19. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 81. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 27. Januar 2020, 14:00 Uhr
Konrad-Adenauer-Str. 1
10557 Berlin
Paul-Löbe-Haus, Raum E 600

Vorsitz: Jochen Haug, MdB

Tagesordnung - Öffentliche Anhörung

Antrag der Abgeordneten Jimmy Schulz, Stephan Thomae, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP

Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken

BT-Drucksache 19/5764

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Wirtschaft und Energie
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Christoph Bernstiel [CDU/CSU]
Abg. Sebastian Hartmann [SPD]
Abg. Jochen Haug [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

Teilnehmerliste

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**	**Weitere Teilnehmer**
CDU/CSU	Bernstiel, Christoph Oster, Josef	Pantel, Sylvia	
SPD	Hartmann, Sebastian		
AfD	Haug, Jochen Wirth, Dr. Christian		
FDP	Höferlin, Manuel Strasser, Benjamin		
DIE LINKE.	Pau, Petra		Domscheit-Berg, Anke
BÜNDNIS 90/DIE GRÜNEN	Notz, Dr. Konstantin von		
fraktionslos			

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 27. Januar 2020, 14.00 – 16.00 Uhr
„Recht auf Verschlüsselung“

Prof. Dr. Jan-Hendrik Dietrich
Hochschule des Bundes für öffentliche Verwaltung, Berlin

Prof. Dr. Hannes Federrath
Präsident – Gesellschaft für Informatik e. V.
Universität Hamburg

Ulrich Kelber
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn

Prof. Dr. Marian Margraf
Freie Universität Berlin

Prof. Dr. Michael Meier
Institute of Computer Science 4, Bonn

Prof. Dr. rer. nat. Rüdiger Weis
Beuth Hochschule für Technik Berlin

Einziger Tagesordnungspunkt

Antrag der Abgeordneten Jimmy Schulz, Stephan Thomae, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP

Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken

BT-Drucksache 19/5764

Stv. Vors. **Jochen Haug** (AfD): Meine sehr verehrten Damen und Herren, ich eröffne die 81. Sitzung des Ausschusses für Inneres und Heimat. Ich begrüße Sie alle sehr herzlich. Mein Name ist Jochen Haug. Ich bin der stellvertretende Vorsitzende des Ausschusses für Inneres und Heimat und werde die öffentliche Anhörung von Sachverständigen leiten. Ich danke Ihnen, sehr geehrte Sachverständige, dass Sie unserer Einladung nachgekommen sind, um die Fragen der Kolleginnen und Kollegen aus dem Ausschuss für Inneres und Heimat und der mitberatenden Ausschüsse zu beantworten. Die öffentliche Anhörung dient dazu, die Beratungen zu den in der Tagesordnung ausgewiesenen Vorlagen vorzubereiten. Weiter begrüße ich alle anwesenden Gäste und Zuhörer. Begrüßen darf ich auch für die Bundesregierung Herrn Abteilungsleiter CI Andreas Könen. Die Sitzung wird im Parlamentsfernsehen des Deutschen Bundestages und auf der Homepage des Deutschen Bundestages übertragen. Schriftliche Stellungnahmen hatten wir erbeten. Für die eingegangenen Stellungnahmen bedanke ich mich bei den Sachverständigen. Sie sind an die Mitglieder des Ausschusses für Inneres und Heimat und der mitberatenden Ausschüsse verteilt worden und werden dem Protokoll über diese Sitzung beigefügt. Ich gehe davon aus, dass Ihr Einverständnis zur öffentlichen Durchführung der Anhörung auch die Aufnahme der Stellungnahmen in eine Gesamtdrucksache umfasst. Von der heutigen Anhörung wird für ein Wortprotokoll eine Abschrift der digitalen Aufzeichnung gefertigt. Das Protokoll wird Ihnen zur Korrektur übersandt. Im Anschreiben werden Ihnen Details zur Behandlung mitgeteilt. Die Gesamtdrucksache bestehend aus Protokoll und schriftlichen Stellungnahmen wird im Übrigen auch ins Internet eingestellt. Zum zeitlichen Ablauf möchte ich anmerken, dass insgesamt eine Zeit von 14.00 Uhr bis 16.00 Uhr vorgesehen ist. Einleitend möchte ich jedem Sachverständigen die Gelegenheit geben, in einer Erklärung, die fünf Minuten nicht überschreiten sollte, zum Beratungsgegenstand Stellung zu beziehen. Danach würden wir orientiert an Fraktionsrunden mit der Befragung der Sachverständigen durch die Berichterstatterinnen und Berichterstatter sowie weiterer Abgeordneter beginnen. Ich bitte, dass die Fragesteller diejenigen Sachverständigen ausdrücklich benennen, an die sie die Frage richten wollen. Zu den Frageregeln gilt: In der ersten Fraktionsrunde kann jeder Fragesteller entweder zwei Fragen an einen Sachverständigen, eine gleiche Frage an zwei Sachverständige oder an zwei Sachverständige jeweils eine unterschiedliche Frage richten. Für die zweite Fraktionsrunde würde ich situativ entscheiden, nämlich ob es zeitlich noch möglich ist, zwei Fragen an einen Sachverständigen oder eine gleiche Frage an zwei Sachverständige zu stellen oder ob das Zeitfenster es nur noch hergibt, eine Frage an einen Sachverständigen zu stellen. Wenn Sie damit einverstanden sind, würden wir so verfahren. Dankeschön. Entsprechend alphabetischer Reihenfolge darf ich deshalb Herrn Dr. Jan-Hendrik Dietrich um seine Eingangsstellungnahme bitten.

SV **Prof. Dr. Jan-Hendrik Dietrich** (HS Bund, Berlin): Vielen Dank Herr Vorsitzender, sehr geehrte Abgeordnete, meine Damen und Herren. Zunächst darf ich mich herzlich bedanken, dass ich meine Expertise heute hier einbringen darf. Darauf bezieht sich mein einleitendes Statement. Ich möchte gerne eine juristische Perspektive in drei Punkten einnehmen. Erstens komme ich auf den verfassungsrechtlichen Schutz von Verschlüsselung zu sprechen. Ein Recht auf Verschlüsselung, das dem gegenständlichen Antrag hier zugrunde liegt, das kennt unsere Verfassung nicht. Auch in der Rechtsprechung des Bundesverfassungsgerichts und im einfachen Recht kommt ein Recht auf Verschlüsselung nicht vor. Ein Recht auf Verschlüsselung ist ein politischer Begriff. Das bedeutet aber nicht, dass Verschlüsselung verfassungsrechtlich schutzlos wäre. Vielmehr unterfällt die Verwendung von Verschlüsselungstechniken einer ganzen Menge von Grundrechten. Ich greife einmal ein Beispiel heraus. Artikel 10 des Grundgesetzes schützt das Fernmeldegeheimnis. Das Fernmeldegeheimnis schützt die Vertraulichkeit von Kommunikation bei räumlicher Distanz. Die Verwendung von Verschlüsselungstechniken soll diesen Schutz verstärken. Das ist vergleichbar mit dem Briefgeheimnis. Die Nutzung eines Umschlags dient der Wahrung des Briefgeheimnisses. Auch vom Schutzbereich

anderer Grundrechte wird die Verschlüsselung erfasst. Näheres kann meiner schriftlichen Stellungnahme entnommen werden. Damit wird klar, Verschlüsselung ist verfassungsrechtlich geschützt. Dieser Schutz wird aber nicht schrankenlos gewährleistet. Die betroffenen Grundrechte können einem Eingriff unterliegen. Damit komme ich zweitens zur Frage ob und inwieweit Verschlüsselung eigentlich regulierbar ist. Zunächst einmal ist nach dem Regelungsbedarf zu fragen. Sicherheitsbehörden in ganz Europa warnen immer wieder vor einem sogenannten Going-Dark-Problem. Danach stoßen klassische Überwachungsinstrumente infolge des verbreiteten Einsatzes von Verschlüsselungen an Grenzen. Der Staat kann es nicht akzeptieren, wenn der Vollzug seiner Gesetze infolge von missbräuchlicher Verwendung von Verschlüsselung erschwert oder unmöglich gemacht wird. Das Internet ist bekanntlich kein rechtsfreier Raum. Insofern kann es im Einzelfall notwendig sein, an unverschlüsselte oder entschlüsselte Informationen zu gelangen. Hierfür sind verschiedene Regelungsansätze denkbar. Sie reichen vom allgemeinen Verbot von Verschlüsselung über gesetzliche Pflichten zum Einbau von Backdoors bis hin zu Schlüsselhinterlegungs- oder -herausgabepflichten. Aus verfassungsrechtlicher Sicht sind solche Regelungen überwiegend zweifelhaft. Ein generelles Verbot des Einsatzes von Verschlüsselungen ist verfassungswidrig. Gleiches gilt für gesetzliche Verpflichtungen zum Einbau von Hintertüren. Auch gesetzlich normierte Schlüsselherausgabepflichten begegnen verfassungsrechtlichen Bedenken, jedenfalls bei offenen Ermittlungen der Strafvollzugsbehörden, wenn diese den Beschuldigten adressieren. Verfassungsrechtlich vertretbar erscheint allein, gesetzliche Lösungen anzustreben, Diensteanbieter zur Herausgabe von Schlüssel zu verpflichten. Das gibt es zum Teil im Gesetz schon, allerdings besteht hier zum gegenwärtigen Zeitpunkt eine Pflichtenkollision mit dem Datenschutzrecht, denn bei gesetzestreuer Anwendung der Datenschutzgrundverordnung wird kein Anbieter über Schlüssel verfügen, die er herausgeben kann. Was folgt daraus? Verschlüsselung ist zum gegenwärtigen Zeitpunkt schwer einer Regulierung zugänglich. Drittens ist deshalb danach zu fragen, wie die Verfolgung von Straftaten, die Bekämpfung von Extremismus und Terrorismus trotz Verschlüsselung gelingen kann. Hier ist der Gesetzgeber in der Pflicht cybertaugliche Befugnisse und technische Instrumente den Sicherheitsbehörden an die Hand zu geben. Dazu zählt z. B. die praxiskonforme Einführung und die technische Ermöglichung der Quellentelekommunikationsüberwachung. Kontraproduktiv wirken sich dagegen pauschale Meldepflichten für Sicherheitslücken und ein Verbot eines staatlichen Ankaufs von Sicherheitslücken aus. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann kommen wir nunmehr zu Herrn Prof. Federrath.

SV **Prof. Dr. Hannes Federrath** (Gesellschaft für Informatik; Uni Hamburg): Vielen Dank sehr geehrter Herr Vorsitzender, sehr geehrte Abgeordnete, meine Damen und Herren. Die verfügbaren kryptografischen Algorithmen, die wir kennen, sind seit Jahren so ausgereift, dass ihr breiter Einsatz problemlos möglich ist. Die EU-Datenschutzgrundverordnung verpflichtet im Übrigen in Artikel 32 explizit zur Verschlüsselung personenbezogener Daten. Die Umsetzung solcher technischen und organisatorischen Maßnahmen zum Schutz der informationellen Selbstbestimmung ist dementsprechend unabdingbar. In diesem Sinn ist es sowohl für den Schutz von Betriebs- und Geschäftsgeheimnissen, als auch zur Durchsetzung des Rechts auf informationelle Selbstbestimmung aus technischer Sicht möglich und mit Blick auf die Risiken der Digitalisierung auch geboten, ein Recht auf Verschlüsselung zu verankern und vielleicht sogar noch weitergehend, eine Pflicht des Diensteanbieters zur Datenverschlüsselung zu etablieren, soweit dies technisch möglich und zumutbar ist.

Zuletzt bestätigt wurde die Position der Bundesregierung zum freien Einsatz von Kryptografie zumindest im Jahr 2015. An diesen Eckpunkten sollte weiter festgehalten werden, da sich die technischen Rahmenbedingungen, die gegen eine Kryptoregulierung sprechen, seither kaum geändert haben. Die gesetzliche Einschränkung von Verschlüsselungen oder gar ein Verbot von Verschlüsselungen sind nicht durchsetzbar und nicht kontrollierbar.

Dies hat zwei Gründe: Erstens. Steganographische Verfahren sind dazu geeignet, auch Daten vertraulich zu transportieren, obwohl diese nicht verschlüsselt sind. In modernen Messenger-Apps etwa werden solche Funktionen leicht integrierbar und in Verbindung mit existierenden Anonymisierungsverfahren, wie etwa dem Tor-System, dazu geeignet, geheime Kommunikation sogar noch effektiver

zu schützen, als wir es von heutigen Produkten kennen. Zweitens sind die Verfahren zur rechtsverbindlichen Kommunikation, also etwa die elektronische Signatur und die Verfahren zum Schutz vor unbemerkten oder unerlaubten Veränderungen von Nachrichten und Dokumenten auf Kryptografie angewiesen und ohne sie also nicht denkbar. Im Ergebnis läuft eine etwaige Einschränkung von Kryptografie somit leer, schwächt die Wirtschaft, das Recht auf informationelle Selbstbestimmung und erschwert schlimmstenfalls sogar die Strafverfolgung. Dennoch gibt es Forschungs- und Entwicklungsbedarf. Erstens sind hier die Fortschritte bei der Entwicklung von Quantencomputern zu nennen. Diese werden mittelfristig einige Verfahren unsicher machen und neue Verfahren müssen in diesem Bereich entwickelt werden und die Forschung vorangetrieben werden. Zweitens. Wir haben ein Usability-Problem im Zusammenhang mit Kryptografien. Es gibt existierende Lösungen, die für den Endbenutzer allerdings aufwendig zu installieren sind und sehr mühsam und fehleranfällig zu bedienen sind. An dieser Stelle ist dringender Nachholbedarf, sowohl in Forschung als auch in Entwicklung geboten. Drittens. Bei der heute üblichen Beglaubigung von Schlüsselmaterial, etwa nach dem X509-Standard, gibt es viele Probleme, insbesondere bei der Überprüfung auf Echtheit der Schlüssel. Und auch hier haben wir noch erheblichen Forschungs- und Entwicklungsbedarf.

In der Vergangenheit hat sich der Gesetzgeber zwar durchaus proaktiv gezeigt, wenn es darum ging, den Schutz von informationeller Selbstbestimmung zu stärken und auch den Schutz der Wirtschaft. Allerdings gingen die Bemühungen noch nicht so weit, ein Verschlüsselungsgebot, also eine Pflicht zur Verschlüsselung, zu etablieren, allerdings wäre dies durchaus denkbar, da die Technik inzwischen soweit ist. Man könnte sich etwa vorstellen in Anlehnung an den § 13 Abs. 6 des Telemediengesetzes (TMG), der eine Pflicht zum anonymen Angebot oder unter Pseudonym regelt, auch eine ähnliche Regelung zu schaffen verpflichtend Verschlüsselungsdienste anzubieten, soweit dies technisch möglich und zumutbar ist. Das TMG ist vielleicht hier nicht die richtige Stelle, um so etwas zu regeln, aber etwa bei der Gestaltung der ePrivacy-Verordnung könnte man versuchen, das sogar EU-weit durchzusetzen. Insgesamt komme ich zu dem Ergebnis, dass die Forderungen des Antrags „Recht auf Verschlüsselung, Privatsphäre und Sicherheit im digitalen Raum stärken“ in vollem Umfang aus informatisch-technischer Perspektive zu begrüßen sind. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zu Herrn Kelber.

