Sekunden verschwindet, glauben sie, dass das Foto wirklich weg ist?

Das wurde eigentlich immer ziemlich gut angenommen. Mein Eindruck ist, Verbraucher haben an solchen Informationen Interesse. Es gibt genug Leute, die gerne mehr darüber wissen würden, die aber Schwierigkeiten haben, in der Flut von Informationen im Internet irgendetwas Sinnvolles zu finden – vor allem, wenn sie Informationen auf Deutsch suchen. ⊡

> **Die Software- und Sicherheitsindustrie hat noch einen sehr weiten Weg vor sich und muss noch viel verbessern.**
>
> Tim Taubert

ist –, sind zwei voneinander unabhängige Sicherungsmittel erforderlich, also beispielsweise die Eingabe eines Passwortes und die Nutzung der eID-Funktion des elektronischen Personalausweises.[102]

Auch die Registrierung zum E-Postbrief erfordert anfänglich einen gewissen Aufwand für den Nutzer: So muss zunächst der Ausweis bei einer Postfiliale vorgelegt werden. Daneben wird 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. Dieses Verfahren ist etwas zeitaufwendiger als die im Vergleich schnelle Registrierung eines neuen Kontos bei einem normalen E-Mail-Dienstleister, für die Sicherstellung einer eindeutigen Identifikation des E-Postbrief-Kontoinhabers und zur Vermeidung von Sicherheitsbrüchen im Anmeldeprozess aber notwendig.

Die Anmeldung beim Webportal des E-Postbrief-Dienstes ist für gewöhnlich mit einem einfachen, selbst gewählten 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-Postbrief-Kontos zu erhöhen.

> **„Verschlüsselungen in der digitalen Kommunikation müssen sich zunächst in der Nutzer-Community durchsetzen. Obwohl bereits Angebote existieren, die der Nutzer relativ einfach umsetzen kann, ist dies noch nicht der Fall."**
>
> **Matthias Gärtner,** Pressesprecher beim Bundesamt für Sicherheit und Informationstechnik, Konsultation

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.[103] Das Problem ist hierbei allerdings, dass der Einsatz der genannten Verschlüsselungstechnologien bislang kaum laientauglich ist. Neuere Browser-Plug-ins wie beispielsweise Mailvelope sind zwar benutzerfreundlicher, stehen bislang aber nur für wenige E-Mail-Dienste zur Verfügung.[104] Darüber hinaus besteht bei dieser asymmetrischen Verschlüsselungsmethode[105] die zusätzliche Gefahr, dass der Nutzer seinen privaten, geheimen Schlüssel vergisst. Ist dies geschehen und hat der Nutzer nicht die Vorsichtsmaßnahme der Anfertigung einer 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.[106]

Angesichts der aufgeführten Probleme im Hinblick auf die Nutzerfreundlichkeit besonders sicherer digitaler Kommunikationsmittel versuchen Anbieter wie ProtonMail, einen Kompromiss anzubieten.[107] 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.

102 Vgl. Wikipedia, De-Mail, https://de.wikipedia.org/wiki/De-Mail#De-Mail-Nutzerkonten_und_-Adressen.
103 Heckmann, S. 68.
104 Michael Herfert, Annika Selzer und Ulrich Waldmann, Laientaugliche Schlüsselgenerierung für die Ende-zu-Ende-Verschlüsselung, DuD 2016, S. 290, 291.
105 Zur Erläuterung des Begriffs „asymmetrische Verschlüsselungsmethode" siehe den Annex.
106 Heckmann, S. 68.
107 https://protonmail.com; nach Aussage des Unternehmens hatte ProtonMail Anfang 2017 über zwei Millionen Nutzer, siehe https://protonmail.com/blog/tor-encrypted-email/. 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.

Die Benutzerfreundlichkeit von Portallösungen hängt stark von der konkreten Ausgestaltung des jeweiligen Portals ab. Wird Zwei-Faktor-Authentifizierung eingesetzt, mag diese 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. Hier findet ein Übergang von einer Bring- zur Holschuld bei der Kommunikation mit Behörden und Unternehmen statt. 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 mehrere 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 von Passwörtern für die verschiedenen Portale macht diese Verfahren nicht nur nutzerunfreundlich, sondern stellt potenziell 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 mit diesem Passwort gesichert wurden, gleichzeitig kompromittiert, sofern der Dienst die Passwörter nicht ausreichend gesichert hat.[108]

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.[109] Als Vorbild für ein solches zentralisiertes Portal bietet sich auch ein Blick nach Estland[110] 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.[111] 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 sollten 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.

108 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).

109 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.

110 Die Vorbildfunktion ist allerdings mit Einschränkungen zu verstehen, da Estland als kleines Land und durch die Chance, nach der Unabhängigkeit die digitale Infrastruktur von Grund auf neu aufzubauen, andere Rahmenbedingungen bei der Digitalisierung als größere Länder mit einer etablierten Infrastruktur hatte.

111 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.

INTERVIEW MIT LARS KLINGBEIL

Bedienerfreundliche und sichere Produkte können ein Wettbewerbsvorteil sein

? Herr Klingbeil, was bedeutet Vertrauen in digitale Kommunikation für Sie, und welchen Stellenwert hat dieses Vertrauen für unsere Gesellschaft?

Lars Klingbeil: Vertrauen in digitale Kommunikation bedeutet für mich, dass ich mich darauf verlassen können muss, dass die Unternehmen ihr Bestes geben, damit meine Kommunikation unter denjenigen bleibt, für die die Kommunikation bestimmt ist. Außerdem muss ich mich darauf verlassen können, dass sie wenigstens versuchen, andere Akteure – wie zum Beispiel Staat, Geheimdienste oder auch Hacker – aus dieser Kommunikation herauszuhalten. Kurz gefasst: Beim Vertrauen geht es um die Sicherstellung der Integrität, Vertraulichkeit und Authentizität der digitalen Kommunikation.

? Was muss denn passieren, damit das Vertrauen gerechtfertigt ist?

Lars Klingbeil

Lars Klingbeil, SPD, geboren 1978 in Soltau, ist seit 2005 Mitglied des Bundestages. Er war 2006 Mitglied im Bundesvorstand der Jusos und während des Studiums Mitarbeiter im Abgeordnetenbüro des damaligen Bundeskanzlers Gerhard Schröder. 2005 rückte er in den Deutschen Bundestag nach, 2009, 2013 und 2017 wurde er erneut als Mitglied des Bundestages gewählt. Seit 2006 führt er die SPD im Landkreis Heidekreis. Er ist Vorsitzender der Landesgruppen Niedersachsen und Bremen der SPD-Bundestagsfraktion, er ist Mitglied im SPD-Fraktionsvorstand, Mitglied im Ausschuss für Digitale Agenda und dort Sprecher der SPD-Bundestagsfraktion, und er ist ebenfalls Mitglied im Verteidigungsausschuss.

Foto: Tobias Koch

Die Unternehmen sollten meiner Ansicht nach viel mehr in Verschlüsselung und in vertrauliche Kommunikation investieren. Lars Klingbeil

LK: Die Unternehmen müssen sich anstrengen, dass sie die sicherste Kommunikationstechnik zur Verfügung stellen, und der Staat muss sich vernünftig verhalten und einen entsprechenden Rahmen setzen. Dann muss die Technik schauen, wie sie die Schwachstellen in den Kommunikationsinfrastrukturen ausbügelt, etwa durch vertrauenswürdige und sichere Verschlüsselungsmethoden. Allerdings habe ich momentan überhaupt kein Vertrauen. Spätestens seit den Enthüllungen von Edward Snowden in der NSA-Affäre ist es bei mir völlig zerstört. Unser Innenminister redet darüber, dass der Staat mit Sicherheitslücken arbeiten und diese ggf. sogar einkaufen sollte, und Vorratsdatenspeicherung wird wieder ernsthaft diskutiert. Das sind alles Punkte, die das Vertrauen beschädigen.

? Brauchen wir dann mehr Engagement von den Unternehmen oder der Zivilgesellschaft in diesem Bereich?

LK: Die Unternehmen sollten meiner Ansicht nach viel mehr in Verschlüsselung und in vertrauliche Kommunikation investieren. Das könnte ein großer Wettbewerbsvorteil sein. Leider sind sichere Kommunikationskanäle häufig viel zu kompliziert und werden deswegen nicht verwendet. Wenn jemand Produkte auf den Markt bringen würde, die bedienerfreundlich sind und gleichzeitig hohe Sicherheitsstandards haben, würde das sicher sehr nachgefragt sein. Ein Beispiel können die Messenger-Dienste sein.