SV **Ulrich Kelber** (BfDI, Bonn): Vielen Dank Herr Vorsitzender. Auch vielen Dank für die Möglichkeit, aus meiner Sicht Einschätzungen zu dem Thema Recht auf Verschlüsselung abzugeben. Wir befinden uns in dem klassischen Spannungsfeld zwischen Freiheit und Sicherheit. In meiner Rolle als Bundesdatenschutzbeauftragter ist mein Plädoyer eindeutig. Drei Punkte. Erstens. Verschlüsselung ist Grundrechtsschutz. Sie schafft erst den Freiraum für jeden Einzelnen, selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen, die ihn als Person ausmachen. Die Forderung nach einer gesetzlichen Verankerung eines Rechts auf Verschlüsselung ist daher zu begrüßen. Es ist aus meiner Sicht auch eine logische Konsequenz bereits bestehender Ausprägung geltenden Rechts und auch der Rechtsprechung des Bundesverfassungsgerichts. Zweitens. Verschlüsselung ist existentieller Vertrauensanker in der digitalen Welt. Sie ist die Basis für den Schutz der Privatsphäre, aber auch für fast jede wirtschaftliche Betätigung in der digitalen Welt. Daher sollte es staatliche Aufgabe sein, die Nutzung der Verschlüsselung bestmöglich zu fördern und in ihrer gesamten Breite zu ermöglichen. Sie ist auch in ihrer Funktion für Datenschutz und IT-Sicherheit Erfolgsfaktor für eine Wirtschaftspolitik. Und eine verantwortungsbewusste und sinnvolle technologische Weiterentwicklung in den Geschäftsmodellen ist ohne Verschlüsselung undenkbar. Wir sind deswegen gut beraten, den Einsatz zu forcieren und auch die Weiterentwicklung. Das ist wichtig zum Schutz gegen Spionage, Sabotage, Datendiebstahl, sowohl im Privatbereich als auch im Unternehmensbereich, und jegliche gesetzliche Beschränkung oder Verbote oder Schwächung kryptografischer Sicherheitssysteme wären vor diesem Hintergrund kontraproduktiv und gefährlich. Eine Herabsenkung des Kryptoniveaus unterwandert das Vertrauen in elektronische Kommunikation und würde deswegen Digitalisierung verlangsamen. Auch das sollte verhindert werden. Wir brauchen stattdessen in der Tat einfachere und sicherere Lösungen als bisher, die in Breite ausgerollt werden. Einfach zu bedienende Verschlüsselungsverfahren müssen ohne

Einschränkung für alle Bürgerinnen und Bürger nutzbar sein. Drittens. Das Recht auf Verschlüsselung ist gar nicht so neu, sondern eigentlich eine Konsequenz des Bestehenden. Die Datenschutzgrundverordnung – das ist schon mal kurz erwähnt worden – fordert bereits nach geltendem Recht, europäisch bindenden geltendem Recht, personenbezogene Daten gegen Datenschutzrisiken abzusichern. Verschlüsselung ist hierfür grundsätzlich ein essenzielles, nicht optionales Instrument und ist deswegen auch mehr als eine unverbindliche Empfehlung. Sie werden in der Datenschutzaufsicht Fälle erleben, wo die Nichtverschlüsselung von Daten zu empfindlichen Sanktionen für Unternehmen und auch Behörden führen würden. Auch in der Telekommunikation ist Verschlüsselung essenziell. Es stehen da ja auch Entscheidungen und Ausprägungen an. Sie ist einmal ein verfassungsrechtlich verbrieftes Grundrecht, Artikel 10 Grundgesetz, aber auch bereits nach dem Abschluss der Kommunikation hört dieser Schutz nicht auf. Also nicht mehr Artikel 10 Grundgesetz unmittelbar gilt, sondern das Bundesverfassungsgericht hat klargestellt, dass auch das allgemeine Persönlichkeitsrecht bereits die Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme umfasst. Das ist umso wichtiger, weil wir uns natürlich über immer mehr Daten unterhalten, die von solchen Systemen aufgenommen werden mit der totalen Verschränkung des digitalen und des nichtdigitalen Lebens. Und wenn diese Daten in falsche Hände geraten, geben sie ein ganz anderes Abbild über einen Menschen, als es in der Vergangenheit der Fall war. Deswegen ist Verschlüsselung der Garant für grundrechtlich geschützte Rechtsgüter und eine positiv rechtliche Verankerung eines Rechts auf Verschlüsselung wäre wichtig und eben nicht Folge der weiteren Schwächung.

Herausgabepflichten für Schlüssel oder Passwörter würden dem widersprechen. Übrigens aus meiner Sicht auch der im Grundgesetz verankerten Selbstbelastungsfreiheit an der Stelle, wenn es um Privatpersonen geht. Aber wie ich gerade eben auch dargestellt habe, im Bereich der Unternehmen. Der Staat sollte vielmehr darauf drängen, dass Anbieter mehr verschlüsseln und verschlüsseln müssen als Schutz der Bürgerinnen und Bürger und der Unternehmen vor Kriminellen, privater und fremdstaatlicher Überwachung. Dass er damit automatisch auch ein Abwehrrecht gegen sich selber in Kauf nimmt, ist in dieser Abwägung hinzunehmen und deswegen ist das aus meiner Sicht Aufgabe des Staates. Wir werden ohnehin nicht erreichen, dass der Staat immer und im besten Fall voraus alle möglichen Straftaten erfassen kann dadurch, dass er die Daten von allem, jedem und von allen Gelegenheiten wahrnimmt und deswegen ist dieses Spannungsfeld tatsächlich in dieser Zeit nur aufzulösen, indem wir digitale Kommunikation als Grundlage unserer Gesellschaft möglichst sicher ausgestalten. Das geht nicht ohne Verschlüsselung.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zu Herrn Prof. Margraf.

SV **Prof. Dr. Marian Margraf** (FU Berlin): Ich möchte mich auch nochmal herzlich für die Einladung bedanken und dass ich zu dem Antrag Stellung nehmen kann. Ganz kurz. Ich unterstütze eigentlich alle im Antrag der FDP-Bundestagsfraktion aufgeführten Vorschläge und möchte in meinem Eingangsstatement zwei Punkte ein bisschen deutlicher herausstellen. Meines Erachtens ist das Recht, vertraulich zu kommunizieren, das leitet sich ab aus dem Grundrecht der informationellen Selbstbestimmung und Verschlüsselung ist sozusagen die einzige Möglichkeit dieses Schutzziel tatsächlich umzusetzen. Wir Kryptografen wissen welche Verfahren da sicher sind. Allerdings zeigen ja Untersuchungen, dass die meisten Nutzerinnen und Nutzer diese Verfahren nicht einsetzen. Das hat zum einem, das wurde auch schon angesprochen, Usability-Probleme. Technisch nicht affine Nutzerinnen und Nutzer begreifen einfach unsere kryptografischen Konzepte nicht. Also was ist ein öffentlicher Schlüssel? Was ist ein geheimer Schlüssel? Welcher Schlüssel wird wann wofür eingesetzt? Was sind Signaturen? Und so weiter und so fort. Und gerade vor dem Hintergrund, dass wir eigentlich Ende-zu-Ende-Sicherheit, wie im Antrag ja auch gefordert, umsetzen wollen, wo dann nochmal wesentliche Teile dieses Schlüsselmanagements ja bei den Nutzerinnen und Nutzern verbleiben, ist die Wissenschaft aufgefordert, hier deutlich mehr Forschung zu betreiben im Sinne der Benutzbarkeit. Also diese Prozesse müssen deutlich intuitiver umgesetzt werden können. Also das ist der eine Punkt, die Benutzbarkeit voranzutreiben.

Herr Federrath hatte auch noch den Punkt Quantencomputer angesprochen. Alle Experten, also zumindest die Physiker sagen, Quantencomputer

wird es in ausreichender Größe in zehn Jahren geben. Wir wissen, die werden erhebliche Auswirkungen auf die heute eingesetzte Kryptografie haben. Gerade auf die asymmetrische Kryptografie. Einfach gesprochen, bricht das alles, was wir heute benutzen. Und da müssen wir die Forschung ebenfalls vorantreiben. Das BMBF hat sich dieses Themas letztes Jahr angenommen und fördert derzeit sieben Forschungsprojekte, die sich genau mit diesem Thema beschäftigen. Also zwei wichtige Punkte, die ich da sehe.

Ein weiterer Schwerpunkt im Antrag war ja das Thema Backdoors und Ausnutzung von Sicherheitslücken. Das halte ich für sehr kritisch. Also nicht die Forderung, die Sie aufgestellt haben, sondern diese Sicherheitslücken auszunutzen und geheim zu halten, denn diese können ja dann auch von Kriminellen ausgenutzt werden und haben eben nicht nur erheblichen Schaden auf die informationelle Selbstbestimmung, sondern im Hinblick auf Wirtschaftsspionage, die damit betrieben werden kann, eben auch auf unsere deutsche Wirtschaft. Ähnlich wird ja häufig diskutiert, das ist auch schon angesprochen worden, dass Dienstanbieter aufgefordert werden sollen, unter bestimmten Bedingungen Passwörter oder kryptografische Schlüssel herauszugeben. Ich beurteile das jetzt mal aus technischer Sicht. Also im Sinne von Ende-zu-Ende-Sicherheit haben diese Diensteanbieter diese kryptografischen Schlüssel gar nicht mehr. Also die liegen bei den Nutzerinnen und Nutzern. Können also gar nicht herausgegeben werden. Ähnlich ist es bei Passwörtern. Wenn man das vernünftig technisch – also wie technisch heute gefordert – umsetzt, sind die Passwörter nicht im Klartext bei den Diensteanbietern hinterlegt, sondern halt verschlüsselt oder wie auch immer mit verschiedenen Methoden, sodass Diensteanbieter nur kontrollieren können, ist das eingegebene Passwort tatsächlich das richtige Passwort, aber herausgeben können sie diese Passwörter nicht. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zu Herrn Prof. Meier.

SV **Prof. Dr. Michael Meier** (Institute of Computer Science 4, Bonn): Vielen Dank Herr Vorsitzender, sehr geehrte Damen und Herren Bundestagsabgeordnete, sehr geehrte Damen und Herren. Vielen Dank für die Gelegenheit, hier zu dem Antrag der Fraktion der FDP Stellung zu beziehen und ich fasse einige Punkte kurz, weil wir sie ich denke schon gehört haben. Wir haben bereits gehört, dass Grundrechte existieren, die ein Recht auf Vertraulichkeit zusichern und daraus ergibt sich aus meiner Sicht, weil Verschlüsselung das einzige wirksame Mittel ist, mit dem wir Vertraulichkeit heute schützen können, tatsächlich ein Recht auf Verschlüsselung. Tatsächlich ist es auch schon angesprochen worden von meinen Vorrednern, ist es so, dass IT-Sicherheitsmechanismen, insbesondere auch Verschlüsselung tatsächlich ihre Wirksamkeit nur auf Zeit behalten. Das heißt, wir müssen am Ball bleiben und von daher möchte ich nochmal unterstreichen und begrüße diese Forderung aus dem Antrag explizit, dass wir die Weiterentwicklung und Forschung zu Verschlüsselung und zu IT-Sicherheitsmechanismen weiter fördern und vorantreiben müssen. Das schließt in meinen Augen ein, dass wir insbesondere die Anbindung von Verschlüsselung in der Breite, insbesondere organisationsübergreifend und auch durch die Bevölkerung weiter vorantreiben müssen und tatsächlich ist aus meiner Sicht die große Hürde, der wir uns da aktuell gegenüber sehen, eben die angesprochene Benutzbarkeit der Systeme auf der einen Seite, zum anderen aber auch irgendwie eine staatliche Verantwortlichkeit dafür, die Infrastrukturen, die dafür erforderlich sind, tatsächlich zu realisieren. Also ich spreche über Schlüsselaustauschmechanismen, über Verzeichnisse, in denen diese Informationen abgefragt werden können, die wir innerhalb von einzelnen Unternehmen und Organisationen vorfinden, sodass innerhalb der Organisation verschlüsselt kommuniziert werden kann. Aber wenn, wie es erklärtes Ziel der Bundesregierung ist, Deutschland Verschlüsselungsstandort Nummer 1 werden soll, dann reicht das nicht aus, sondern da muss an dieser Stelle mehr investiert werden.

Unter dem Gesichtspunkt verbieten sich aus meiner Sicht jegliche Versuche, Kryptografie zu beschränken oder gar mit Verboten zu versehen. Genauso wie Versuche irgendwie Schlüsselkopien oder Schlüsselmaterial zugänglich zu machen, weil es eben tatsächlich diesen einzigen wirksamen Mechanismus, mit dem wir Vertraulichkeit schützen können, aushebeln würde und damit eben diese Grundrechte auf Vertraulichkeit tatsächlich aushöhlt.

Zum Thema Backdoors und Schwachstellenmärkte: Tatsächlich Schwachstellen, Sicherheitslücken, mit

denen kann man nur eins machen. Die kann man nur sinnvoll schließen. Also möglichst zügig auch. Denn so eine Sicherheitslücke ist im Prinzip eine Gefahr für alle. Und aus meiner Sicht ist es nicht tolerierbar, dass aus vielleicht grundsätzlich nachvollziehbaren Motiven die Interessen von Ermittlungsbehörden hier überwiegen können und letztlich eine Gefahr dadurch für alle ausgeht. Deswegen ist es abzulehnen tatsächlich Schwachstellen, Sicherheitslücken auf solchen Märkten zu erwerben, um sie geheim zu halten und zu nutzen beispielsweise für Ermittlungsaufgaben. Ich würde aber eine Beteiligung an solchen Märkten nicht pauschal ablehnen, sondern aus meiner Sicht ist es durchaus sinnvoll eine Aufklärung dieser Märkte dahingehend zu betreiben, dass man Kenntnis davon bekommt, was für Sicherheitslücken werden dort eigentlich gehandelt, sofern das möglich ist. Mir ist die Organisation der Märkte heute und in der Zukunft tatsächlich nicht klar, denn wenn man diese Informationen hat, dann kann man die nicht ausschließlich nur geheim halten und nutzen, sondern man kann davon ausgehen, tatsächlich Empfehlungen hinsichtlich bestimmter Systemumgebungen oder Produkte aussprechen und das BSI z. B. empfiehlt ja auch nicht ohne Grund sowas wie eine Zwei-Browser-Strategie. Das heißt, man hat in bestimmten Situationen die Möglichkeit, wenn die Ansage kommt: „Ihr Browser 1 ist aktuell verwundbar, bitte nutzen Sie den nicht, sondern nutzen Sie den zweiten“. Genau um solche Warnungen formulieren zu können und dann eben in bestimmten Situationen ausweichen zu können, ist es tatsächlich aus meiner Sicht sinnvoll, solche Märkte aufzuklären.

Meldepflicht für staatliche Stellen aus meiner Sicht ein Selbstverständnis. Wenn ich merke, dass irgendwo eine Sicherheitslücke vorliegt als staatliche Stelle, dass ich diese an die verantwortlichen Organisationen zu melden habe. Wir fordern dies ja auch von KRITIS-Unternehmen, die einer Meldepflicht unterworfen sind. Und dies hier an das BSI zu tun, ist aus meiner Sicht selbstverständlich. Ich will an der Stelle aber auch nicht verschweigen, dass ich gerade in den letzten Tagen wieder Diskussionen verfolgt habe, wo es tatsächlich so war, dass Mitarbeiter von KRITIS-Unternehmen Kenntnis von einer Sicherheitslücke bekommen haben und diese nicht gemeldet haben beziehungsweise verzögert gemeldet haben. Einfach weil Bedenken bestanden haben, dass Organisationen im Umfeld, im weiteren Umfeld des BSI diese möglicherweise geheim halten und nutzen können würden. Und um eben genau diesen Konflikt aufzuweichen und tatsächlich eine schnellstmögliche Meldung von Sicherheitslücken zu realisieren, ist es aus meiner Sicht erforderlich, dass die Meldungen von Sicherheitslücken an eine unabhängige Organisation zu erfolgen hat. Beispielsweise an ein unabhängiges BSI. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zu Herrn Prof. Weis.

SV **Prof. Dr. rer. nat. Rüdiger Weis** (Beuth Hochschule für Technik Berlin): Vielen Dank Herr Vorsitzender. Sehr geehrte Damen und Herren Abgeordnete, sehr geehrte Damen und Herren Zuhörerinnen und Zuhörer. Ich bin von Hause aus Mathematiker und Professor für sichere Betriebssysteme. Insofern sei mir verziehen, wenn ich an ein paar Stellen wirklich sehr runter in die Technik gehe, also bis zu Zahlen im Bereich der Kryptografie und bis zu den Bits und sogar darunter hinaus im Bereich von sicheren Systemen. Ich glaube, es ist relativ hilfreich, weil das wirklich aus technischer Seite analysiert, welche Regelungsmöglichkeiten möglich sind und welche technisch einfach nicht durchführbar sind.

Lassen Sie mich mit der Kryptografie beginnen. Die Kryptografie hat die interessante Eigenschaft, dass sie entweder von niemandem brechbar ist oder faktisch von jedem Interessierten und Motivierten. Erlauben Sie mir, dass ich ein Praxisbeispiel mache, was ich mit Motivierten meine. Das ist durchaus ein aktueller Fall. Wir haben einen wirklich sicherheitsrelevanten Angriff gegen die SHA1-Hash-Funktion. Das ist ein sehr wichtiger Buildingblock für Signaturen und allgemein Systemsicherheit. Da haben wir einen Angriff von einer akademischen Gruppe, die hat zusätzlich für etwa 70.000 Euro Rechenkapazität gekauft und konnte damit einen praxisrelevanten Angriff erstellen. Also man kann sagen, dass man entweder die Möglichkeit hat, Sachen richtig und ordentlich zu machen oder so zu machen, dass es nicht nur staatliche Stellen angreifen können, sondern auch motivierte Wissenschaftler. Und was motivierte Wissenschaftler können, können – glaube ich – Organisationen mit höherem finanziellem Interesse in den meisten Fällen auch. Manchmal ist die Wissenschaft voran, aber aus Sicherheitsgründen sollte man sich darauf nicht verlassen. Also insofern sind Regelungsmöglichkeiten,

dass man die Kryptografie hinreichend schwächt für Zugänge, einfach technisch nicht möglich.

Noch drastischer ist die Situation im Bereich der sogenannten Cyberangriffswaffen. Ich weiß nicht, ob es allen Leuten klar ist: Diese Cyberwaffen sind kopierbare Programme. Das bedeutet, wenn irgendein Geheimdienst seinen Werkzeugkasten verliert, dann kann man den einfach kopieren. Das klingt jetzt sehr obskur, aber wenn Sie sich mal die Situation bei WannaCry angucken, da war genau die Situation. Die NSA hat ihren Werkzeugkasten stehen lassen, offen stehen lassen. Das ist dann – wahrscheinlich nicht nach Lizenzbedingungen berechtigt – kopiert worden. Lange Rede kurzer Sinn: Es gab dann ein Angriffstool, das dann Hunderte, Tausende oder Millionen Rechner angegriffen hat. Das WannaCry sind Sachen, wo ich ganz deutlich als Informatiker sagen kann, das waren relativ dilettantische Programmierer. Wenn ich schlecht gelaunt da ein paar Zeilen ändern würde, dann wäre das fast unmöglich, dann dieses Programm zu deaktivieren. Machen Sie sich keine Sorgen, ich bin ein über 50-jähriger Professor mit Kleingarten. Also insofern bin ich da wenig motiviert, so Sachen zu machen. Aber es gibt durchaus Leute mit ähnlich guter oder besserer Kenntnis über Angriffe, die da keinen derartigen moralischen Kompass haben. Noch einmal, Waffen, die da draußen sind, sind ein Angriff gegen uns alle und es ist auch kein akademisches Problem. Ich habe die schriftliche Stellungnahme am 23. abgeben müssen. Ich habe mir den Spaß gemacht bis zum 27. Mal zu gucken, was passiert ist. Wir haben die Situation, dass wir immer noch Nachwirkungen einer Windows-Kernschmelze hatten im Bereich der Kryptografie. Wir haben diese Citrix-Sachen, die im Moment gerade die EDV der Landeshauptstadt Potsdam weitgehend lahmlegen und wir haben auch den Fall, dass im Moment drei Millionen Daten von Nutzern von einer Autovermietung veröffentlicht wurden. Also insofern diese Sachen, dass erstens jeder angreifen kann. Zweitens ist es ein Problem, das im Zweifelsfall so gut wie alle oder zumindest Millionen Bürgerinnen und Bürger betrifft, es ist keine akademische Sache, sondern eine deutliche Warnung aus der Praxis. Die Frage ist, wie geht man damit vor. Meine klare Ansage: Wenn wir Sicherheitslücken haben, müssen wir die umfangreich schließen. Ich bin in meiner Stellungnahme umfangreich darauf eingegangen, dass neben der Gefährdung der digitalen Welt auch die praktische, die offline-Welt gefährdet ist. Wir haben Industrievernetzung. Die Sachen hängen am Netz. Wir haben IoT-Geräte, wo die Sicherheitssituation verheerend ist. Und ich muss ehrlich sagen, jede Sicherheitslücke, die im Moment ungepatcht ist, kann wirklich ganze Städte und ganze Verwaltungen runterfahren und damit ist wirklich das Handeln mit Sicherheitslücken eine Bedrohung der inneren Sicherheit.

Zur letzten Minute noch ein paar konstruktive Punkte. Ich glaube, die Bundesregierung kann durchaus auf ein paar positive Sachen aufbauen. Die Förderung von GPG ist schon seit Jahren irgendwie gut am Laufen. Wir haben von den Kollegen gehört, dass da das Problem ist der praktischen Anwendbarkeit. Da muss sicher deutlich geforscht werden. Es muss im Bereich der Quantencomputer geforscht werden und die Stellung des BSI sollte in meinen Augen auch ausgebaut werden. Ich möchte wirklich als letzte Bemerkung machen – das ist den meisten Leuten nicht klar – aber ich habe mit vielen Leuten aus sehr verschiedenen Communitys geredet und in dieser Diskussionen des möglichen Handelskriegs USA gegen Huawei muss ich sagen, waren die Stellungnahmen des BSI eine der wenigen weltweiten Organisationen, die dort für Vernunft beigetragen haben. Und aus dem Grund ist da durch die Handlung der Bundesregierung wirklich eine vertrauenswürdige Organisation geschaffen, die in meinen Augen weiter gestärkt werden sollte. Vielen Dank für Ihre Aufmerksamkeit.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann sind wir am Ende der Stellungnahmen. Vielen Dank für die Eingangsstellungnahmen. Wir beginnen mit der Fraktionsrunde. Wie immer gilt die Regel drei Minuten Fragezeit pro Fraktion. Wir beginnen bei der CDU/CSU-Fraktion und Herrn Bernstiel.

BE **Christoph Bernstiel** (CDU/CSU): Zunächst einmal vielen Dank an die Sachverständigen für Ihre im Vorfeld zugesandten Berichte und auch für die hier eingebrachten Statements. Wir reden ja heute über ein Thema, was wir bereits auch im Plenum behandelt hatten und dazu bereits einige Meinungen ausgetauscht wurden. Ich möchte für meine Fraktion zumindest mal klarstellen, dass wir natürlich auch Verschlüsselungsverfahren fördern und auch das BSI stärken. Das sehen Sie in den letzten Haushaltsansätzen, dass das BSI massiv aufgebaut

werden soll und wir ja auch das hehre Ziel verfolgen ein BSI für Bürger aufzubauen, sodass also quasi wirklich jeder Bundesbürger sich mit diesem Thema IT-Sicherheit auseinandersetzen kann und über das Programm oder beziehungsweise über die Förderung des sogenannten Easy-GPG, also E-Mail-Verschlüsselung haben Sie schon ja besprochen. Das sind alles Initiativen, die die Bundesregierung betreibt. Dazu zwei Fragen. Eine an Herrn Prof. Dietrich. Und zwar würde mich nochmal interessieren, wenn Sie nochmal darauf eingehen könnten, wie hat sich denn aus Ihrer Sicht die Ermittlungsfähigkeit unserer Sicherheitsbehörden in den letzten Jahren entwickelt, insbesondere mit dem Blick auf zunehmende Verschlüsselung, insbesondere auch von kriminellen Organisationen und ist das etwas, was Sie als Herausforderung sehen oder können wir das noch handhaben. Also dass Sie das Phänomen Going-Dark vielleicht nochmal etwas stärker beleuchten. Das würde mich sehr interessieren.

Und eine zweite Frage an Herrn Prof. Margraf wäre die, mal angenommen ich folge jetzt dem FDP-Antrag und sage es gibt jetzt ein Recht auf Verschlüsselung. Sie hatten ja auch dargestellt, dass es das so ganz einfach sich nicht ableitet. Aber wie soll sich das denn im Alltag tatsächlich umsetzen? Also wir sagen jetzt, wir hätten ein Grundrecht auf Verschlüsselung. Wäre denn der Staat verantwortlich, jedwede Kommunikation, die man als Privatbürger kommuniziert, zu verschlüsseln? Das irgendwie zur Verfügung zu stellen? Könnten Sie da vielleicht mal darauf eingehen, ob so etwas überhaupt realistisch ist und wie sich das umsetzen ließe. Das erstmal die Fragen in der ersten Runde. Danke.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen zur AfD-Fraktion und Herrn Dr. Wirth.

Abg. **Dr. Christian Wirth** (AfD): Auch von mir vielen Dank für die interessanten Vorträge. Meine erste Frage an Herrn Kelber. Wie sieht der konkrete Zeitplan für den Aufbau der Agentur für Innovation in der Cybersicherheit aus, der für dieses Jahr geplant ist und wird im Zusammenhang mit dem Recht auf Verschlüsselung dort geförderte Technologie grundsätzlich Privatpersonen beziehungsweise Unternehmern zugänglich gemacht werden oder ist das ausgeschlossen? Und dann hätte ich ebenfalls eine Frage an Herrn Prof. Meier. Bei vollständigem Verzicht auf Backdoors, welche Möglichkeiten blieben Behörden z. B. zur konkreten Gefahrenabwehr auch kurzfristig Zugriff auf kritische Daten zu erhalten bei allem gebotenen Schutz der Privatsphäre? Danke.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann kommen wir SPD-Fraktion und Herrn Hartmann.

BE **Sebastian Hartmann** (SPD): Herr Vorsitzender herzlichen Dank. Ich möchte zwei Fragen an einerseits den Bundesdatenschutzbeauftragten Herrn Kelber richten und die zweite Frage dann an Herrn Prof. Dr. Weis. Natürlich teile ich die Auffassung des Kollegen der Union, was die Stärken des BSI angeht und die entsprechenden Haushaltsmittel, die wir zur Verfügung gestellt haben. Aber Herr Kelber, Sie haben natürlich das Spannungsverhältnis formuliert als es darum ging, wie gelingt denn Freiheit im Netz, wenn es darum geht, entsprechend Verschlüsselungsstandort Nummer 1 zu werden. Nun gibt es ja auch Bestrebungen bis hin zu der Pflicht der Passwortherausgabe, was Nutzerinnen und Nutzer angeht im Fall des Falles. Wie würden Sie den Konflikt auflösen aus Sicht des Bundesdatenschutzbeauftragten, dass wir einerseits der Verschlüsselungsstandort Nummer 1 werden wollen in der Welt, Sicherheit für Bürgerinnen und Bürger einerseits aus der verbraucherschutzpolitischen Perspektive beim BSI, aber auf der anderen Seite aber auch für die Wirtschaft entsprechende Techniken anzufertigen. Es gab da ja auch einen Hinweis, dass es Grenzen gibt, dass man sich nicht selbst belasten muss. Welche Empfehlungen haben Sie dazu und wie bringen Sie das ein?

Und die zweite Frage würde ich auch in dem Feld der Verschlüsselung an Herrn Prof. Dr. Weis richten. Sie haben in der letzten Minute Ihres Beitrages nochmal auf die Technikausrüstung hingewiesen. Wir haben eine aktuelle Debatte in Deutschland um das Thema 5G und den möglichen Ausschluss bestimmter Technikausrüster. Ich will das jetzt nicht regionalspezifisch oder länderspezifisch aufschlüsseln. Ist aus Ihrer Sicht die Form oder der Einsatz von Verschlüsselungstechnologien – was Kommunikation angeht – ein möglicher Weg, einerseits die Technikausrüstung – sagen wir mal – eines chinesischen Ausrüsters zuzulassen, auf der anderen Seite aber auf Verschlüsselungstechnologien zuzugreifen, die Möglichkeit Spionage auf der einen Seite und im anderen Feld Sabotage vorzugreifen. Sie haben da einen kurzen Hinweis gerade gegeben, einen kurzen Hinweis auch in Ihrer Stellungnahme. Das

wäre doch sehr interessant, wenn Sie das nochmal ausführen. Danke.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann kommen wir nunmehr zur FDP-Fraktion und Herrn Höferlin.

BE **Manuel Höferlin** (FDP): Vielen Dank Herr Vorsitzender. Herzlichen Dank an die Sachverständigen für die ausführlichen Stellungnahmen. Es freut mich natürlich besonders zu hören, dass sich eigentlich alle Sachverständigen ausnahmslos darüber einig sind, dass wir eine starke Verschlüsselung haben müssen, brauchen, dass es ein effektiver Weg ist zum Schutz von Vertraulichkeit und Kommunikation. Interessant fand ich auch die Ausführungen zur Steganografie, weil Steganografie ja auch nicht ganz neu ist, sondern das gibt es ja nun auch schon seit – ich weiß gar nicht – 15 Jahren oder so oder länger, zumindest in der Anwendung. Ich würde ganz gerne zwei Themenkomplexe nochmal ein bisschen näher beleuchten. Das ist einmal die Frage zur Kultur der grundsätzlichen Verschlüsselung und zum anderen der sehr hitzig geführten Debatte auch zu den Befugnissen von Sicherheitsbehörden, einer Schwächung von Verschlüsselung. Interessant ist ja bei der ganzen Diskussion, dass die Bundesregierung selbst in ihrem Koalitionsvertrag eigentlich wortwörtlich darauf schreibt, dass sie die Verschlüsselung für jedermann verfügbar machen möchte, auch Ende-zu-Ende, dass sie PGB fördern möchte. Ich frage mich dann nur, warum es dann eben nicht stattfindet. Deswegen Herr Prof. Federrath die Frage an Sie, welche Schritte und Maßnahmen sind denn Ihrer Ansicht nach notwendig, um eine flächendeckende, effiziente, möglichst unkomplizierte Verschlüsselung von E-Mail auch gerade über Anbietergrenzen hinweg, also offen zu etablieren und würde da irgendwie eine Verpflichtung für Telekommunikations-, Telemedienanbieter, wie Sie es ja ins Spiel gebracht haben, helfen?