Was die Zivilgesellschaft betrifft: Wir haben in Deutschland so großartige Initiativen wie den Chaos Computer Club. So etwas muss man auf jeden Fall stärken. Dazu gehört für mich auch die Frage, wie man digitale Kompetenzen in den Schulen stärkt. Bürger müssen digital selbstständig werden, damit sie in der Lage sind, sich sicher im Internet zu bewegen und vertraulich zu kommunizieren.

? Sie haben vorhin die Schulen erwähnt, dass mehr digitale Bildung im Unterricht notwendig ist. Was ist mit den Menschen, die nicht mehr zur Schule gehen? Brauchen wir staatlich geförderte Volkshochschulkurse?

LK: Die Schule ist für mich der primäre Ort, aber natürlich muss digitale Bildung auch im Erwerbsleben stattfinden. Das könnte so etwas sein wie ein Recht auf Weiterbildung, wo man lernt, wie man sich im digitalen Raum bewegt. Jeder Betrieb sollte so etwas machen. Wir sehen, dass die größten Angriffspunkte bei Cyberattacken auf Unternehmen die Mitarbeiter sind, die irgendwann doch auf den falschen Link klicken oder einen infizierten USB-Stick verwenden. Deswegen ist gerade die Sensibilisierung und Schulung von Mitarbeitern in Unternehmen ganz wichtig, um die Vertraulichkeit der Kommunikation zu stärken.

? Wie bekommt man denn die Unternehmen dazu, sich hier stärker zu engagieren? Wird der Markt es schon richten?

LK: Nein, das kann der Markt in dieser Übergangsphase nicht alleine regeln. Da es auch um Grundrechtsschutz geht, ist dies auch eine staatliche Aufgabe. In der Tat brauchen wir eine Sensibilisierung, die über staatliche Programme geschehen kann. Wir haben deutschlandweit „Mittelstand 4.0"-Kompetenzzentren eingerichtet, die Unternehmen bei der Digitalisierung unterstützen sollen.

INTERVIEW MIT LARS KLINGBEIL

> **Gütesiegel sind erst einmal für die Verbraucher gedacht, damit sie sich einen schnellen Überblick verschaffen können.**
>
> Lars Klingbeil

Es kann auch andere Akteure geben – über die Industrie- und Handelskammern, über Datenschutzbeauftragte, über das BSI – das Bundesamt für Sicherheit in der Informationstechnik –, das stärker mit Unternehmen zusammenarbeiten und Unternehmen und Bürgerinnen und Bürger beraten soll.

? Wie stehen Sie zu Zertifizierungen und Gütesiegeln? Dann hätten die Unternehmen, wenn sie ihre Hausaufgaben gemacht haben, etwas, das sie herzeigen können.

LK: Ich halte Gütesiegel für absolut hilfreich. Wobei ich noch einen Schritt weiter gehen und gleich die Produkthaftung einführen würde. Damit kann man von Unternehmen erwarten, dass sie Sicherheitslücken bekannt machen und schließen und Software weiterentwickeln. Sie wären verpflichtet, für technische Lösungen immer die höchsten Standards einzuhalten. Gütesiegel sind erst einmal für die Verbraucher gedacht, damit sie sich einen schnellen Überblick verschaffen können. Die Produkthaftung sichert dann den konkreten Nutzer ab, wenn er die Geräte schon hat.

? Viele technische Lösungen brauchen eine Zusammenarbeit unterschiedlicher Unternehmen und Akteure. Zum Beispiel müsste E-Mail-Verschlüsselung mit vielen unterschiedlichen Akteuren koordiniert werden. Wie könnte man das organisieren?

LK: Wir brauchen offene Schnittstellen und Standardisierungsgremien. Interoperabilität ist ein wichtiges Thema. Außerdem muss die Nutzbarkeit des Ganzen noch mehr im Fokus stehen, denn wenn es nicht einfach nutzbar ist, dann ist es für die Nutzer unattraktiv. Solche Initiativen – Vereinbarungen und runde Tische, wo ein Dialog stattfinden kann – müssen wahrscheinlich aus der Politik kommen, weil die Wirtschaft kein Interesse daran hat, andere auf ihre Plattformen zu lassen. Ich setze mich dafür ein, dass der Staat sichere und vertrauenswürdige Verschlüsselungstechnologie sowie insbesondere deren einfache Implementierung etwa in die Mailprogramme fördert.

? Es gibt Bevölkerungsgruppen, die das Internet nicht benutzen wollen. Haben Sie Ideen, wie man diese Menschen erreichen könnte, damit sie auch irgendwann Vertrauen in die digitalen Kommunikationsmittel fassen?

LK: Ich glaube, es wird immer eine Gruppe von Menschen geben, die sich der digitalen Kommunikation verweigern – auch in 20 Jahren. Dafür muss in der Gesellschaft Platz sein. Als Politiker konzentriere ich mich eher darauf, diejenigen zu erreichen, die eigentlich digital kommunizieren wollen, dann aber das Vertrauen verloren haben. Für diese Skeptiker brauchen wir Bildungs- und Weiterbildungsangebote, aber auch Anforderungen aus der Politik, dass es hohe Standards bei Verschlüsselung und Vertraulichkeit von Kommunikation geben muss. Hier sehe ich auch das BSI in der Pflicht, entsprechende Angebote zu machen und den digitalen Selbstschutz zu stärken.

4.3 Dem Nutzer gegenüber sollte der gewährleistete Sicherheitsstandard kommuniziert werden

Den gewährleisteten Sicherheitsstandard dem Nutzer gegenüber transparent zu kommunizieren, fördert das Vertrauen in digitale Kommunikation. Wenn der Nutzer leicht erkennen kann, welches Sicherheitsniveau beim jeweiligen Kommunikationsvorgang gegeben 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. Ein Übermaß an Information erreicht dann im Zweifel das Gegenteil: Zu viele technische Details führen eher zu einem Verlust an Vertrauen. Wie auch auf anderen Gebieten, in denen Verbraucherinformationen über die Spezifika des Produkts aus diesem Grund sinnlos sind, bieten sich hier deshalb vertrauensfördernde Maßnahmen insbesondere in Form der Vergabe und Veröffentlichung von Gütesiegeln und Zertifikaten an, die die Überprüfung des Dienstes durch vertrauenswürdige Dritte kennzeichnen. Diese können solchen Unternehmen und öffentlichen Stellen verliehen werden, die durch ihr spezielles Know-how sicherstellen können, dass für die jeweilige Konstellation angemessene Kommunikationssicherheit gewährleistet ist. Dabei ist es notwendig, dass die Prüfinstanz unabhängig ist und selbst offene und transparente Prüfstandards zugrunde legt.[112]

> **„Zertifizierungen sind grundsätzlich sinnvoll, allerdings sollte gewährleistet sein, dass sie keine Wettbewerbsverzerrungen zur Folge haben."**
>
> **Prof. Dr. Wolfgang Schulz,** Direktor am Hans-Bredow-Institut für Medienforschung an der Universität Hamburg, Konsultation

Dass zum Beispiel die Verbindung zwischen dem eigenen Computer (Client) und dem Webserver, auf dem die gerade abgerufene Webseite gespeichert ist, mittels TLS[113] 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 dadurch signalisiert, dass 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.[114] 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.[115] 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.

> **„Wir vertrauen Stempeln und Testaten und treffen anhand solcher Entscheidungshilfen unsere Entscheidungen."**
>
> **Matthias Gärtner,** Pressesprecher beim Bundesamt für Sicherheit und Informationstechnik, Konsultation

112 Günter Krings und Lars Mammen, Zertifizierungen und Verhaltensregeln – Bausteine eines modernen Datenschutzes für die Industrie 4.0, RDV 2015, S. 231, 232.
113 Siehe dazu den Annex.
114 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.
115 Bundesamt für Sicherheit in der Informationstechnik, Qualifizierung als Vertrauensdiensteanbieter, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/VDA_Qualifizierung/VDA_Qualifizierung.html.

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 entsprechend sorgfältig umgehen.[116] 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.[117] 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.[118] Eine entsprechende Funktion erfüllt auch das europaweit vergebene European Privacy Seal.[119]

Die neue europäische Datenschutzgrundverordnung sieht in Artikel 42 ebenfalls Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen vor, um den Nutzern gegenüber klar zu kommunizieren, welche Datenschutzstandards gewährleistet werden. Die Nutzer sollen anhand dieser Zertifikate schnell und einfach erkennen können, welches Datenschutzniveau bei einem bestimmten Produkt oder einer Dienstleistung erreicht wird.[120]

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.

4.4 Dem Nutzer sollten mehrere – auch analoge – alternative Kommunikationsmittel angeboten werden

Wie bereits erörtert, 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[121] oder Dänemark[122], 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 allem, wenn es um essenzielle 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

116 Plath, S. 369.
117 Siehe https://www.datenschutzzentrum.de/guetesiegel/.
118 https://www.datenschutzzentrum.de/guetesiegel/faq/.
119 https://www.european-privacy-seal.eu/EPS-en/Home.
120 So Erwägungsgrund 100 der Datenschutzgrundverordnung.
121 Leonid Bershidsky, Envying Estonia's Digital Government, Bloomberg, 4. März 2015, https://www.bloomberg.com/view/articles/2015-03-04/envying-estonias-digital-government.
122 Danish Agency for Digitisation, Campaigning for Mandatory Digital Communication, 3. Dezember 2013, https://www.digst.dk/servicemenu/english/news/campaigning-for-mandatory-digital-communication.

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.[123] 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 Nutzer mit sicheren digitalen Kommunikationsmitteln umgehen können, muss gerade in bedeutenden Kommunikationsverhältnissen (wie vor allem G2C, aber auch beispielsweise bei Bankdienstleistungen, Diensten des Gesundheitssektors und der Energieversorgung) 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.[124]

„Der Staat sollte kontinuierlich und langfristig weiter auch die Möglichkeit analoger Kommunikation gewährleisten. Nur da, wo es wirklich schlagkräftige Gründe gibt, sollte ein Zwang für digitale Kommunikation mit staatlichen Behörden möglich sein."

Prof. Dr. Georg Borges, Lehrstuhl für Bürgerliches Recht, Rechtsinformatik, deutsches und internationales Wirtschaftsrecht sowie Rechtstheorie an der Universität des Saarlandes, Konsultation

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.[125] Dementsprechend sind bislang nur wenige Gruppen von Steuerpflichtigen, wie beispielsweise Unternehmen, verpflichtet, die Steuererklärung elektronisch zu erledigen.[126]

Einen anderen Weg, mit der – kleiner werdenden[127] – 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 wurden in jenem Jahr bereits 80 Prozent der G2C-Kommunikation auf elektronischem Wege erledigt.[128] Von dieser Verpflichtung gibt es aber wichtige Ausnahmen. So sind die Behörden einerseits gesetzlich verpflichtet, den „digital Ausgeschlossenen" in den örtlichen Gemeindezentren Hilfe bereitzustellen, damit auch sie ihre Angelegen-

123 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, unabhängig davon, über welches Verwaltungsportal sie eingestiegen sind; vgl. IT-Planungsrat, Projektsteckbrief Portalverbund, 4. August 2016, http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/21_Sitzung/6_Anlage1_Portalverbund.pdf?__blob=publicationFile&v=2.

124 § 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.

125 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.

126 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_.

127 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 andere 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.

128 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.

INTERVIEW MIT THOMAS JARZOMBEK

Nutzer wollen vertrauliche Kommunikation – aber ohne Mehraufwand

? Was bedeutet Vertrauen in digitale Kommunikation, und welchen Stellenwert hat dieses Vertrauen für unsere Gesellschaft?

Thomas Jarzombek: Das Post- und Fernmeldegeheimnis ist in Deutschland ein etablierter Grundsatz. Viele Menschen, die im Unrechtsregime der DDR gelebt haben, haben Erfahrungen damit gesammelt, dass ein Staat sie belauscht und das zu ihrem Nachteil nutzt. Sie sind bei dem Thema vertrauliche Kommunikation aufgrund dieser Erfahrungen sehr sensibel. Als Politiker möchte ich natürlich auch davon ausgehen, dass keine Dritten mithören, wenn ich mit meinen Mitarbeitern oder mit Kollegen kommuniziere.

? Unter welchen Umständen ist ein Vertrauen in die Sicherheit der Kommunikation gerechtfertigt und wann nicht?

Thomas Jarzombek

Thomas Jarzombek, IT-Berater, ist seit 2009 Mitglied des Bundestages. Er ist Mitglied der Ausschüsse „Verkehr und digitale Infrastruktur“ und „Digitale Agenda“ sowie stellvertretendes Mitglied im Ausschuss „Wirtschaft und Energie“, und er ist internetpolitischer Sprecher der CDU/CSU-Fraktion. 1996, nach seinem Studium und dem Vordiplom in Wirtschaftswissenschaften an der Heinrich-Heine-Universität, gründete er ein Unternehmen für IT-Dienstleistungen in Düsseldorf, in dem er seit 2013 noch Gesellschafter ist. Seit 1991 ist er Mitglied der CDU, 2005 wurde er in Düsseldorf in den nordrhein-westfälischen Landtag gewählt, hier war er medienpolitischer Sprecher der Fraktion. Seit 2014 ist er Kreisvorsitzender der CDU Düsseldorf.

Foto: Tobias Koch

> **Wenn es für sie selbst aber Mehraufwand oder eine zusätzliche Komplikation bedeutet, dann sind sehr viele nicht bereit, irgendetwas zu investieren, um ihre persönliche Datensicherheit zu verbessern.**
>
> Thomas Jarzombek

TJ: Als Politiker erleben Sie häufig, dass interne Informationen nach außen gelangen. Und zwar weniger, weil die IT-Infrastrukturen kompromittiert sind, sondern weil Beteiligte das an Dritte, etwa an Journalisten, herausgeben. Auch wenn ich den Wunsch hätte, dass ich wirklich vertraulich kommunizieren könnte, muss ich immer davon ausgehen, dass alles den Weg in die Öffentlichkeit findet. Das denke ich bei allem, was ich sage oder schreibe, immer mit. Vertrauen in die Kommunikation ist also nicht nur eine technische Frage, sondern auch eine gesellschaftliche.

? Welche Faktoren haben für die einfachen Nutzerinnen und Nutzer einen Einfluss darauf, ob sie der Kommunikation vertrauen?

TJ: Das Thema Ende-zu-Ende-Verschlüsselung erlebte erst dann den Durchbruch, als es einer der großen Anbieter, sprich WhatsApp, eingeführt hatte und man die Verschlüsselung ohne weiteren Aufwand nutzen konnte. In meiner Wahrnehmung fordern die Menschen zwar gegenüber der Politik eine vertrauliche Kommunikation ein. Wenn es für sie selbst aber Mehraufwand oder eine zusätzliche Komplikation bedeutet, dann sind sehr viele nicht bereit, irgendetwas zu investieren, um ihre persönliche Datensicherheit zu verbessern. Das muss man einfach zur Kenntnis nehmen. Das sieht man auch daran, dass sich E-Mail-Verschlüsselung mit PGP auf breiter Front nie durchgesetzt hat, weil es zu kompliziert ist. Da muss man tatsächlich auf einfache Nutzer-Interfaces setzen. Da sind die Softwareentwickler gefragt.

? Muss der Staat es den Anbietern auferlegen, Verschlüsselung zu benutzen? Oder wären Sie eher dagegen?

TJ: Ich glaube nicht, dass das der Staat verpflichtend machen muss. Wir leben ja in einer sozialen Marktwirtschaft. Das bedeutet, dass es Wettbewerb gibt. Möglicherweise wird der eine oder andere Anbieter für sich erkennen, dass er mit dem Argument „Ich gebe euch eine bessere Sicherheit als meine Konkurrenz" den Leuten einen Grund dafür geben kann, sein Produkt zu kaufen. Und genau das kann man gegenwärtig beobachten. Zumal es auch Gründe dafür geben mag, dass es Dienste gibt, die keine Ende-zu-Ende-Verschlüsselung einsetzen. Wenn man zum Beispiel eine Plattform hat, auf die man mit verschiedenen Geräten zugreifen soll, ist vollständige Verschlüsselung technisch schwierig. Beim Messenger von Facebook zum Beispiel können Sie auswählen, ob Sie verschlüsselt oder unverschlüsselt kommunizieren. Das hat dann aber Auswirkungen darauf, ob Sie die Chats auf jedem Gerät lesen können.

? Kann der Staat etwas dafür tun, um eine vertrauenswürdige Kommunikation zu gewährleisten?