Und die zweite Frage an Sie Herr Kelber, wenn wir über eine sichere Ende-zu-Ende-Verschlüsselung sprechen und damit das einhergehende Grundrecht für Bürger auf abhörsichere, vertrauliche Kommunikation auch etablieren wollen. Wie stehen Sie denn da und wie ordnen Sie ein die Ideen, die wir ja gerade immer von Seiten der Union z. B. hören zum Thema, wir wollen nicht in die Backdoors, sondern durch die Frontdoor jetzt und wollen z. B. eine Ghost Communication drin haben, also jemand, der mithören kann, einen Drittschlüssel etablieren, umschlüsseln, nur für eine Millisekunde. Es ist ja nicht schlimm. Also diese Argumente höre ich ja immer wieder. Als ob das etwas ausmachen würde, wie lange das ist. Also was für Auswirkungen hat das dann.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zur Fraktion DIE LINKE. und Frau Pau.

BE **Petra Pau** (DIE LINKE.): Erstmal herzlichen Dank für alle Stellungnahmen. Ich habe zwei Fragen an Prof. Weis. Einmal, Sie schreiben in Ihrer Stellungnahme, dass es bereits Angriffe mit Millionen übernommener IoT-Geräte gegeben hat und dass in der Fachwelt entsprechende Szenarien theoretisch entwickelt und dargestellt werden können. Können Sie einmal plastisch und an konkreten Beispielen erläutern, was da stattfindet und auch auf Ihre Lösungsvorschläge eingehen. Ich will noch zwei Stichworte in den Raum stellen, einerseits Herstellerhaftung, andererseits auch Pflichten von Nutzerinnen und Nutzern. Das war die erste Frage. Die zweite, Sie gehen am Ende Ihrer Stellungnahme kurz auf die fachliche Auseinandersetzung um geschlossene und offene Systeme hinsichtlich ihrer Systemsicherheit am Beispiel der Intel-Chiparchitektur ein. Können Sie uns das auch nochmal etwas plastischer darstellen und in dem Fall ich meine, wir machen das ja einerseits um hier sachkundig zu entscheiden, aber diese Anhörung wird ja auch öffentlich wahrgenommen und übertragen. Insofern wäre es gut, wenn Sie uns auch nochmal die Unterschiede zwischen geschlossenen und offenen Systemen darstellen.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Und dann kommen wir abschließend zu der Fraktion BÜNDNIS 90/DIE GRÜNEN und Herrn Dr. von Notz.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank Herr Vorsitzender. Vielen Dank für die Eingangsstatements. Auch vielen Dank für das Thema überhaupt an die Fraktion der FDP. Unserem Freund Jimmy Schulz würde das Thema gut gefallen am heutigen Tag und es ist ein unbestritten wichtiges. Ich habe zwei Fragen an Herrn Kelber. Die erste Frage klang auch schon in den Eingangsstatements an der einen oder anderen

Äußerung durch. Kann das unbestritten fachkundige BSI unabhängig beraten, wenn es in den Weisungsstrang des BMI eingestellt ist? Oder ich kann die Frage auch mal umdrehen, damit Sie nicht ganz so den Zwängen ausgeliefert sind. Wären Sie unabhängig, wenn Sie in den Weisungsstrang des BMI gestellt sind? Und was würde das an Ihrem Leben eigentlich verändern, Herr Kelber?

Die zweite Frage: Bei De-Mail hat man ja ganz bewusst verzichtet auf durchgehende Ende-zu-Ende-Verschlüsselung. Ich frage mich, bei welchem Projekt man das zukünftig eigentlich allen Ernstes noch propagieren würde. Ich kann mich an die De-Mail-Diskussion sehr gut auch in verschiedenen Anhörungen erinnern. Da haben hier Notar- und Anwaltskammern und alle möglichen Beteiligten wirklich darum gebeten, dass muss Ende-zu-Ende verschlüsselt werden. Die Bundesregierung, die große Koalition hat es nicht gemacht. Aber wie ist das denn? 5G, autonomes Fahren, Daten nicht Ende-zu-Ende verschlüsseln und was für Großprojekte zukünftig gilt, soll das nicht für unsere Kommunikation gelten? Oder wie ist das eigentlich mit der Kommunikation der Bundesregierung? Ist die unverschlüsselt oder verschlüsseln Sie grundsätzlich die Kommunikation auf Seiten der Bundesregierung und nur die Bürgerinnen und Bürger sollen das nicht grundsätzlich machen oder …? Das würde mich interessieren. Vielleicht können Sie da mal so einen pauschalen Abriss drauf machen. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann kommen wir zur Antwortrunde und wir beginnen mit Herrn Prof. Dietrich.

SV **Prof. Dr. Jan-Hendrik Dietrich** (HS Bund, Berlin): Vielen Dank. Was Sie angesprochen haben betrifft das Problem Sicherheit trotz Verschlüsselung. Wir finden in den Gazetten dieses Going-Dark-Problem, dass die Sicherheitsbehörden immer wieder beklagen und das ist keineswegs neu. Auch schon in den 90er Jahren gab es mal so etwas, was sich Kryptokontroverse nannte und zu dieser Zeit wurden tatsächlich noch Vollverbote von Verschlüsselungen gefordert. Inzwischen sind wir da ein bisschen weiter. Verschlüsselung ist gut und alle wollen, das entnehme ich allen Sachverständigenäußerungen, alle wollen Verschlüsselung. Verschlüsselung führt aber dazu, dass das gewissermaßen alte Recht, das wir in den Gesetzen der Sicherheitsbehörden haben, dass dieses alte Recht an Grenzen stößt und damit auch die klassischen Überwachungsinstrumente, die die Sicherheitsbehörden haben. Europol evaluiert sicherheitsbehördliche Aktivitäten im Cyberraum in einem sogenannten Internet Organised Crime Threat Assessment. Das machen die seit mehreren Jahren und seit vielen, vielen Jahren warnt Europol davor, dass zunehmend Bereiche, die verschlüsselt sind, einer Strafverfolgung nicht mehr zugänglich sind. Ich zitiere Ihnen einmal aus dem Bereich der Kinderpornografie, Europol-Bericht von 2016, im Bericht aus 2019 da ist es ebenso drin. „The use of end-to-end encrypted platforms for sharing media, coupled with the use of largely anonymous payment systems, is facilitating an escalation in the live streaming of child abuse.“ Das bedeutet, die Ermittler kommen immer weniger an die Verbrecher heran. Und das bezieht sich nicht nur auf die Kinderpornografie, sondern auch auf viele, viele andere Bereiche. Und wenn Verschlüsselung diesen Effekt hat und wenn die Rechtslage so ist, wie ich sie skizziert habe und Herr Kelber hatte das ja auch dargelegt, dass wir also grundrechtlich gesehen an die Verschlüsselungen gar nicht mehr herankommen, dann müssen wir uns etwas anderes überlegen. Und da gibt es verschiedene Instrumente, wie z. B. die Quellentelekommunikationsüberwachung, die eben nicht am Übertragungsweg, der ja verschlüsselt ist, ansetzt, sondern vor der Verschlüsselung. Aber dann müssen wir eben solche Instrumente der Sicherheitsbehörden stärken. Es gibt einige Gesetze der Sicherheitsbehörden, die die Quellen-TKÜ noch nicht aufweisen und da muss sich der Gesetzgeber überlegen, ob man nicht im Falle eines zunehmenden Versiegens von klassischen Überwachungsinstrumenten den Sicherheitsbehörden jetzt diese Instrumente dann zunehmend an die Hand geben möchte. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zu Herrn Prof. Federrath.

SV **Prof. Dr. Hannes Federrath** (Gesellschaft für Informatik; Uni Hamburg): Vielen Dank. Ich wurde gebeten, kurz zur Frage Stellung zu nehmen, welche Schritte und Maßnahmen notwendig seien, um möglichst schnell, effizient und sicher eine Infrastruktur aufzubauen, die eben auch in einer offenen Welt funktionieren würde, vielleicht nicht nur für E-Mails, sondern generell für sichere Kommunikation. Ich möchte vorausschicken, dass es schon sehr paradox ist, dass es Anbieter wie Apple mit

iMessage und Facetime, aber auch Facebook mit WhatsApp inzwischen gelungen ist, eine Infrastruktur aufzubauen, die geeignet ist, wirklich Ende-zu-Ende verschlüsselt zu kommunizieren. Von daher können sich heute Nutzer mit diesen proprietären Tools schützen und zugleich macht einem das natürlich Sorge, weil die Möglichkeit, über Metadaten viel Informationen über den Nutzer zu sammeln, aber auch über Firmenaktivitäten und ähnliches, natürlich nicht der Weg sein kann, um dann eben zu sagen, das Problem ist gelöst. Wir brauchen offene Standards, die in der Lage sind, interoperabel in den Systemen, die heute existieren, zu kommunizieren, und dies wäre der erste Schritt, offene Standards der nächsten Generation zu entwickeln und eben nicht an den Standards von 1969 festzuhalten, die das Internet seinerzeit formuliert hat. Diese Standards sind gut, aber sie sind in einem kooperativen Vertrauensmodell des Internet entstanden, und dies ist längst überholt. Und genau da liegt auch eines der Hauptprobleme bei heutigen Systemen. Wir sagen, die Sicherheit muss irgendwo einen Vertrauensanker haben. Und dieser Vertrauensanker wird heute bei den Verschlüsselungsverfahren im Wesentlichen in der Schlüsselzertifizierung gesehen. Das heißt, die Beglaubigung von Schlüsselmaterial über vertrauenswürdige dritte Stellen ist so lange gut und für Nutzer auch ausreichend sicher, wie ich den Anbietern dieser Vertrauensinfrastrukturen eben vertrauen kann. Sonst hießen sie auch nicht Vertrauensinfrastrukturen. Und diese Anker, sind – muss man wirklich sagen – eine Illusion, denn sie haben sich über kurz oder lang als nicht vertrauenswürdig herausgestellt, sprich Schlüsselmaterial war im Umlauf, das nicht authentisch war und dieses Integritätsproblem führt letztendlich direkt zu einem Vertraulichkeitsproblem. Sehen Sie es mir nach, dass ich das nicht allzu ausführlich erläutern möchte, da ich ja weiß, dass Herr Weis an dieser Stelle explizit auch eine Frage dazu bekommen hat und er sicherlich darauf noch eingehen wird. Das heißt, wir müssen an den Vertrauensinfrastrukturen arbeiten. Das wäre der zweite Schritt, nachdem offene Standards etabliert sind. Der dritte Schritt wäre, in die Technologien verpflichtend Verschlüsselungen einzubauen. Lassen Sie mich kurz sagen, dass man bei der Standardisierung des Mobilfunknetzes GSM genau dies versäumt hat. Das war etwa Mitte der 90er Jahre des letzten Jahrhunderts. Man hat auch bei der Standardisierung von UMTS nicht den Mut gehabt, genau dies zu tun, obwohl es zwischenzeitlich möglich gewesen wäre; das war kurz vor der Jahrtausendwende. Und man hat bei der Standardisierung von LTE wenigstens den Mut gehabt, über Technologien, die als IPSec bezeichnet werden, zumindest die netzinterne Kommunikation verpflichtend zu verschlüsseln. Bei 5G wäre es geboten, eine solche verpflichtende Verschlüsselung, die für netzinterne Kommunikation notwendig ist, auch auszuweiten auf die Ende-zu-Ende-Verschlüsselung aller Kommunikation und ich glaube, das würde auch – auch wenn es nicht meine Frage war – die Vertrauenswürdigkeit in ausländische Anbieter von Telekommunikationssystemen innerhalb des 5G-Netzes verbessern.

Und ein letztes. Ich mache es kurz. Die Bundesregierung hat ja mit der Forschungsstrategie und dem Forschungsprogramm „Selbstbestimmt und sicher in der digitalen Welt“ schon in die richtige Richtung die Forschungsförderung unternommen. Dies muss fortgesetzt werden. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann kommen wir nunmehr zu Herrn Kelber.

SV **Ulrich Kelber** (BfDI, Bonn): Vielen Dank Herr Vorsitzender. Ich muss allerdings bei der ersten Frage des Herrn Abgeordneten Wirth auch die Frage gleich an die Bundesregierung weitergeben, weil ich Ihnen als unabhängige Behörde nichts zum Aufbauplan der Agentur sagen kann. Sie wird allerdings danach datenschutzmäßig meiner Aufsicht unterliegen. Das heißt, wir werden bestimmt einen Informationsbesuch und irgendwann auch einen Kontrollbesuch dort durchführen.

Zur Frage des Herrn Abgeordneten Hartmann, Passwortherausgabe, vorhin schon einmal angerissen. Bei einer Privatperson verstößt es eigentlich sogar gegen dessen Recht, sich selbst nicht zu belasten. Es wäre also in der Form wesensfremd. Bei Unternehmen würde es gegen die Vorgaben des Datenschutzes verstoßen, dass diese eben nicht im Besitz eines Passwortes in Klartext oder in einer einfach herzustellenden Form sein dürfen, was wiederum eine Voraussetzung überhaupt zum Schutz dort ist. Ich habe mich in letzter Zeit wegen meiner Aufgabe im Bundesdatenschutzgesetz, auch allgemein zu beraten zu Fragen des Datenschutzes und nicht nur spezifisch beim dem Thema Sicherheit geäußert mit der etwas umstrittenen These des Sicherheitsgesetzmoratoriums, das ja beinhaltet, sich ein

Stückchen zu lösen von der Frage immer des nächsten Eingriffs, der nächsten Datumsbeschaffung. Insgesamt zu einem etwas größeren Sicherheitsbegriff – Sie selber kennen das besser als ich – warum radikalisieren sich Menschen im Gefängnis, warum ist dieses, warum ist jenes? Und was man gemacht hat zu evaluieren, was es bringt. Nicht alles dürfen wir ja öffentlich benennen, aber in unserem letzten Tätigkeitsbericht haben wir auch verwiesen auf verschiedene Dateien, die unter großen verfassungsrechtlichem Getöse geschaffen wurden und heute für die praktische Arbeit der Sicherheitsbehörden keine Bedeutung haben, aber nach wie vor Ressourcen verschlingen. Von daher diese Evaluierung, was benötigt man an welcher Stelle, wäre die allererste Voraussetzung um in dem Thema weiterzukommen? Um danach natürlich die Behörden in der Tat in die Lage zu versetzen, dort, wo es eine Grundlage für einen solchen Eingriff gibt, ihn auch durchführen zu können. Aber selbst, wenn Sie eine Ende-zu-Ende-Verschlüsselung haben, können Sie natürlich mit einer entsprechenden Software auf dem Gerät wiederum bestimmte Inhalte abgreifen. Das ist möglich.