TJ: Auch ohne staatliches Zutun entwickelt sich in diesem Bereich viel. Außerdem gibt es Dinge, die der Staat schon tut. Einmal:

INTERVIEW MIT THOMAS JARZOMBEK

> **Wir fordern von den Anbietern nicht, dass sie Hintertüren oder Ähnliches in ihre Produkte einbauen, durch die Strafverfolgungsbehörden Kommunikation mitlesen können.** Thomas Jarzombek

Es gibt zum Beispiel keine Beschränkung seitens des Staates, was die Stärke von Verschlüsselung betrifft. In den USA etwa dürfen Verschlüsselungsmethoden ab einer bestimmten Stärke nicht ins Ausland exportiert werden. Zum Zweiten: Wir fordern von den Anbietern nicht, dass sie Hintertüren oder Ähnliches in ihre Produkte einbauen, durch die Strafverfolgungsbehörden Kommunikation mitlesen können. Das sind zwei maßgebliche Beiträge, die der Staat dazu leistet, damit vertrauenswürdige Kommunikationsmethoden von Anbietern in Deutschland und Europa genutzt werden können.

? Sollte das stärker kommuniziert werden, um das Vertrauen zu stärken – wäre das hilfreich?

TJ: Das müssen schon die Medien und Journalisten in die Öffentlichkeit tragen. Das ist nicht die Aufgabe des Staates. Ich will aber nicht verschweigen, dass es auf der anderen Seite in Deutschland einen gesetzlichen Rahmen gibt, der es nach richterlichem Beschluss in besonders extremen Fällen – wir reden hier von wenigen Fällen pro Jahr – den deutschen Behörden ermöglicht, auf die Geräte von sogenannten Gefährdern zuzugreifen. Dazu braucht es wirklich plausible Anlässe, also etwa, dass sie einen Terroranschlag verüben könnten. Das geschieht über sogenannte Zero Day Exploits. Das sind Sicherheitslücken, die zwar bekannt, aber nicht öffentlich sind. Sie werden auf dem Schwarzmarkt verkauft – an Computerkriminelle, aber auch an Staaten. Der Handel mit solchen Sicherheitslücken funktioniert aber auch ohne die Staaten recht gut. Darüber gibt es natürlich eine politische Diskussion, ob das richtig ist oder nicht. Solange solche Exploits da sind, wird der Staat sich nicht blind machen können. Hier sind die Softwareentwickler gefragt, die Produkte sicherer zu machen.

? Wie bewerten Sie die Nutzung von solchen Exploits? Spielt das eine große Rolle bei den Bürgern?

TJ: Da gibt es ganz unterschiedliche Meinungen. Aber wenn Sie das Thema im laufenden Wahlkampf mit den Menschen am Infostand oder auf der Straße diskutieren, dann ist das für viele keine relevante Frage. Wir hören von vielen Bürgern eher: „Ihr müsst unsere Sicherheit gewährleisten. Das sind Terroristen, die wollen Menschen in Deutschland umbringen. Wir erwarten von euch als Staat, dass ihr uns gegen diese Leute schützt."

heiten 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.[129] 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.

4.5 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. Öffentliche Stellen müssen dabei Mittel einsetzen, die von den Steuerzahlern aufgebracht werden.[130]

Davon abgesehen aber sollte die Förderung digitaler Kommunikation nicht mit unmittelbaren Mehrkosten für den Nutzer verbunden sein. Das bedeutet einerseits, dass digitale Angebote nicht kostenpflichtig sein sollten, wenn die entsprechenden analogen Kommunikationswege (bislang) kostenfrei waren. Umgekehrt sollte eine analoge Alternative nicht plötzlich mit finanziellem Aufwand für den Nutzer verknüpft sein, wenn sie vor Einführung des digitalen Kommunikationsmittels den Nutzer nichts gekostet hatte. Diese Grundsätze sind eine Folge des Prinzips der Freiheit bei der Auswahl 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 Geld gezahlt werden muss – 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.[131]

129 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.

130 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/.

131 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.

5. Zusammenfassende Erwägungen

Die fünf Grundsätze lassen sich, etwas verkürzt, auf die Begriffe Sicherheit und Verlässlichkeit, Nutzerfreundlichkeit, Transparenz, Angebot von Alternativen und Nichtdiskriminierung bringen. Diese Begriffe unterliegen verschiedenen Abhängigkeiten.

Sicherheit und Nutzerfreundlichkeit stehen in einem direkten Spannungsverhältnis. Die Erfahrung hat gezeigt, dass eine erhöhte Sicherheit und Verlässlichkeit 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 und Verlässlichkeit 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 und Verlässlichkeit bei der Kommunikation zu haben.

Die Verfügbarkeit alternativer Kommunikationsmittel trägt zu Sicherheit und Verlässlichkeit 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 sind Sicherheit und Verlässlichkeit wesentliche Faktoren, ohne die 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 schließlich öffnet Wege für vertrauensvolle Kommunikation auch für diejenigen Nutzer, denen aus verschiedenen Gründen der Einsatz der üblichen digitalen Wege verschlossen bleibt.

INTERVIEW MIT DR. THOMAS KREMER

Vertrauen kann man nicht erzwingen

? Was bedeutet Vertrauen in digitale Kommunikation für Sie? Welchen Stellenwert hat dieses Vertrauen für unsere Gesellschaft?

Thomas Kremer: Das Vertrauen in die Kommunikation bedeutet auf der einen Seite, dass die Inhalte wirklich sicher sind, auf der anderen Seite, dass sie vertraulich behandelt werden. Das eine ist eine technische Frage, das andere ist eine Frage des Umgangs mit den Inhalten. Wir sollten nicht vergessen: Das Fernmeldegeheimnis ist aus gutem Grund im Grundgesetz verankert. Wir haben als Gesellschaft das Thema Vertrauen in die Kommunikation sehr hoch angesetzt: Wir haben es in unsere Verfassung geschrieben.

? Ist denn mein Vertrauen als Bürger in meine Kommunikation – egal ob per E-Mail oder per Telefon – gerechtfertigt? Wie kann man es stärken?

Foto: Deutsche Telekom

Dr. Thomas Kremer

Dr. Thomas Kremer, Jahrgang 1958, ist seit Juni 2012 Vorstand für Datenschutz, Recht und Compliance bei der Deutschen Telekom AG. Von Januar 2014 bis März 2015 leitete er zusätzlich kommissarisch das Vorstandsressort Personal.

Im September 2013 wurde Thomas Kremer in die Regierungskommission Deutscher Corporate Governance Kodex berufen. Seit November 2015 ist Thomas Kremer zudem Vorsitzender des Vereins „Deutschland sicher im Netz“.

INTERVIEW MIT DR. THOMAS KREMER

> **Wir brauchen neben den technischen Lösungen auch Verbraucheraufklärung, damit die Nutzer lernen, sicher mit den digitalen Medien umzugehen.** Dr. Thomas Kremer

TK: Ich denke schon, dass Vertrauen gerechtfertigt ist, aber man kann es nicht erzwingen. Man muss es sich erarbeiten. Unsere Gesellschaft wird immer digitaler, damit nimmt der Datenaustausch zwangsläufig zu. Die Digitalisierung und alles, was damit zusammenhängt, etwa mobiles Arbeiten oder smarte Infrastrukturen, können nur gelingen, wenn die Menschen darauf vertrauen können, dass die Kommunikation sicher ist.

Das setzt konkret voraus, dass Sie auf der technischen Seite mit starken Verschlüsselungstechnologien arbeiten. Zusätzlich sind internationale Sicherheitsstandards notwendig. Die sind schwierig zu etablieren, aber unabdingbar. Ein anderes wesentliches Element sind verlässliche rechtliche Rahmenbedingungen. In Deutschland beziehungsweise Europa haben wir das ja schon mit unseren hohen Datenschutzstandards, die in der europäischen Datenschutzgrundverordnung geregelt werden.

Außerdem ist es wichtig, gesellschaftlich darüber zu diskutieren, wo wir Regeln brauchen und wo wir uns auf Selbstkontrolle und Best Practice verlassen können. Neue Trends, wie künstliche Intelligenz oder die Nutzung von Robotern, müssen in einem breiten gesellschaftlichen Prozess diskutiert werden. Welche Regeln brauchen wir dafür?

? Für wie wichtig halten Sie es, dass sichere Kommunikationsmittel nutzerfreundlich gestaltet werden?

TK: Aus meiner Sicht sind einfache Lösungen ganz zentral – vor allem für die Durchschnittsnutzer, die an der digitalen Welt teilnehmen. Früher war Sicherheit etwas für Experten. Das hat sich inzwischen geändert – und das ist auch richtig so. Wir brauchen neben den technischen Lösungen auch Verbraucheraufklärung, damit die Nutzer lernen, sicher mit den digitalen Medien umzugehen. Es geht im Kern um das Thema digitale Souveränität: Der Mensch muss Herr seiner Daten sein. Dazu gehört auch Verschlüsselung – einer der Kernpunkte. Ich halte es für sehr sinnvoll, wenn wir die Transportwege von Nachrichten verschlüsseln. Dadurch können wir das Vertrauen der Menschen in digitale Kommunikation enorm steigern.

? Zuverlässige Ende-zu-Ende-Verschlüsselung vor allem bei E-Mails ist in der Anwendung für normale Nutzer immer noch zu kompliziert. Haben Sie einen Vorschlag, wie Unternehmen es realisieren können, dass es in der Handhabbarkeit einfacher wird?

TK: Die Telekom hat gemeinsam mit dem Fraunhofer-Institut das Produkt Volksverschlüsselung[132] entwickelt. Es erlaubt einfache Ende-zu-Ende-Verschlüsselung. Es bleibt aber die Frage, warum die Verbraucher das nicht ausreichend nutzen. Verschlüsselungen wie bei WhatsApp oder anderen Messen-

132 https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/verschluesselung.

gern, die im Programm eingebaut sind, haben es einfacher, weil sich die Nutzer überhaupt nicht darum kümmern müssen – es wird einfach im geschlossenen System verschlüsselt. So etwas funktioniert auch schon bei der Telekom-E-Mail. Daran müssen alle noch arbeiten.

? Was halten Sie von Zertifizierungen und Gütesiegeln, die man bekommen kann, wenn man gewisse Sicherheitsstandards erfüllt? Meinen Sie, dass das einen Effekt hat auf das Vertrauen der Nutzer in die Kommunikationsmittel?

TK: Das ist ganz zweifellos so. Dadurch hat der Bürger die Wahl, sichere, zertifizierte Produkte und Dienstleistungen in Anspruch zu nehmen. In dem Zusammenhang ist wichtig, dass diese Zertifizierung von anerkannten Einheiten durchgeführt wird, zum Beispiel, wie wir es vom Auto kennen, vom TÜV. Das ist eine Organisation, die staatlich kontrolliert wird. So eine Einheit kann dann in Bezug auf bestimmte festgelegte Standards überprüfen, ob die Vertrauenswürdigkeit gegeben ist. Ich bin davon überzeugt, dass das dazu führt, dass das Vertrauen steigt.

? Brauchen wir auf der anderen Seite eine strengere Kontrolle und eine Haftung, wenn man keine ausreichenden Sicherheitsstandards verwendet?

TK: Das haben wir ja zum Teil heute schon. Wenn es darum geht, kritische Infrastrukturen zu sichern, haben wir das IT-Sicherheitsgesetz und auf europäischer Ebene die NIS-Richtlinie. Sie sorgen für Sicherheit, zum Beispiel indem sie Meldepflichten einführen, sodass Sicherheitsvorfälle gegenüber Behörden transparent werden. Viele Sicherheitslücken beruhen auf Schwachstellen in der Software. Daher werden wir mehr Sicherheit nur dann erreichen, wenn für kritische Softwarefehler Sicherheits-Updates zur Verfügung gestellt werden, und zwar über den gesamten Lebenszyklus eines Produkts. Hard- und Softwarehersteller müssen verpflichtet sein, in solchen Fällen tatsächlich Aktualisierungen zur Verfügung zu stellen.

Ein zweiter Punkt ist mir sehr wichtig: Wenn man Schwachstellen in Software erkennt – und ich rede hier von kritischen Schwachstellen –, muss man sie melden und offenlegen. Das gilt auch für Sicherheitsbehörden. Diese Schwachstellen dürfen nicht einfach versteckt werden, weil man sie zum eigenen Vorteil nutzen möchte, um zum Beispiel jemanden auszuspionieren oder abzuhören. Das ist nach meiner Meinung eine grundfalsche Einstellung. Denn jede Schwachstelle, die erkannt wird und nicht veröffentlicht wird, birgt das Risiko, dass Kriminelle sie ausnutzen. Wenn sie nicht bekannt ist, können wir uns dagegen nicht verteidigen. Und das ist ein Risiko, das wir nicht eingehen sollten. ⊡

> **Viele Sicherheitslücken beruhen auf Schwachstellen in der Software.**
>
> Dr. Thomas Kremer

6. Epilog

Auf die fünf Grundsätze für sichere digitale Kommunikation, die in den vorangegangenen Abschnitten aufgestellt und erläutert wurden, folgt zum Abschluss die Frage nach ihrer Umsetzung, die hier in Form von Forderungen an Wirtschaft und Politik beantwortet wird.

Bislang ist lediglich als theoretische Überlegung erörtert worden, wie das Vertrauen der Nutzerinnen und Nutzer in digitale Kommunikationsmittel, die bei der Übermittlung sensibler Inhalte durch Unternehmen und Verwaltung eingesetzt werden, gestärkt werden kann. Einige dieser Aspekte sind schon durch bereits existierende rechtliche Vorgaben abgedeckt. Wie die Ausführungen aber gezeigt haben, liegt der Fokus der anwendbaren Gesetze vorrangig auf dem Aspekt der Sicherheit der Kommunikation. Hier zeigt sich aber trotz des Rechtsrahmens mitunter noch immer eine beträchtliche Lücke zwischen (rechtlichem) Anspruch und Wirklichkeit. Denn trotz mitunter recht detaillierter Bestimmungen zeigen die in schöner Regelmäßigkeit auftretenden Datenschutzskandale, dass die Sicherheit digitaler Kommunikationsmittel noch immer unzureichend ist.

I. Es ist zunächst zu fordern, dass das Sicherheitsniveau auf Seiten der Dienstleister insgesamt erhöht wird, indem Entwickler verstärkt dazu angehalten werden, auf „Security by Design" zu setzen. Zumindest was den E-Mail-Verkehr angeht, sollte zum Erreichen dieses Ziels weiter verstärkt auf modernste Verschlüsselungstechnologien und insbesondere auf die flächendeckende Einführung von Ende-zu-Ende-Verschlüsselung gesetzt werden.

Diese Forderung allerdings führt zu dem bereits erörterten Problem, dass bei bislang angebotenen Lösungen Sicherheit zu oft auf Kosten der Nutzerfreundlichkeit erkauft worden ist. Dieser Umstand wiederum hat unmittelbar Auswirkungen auf die Sicherheit selbst. Denn 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 letztendlich nicht verwendet werden. Sie werden sich am Markt nicht durchsetzen, sodass der angebotene Sicherheitsstandard wirkungslos bleibt.

> **„Die Nutzerfreundlichkeit bei verschlüsselter Kommunikation ist extrem wichtig. Dies liegt an einem einfachen Kosten-Nutzen-Modell: Wenn man einmal Ärger mit einer gefälschten E-Mail hat und diesen Ärger mit wenigen Stunden oder Tagen Arbeit auflösen kann, ist es besser, als wenn man sein ganzes Leben lang mit Schwierigkeiten der PGP-Verschlüsselung bei jeder E-Mail-Kommunikation kämpfen muss."**
>
> **Prof. Dr. Georg Borges,** Lehrstuhl für Bürgerliches Recht, Rechtsinformatik, deutsches und internationales Wirtschaftsrecht sowie Rechtstheorie, Universität des Saarlandes, Konsultation

II. Die Forderung nach Herstellung von Sicherheit ist stets durch die ebenso gewichtige Forderung danach zu ergänzen, Sicherheitstechnologien so zu implementieren, dass das Endprodukt dennoch stets intuitiv und

von durchschnittlich versierten Nutzerinnen und Nutzern einfach zu bedienen ist. Die Aspekte Sicherheit und Nutzerfreundlichkeit bilden ein einheitliches Ganzes.

Darüber hinaus sind die Wünsche der Bürger und Verbraucher, die die angebotenen Dienste digitaler Kommunikation ja schließlich verwenden sollen, ernst zu nehmen. Wie bereits in der Einleitung erwähnt, sprechen sich nicht weniger als 92 Prozent dafür aus, eine Wahlmöglichkeit dahingehend beizubehalten, auf welche Weise ihnen Dokumente mit sensiblen Informationen zugestellt werden.[133]

III. *Von den Dienstleistern ist zu fordern, eine Wahlmöglichkeit zwischen analoger und digitaler Kommunikation aufrechtzuerhalten. Das heißt zudem, dass ökonomische Nichtdiskriminierung zu fordern ist, um das Ziel zu erreichen.*

Weiterhin hat die jüngste Befragung gezeigt, dass Nutzerinnen und Nutzer Online-Postfächer zwar als praktisch empfinden und solche Angebote mehrheitlich auch nutzen. Zugleich betrachten sie die Verteilung wichtiger Dokumente auf unterschiedliche Postfächer bei mehreren Anbietern überwiegend als negativ. Ein Drittel fürchtet gar, aufgrund der großen und weiter steigenden Anzahl solcher Portale irgendwann den Überblick zu verlieren.[134]

IV. *Es ist zu fordern, eine technische Lösung zu schaffen, mit der die Online-Postfächer unterschiedlicher Anbieter bzw. Unternehmen zusammengeführt werden können. Solche Bündelungslösungen würden es einerseits unnötig machen, sich eine Vielzahl an Passwörtern merken zu müssen. Vor allem aber würden sie das genannte Problem zunehmender Unübersichtlichkeit beseitigen und könnten – sofern entsprechend gut designt – wie Online-Portale allgemein Nutzerfreundlichkeit gewährleisten.*

Für die Schaffung einer solchen technischen Lösung bedarf es einer konzertierten Aktion, an der sich sowohl der Staat als auch Stakeholder aus Zivilgesellschaft (wie z. B. im Bereich von Datenschutz und Internetsicherheit tätige Nichtregierungsorganisationen und unabhängige Beauftragte für Datenschutz) und Wirtschaft (einerseits Unternehmen, die mit ihren Kundinnen und Kunden zunehmend digital kommunizieren, wie Versicherer, Banken, Energieversorger etc.; andererseits Kommunikationsdienstleister wie z. B. E-Mail-Provider) beteiligen sollten.