Wir haben natürlich verschiedene Stufen, wo Verschlüsselung eintritt. Transportverschlüsselung ist besser als gar keine. Ende-zu-Ende-Verschlüsselung ist besser als Transportverschlüsselung. Wir uns natürlich darüber hinaus wünschen, dass da nicht nur der unmittelbare Kommunikationsinhalt verschlüsselt ist, das ist ja die Ende-zu-Ende-Verschlüsselung, sondern angefangen von den Metadaten – das ist schon genannt worden – zu anderen Daten, die damit zu tun haben ebenfalls. Also eigentlich eine Ausweitung, dass z. B. Daten in Clouddiensten verschlüsselt liegen. Dass in den Betriebssystemen wichtige Daten wie Kontakte und anderes verschlüsselt liegen. Dass man sich fragen muss, Sie kennen die ganze Debatte über die, die immer genannt werden, WhatsApp und Facebook. Aber warum werden Speicherabbilder bei der Nutzung von Windows unter bestimmten Systemen übertragen? Warum, wenn Sie eine Rechtschreibprüfung machen, wird der gesamte Inhalt des Dokumentes auf einen Server unverschlüsselt übertragen. Alle diese Punkte müssen dringend angesprochen werden. Ich halte sie auch für eine Sicherheitsfrage, nämlich die Sicherheit einer digitalen freiheitlichen Gesellschaft. Und jede Form von Verschlüsselung muss eine Schwachstelle haben, wenn Sie sich mittenrein setzen wollen, um sie abzuhören. Es geht das eine nicht ohne das andere. Das kann man sich im analogen genauso vorstellen. Wenn Sie die Haustür so schwächen würden, dass es für die Polizei leichter ist reinzukommen, dann ist es für Menschen mit vergleichbaren Kenntnissen eben auch leichter reinzukommen. Da ist es tatsächlich nicht möglich an dieser Stelle zu arbeiten, ohne uns alle insgesamt zu gefährden auch gegenüber Einfluss von außen.

Herr Abgeordneter von Notz, Sie bringen mich natürlich wirklich in eine unangenehme Situation. Ich spiele den Ball zurück. Der Gesetzgeber Deutscher Bundestag hat sich wahrscheinlich aus üblich guten Gründen dafür entschieden, den BfDI unabhängig zu machen, als er klären musste, wie er eine unabhängige Beratung und Kontrolle gewährleisten kann. Ich halte das nach wie vor für ein gelungenes Modell, wenn ich das so vielleicht sagen darf. In der Tat sollte, wenn man bei allem, was man neu macht, Verschlüsselung von Anfang an anlegen und gerade beim Mobilfunk kennen wir die Schwächen des GSM-Protokolls, die ja nun absichtlich so geschaffen wurden. Das sollte sich natürlich bei 5G nicht wiederholen. Die Bundesregierung sollte in ihrer eigenen Arbeit, auch in dem Angebot an Bürgerinnen und Bürger das Thema Verschlüsselung hoch ansetzen. Das ist nicht der Fall. Ich darf Ihnen ein Beispiel aus den letzten Monaten nennen. Nachdem wir mehrfach kritisiert hatten in unserer Aufsicht über die Finanzbehörden des Landes, Sie haben sie ja zu uns gegeben im letzten Jahr, alle Finanzämter, dass dort wesentliche personenbezogene Daten – Sie glauben gar nicht, was im Gesundheitssektor noch dazu käme, aber jetzt waren wir erstmal im Finanzsektor – mit E-Mail übertragen werden. Früher sind sie nicht besonders schön per Fax übertragen worden. Da war nicht die Reaktion des Deutschen Bundestages, dass Finanzministerium und die Finanzbehörden zu verpflichten, jedem Bürger verschlüsselte Kommunikation auch anzubieten. Sondern Sie haben tatsächlich per Gesetz festgelegt, dass auf Wunsch des Bürgers auf die Verschlüsselung seiner sensiblen personenbezogenen Daten verzichtet werden darf. Ich habe das für nicht angemessen gehalten, wenn ich diese Kritik an dieser Stelle loswerden darf nochmal.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann kommen wir nunmehr zu Herrn Prof. Margraf.

SV **Prof. Dr. Marian Margraf** (FU Berlin): Also meine Frage von der CDU/CSU-Bundestagsfraktion war, wie kann man denn das Recht auf Verschlüsselung konkret oder was auch immer umsetzen. Also ich glaube nicht, dass die Bundesregierung dann dafür verantwortlich ist, alle Leute oder alle Nutzerinnen und Nutzer zu verpflichten, nur noch verschlüsselt zu kommunizieren. Vielmehr müssen die Rahmenbedingungen stimmen und dazu gehört einerseits natürlich keine Schwächung der Kryptografie, um das überhaupt zu gewährleisten, Weiterentwicklung der Kryptografie, gerade – was hier auch schon mehrmals angesprochen wurde – im Hinblick auf die Bedrohung von Quantencomputern. Aber da macht das BMBF schon relativ viel. Förderung der Benutzbarkeit. Auch das hatte ich schon in meiner Stellungnahme angesprochen. Gerade wenn es um das Thema Ende-zu-Ende-Sicherheit geht, wo eben wesentliche Teile – ich wiederhole das nochmal – des Schlüsselmanagements verlagert werden auf die Nutzerinnen und Nutzer. Hier müssen intuitive Prozesse einfach entwickelt werden. Dass man einfach weiß, was sind öffentliche Schlüssel, was sind geheime Schlüssel. Es gibt eine berühmte Untersuchung – die ist schon ein bisschen älter – aber ich glaube, da hat sich nicht so viel geändert. Da wurde danach gefragt, also es wurden – glaube ich – acht Studierende befragt, sollten GPG nutzen. Und es ist – glaube ich – einem gelungen alles durchzuführen, alle Schlüssel zu generieren, die richtigen Schlüssel zu versenden, Texte zu verschlüsseln und auch wieder zu entschlüsseln. Das Problem war, dass eben viele z. B. ihre Geheimschlüsselanteile verschickt haben an andere. Also das soll nur ich. Der geheime Schlüssel ist eben dafür da, dass die Nachrichten, die an mich gehen, auch dass ich die entschlüsseln kann und eben kein anderer. Mit dem öffentlichen Schlüssel kann jeder verschlüsseln. Also das sind große Probleme und da gilt es eben, einfach Mechanismen zu entwickeln, die das verbessern. Der dritte Punkt vielleicht ist, dass Behörden es auch ermöglichen, dass ich verschlüsselt mit ihnen kommunizieren kann. Also dass sie auch diese Open Source-Tools, die es da gibt, anwenden können.

Und nochmal ganz kurz ein Beitrag – das ist auch schon mal angesprochen worden – Vertrauensdienste. Eben die Infrastruktur zu verbessern. Ich denke, da ist z. B. der neue Personalausweis oder die Online-Ausweisfunktion des Personalausweises ein wesentliches Instrument, damit man auch nachweisen kann, ich bin derjenige, der ich vorgebe zu sein und das ist mein Schlüssel, also dass man dann eben zertifiziert. Und ich glaube auch, da war damals das Problem bei De-Mail. Also klar war die Forderung bei der De-Mail immer Ende-zu-Ende-Sicherheit umzusetzen, aber das ist eben da genau ein Benutzbarkeitsproblem gewesen. Also die Schlüsselanteile liegen dann eben beim Nutzer. Und wenn dann nur 15 Prozent der Bevölkerung in Deutschland weiß, wie sie damit umgehen kann, dann kann man eben De-Mail auch nicht breit einsetzen. Dankeschön.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann kommen wir nunmehr zu Herrn Prof. Meier.

SV **Prof. Dr. Michael Meier** (Institute of Computer Science 4, Bonn): Vielen Dank. Ich darf auf die Frage eingehen von dem Abgeordneten Wirth und die Frage war, wenn es keine Backdoors gibt, was bleiben denn eigentlich überhaupt noch für Ermittlungsansätze und Möglichkeiten für beispielsweise Strafverfolger. Und ich will auf ein paar Aspekte dazu eingehen. Zum einen fehlt mir in der ganzen Diskussion tatsächlich und vielleicht macht es das auch ein bisschen schwierig jetzt für mich diese Frage zu beantworten, der Einblick in die tatsächlichen Möglichkeiten, die Strafverfolger heute haben. Worauf ich hinaus will ist, mir fehlt ein bisschen mehr Transparenz hinsichtlich der Wirksamkeit von verfügbaren Mitteln. Beispiel: Wir hatten mal sowas wie eine Vorratsdatenspeicherung. Was hat damals funktioniert bei den Ermittlern, was heute nicht mehr funktioniert, wo wir die Vorratsdatenspeicherung nicht mehr haben? Wenn da keine Aussage kommt, dann hat man sie wohl nicht benötigt, wäre meine Schlussfolgerung. Und wenn wir da tatsächlich mehr Transparenz bekommen würden, wäre das – glaube ich – tatsächlich hilfreich.

Ein anderer Aspekt, bei dieser ganzen Going Dark-Diskussion mit zunehmender Digitalisierung und Technik und natürlich auch mehr Umsetzung von Sicherheitsmechanismen, beispielsweise Verschlüsselung. Was ich da vermisse ist tatsächlich auch einfach eine Würdigung der Tatsache, dass auch ganz, ganz viele neue Möglichkeiten für Ermittlungsbehörden dazukommen. Ja, es ist richtig, man kann nicht mehr in die kommunizierten Inhalte reingucken, aber dafür wird eine Flut an Metadaten generiert. Einfaches Beispiel: So ein Mobiltelefon von früher, damit konnten Sie telefonieren

und vielleicht noch SMS schicken. Heute ist da auch ein WLAN drin oder ein Bluetooth. Es wirft mit Daten um sich dieses Gerät. Was da für Möglichkeiten draus entstehen wird überhaupt nicht thematisiert. Jetzt weiß ich nicht genau, ob die Kolleginnen und Kollegen in den Ermittlungsbehörden da noch nicht drauf gekommen sind oder vielleicht einfach aus anderen Motiven diese neuen Möglichkeiten noch nicht dargestellt haben. Und ich bin auch gerne bereit dort zu sagen, ja auch diese Dinge müssen wir intensiver erforschen. Natürlich brauchen wir Möglichkeiten und Fähigkeiten auf Seiten der Ermittlungsbehörden, aber die dürfen nicht dazu führen, dass wir die normalen Bürger überall schwächen, indem wir quasi Sicherheitslücken offenlassen, die letztlich bei allen offen sind.

Und vielleicht noch als weiteres Instrument, der Begriff der Frontdoor ist tatsächlich schon gefallen. Aus meiner Sicht ist der – glaube ich – noch nicht, zumindest ich habe ihn noch nicht abschließend verstanden, wenn ich ehrlich bin. Und wie ich ihn jetzt wahrgenommen habe, wäre z. B. ein Ansatz für so eine Frontdoor, dass man sagt z. B. bei einem Messenger, der verschlüsselte Kommunikation Ende-zu-Ende zulässt und die ermittelnde Behörde möchte sich Zugang zu den Inhalten verschaffen, dass man die Kooperation des Diensteanbieters beziehungsweise Software-Herstellers sucht und dann ein Update ausrollt zu der betroffenen Person. Und diese aktualisierte Messenger-Software auf dem Endgerät dann eben z. B. Schlüsselmaterial ausleitet oder vielleicht einfach eine Kopie, eine Klartextkopie der kommunizierten Nachricht. Wenn ich das jetzt ad hoc, wie gesagt, es ist nicht gut verstanden und ich glaube auch noch nicht intensiv genug diskutiert nach meinem Kenntnisstand. Wenn ich es jetzt vergleiche mit der Backdoor-Variante, dann ist das für mich tatsächlich ein weniger intensives Mittel als eine Backdoor. Von daher finde ich es auch nicht völlig abwegig da weiter drüber nachzudenken. Insbesondere finde ich es gut, dass hier die Kooperation von dem Dienste- beziehungsweise Software-Anbieter erforderlich ist. Ich formuliere es mal plastisch. Nicht irgendwelche Leute, die das System eigentlich nicht gebaut haben, nicht betreiben und nicht wirklich verstehen, versuchen über eine Hintertür sich Zugriff zu verschaffen, sondern in Kooperation mit dem, der tatsächlich das System betreibt, der es entwickelt, der es weiterentwickelt wird versucht Zugangsmöglichkeiten zu schaffen. Das wäre für mich tatsächlich ein Punkt, den man weiter diskutieren kann, auch wenn es – ich bin da hin- und hergerissen – schon ein heftiger Eingriff ist und eine Konsequenz wird sein, dass man wahrscheinlich das Vertrauen in diese Software-Diensteanbieter als normaler Bürger auch ein bisschen verliert. Denn potentiell jubeln die einem mit der Aktualisierung irgendwas unter, weil man auf irgendeine Liste gerutscht ist oder so was. Also da muss man – glaube ich – noch intensiver diskutieren und sich die Vor- und Nachteile nochmal genauer klarmachen. Mal ganz abgesehen davon bin ich auch nicht sicher, ob wir die ins Boot zu holenden Diensteanbieter tatsächlich überzeugen können, ob wir Mittel in der Hand haben sie zu solchen Maßnahmen zu bewegen. Und das waren die Punkte, auf die ich in dem Zusammenhang eingehen möchte.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön und wir kommen nunmehr zu Herrn Prof. Weis.

SV **Prof. Dr. rer. nat. Rüdiger Weis (**Beuth Hochschule für Technik Berlin): Vielen Dank für die Fragen. Ich möchte noch gerade zwei Sätze aus professoraler Sicht über Steganografie und allgemeine Sicherheit machen. Ich höre immer in den Diskussionen: „Ja, es ist ein problematischer Eingriff nach Grundrecht“. Es ist aber ein problematischer Angriff in technischer Sache. Gehen wir mal auf den Standpunkt, dass man mal diese politische, juristische und gesellschaftliche Sache völlig nach hinten drehen, sondern nur die Technik angucken. Und da ist der Begriff Steganografie erwähnt worden. Ich möchte noch zu Protokoll geben, seit 15 Jahren vielleicht ein bisschen öffentlicher, die Steganografie hat wirklich eine Geschichte, ungelogen bis 3.000 vor Christus. Also das versteckte Errechnen gab es auch schon bei den alten Römern. Ich möchte jetzt von den alten Römern gleich zu meiner Vorlesung übergehen. In meiner Mastervorlesung IT-Sicherheit, was eine Pflichtveranstaltung ist, ist es Aufgabenblatt 2 - Programmieren ist ein steganografisches Tool, mit dem Sie Nachrichten sicher verschlüsselt verschicken. Und dieses Tool hat meine beste Studentin in – glaube ich – unter 100 Zeilen programmiert und das ist jetzt ein Tool, damit können Sie, wenn Sie wirklich böse sind und böse Nachrichten versenden wollen in der Welt, wo alle Nachrichten abgehört und aufgezeichnet werden, sicher kommunizieren. Also meine talentierten Studenten könnten das. Ich gehe mal davon aus, dass wirklich böse, böse Angreifer

(terroristischer Sachen) möglicherweise ein paar Leute haben, die auf dem Stand meiner sehr guten Studentinnen und Studenten sind und das dann halt auch komplett umgehen könnten. Also, wir hätten eine komplette Überwachung, die richtig bösen Damen und Herren können immer noch sicher kommunizieren. Zweiter Punkt – auch aus der Praxis: Wie einfach ist es ein GSM-System abzuhören? Da ist auch eine Masterarbeit im Moment am projektiert werden, die rekurriert einfach auf einen Vortrag aus dem Chaos Communication Congress von vor drei Jahren, wo Open-Source-Tools vorgestellt worden sind. Und ich kann vielleicht technisch sagen, sogenannte Rainbow-Table, die wir vorberechnet hatten, sind drei Terrabyte an Daten, wenn man die auf den Rechner kriegt, was im Moment ein bisschen Schrauberei ist bei drei Terrabyte, aber durchaus nicht unmöglich ist, kann man damit in Echtzeit mit freier Software abhören. Das ist auch kein Geheimnis, es sind öffentliche Sachen, die da zugänglich sind. Also, so ist die Sicherheitssituation. Mit anderen Worten, ich glaube manchen Leuten ist nicht klar, wie nahe die Einschläge da sind, wenn wir Sicherheitslücken auflassen.