> **„Die Anstrengungen, digitale Kommunikation sicherer zu gestalten, müssen stärker gebündelt werden. Das BSI als die nationale Cyber-Sicherheitsbehörde ist dazu im Dialog mit Wirtschaft und Gesellschaft und treibt entsprechende Lösungen zur sicheren Kommunikation im Internet voran, etwa im Bereich der Verschlüsselung."**
>
> **Matthias Gärtner,** Pressesprecher beim Bundesamt für Sicherheit und Informationstechnik, Konsultation

Eine solche Multi-Stakeholder-Aktion ist insbesondere für die privatwirtschaftlichen Unternehmen mit Kosten verbunden, die sich nicht unmittelbar auszahlen. Solange ihre Kunden die von ihnen angebotenen individuellen Online-Portale nutzen, wie es bislang, wenn auch mit Bauchschmerzen, geschieht, besteht für die Unternehmen eigentlich kein unmittelbarer Anlass, sich an einem solchen Vorhaben mit eigenen Ressourcen zu beteiligen. Ein entsprechender Anreiz könnte allerdings

133 Siehe DIVSI, Digitalisierung – Deutsche fordern mehr Sicherheit. Was bedeutet das für Vertrauen und für Kommunikation? Eine Studie von dimap im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI), Hamburg, August 2017.
134 Ebd.

durch Konkurrenzdruck entstehen, wenn es gelänge, einige Unternehmen davon zu überzeugen, dass eine Teilnahme an solchen vereinheitlichten Portalen einen Reputationsgewinn bringen würde, da es dem Kundenwunsch entspricht, über die derzeit bestehende fragmentierte Landschaft Dutzender Online-Postfächer hinwegzukommen. Hier könnte wiederum den angesprochenen Gütesiegeln eine entscheidende Rolle zukommen.

V. Unternehmen, die sich an der technischen Lösung zur Bündelung von Online-Postfächern beteiligen und ihren Dienst entsprechend gestalten, sollten mit einem entsprechenden Siegel ausgezeichnet werden, das den Nutzerinnen und Nutzern diesen Umstand leicht erkennbar kommuniziert.

Anderen Unternehmen, die es dagegen vorziehen, außen vor zu bleiben, könnte dann das Vertrauen der Kunden in die Sicherheit ihrer angebotenen digitalen Kommunikationsmittel abhandenkommen. Das Siegel schafft damit den Anreiz auch für privatwirtschaftliche Akteure, zu dem Gelingen einer sicheren, nutzerfreundlichen digitalen Kommunikation beizutragen.

> **„Von staatlicher Seite sollten nicht einfach irgendwelche Vorgaben gemacht werden, sondern Sicherheitsstandards oder Gütesiegel müssen mit den Unternehmen zusammen erarbeitet werden."**
>
> **Suanne Dehmel,** Mitglied der Geschäftsleitung Recht & Sicherheit, Bitkom e.V., Konsultation

Gefordert wird mithin, dass die fünf Grundsätze für sichere digitale Kommunikation mittels der fünf folgenden Maßnahmen umgesetzt werden: (I) Security by Design, (II) Nutzerfreundlichkeit, (III) Wahlmöglichkeit und ökonomische Nichtdiskriminierung, (IV) Schaffung einer technischen Lösung zur Bündelung von Online-Postfächern, (V) Kennzeichnung der teilnehmenden Unternehmen durch Siegel.

Annex

Technische Erläuterungen

In diesem Annex finden sich in Ergänzung zu Abschnitt 4.1.2 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 Maße 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".[135] Auch die Datenschutzgrundverordnung verpflichtet nach Art. 24 Absatz 1 diejenigen Personen, die für die Verarbeitung personenbezogener Daten verantwortlich sind, entsprechende Verschlüsselungstechnologien einzusetzen.[136] 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.[137] 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 kryptografischer 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.[138] Ein Beispiel für diese Methode ist der Advanced Encryption Standard (AES), der in seinen komplexeren Varianten als sehr sicher gilt und

135 Siehe Satz 2 Nr. 4 und Satz 3 der Anlage zu § 9 Satz 1 BDSG.
136 Plath, S. 117f.
137 Ebd., S. 365.
138 Vgl. Kryptowissen.de, Symmetrische Verschlüsselung, http://www.kryptowissen.de/symmetrische-verschluesselung.html.

aus diesem Grund unter anderem in den Vereinigten Staaten zur Verschlüsselung staatlicher Dokumente der höchsten Geheimhaltungsstufe zugelassen ist.[139] 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.[140]

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.[141] 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.[142] 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[143]). 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 Verfahrens verschlüsselt. Anschließend wird lediglich der symmetrische Schlüssel selbst asymmetrisch verschlüsselt und kann so sicher übermittelt werden.[144]

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 an-

139 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.
140 Siehe E-Post, Datenschutz und Datensicherheit, Hohe Sicherheits- und Datenschutzstandards sowie moderne Verschlüsselungstechniken, https://www.epost.de/privatkunden/sicherheit.html#sicherheit-und-verschluesselungstechniken.
141 Vgl. Wikipedia, Asymmetrisches Kryptosystem, https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem.
142 Heckmann, S. 66.
143 Vgl. Wikipedia, Asymmetrisches Kryptosystem, https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem.
144 Ebd.

derer 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 kryptografischer Schlüssel erstellt und ausgetauscht. Anhand dieses Schlüssels wird im Anschluss die gesamte Kommunikation zwischen Client und Server mit einem symmetrischen Verfahren verschlüsselt.[145] 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.[146]

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 brechen. 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 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 –, sodass 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, sodass der Angriff unentdeckt bleiben kann.[147] 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.[148]

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.[149] Solche Maßnahmen werden insbesondere nach terroristischen Anschlägen immer wieder gefordert, weil viele Terrororganisationen bevorzugt auf solche Mes-

145 Vgl. Wikipedia, Transport Layer Security (TLS), https://de.wikipedia.org/wiki/Transport_Layer_Security.
146 Bundesamt für Sicherheit in der Informationstechnik, Qualifizierung als Vertrauensdiensteanbieter, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/VDA_Qualifizierung/VDA_Qualifizierung_node.html.
147 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.
148 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/.
149 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.

senger-Anwendungen zurückgreifen, die Ende-zu-Ende-Verschlüsselung anbieten.[150] 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.[151]

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[152], während bei OpenPGP diese Funktion durch ein „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.[153]

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.[154] 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.[155] 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.[156]

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 sym-

150 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.

151 Harold Abelson u. a., Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, Journal of Cybersecurity, 2015, S. 1.

152 Siehe Wikipedia, E-Mail-Verschlüsselung, https://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung.

153 Wikipedia, Web of Trust, https://de.wikipedia.org/wiki/Web_of_Trust.

154 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.

155 ProtonMail, What Is End-to-End Encryption?, 4. Mai 2015, https://protonmail.com/blog/what-is-end-to-end-encryption/.

156 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.

metrischer 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 erfolgreich, wird der Inhalt der E-Mail anschließend lokal auf dem Endgerät des Empfängers entschlüsselt.[157] 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[158], 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.[159] 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.[160]

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 Vertrauensdiensteanbieter erwerben und auf die Ausweiskarte laden. Zusätzlich wird ein Lesegerät benötigt, das an den eigenen Computer angeschlossen wird.[161] Während in Deutschland die Nutzung der elektronischen Funktionen des neuen Personalausweises auch wegen Datenschutzbedenken nach Angaben des Bundesinnenministeriums bislang eher die Ausnahme darstellt[162], sind vergleichbare Mechanismen beispielsweise in Estland gesetzlich verpflichtend und werden von den Bürgern angenom-

157 Ebd.
158 Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/EGovernment/DeMail/Akkreditierte_DMDA/Akkreditierte_DMDA.html.
159 Vgl. Wikipedia, Asymmetrisches Kryptosystem, https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem.
160 Vgl. Wikipedia, Signaturgesetz (Deutschland), https://de.wikipedia.org/wiki/Signaturgesetz_(Deutschland).
161 Bundesministerium des Innern, Die elektronischen Funktionen des Personalausweises, http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Funktionen/funktionen_node.html.
162 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/.

men.[163] 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.[164]

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.[165]

Sicherheit von Passwörtern und Zwei-Faktor-Anmeldung

Viele Experten vertreten inzwischen die Ansicht, Passwörter sollten aufgrund ihrer inhärenten Unsicherheit mittelfristig der Vergangenheit angehören.[166] 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 veröffentlicht, die eine Reihe von Tipps für ein gutes Passwort aufführt.[167] 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.[168]

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.[169] 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[170] gespeichert worden sind.

Das Verfahren der Zwei-Faktor-Anmeldung gilt als sehr sicher, 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

163 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 war, 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.

164 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.

165 Bundesministerium des Innern, Gute Kombination für mehr Sicherheit im Internet, http://www.personalausweisportal.de/DE/Wirtschaft/Anwendungsbeispiele/De-Mail/De-Mail_node.html.

166 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.

167 https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html.

168 Siehe z. B. beim E-Postbrief der Deutschen Post, https://www.epost.de/privatkunden/sicherheit.html#sicherheit-und-verschluesselungstechniken.

169 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.

170 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.

an eine App des Mobiltelefons. Auch bei einem Fingerabdruck-Scanner, der nach der Passworteingabe zum Einsatz kommt (und nicht bloß an dessen Stelle), handelt es sich um einen solchen zweiten Faktor.[171] 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.[172]

171 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.
172 Siehe z. B. bei Yahoo Mail, https://de.hilfe.yahoo.com/kb/SLN5013.html.

Literatur

Abelson, Harold u. a. (2015): Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications, Journal of Cybersecurity, 2015, S. 1

Bamberger, Walter (2010): Interpersonal Trust – Attempt of a Definition, http://www.ldv.ei.tum.de/en/research/fidens/interpersonal-trust/

Bitkom (2013): Vertrauen in Datensicherheit im Internet schwindet weiter, https://www.bitkom.org/Presse/Presseinformation/Vertrauen-in-Datensicherheit-im-Internet-schwindet-weiter.html

DIVSI (2017): Digitalisierung – Deutsche fordern mehr Sicherheit. Was bedeutet das für Vertrauen und für Kommunikation? Eine Studie von dimap im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet

DIVSI (2017): Elektronische Dokumentenzustellung, repräsentative dimap-Umfrage ab 18 Jahren, 1. und 2. März 2017, https://www.divsi.de/wp-content/uploads/2017/03/2017-03-08_Unterlage_DIVSI-dimap-Umfrage_Dokumentenzustellung.pdf

Goldberg, Rafi u. a. (2016): Trust in Internet Privacy and Security and Online Activity, NTIA Working Paper, https://ssrn.com/abstract=2757369

Heckmann, Dirk u. a. (2012): Adäquates Sicherheitsniveau bei der elektronischen Kommunikation: Der Einsatz des E-Postbriefs bei Berufsgeheimnisträgern, Stuttgart

Herfert, Michael u. a. (2016): Laientaugliche Schlüsselgenerierung für die Ende-zu-Ende-Verschlüsselung, Datenschutz und Datensicherheit 5/2016, S. 290, https://www.sit.fraunhofer.de/fileadmin/dokumente/artikel/DuD-Volksverschluesselung.pdf?_=1465887310

IPIMA und Initiative D21 (2016): eGovernment MONITOR 2016 – Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, http://initiatived21.de/app/uploads/2016/12/egovmon2016_web.pdf

Krings, Günter/Mammen, Lars (2015): Zertifizierungen und Verhaltensregeln – Bausteine eines modernen Datenschutzes für die Industrie 4.0, RDV 2015, S. 231

Luhmann, Niklas (1989): Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität, 3. Aufl. Stuttgart

McKinsey & Company (2015): E-Government in Deutschland – Eine Bürgerperspektive, https://www.mckinsey.de/files/e-government_in_deutschland_eine_buergerperspektive.pdf

Meinel, Christoph/Sack, Harald (2009): Digitale Kommunikation. Vernetzen, Multimedia, Sicherheit. Berlin
Meinel, Christoph/Sack, Harald (2014): Sicherheit und Vertrauen im Internet. Eine technische Perspektive. Berlin
Nissenbaum, Helen (2004): Will Security Enhance Trust Online, or Supplant It?, in: R. Kramer und K. Cook (Hg.), Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions
Schmid, Alexander/Heudecker, Claudia (2017): Der vollständig automatisierte Erlass eines Verwaltungsakts (§ 35a VwVfG) sowie die Bekanntgabe eines Verwaltungsakts über öffentlich zugängliche Netze (§ 41 Abs. 2a VwVfG) (Teil 2), jurisPR-ITR 8/2017, http://bit.ly/2qaOKqG
Schulzki-Haddouti, Christiane (2016): Datenschutz-Verstöße werden sehr selten sanktioniert, Der Datenschutz-Blog, https://www.datenschutzbeauftragter-online.de/datenschutz-verstoesse-werden-sehr-selten-sanktioniert/9536/
Vosshoff, Andrea (2014): Vertrauen und Kommunikation in einer digitalisierten Welt aus Sicht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Vortrag, https://www.bfdi.bund.de/DE/Infothek/Reden_Interviews/2014/VertrauenundKommunikation_Muenster171114.html?nn=5217192

Über die an diesem Bericht beteiligten Organisationen und Institutionen

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)

Das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI) ist eine gemeinnützige und unabhängig tätige Einrichtung, gegründet 2011 von der Deutsche Post AG. Die Arbeit von DIVSI fußt im Wesentlichen auf „Fünf Thesen zu Vertrauen und Sicherheit im Internet", die bei Institutsgründung zusammen mit dem DIVSI-Schirmherrn Bundespräsident a.D. Joachim Gauck entwickelt wurden.

DIVSI gestaltet einen offenen und transparenten Dialog zu den Auswirkungen der Digitalisierung auf alle Lebensbereiche. Die damit einhergehenden komplexen Veränderungsprozesse werden im Diskurs mit Experten und Akteuren aus Politik, Wirtschaft, Wissenschaft, Medien und Zivilgesellschaft analysiert und bewertet. Ferner fördert das Institut Wissenschaft und Forschung – u.a. mit dem Stiftungslehrstuhl „Cyber Trust" an der Technischen Universität München.

Wichtiger Baustein der gesellschaftsübergreifenden Auseinandersetzung ist die Grundlagenarbeit von DIVSI, in der zu sozialen, rechtlichen, wirtschaftlichen, partizipativen und ethischen Aspekten der Digitalisierung geforscht wird.

Die mit anerkannten Forschungsinstituten und weiteren namhaften Projektpartnern erarbeiteten Studien und sonstigen Ergebnisse stellt DIVSI grundsätzlich für jedermann kostenlos zur Verfügung. So soll der gesellschaftliche Diskurs auch über das eigene Wirken hinaus unterstützt werden.

iRights.Lab

Das iRights.Lab ist ein unabhängiger Think Tank zur Entwicklung von Strategien und praktischen Lösungen, um die Veränderungen in der digitalen Welt vorteilhaft zu gestalten. Wir unterstützen öffentliche Einrichtungen, Stiftungen, Unternehmen, Wissenschaft und Politik dabei, die Herausforderungen der Digitalisierung zu meistern und die vielschichtigen Potenziale effektiv und positiv zu nutzen. Dazu verknüpfen wir rechtliche, technische, ökonomische und gesellschaftspolitische Expertise.

Wir erfassen komplexe Prozesse, identifizieren relevante Kernaspekte und strukturieren Informationen zu den schnelllebigen Neuerungen des digitalen Wandels, um übergeordnete Trends und Veränderungen gesellschaftlich und politisch greifbar zu machen. Dabei überblicken wir neue aktuelle Sachlagen und Möglichkeiten genauso wie bestehende Wechselwirkungen und Abhängigkeiten. Wir eröffnen Diskussionsräume sowohl in der Öffentlichkeit als auch unter Stakeholdern und schaffen Möglichkeiten für politischen Austausch, Meinungsbildung und Ideenfindung, die wir durch verlässliche und prägnante Informationen und Einschätzungen gestalten und unterstützen.