Vielen Dank auch nochmal an die Frage von dem SPD-Abgeordneten Hartmann, die mich auch auf eine interessante Beobachtung hinbringt. Ja, es ist hilfreich Ende-zu-Ende-Verschlüsselungen zu machen, weil, dann muss man diesen Betreibern der Infrastruktur weniger vertrauen. Also, wenn ich irgendwie dafür sorge, dass – sagen wir mal – diese Huaweis nur als Transport von verschlüsselten Daten verwendet werden, dann sind die Angriffsmöglichkeiten geringer. Die Frage, ob da Backdoors in den Systemen da sind? Da sage ich Ihnen einfach als jemand, der seit Jahrzehnten davor gewarnt hat, bin ich jetzt wenig überrascht, dass das jetzt in der Handelskonfrontation da ist. Machen Sie sich aber mal folgenden Spaß: Tun Sie mal zwei verschiedene Suchmaschinen auf und geben dann ein, Huawei Backdoor und dann Juniper Backdoor und Cisco Backdoor, und dann sehen Sie bei Juniper und Cisco irgendwie drei, vier Seiten von nachgewiesenen Backdoor Vorfällen. Nochmal, als Mathematik ist es amüsant. Man kann eine Backdoor von den Behörden ausbauen und eine eigene anbauen, indem man einfach eine Zahl ändert. Man ändert eine Zahl. Also, wer es genau wissen will, Struktur der elliptischen Kurven, da kann man mit einer Zahl dafür sorgen, dass man da einen eigenen Zugang hat. Also, so ist die Sicherheitslage und zu dieser Huawei-Diskussion auch nochmal eine klare Ansage. Ja, wenn wir über fremde Mächte oder regierungsnahe Firmen usw. unsere ganze Infrastruktur aufbauen lassen, dann sollten wir uns sorgen, dass da Backdoors da sind. Und – wie gesagt – da sollten wir uns Sorgen bei Huawei machen, die bisher noch nicht relevant erwischt worden sind. Da sollten wir uns aber deutlich mehr Sorgen bei Juniper …

BE **Christoph Bernstiel** (CDU/CSU): Bei Huawei nicht?

SV **Prof. Dr. rer. nat. Rüdiger Weis (**Beuth Hochschule für Technik Berlin): Da müsste man nochmal genau nachgucken. Ich räume ein, es sind ein paar kritische Sachen, aber im Vergleich: Gehen Sie in Ihr Büro, machen Sie zwei verschiedene Suchmaschinen auf mit Juniper und Cisco, dann muss ich sagen, bei Huawei gibt es ein paar berechtigte Verdachtsfälle, wo man kritisch nachgucken sollte, völlig in Ordnung, aber bei Juniper und Cisco würde ich bis heute Abend nur die Probleme aufzeigen. Also insofern noch einmal, darum ist es ungeheuer wirksam, wenn eine europäische Behörde – und da eine besonders unabhängige Behörde wie das BSI – dann sich das weltweit anguckt und sagt, Leute, wir machen ein Sicherheitslabor, wir gucken in den Code ein, wir versuchen das ordentlich zu machen. Das ist in einer immer mehr aus dem Ruder laufenden Weltsituation einer der wenigen stabilisierenden Punkte. Also noch einmal, dieser langweilige deutsche Datenschutz, der übrigens auch, um mal jemand anderen aus diesem Haus hier zu ehren, sehr stark von dem ehemaligen Abgeordneten Prof. Brunnstein mit gestaltet worden ist, ist wirklich ein Punkt, der uns irgendwie weltweit heraushebt. Und wer sich jetzt die aktuelle Berichterstattung von Davos anhört, der wird irgendwie erkennen, dass selbst große amerikanische Firmen jetzt die Datenschutzgrundverordnung als vernünftig ansehen. Also, hier noch einmal die klare Antwort: Ja, sichere Ende-zu-Ende-Verschlüsselung hilft schon auch bei vertrauenskritischen Infrastruktursachen. Umgekehrt noch einmal, bei Huawei und diesen anderen Einrichtern halte ich diesen Gang über das BSI, was nicht besonders spektakulär ist, was auch nicht groß durch die Presse geht, für den richtigen, absolut zu unterstützenden Ansatz.

Komme ich dann bei der praktischen Sache nochmal auf die Fragen aus der Linksfraktion. Diese Sache mit den IoT-Geräten ist relativ einfach zu erklären: Die sind billig, da hat man drei Euro für die ganze Internetsache, insofern ist es bei der Sicherheitssituation verheerend. Also, wir haben eine Studie für das Justizministerium gemacht und das hat mir wirklich – nicht philosophisch – schlaflose Nächte gemacht. Weil die Forderung, dass man irgendwie Entwicklungen in dem Bereich stark standardisiert und zertifiziert machen könnte, glauben Sie mir, das macht jemanden, der es stärker auf Open Source, Wissenschaft und freie Entwicklung ohne Bürokratie anlegt, macht das wirklich schlaflose Nächte. Trotzdem haben wir gesagt, im Bereich IoT-Sicherheit ist es so verheerend, dass wir da eine Art guten Handlungsbedarf haben. Also, der dumme Witz, dass irgendwie eine Cruise Missiles in Ihren Kühlschrank einschlagen kann, aus juristischen Gründen, weil dieser Kühlschrank am Internet hängt und sich möglicherweise an einem Angriff gegen eine US-Militäreinheit beteiligt, das ist keine philosophische Sache, das ist durchaus eine realistische Bedrohung. Noch einmal, die Dinger hängen am Netz und das bedeutet, ein Kühlschrank kann einem – wenn der ein bisschen talentiert ist – einen üblen Angriff gegen kritische Infrastruktur führen. Also, der Kühlschrank wird über eine Sicherheitslücke übernommen. Die meisten Kühlschränke sind nicht bösartig – aber übernommene Kühlschränke können da in der Tat einige an Problemen triggern. Also hier nochmal der Hinweis, ich wundere mich …

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Hellfire-Raketen?

SV **Prof. Dr. rer. nat. Rüdiger Weis (**Beuth Hochschule für Technik Berlin): Also wie gesagt, also auch nochmal ganz deutlich, die US-Regierung hat wirklich die Rechtslage geändert, dass Hackerangriffe auch mit Hellfire-Raketen zu beantworten sind. Also, der Witz, dass wir damit rechnen müssen, dass eine Hellfire – juristisch einwandfrei aus US-Sicht – in Ihren Kühlschrank einschlägt, ist eine Beschreibung der juristischen Situation. Wie gesagt, wir sind in einer Weltsituation, wo man nicht übertreibt. Die Sache ist in der Sache relativ skurril.

Dann kommen wir zur letzten Frage, die sich auch sehr gut einreiht, die Frage geschlossene und offene Systeme. Das ist genau die Sache, wo auch die Anfrage Hartmann hingeht, wenn wir Huawei uns hinsetzen, wissen wir, was die da drin machen? Wir haben jetzt die Citrix, dass da so ein Fernwartungstool gerade um die Ohren fliegt, da können wir nichts machen, weil, das ist Closed Source und die Firma lässt sich Zeit und Zeit und Zeit. Gucken Sie einfach mal den Ablauf an, das gefährdet im Moment aktuell die Industrie und die Patches sind seit ein paar Stunden erst da. Wenn wir irgendwie Systeme haben, wo wir uns abhängig machen von privat geführten Firmen in anderen Ländern, die mit Microsoft und anderen, die die Größe von ganzen Ländern haben, dann haben wir auch rein rechtsphilosophisch eine schwierige Situation. Also noch einmal, wir brauchen für diese IoT-Geräte eine Open Source Lösung, eine verlässliche Trust-Basis, um damit die Industriesteuerungen voranzutreiben, ansonsten haben wir wirklich eine Sicherheitslücke, die von Geheimdiensten nutzbar sind, die wir nicht selber fixen können, wenn es uns um die Ohren fliegt, und das gefährdet, wenn wir alles am Internet hängen, nicht nur die digitale Welt, sondern schlicht und einfach auch ganz physikalisch die innere Sicherheit.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann haben wir die erste Fragerunde abgeschlossen und kommen zur zweiten Fragerunde. Gleiche Regeln, wie bei der ersten, wir beginnen mit der CDU/CSU-Fraktion und Herrn Bernstiel.

BE **Christoph Bernstiel** (CDU/CSU): Vielen Dank für die Antworten. Jetzt wurde ja ein sehr spannender Themenbereich angeschnitten, Stichwort 5G-Ausbau und Huawei, da kenne ich mich zufälligerweise ein ganz kleines bisschen mit aus. Dazu möchte ich erstmal sagen, dass wir ja bei der 5G-Technologie schon die hier oft angemahnte Verschlüsselung haben werden, insbesondere der Kommunikation, aber auch der Metadaten. Das heißt, das Problem befindet sich ja sozusagen schon auf der Zielgeraden, was wir noch nicht als solches Problem sehen. Wichtig ist allerdings nochmal nachzufragen, und das geht an Herrn Kelber und auch Sie Dr. Weis. Wenn wir über das Checken von Codes reden, wir haben ja jetzt eben auch über das BSI geredet, dann ist es ja meiner Kenntnis nach so, dass so ein Mobilfunk-Code oder so eine Software, die dann benutzt wird, um sozusagen die Kryptografie herzustellen, zwischen drei und zehn Millionen Codezeilen hat und Sie haben es ja gerade –

Herr Dr. Weis – selber gesagt, mit der Veränderung einer einzigen Zahl kann ich bereits diesen ganzen Code in eine Richtung lenken, schädlich/unschädlich, wie auch immer. Die Frage an Sie beide lautet daher, erstens. Ist es denn technisch überhaupt möglich, so einen Code zu prüfen? Zweitens. Wenn ja, wie lange dauert das? Und drittens, welche Rolle spielt denn die Vertrauenswürdigkeit der Hersteller in diesem Zusammenhang? Denn Sie haben ja gerade von amerikanischen Unternehmen gesprochen, ich würde Ihnen an dieser Stelle auch widersprechen, dass man jetzt bei den von Ihnen genannten chinesischen Unternehmen nichts gefunden hat, ich weise da mal auf das Hauptquartier der Afrikanischen Union hin, was quasi komplett verwanzt und mit Software unterwandert wurde von dem eben von Ihnen genannten Hersteller, sodass für mich natürlich die Frage auch im Vordergrund steht: Müssen wir sowas eigentlich als Staat selber gewährleisten, um sicherzugehen, dass es da keine andere Einflussnahme gibt oder können wir das blindlinks sozusagen einem privatwirtschaftlichen oder einem staatlich kontrollierten Unternehmen anvertrauen? Ist das technisch überhaupt klug? Danke.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Keine Fragen mehr bei der AfD-Fraktion, dann kommen wir zur SPD-Fraktion und Herrn Hartmann.

BE **Sebastian Hartmann** (SPD): Vielleicht nochmal in Richtung des geschätzten Kollegen Koalitionspartners. Wenn man das dann richtig zu Ende denkt, müsste man ja ein staatliches Kombinat herstellen, das das alles macht und keinem privaten Unternehmen – egal wo auf der Welt – überlassen. Aber vielleicht ist das ja der Ansatzpunkt über digitale Souveränität in unserem Bereich der Jurisdiktion zu sprechen, dass es Direktinvestitionen gibt und europäische Hersteller, die in der Lage sind, ähnlich auf einem Niveau wie es Herr Prof. Dr. Weis ausgeführt hat, Quellcodes offenzulegen und zwar für alle, die sich um den Titel vertrauenswürdige Hersteller bewerben und vielleicht in Kombination mit Zertifizierung entsprechender technischer Gerätschaften einen Lösungsweg zu finden …

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Es gibt einen super Grünen-Antrag dazu!

BE **Sebastian Hartmann** (SPD): Ja, Du wirst es nicht glauben, aber mit Dir kann man ja auch gern koalieren, nicht, also lassen wir das. Ich würde jetzt gerne an den Prof. Dr. Meier die Frage richten, Sie haben in Ihrer Stellungnahme – zurück zum Thema – ein paar Hinweise gegeben, was wir für den Standort Deutschland tun könnten in Punkto Verschlüsselung, es ist das Wort Quantenüberlegenheit umgangssprachlich formuliert worden. Wir sind stolz darauf, dass im Forschungszentrum Jülich ja formuliert worden ist, welche Hersteller sind wie weit in der Quantentechnologie. Die Frage ist: Was können wir eigentlich in Deutschland tun, um die nötigen Investitionen an Wissenschaft und Wirtschaft anzustoßen, um nicht nur den Verschlüsselungsstandort Nummer Eins zu schaffen, sondern auch führend zu werden, was die Technologie danach wird? Was würden Sie aus Sicht der Wissenschaft uns empfehlen, vielleicht an gesetzgeberischen Maßnahmen, an notwendigen Investitionen, bis hin zur Einrichtung von Forschungsinstituten oder vielleicht auch Lehrstühlen, die wir da schaffen.

Ich würde als zweite Frage nochmal in Richtung des Bundesdatenschutzbeauftragten gehen, nachdem Sie Ausführungen getroffen haben zum Thema Pflicht zur Passwortherausgabe, Verschlüsselung. Es gibt ja die Säule des Verbraucherschutzes beim BSI. Können Sie sich denn dort vorstellen, dass es – möglicherweise in Kombination mit Ihrer Behörde – eine Stärkung auch des Standortes Deutschland für Verbraucherinnen und Verbraucher gibt, also dass wir das Stichwort Verbraucherschutz stärken? Es ist von den Schwierigkeiten der Anwendung von Verschlüsselungstechnologien gesprochen worden. Jetzt gibt es Ansätze, IT-Gütesiegel einzuführen oder auch über Zertifizierungen zu sprechen. Sehen Sie da Möglichkeiten der Kooperation, dass wir Bürgerinnen und Bürger besser in die Lage versetzen, was vertrauenswürdige Hersteller angeht, was die Nutzung von Technologien angeht, was Patches und Updates angeht, vielleicht auch in Kombination, in Zusammenarbeit mit anderen Behörden wie BSI – schon genannt – oder auch Ihrer Behörde gibt, dass mir dieser Aspekt aus Sicht der Bürgerinnen und Bürger nochmal wichtig ist?

Stv. Vors. **Jochen Haug** (AfD): Dankeschön, dann kommen wir nunmehr zur FDP-Fraktion und Herrn Höferlin.

BE **Manuel Höferlin** (FDP): Danke Herr Vorsitzender. Ja, vielleicht nochmal Schwenk zu der Frage, wie Ende-zu-Ende-Verschlüsselung in Kommunikation definiert wird. Herr Prof. Meier sprach ja da von der Möglichkeit oder den Ideen, wie man in verschlüsselte Kommunikation vielleicht anders eindringen kann als die Verschlüsselung zu brechen. Ich glaube, das ist bei den proprietären Systemen nicht so schwer. Da nimmt man einfach einen weiteren öffentlichen Schlüssel in die Kommunikation rein und dann wird ein dritter Adressat in die Lage versetzt, die Kommunikation mitzulesen und dann muss nur der Anbieter dafür sorgen, dass der Schlüssel eben nicht sichtbar ist in der Kommunikation. Und das ist ja genau das, was gefährlich ist an der proprietären Lösung, wenn man darauf Vertrauen hat, weil, das Vertrauen wird – glaube ich – schwinden. Aber dazu vielleicht insgesamt, weil auch Prof. Federrath – da geht meine erste Frage hin – vorhin ja gesagt hat, das Schwierige ist vor allen Dingen, in den offenen Systemen eine Lösung zu finden, die eben überall anwendbar ist. Also eine offene Lösung, die man in allen möglichen Kommunikationsmedien – E-Mail, Messengerdiensten, wie auch immer – verwenden kann und die vor allen Dingen auch über die Anbietergrenzen hinweggehen. Sie haben ja selbst beschrieben in Ihrem Statement, dass das ja sehr gut funktioniert bei proprietären Lösungen, aber dort eben solche Probleme auftreten. Sie haben selbst gesagt, es fallen Unmengen Metadaten an, aber auch – wie ich es beschrieben hab – man kann einfach anbieterseitig in die Kommunikation eingreifen, indem man eben – nicht sichtbar für den Anwender – einen weiteren Kommunikationspartner hinzufügt. Dann bleibt die Verschlüsselung allerdings verschlüsselt, nur eben dann auch z.B. einer Überwachungsabteilung irgendeiner Behörde. Also, meine Frage an Sie: Wie stufen Sie denn die Verwässerung dieses Begriffs – und das ist mit Frontdoor, glaube ich, gemeint – diese Verwässerung des Begriffs Ende-zu-Ende-Verschlüsselung, wie stufen Sie das ein? Was hat das für eine Auswirkung auch auf informationstechnische Systeme, auch auf vielleicht die Programmierer insgesamt, das Vertrauen in Programmierung insgesamt, wenn man so etwas einbaut?

Die zweite Frage geht an Prof. Margraf. Sie haben ja darüber gesprochen – wie viele übrigens – wie die Schlüsselorganisation läuft und haben kurz in einem ganz kleinen Schlenker den Personalausweis angesprochen. Halten Sie es denn für möglich, dass wir zumindest für Deutschland, aber auch für andere Länder, die ja ähnliche Identifikationskarten haben mit Chips an Bord, die vielleicht in der Lage wären, Schlüssel zu halten und dann eben in einer größeren Organisation – durch welche Institution auch immer – ein Schlüsselsystem aufzubauen und dadurch hätte man ja einen nicht veränderbaren Faktor auf einer Karte. Jetzt ist das Problem der Anwendbarkeit auch nicht mehr so schwierig wie vor Kurzem, wo man noch Kartenlesegeräte gebraucht hat, jetzt kann man das vielleicht dann einfacher und möglicherweise mit weiteren Sicherheitslücken bei der Übertragung über Funk, aber trotzdem doch ein erhebliches Anheben – sage ich mal – des Sicherheitsniveaus insgesamt ermöglichen. Wo sehen Sie da Möglichkeiten, dass vielleicht der Personalausweis da eine Rolle spielen könnte, Schlüsselhierarchien ordentlich zu gestalten und aufzubauen, mindestens national, wenn nicht europäisch?

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen zur Fraktion DIE LINKE. und Frau Domscheit-Berg.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich möchte an Herrn Weis meine Fragen stellen und bei der ersten Frage anschließen an ein Thema, das meine Kollegin Petra Pau schon angesprochen hat, nämlich: Welche Lösungsvorschläge es denn gibt für das Thema IoT-Sicherheit und allgemein welche IT-Mindestsicherheitsstandards sollte oder könnte man denn regulierend vorgeben? In der Debatte sind so Sachen wie Herstellerhaftung, wie Mindest-Update-Pflichten, aber mir schweben da auch so Sachen vor wie: Darf überhaupt ein IT-Produkt ein Passwort 12345 akzeptieren oder kann man die Top – weiß ich nicht wieviel – Passwörter einfach zwingend verbieten, dass die einfach nicht mehr akzeptiert werden? Zum Thema Mindest-Update-Pflichten haben Sie sich ja in Ihrem Statement auch geäußert. Dazu wüsste ich gerne, Sie fordern da ja eine für die Lebensdauer eines Produkts existierende Sicherheits-Update-Pflicht, wer definiert denn, wie lange so ein Produkt lebt? Ja, manche benutzen ja Produkte durchaus sehr lange, wenn die sich nicht von selbst kaputt machen. Also, wer bestimmt das? Und Sie fordern auch, wenn diese Sicherheits-Updates nicht geliefert werden, dass dann der Quellcode offengelegt werden muss. Das – finde ich – ist eine äußerst charmante Forderung, die – glaube ich – in Frankreich ja auch mindestens

debattiert, wenn nicht sogar schon eingeführt worden ist, aber wer haftet denn dann z. B. bei Softwarefehlern, die später passieren? Also, das war sozusagen mein erster Fragekomplex. Und der zweite bezieht sich nochmal auf das Thema proprietäre geschlossene Chiparchitekturen. Da verweisen Sie auf Intel und schreiben in Ihrem Statement, diese Intel eigene Sicherheitsarchitektur hätte höchst problematische Eigenschaften. Welche sind das? Können Sie uns dazu ein bisschen was erzählen? Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Und wir kommen zur Fraktion BÜNDNIS 90/DIE GRÜNEN und Herrn Dr. von Notz.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank Herr Vorsitzender. Anknüpfend an die Gedanken meiner Kollegin Domscheit-Berg vielleicht, wir haben ja im Innenausschuss und eigentlich alle Oppositionsfraktionen haben im Bereich der IT-Sicherheit in dieser Legislaturperiode schon etwas abgeliefert. Es ist wirklich ein drängendes Problem, also, es geht über Verschlüsselung ja hinaus und eigentlich müssten wir wirklich da vorankommen und diese Frage der Haftung und andere angedachte Sachen sind ganz entscheidend, hier reden wir heute über Verschlüsselungsfragen. Deswegen vielleicht nochmal an Sie, Herr Kelber, die Frage bei ZITiS, das ist ja eine interessante Behörde, ich durfte sie neulich mal besuchen. Was machen die eigentlich? Und es gibt ja – glaube ich – keine Gesetzesgrundlage für die Arbeit, die ZITiS macht, und da das ja irgendwie eine Einrichtung ist, in der auch datenschutzrelevante Dinge passieren könnten, kontrollieren Sie die Behörde eigentlich und wenn ja, wie oft oder müssten Sie das nicht eigentlich tun? Oder braucht man nicht, wenn man in einem solchen Bereich unterwegs ist, irgendeine Form von rechtlicher Grundlage, schon aus verfassungsrechtlichen Gründen? Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön, dann kommen wir jetzt zur Antwortrunde, dieses Mal in umgekehrter Reihenfolge. Das heißt, wir beginnen mit Herrn Prof. Weis.

SV **Prof. Dr. rer. nat. Rüdiger Weis (**Beuth Hochschule für Technik Berlin): Vielen Dank für die Frage, auch an den Herrn Bernstiel nochmal die Sache: Nein, ich vertraue Huawei nicht besonders. Also ich vertraue auch dem Justizsystem in der Volksrepublik China noch weniger als dem amerikanischen, was die Geheimdienste angeht. Also noch einmal, diese eine Sache, dass irgendwie die Backdoors bei diesen US-Anbietern eine reiche Historie haben, die jetzt nicht so ausgeprägt ist in Huawei, hängt auch damit zusammen, dass die Firmen länger am Markt sind. Also, ein gesunden Misstrauen gegenüber Anbietern, die auch eine Regierungsnähe haben, die objektiv da ist, die ist nicht so groß wie teilweise irgendwie postuliert wurde, aber ich sehe es durchaus kritisch. Also, ich sehe, dass man da ein privatwirtschaftliches Unternehmen und eine Jurisdiktion, der man nicht unbedingt vertraut, ist kritisch zu sehen. Das ist in China exzessiv der Fall, ich muss zu Protokoll geben, dass mein Vertrauen in das amerikanische Rechtssystem und die Entwicklung seit Trump auch irgendwie sich stark relativiert in ein paar Richtungen. Aber noch einmal, ein gesundes Misstrauen ist da. Auch der Punkt ist klar, das sind Millionen Codezeilen, das ist verdammt schwer, die zu evaluieren. Trotzdem fällt mir keine andere Idee ein. Und schlicht und einfach braucht da das BSI, wenn wir das als vernünftige Forderung sehen – und ich muss sagen, das tut weltweit für die Deeskalation beitragen – dann braucht das BSI schlicht und einfach genug Mittel und genug Unabhängigkeit, um so eine Position zu bauen. Aber ja, es ist verdammt schwer, aber ich habe keine andere Lösung.

Keine andere Lösung – überraschenderweise – habe ich auch in dem IoT-Bereich. Das ist eine Sache, die liegt mir wirklich schwer im Magen, weil, eine Entscheidung zu sagen, wir müssen alles spezifizieren und was am Internet hängt, ist eine Forderung, die sicher Open Source Entwicklungen sehr viel schwieriger macht. Allerdings ist die Bedrohungslage da inzwischen so drastisch geworden, dass ich mir da wenig zu helfen weiß. Wir haben in der Tat dann zusammen sehr lange überlegt und diese eine Idee finde ich in der Tat durchführbar und auch mit relativ geringen Kosten, sowohl für Staat als auch für die Industrie verbunden, dass einfach Firmen definieren, wie lange sie das System wirtschaftlich nutzen wollen. Und für diese Zeit haben sie eine Verpflichtung Updates zu machen, wenn sie sagen…

Zwischenrufe

SV **Prof. Dr. rer. nat. Rüdiger Weis (**Beuth Hochschule für Technik Berlin): ja, ich habe auch.

Meine Vorlesung, mache ich mit einem vierzehn Jahre alten Rechner, damals hat IBM noch Computer produziert, also ist sehr lang her. Und wie gesagt, ab einem gewissen Zeitpunkt gibt es da keinen Kundendienst und dann bin ich der Meinung, dann muss man den staatlichen und privaten Behörden ermöglichen, dann Fehler selber zu patchen. Und das wäre halt in einer Sache, dass der Source-Code freigegeben wird, wenn die Firma sagt, wir möchten das jetzt nicht mehr wirtschaftlich verwerten und machen keine Updates mehr – dass man die Möglichkeit anderen Leuten gibt, dann für Updates zu sorgen. Notabene, da könnte eine eigene Serviceindustrie entstehen. Wir wissen das, durch Bundesbehörden sind auch relativ hohe Beträge an Servicedienstleister zu machen, die z. B. den Sicherheitsunterstützungszyklus für Windows 7 weitertragen. Das ist durchaus nicht unüblich und insofern ist die Forderung – glaube ich – eine interessante da.

Zu der Intel-Sicherheitsarchitektur habe ich ein bisschen komische Gefühle, weil, die haben in der Tat ein „gescheitertes Uniprojekt“, das ich in Amsterdam 2003 mit entwickelt habe, nämlich Minix3 verwendet in ihrer Software eingebaut und dann auch das schlecht gemacht und mit Sicherheitslücken gemacht. Es sind erhebliche Lücken im Closed Source Betrieb, muss nochmal sagen. Intel ME können Sie sich so vorstellen, da ist ein eigener Computer mit eigenem Netzwerkanschluss in Ihrem Prozessor drin. Und wer da Zugang hat, das weiß man nicht genau. Also, man weiß sicher, dass es möglicherweise Dienste haben oder talentierte Hacker. Diese Sicherheitsprobleme mit Intel ME wurden in der Tat mit den üblichen russischen Hackern aufgedeckt, die sich die Sache mal ein bisschen kritisch angeguckt haben. Und das wäre insofern sicherheitstechnisch natürlich ein Alptraum, weil damit würde praktisch ein Netz unterhalb des Radars von Virenscannern und anderer Sicherheitssoftware getrieben werden. Also, insofern bin ich der Meinung, wenn wir jetzt Industrie 4.0 weitertreiben und überall Steuerelektronik reintun, können wir kein Closed Source nutzen, wo es eine Backdoor gibt. Wir brauchen wirklich einen gewissen Grundsatz für eingebettete Systemindustriesteuerung, da brauchen wir möglicherweise eine staatliche Behörde, die irgendwas gibt. Und ich bin in Deutschland ein großer Fan davon, da Konstruktionen zu machen, das nicht staatlich, sondern öffentlich-rechtlich zu machen. Also, wir müssten möglicherweise sowas wie eine sichere Software – Open Source Stiftung – machen und die ganz altmodisch, typisch deutsch halt nach dem Vereinsrecht, nach dem Stiftungsrecht, nach dem Gemeinnützigkeitsrecht begleiten. Ich glaube, das gewinnt keinen Schönheitspreis, das ist nicht die brillanteste innovativste Lösung, aber ich glaube, dass diese langweilige Lösung, mit der wir in Deutschland doch Jahrzehnte lang gute Erfahrungen haben, auch da hilfreich ist. Also mit anderen Worten, wir sollten überlegen, ob wir eine gemeinwirtschaftliche, öffentlich-rechtliche Stiftung für Softwaresicherheit an den Tag holen, die einen Job haben kann, wirklich die elementarste grundlegende Steuerelektronik zu erstellen. Also technisch geht es da um sicheres Booten, U-Boot usw. Es gibt eigentlich auch Projekte im BSI, die wirklich eine sichere Grundarchitektur anstreben und die man für die Industriesteuerung verwenden kann. Vielleicht ist da wirklich die Idee, zwar nicht als staatliche Behörde, weil wir leben hier in einer Stadt, wo schon staatliche Behörden sehr viel gemacht haben im Osten und im Westen, möglicherweise ist da diese Idee einer gemeinnützigen öffentlich-rechtlichen Stiftung die richtige Idee und da – letzte Bemerkung – mit der RISC-V-Five-Förderung innerhalb der EU gibt es inzwischen eine offene Infrastruktur, die ein guter starting Point werden könnte und – wie schon erwähnt – Quantencomputer bringen in den nächsten zehn Jahren grundlegende neue Forderungen. Wir brauchen komplett neue Kryptografie. Lasst uns vielleicht versuchen, damit mal was wirklich ordentlich neu aufzubauen, wenn wir es sowieso neu machen müssen und da sind in der Tat diese in Deutschland schon oft belächelten – öffentlichen-rechtlich und Stiftung – Konstruktionen vielleicht ein sehr lohnender eigener Beitrag, den wir leisten können.

BE **Christoph Bernstiel** (CDU/CSU): Entschuldigung, die Frage, wie lange es dauern würde, so einen Source-Code mit mehreren Millionen Codezeilen zu überprüfen, da würde ich mich noch sehr für interessieren.