DIVSI Studien im Überblick

Digitalisierung – Deutsche fordern mehr Sicherheit (2017)

Die Deutschen stehen der Digitalisierung positiv gegenüber und sehen darin viele Vorteile für sich. Beim Thema Sicherheit im Internet erwarten sie allerdings mehr Engagement – vom Staat und von Unternehmen. Was bedeutet das für Vertrauen und für Kommunikation? Und wie sieht es mit der Eigenverantwortung der Nutzer aus? Die vom Meinungsforschungsinstitut dimap realisierte Umfrage ermittelt auffallende Paradoxien zwischen Verantwortung und Vertrauen.

DIVSI Ü60-Studie: Die digitalen Lebenswelten der über 60-Jährigen in Deutschland (2016)

Silver Surfer, Best Ager, 60+ – die Altersgruppe der über 60-Jährigen wird zunehmend wichtiger für Wirtschaft, Gesellschaft und Politik, denn sie macht jetzt schon etwa 30 Prozent der deutschen Bevölkerung aus – Tendenz steigend. Die Studie liefert erstmals differenzierte, anschauliche und umsetzungsorientierte Erkenntnisse über die digitalen Lebenswelten der über 60-Jährigen und räumt dabei auch mit einigen Vorurteilen auf.

DIVSI Studie „Digitale urbane Mobilität“ (2016)

Die Digitalisierung hat die Mobilitätsdebatte vollends erfasst. Aber wie weit entwickelt sind datengelenkte Verkehrssysteme sowie eine sichere und ressourcenschonende Mobilitätskultur wirklich? Wie sind Schutz der Privatsphäre und Nutzung eines digitalen Assistenzsystems im Auto zu vereinbaren? Insbesondere vor dem Hintergrund der Machbarkeit analysiert und hinterfragt diese Studie eine Vielzahl von Diskussionen und Aktivitäten aus Europa und den USA.

DIVSI Internet-Milieus 2016 – Die digitalisierte Gesellschaft in Bewegung (2016)

Wie beeinflusst der digitale Wandel das Leben der Menschen in Deutschland? Wie hat sich ihr Online-Verhalten in den letzten Jahren verändert? Welchen Stellenwert haben Internet und Smartphone im Lebensalltag? Wie denken die Menschen in der Nach-Snowden-Ära über Datensicherheit? Die repräsentative Studie bietet einen vertieften Blick in die aktuellen Lebenswelten unserer digitalen Gesellschaft.

Big Data (2016)

Zugespitzt auf die Themen „Smart Health“ und „Smart Mobility“ fasst der Bericht Erkenntnisse aus vielen Expertenrunden des DIVSI Forschungsprojekts „Braucht Deutschland einen Digitalen Kodex?“ zusammen. Er liefert Argumente für eine gesellschaftliche Debatte und wägt dabei Chancen und Risiken ab.

Das Recht auf Vergessenwerden (2015)

Die Entscheidung des EuGH zum „Recht auf Vergessenwerden“ lässt gleichwohl Fragen unbeantwortet, die im Spannungsfeld zwischen Persönlichkeitsrechten, Datenschutz und dem Recht auf Meinungs- und Pressefreiheit liegen. Dieser komplexen Problematik widmet sich diese Publikation und formuliert schließlich konkrete Empfehlungen für einen „Lösch-Kodex“.

weitere Studien ›

DIVSI Studie Beteiligung im Internet – Wer beteiligt sich wie? (2015)

Was ist Beteiligung im Internet eigentlich genau? Wie und weshalb bringen Internetnutzer sich ein? Die zweite Studie im Rahmen des DIVSI Forschungsprogramms „Beteiligung im Netz" untersucht Formen, Vorteile und Hürden der Beteiligung im Internet aus Sicht der DIVSI Internet-Milieus. In der qualitativen Untersuchung kommen dabei die Internetnutzer selbst zu Wort.

DIVSI U9-Studie – Kinder in der digitalen Welt (2015)

Wann und wie kommen Kinder mit digitalen Medien und dem Internet in Berührung? Wer begleitet sie auf ihrem Weg in diese Welt? Welche Bedeutung messen Eltern, Erzieher und Lehrer dem Internet für die Zukunft der Kinder bei? Welche Chancen und Risiken werden dabei wahrgenommen, wer trägt die Verantwortung? Die DIVSI U9-Studie hat Kinder zwischen 3 und 8 Jahren in den Blick genommen und lässt sie auch selbst zu Wort kommen.

DIVSI Studie – Daten: Ware und Währung (2014)

In einer repräsentativen Bevölkerungsbefragung untersucht DIVSI das Online-Nutzungs- und -Konsumverhalten in Deutschland. Im Fokus stehen Einstellungen der Internetnutzer zu Themen der Datensicherheit sowie Weiterverwendung von persönlichen Daten.

DIVSI Studie – Wissenswertes über den Umgang mit Smartphones (2014)

Über Smartphones sind Menschen heute nahezu ununterbrochen über das Internet miteinander verbunden. Mit steigendem Nutzungsumfang fällt dabei eine Vielzahl von Daten an. Unter der Leitfrage „Was geschieht mit meinen Daten?" war es Ziel der Studie, das Bewusstsein des einzelnen Nutzers dafür zu stärken, welche Daten auf dem Smartphone sein können, wie sie es verlassen und welche Möglichkeiten der Einsichtnahme und Einflussnahme Nutzer bei unterschiedlichen mobilen Betriebssystemen haben.

Braucht Deutschland einen Digitalen Kodex? (2014)

Mit dem Projekt „Braucht Deutschland einen Digitalen Kodex?" lotet DIVSI aus, ob ein Digitaler Kodex ein geeignetes Mittel ist, verbindliche Regeln im Internet auszuhandeln und durchzusetzen. Der Projektbericht steuert nicht nur zu diesem Gedanken Anregungen bei. Er bietet darüber hinaus generelle Anstöße, über die nachzudenken sicherlich lohnt.

DIVSI Studie zu Bereichen und Formen der Beteiligung im Internet (2014)

Das DIVSI-Forschungsprogramm „Beteiligung im Netz" leistet auf einer breiten theoretischen und empirischen Basis einen Beitrag zum öffentlichen Verständnis der Beteiligungschancen des Internets – und ihrer Voraussetzungen. Die Studie präsentiert einen ersten Schritt in diesem Vorhaben und verschafft einen Überblick über den heutigen Stand der Forschung.

DIVSI U25-Studie (2014)

Die DIVSI U25-Studie liefert erstmals fundierte Antworten auf Fragen, die das Verhalten der nachwachsenden Generation im Hinblick auf das Netz betreffen. Über die Nutzungsformen hinaus werden auch die Denk- und Handlungslogiken sowie der lebensweltliche Hintergrund untersucht.

DIVSI Studie zu Freiheit versus Regulierung im Internet (2013)

Wie sicher fühlen sich die Deutschen im Internet? Wie viel Freiheit und Selbstbestimmung wollen sie? Nach wie viel Regulierung wird verlangt? Die Studie zeigt ein detailliertes Bild des Nutzungsverhaltens der Deutschen im Internet und ihrer Wahrnehmung von Chancen und Risiken.

Entscheider-Studie zu Vertrauen und Sicherheit im Internet (2013)

Wie denken Entscheider über das Internet? Welchen Akteuren schreiben sie welche Verantwortung und welche Einflussmöglichkeiten zu? Was sagen sie zu Sicherheits- und Freiheitsbedürfnissen? Die Studie verdeutlicht erstmals, wie diejenigen über das Internet denken, die wesentlich die Spielregeln gestalten und Meinungsbilder prägen.

Meinungsführer-Studie „Wer gestaltet das Internet?“ (2012)

Wie gut kennen sich Meinungsführer im Netz aus? Wie schätzen sie ihre Einflussmöglichkeiten ein? Welche Chancen, Konfliktfelder und Risiken erwachsen daraus? In persönlichen Gesprächen wurden führende Repräsentanten aus Politik, Wirtschaft, Verwaltung, Wissenschaft und Verbänden interviewt.

Milieu-Studie zu Vertrauen und Sicherheit im Internet (2012) + Aktualisierung (2013)

Die Milieu-Studie differenziert erstmals unterschiedliche Zugangsweisen zum Thema Sicherheit und Datenschutz im Internet in Deutschland, basierend auf einer bevölkerungs-repräsentativen Typologie.

Unter **www.divsi.de** stehen die Studien kostenlos zum Download zur Verfügung.

www.divsi.de