SV **Prof. Dr. rer. nat. Rüdiger Weis (**Beuth Hochschule für Technik Berlin): Je nachdem, wie viele teuer einzukaufende Experten Sie da drauf werfen. Also, es ist aufwendig. Hören Sie, das BSI hat über Jahrzehnte lang da ganz ordentlich Knowledge aufgebaut, die können das sicher sehr gut einschätzen. Ich kann nur sagen, es ist teuer, also, die Leute, die

sich damit auskennen, sind auf dem Markt sehr, sehr, sehr gefragt. Insofern ist das in der Tat schwierig, wie aufwendig es ist, das hängt damit zusammen, wie viele Leute man darauf ansetzt. Was ich Ihnen sagen kann, wenn Sie die bestehende Infrastruktur, Fraunhofer usw. draufwerfen, dann können die wirklich so Analysen machen, dass keine ganz offensichtlich schmerzhaften Backdoors drin sind. Und das wäre auch schon mal der erste Schritt. So Backdoors, die ein bisschen cleverer geschützt sind, die aussehen wie ein Programmierfehler, das ist High-End-Geschichte.

Abg. **Christoph Bernstiel** (CDU/CSU): Zeitraum? Können Sie das sagen?

SV **Prof. Dr. rer. nat. Rüdiger Weis (**Beuth Hochschule für Technik Berlin): Kann ich nicht sagen, je nachdem wieviel Leute sie draufwerfen. Das kann man einigermaßen parallelisieren. Aber ich glaube, also diese Genehmigungssachen gehen durchaus Jahre, also insofern ist doch zum Teil – ich weiß nicht ob Sie da viel schneller sein möchten – wenn Sie schneller sein müssen, müssen Sie deutlich Geld draufwerfen. Ich sage Ihnen ganz einfach, die Leute, die Sie dafür brauchen, sind irgendwie auf dem Markt, rein marktwirtschaftlich derart gefragt, dass das ein sehr großer Aufwand ist. Aber es ist durchaus machbar. Und Sie fragten, Grundvertrauen? Mal ganz banal, wenn die Angreifer sehen, da guckt jemand rein und könnte was finden, dann sind die sehr vorsichtig, da was einzubauen, dann sind sie deutlich vorsichtiger, als wenn niemand da reingucken kann. Also nochmal, das ist kein Golden Bullet, aber – wie gesagt – diese relativ wenig revolutionären Vorträge, die wir jetzt gemacht haben, ja, staatliche Stellen, öffentlich-rechtliche Stellen usw. – ich glaube – das ist wirklich eine Möglichkeit in die richtige Richtung zu laufen. Es ist – da gebe ich Ihnen Recht – unheimlich aufwendig und sehr schwierig.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zu Herrn Prof. Meier.

SV **Prof. Dr. Michael Meier (**Institute of Computer Science 4, Bonn): Vielen Dank, vielen Dank insbesondere an Herrn Hartmann für die interessante Frage: Was kann Deutschland unter andrem im Bereich Wissenschaft eigentlich tun, um führend zu werden, beispielsweise im Bereich Verschlüsselung, IT-Sicherheit? Da geht's besonders ja im Prinzip um „Wünsch dir was", nicht, das spiele ich am liebsten. Aus meiner Sicht, wenn ich mir die Situation so angucke aktuell, was passiert eigentlich gerade, treiben wir die Digitalisierung oder werden wir von der Digitalisierung getrieben? Und ich für mich persönlich würde mit letzterem antworten. Und – ich glaube – das sollte man irgendwie mal ändern. Wir müssen – Entschuldigung für die Phrase – vor die Lage kommen, ja, um einfach frühzeitiger gestalten, auch Sie, ja Politik frühzeitiger regulierend engreifen zu können und überhaupt Regulierungsbedarf erkennen zu können. Was ist dafür aus meiner Sicht erforderlich? Naja, wir sind sicherlich nicht Bummelletzter, was Forschung und Entwicklung angeht in Deutschland, ganz im Gegenteil, an vielen Stellen – das ist auch heute schon mehrfach betont worden – tun wir etwas ordentliches, aber wo aus meiner Sicht wirklich noch Dinge fehlen, ist so der Übergang zwischen Mensch und Technik, also die Schnittstelle Mensch und Technik. Passworte sind auch schon gefallen heute, das ist genau die Schnittstelle Mensch/Maschine, wenn man so will. Und da bricht die IT-Sicherheit tatsächlich an ganz vielen Stellen. Und deswegen ist aus meiner Sicht – glaube ich – erforderlich, mehr Bemühungen zu stecken in dieses Thema Interaktion von Mensch mit Computern. Wie kann man das eigentlich sicher, zuverlässig gestalten und was ergeben sich vielleicht auch für Konsequenzen daraus? Und was ich mir tatsächlich wünsche, ist so etwas wie – ich nenne es mal ad hoc – Ten-Years-Ahead-Sandbox. So ein Sandkasten, wo wir einfach mal so tun, als wären wir schon zehn Jahre weiter. Wie sieht die Welt da eigentlich aus? Was für Technik gibt es da? Und da bauen wir diese Technik auch mal auf, und dann sammeln wir so ein bisschen experimentelle Erfahrung mit dem Umgang mit dieser Technik. Was ergeben sich da für Konsequenzen und wie reagieren die Menschen, wie entwickeln die sich weiter, was hat das für soziale, auch gesellschaftliche Implikationen, dieses Agieren in dieser Technologie in zehn Jahren. Und von mir aus darf da auch das BSI, BfDI, und von mir aus auch das BKA mitspielen, um frühzeitig tatsächlich Erfahrungen zu sammeln damit, wie eben die Welt potentiell aussieht. Und wahrscheinlich liegt man da auch über 50 Prozent daneben, die Dinge kommen anders, aber man liegt vielleicht auch in fast 50 Prozent der Dinge richtig und hat eben dort quasi einen gewissen Vorsprung, ist quasi vor der Lage, kann frühzeitig erkennen, was ergeben sich in so einer Welt eigentlich für

Wertschöpfungsketten für Geschäftsmodelle. Und – ich glaube – das ist das, was wir im Prinzip brauchen, um tatsächlich souveräner und führender zu werden im Bereich Technologie und insbesondere IT-Sicherheitstechnologie in der Zukunft. Das heißt wirklich, ein Spielplatz, einen experimentellen Sandkasten, wo man Dinge mal in größerem Stile ausprobiert, das kann wirklich mal ein Stadtteil oder ein Stadtviertel sein, wo man einfach mal die Dinge lebt, von denen wir heute nur sprechen und dann gucken wir mal, was kommt da eigentlich raus und lassen diese Erkenntnisse einfließen in die Gestaltung weiterer Technologieregularien usw. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Und wir kommen nunmehr zu Herrn Prof. Margraf.

SV **Prof. Dr. Marian Margraf (**FU Berlin): Ja, die Frage war von Herrn Höferlin: Was kann sozusagen – knapp zusammengefasst – die Online-Ausweisfunktion für Ende-zu-Ende-Verschlüsselung tun? Wir reden eigentlich immer von Ende-zu-Ende-Sicherheit, ich will jetzt mal ein bisschen ausholen, das heißt, wir wollen nicht nur von Person zu Person verschlüsseln, sondern auch die Dokumente, die wir hin und herschicken signieren, dass man eben auch weiß, von wem die eigentlich kommen. Und dafür brauchen wir dann zwei Schlüsselpaare, also einmal einen öffentlichen und einen geheimen Schlüssel für die Verschlüsselung und einmal einen öffentlichen und einen geheimen Schlüssel für die Signatur. Ich nutze dann den öffentlichen Schlüssel meines Kommunikationspartners, um für ihn Daten zu verschlüsseln, und ich nutze meinen eignen geheimen Schlüssel, um diese Dokumente zu signieren. Und mein Kommunikationspartner kann mit seinem geheimen Schlüssel entschlüsseln und mit meinem öffentlichen Signaturschlüssel überprüfen, kommt diese Nachricht auch von mir. Das war jetzt ganz kurz zusammengefasst, wie das eigentlich funktioniert. Und jetzt muss ich natürlich wissen, wenn ich für irgendjemanden verschlüssele, ist das tatsächlich sein öffentlicher Schlüssel oder wem gehört der eigentlich? Sonst verschlüssele ich vielleicht für einen Angreifer. Und mein Gegenüber muss meinen öffentlichen Schlüssel kennen, damit er weiß, diese Nachricht kommt tatsächlich von mir. So, und das kann ich jetzt so machen, dass ich mit jedem potentiellen Kommunikationspartner diese öffentlichen Schlüssel austausche. Das kann sicherlich relativ kompliziert werden, gerade eben auf die Zukunft betrachtete, ich weiß ja noch gar nicht, mit wem ich in drei Monaten vielleicht kommunizieren will. Üblicherweise wird das so gemacht, dass diese öffentlichen Schlüssel – also das ist eine Möglichkeit – ein Zertifikat bekommen, wo eben der öffentliche Schlüssel drin steht, da steht drin der Inhaber des öffentlichen Schlüssels, wofür wird dieser öffentliche Schlüssel genutzt und vielleicht ein Gültigkeitszeitraum. Und die Frage ist ja genau, wie stellt man jetzt diese Zertifikate aus? Ich muss ja jetzt, wenn ich irgendwo meinen öffentlichen Schlüssel hinschicke an so eine zentrale Stelle, dann muss die wissen, dieser öffentliche Schlüssel kommt jetzt tatsächlich von mir. Und eine Möglichkeit wäre, das meinte ich vorhin damit, die Online-Ausweisfunktion zu nutzen, die bietet ja ein Authentifizierungsverfahren an, dass ich mich da bei dieser zentralen Stelle anmelde oder einlogge mit der Online-Ausweisfunktion, die wissen, ich bin Marian Margraf, da kann ich meinen öffentlichen Schlüssel hinterher schicken, wenn ich die https-Verbindung sozusagen damit abgesichert habe, und dann können die ein Zertifikat ausstellen. Das wäre sozusagen eine Möglichkeit. Meines Erachtens gibt es da schon ein vom BSI durchgeführtes Projekt, was genau das macht. Beantwortet das die Frage?

BE **Manuel Höferlin** (FDP): Ja, aber weiterhin, was Sie beschrieben haben, was die Ausweisfunktion kann, beruht ja auch auf einer Struktur und auf einer Baumstruktur, die Zertifikate verwaltet, also könnte man die Struktur nicht verwenden, auch für Schlüsselaustausch?

SV **Prof. Dr. Marian Margraf (**FU Berlin): Na, das habe ich ja gerade gesagt, aber das ist eben eine Authentisierungsfunktion und keine Verschlüsselung und keine Signaturfunktion.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zu Herrn Kelber.

SV **Ulrich Kelber (**BfDI, Bonn): Vielen Dank, Herr Vorsitzender. Zur Frage des Herrn Abgeordneten Bernstiel hatte Herr Prof. Weis ja schon einiges zur Möglichkeit der Prüfung großer Codemengen geäußert. Dazu kommt natürlich tatsächlich heute noch die Situation, dass ein Code nicht lange als Monolith irgendwo verbleibt, sondern sich in einem hohen Tempo ändert. Das stellt übrigens auch

uns vor Kontrollprobleme, selbst schon bei öffentlichen Behörden, die wir kontrollieren müssen. Es gibt natürlich neben der händischen oder weitgehend händischen Kontrolle von Codes auch längst Projekte, die auf bestimmte Auffälligkeiten prüfen. Übrigens nicht nur reine Software, sondern auch bereits in Hardware verankerte Regelungen, wo dann Auffälligkeiten bestimmten Verhaltens, das abweicht, auch grafisch dargestellt werden kann. Zum Beispiel nach einer solchen Auswertung überhaupt einen Hinweis zu bekommen, ist aber natürlich kein hundertprozentiger Check. Die Rolle der Vertrauenswürdigkeit von Herstellern, wir haben ja vor kurzem mal als Datenschutzbeauftragte auch gesagt, das überhaupt Vertrauen die Währung des digitalen Zeitalters ist. Übrigens auch bei der Frage, was wird überhaupt eingesetzt, also, wer setzt sich am Markt durch, ist natürlich relevant. Eine große Fragestellung ist die Einbettung der Hersteller in das nationale Recht und auch die Zusammenarbeit dort mit nationalen Sicherheitsbehörden, insbesondere in Ländern, in denen es auch wieder einen Rückfluss von nationalen Sicherheitsbehörden zu privaten Firmen geben kann. Das ist keineswegs nur China, wenn man an andere Beispiele erinnert, wie Ausschreibungen von Hochgeschwindigkeitszügen oder ähnliches in der Vergangenheit. Da war allerdings das Transportmedium Fax, was sowieso nie gut geeignet war für diese Fragestellung. Und deswegen ist das nämlich ein Grund, warum sowohl der IT-Planungsrat als auch die Datenschutzkonferenz sich mit dem Thema digitale Souveränität natürlich beschäftigt. Weil wir glauben, tatsächlich auch über Technologien zu verfügen, über Wahlmöglichkeiten zu verfügen, nicht unbedingt alles selbst zu machen oder zumindest nicht gefangen zu sein in einem System. Möglichst viele prüfbare Wahlmöglichkeiten zu haben, ist von hohem Nutzen und diesem Thema sollten wir in Deutschland auch verstärkte Aufmerksamkeit widmen.

Zur Frage des Herrn Abgeordneten Hartmann: Also, es gibt natürlich kaum eine andere Behörde, außer unseren unmittelbaren Datenschutzkollegen, mit denen wir so eng und so häufig zusammenarbeiten wie mit dem BSI und auch einigen der anderen Regulierungsbehörden im digitalen Umfeld. Sie dürfen BaFin, Bundesnetzagentur und Bundeskartellamt gar nicht unterschätzen, wie viel die dort tun. Macht übrigens dann auch Sinn, dort ein Cluster an einer Stelle zu haben, wenn ich das als Leiter einer Bonner Behörde mal bemerken darf. Das erleichtert es auch an der Stelle. Ich glaube, die Arbeit BSI für Bürger ist sehr gut, ist eine gute Investition, die Sie als Bundestag dort machen, eine andere hoffentlich gute Investitionen haben Sie, als Sie unserer Bitte nachgekommen sind, unsere Öffentlichkeitsarbeit zu stärken. Was ich nämlich als nächsten Schritt machen möchte, ist, auf meine 17 Kolleginnen und Kollegen in den Ländern zuzugehen und diesen anzubieten, gemeinsam mit uns, die dann etwas mehr Ressourcen haben, die ganzen vorhandenen Informationen für Bürgerinnen und Bürger mal zusammenzufassen. Und gemeinsam zu entwickeln, dass alles an einer Stelle auffindbar ist von den Handreichungen für einzelne Bürgerinnen und Bürger bis hin zu Ehrenamtlichen, Klein- und Mittelunternehmen. Das ist eines unserer Projekte für dieses Jahr. Dass wir aber die erleichterte Nutzung - für Einzel-/Privatpersonen bis hin auch gerade zu Klein- und Mittelunternehmen – stärken könnten über Fragen wie klare Kennzeichnungen. Also, dass ich vielleicht sogar auch schon mit einem Symbol erkennen kann, ist dies ein Produkt, das mir zusichert, Daten z. B. nicht mit Dritten zu teilen, das state of the art Technologien einsetzt für Verschlüsselungen oder ähnliches, dass das gekennzeichnet werden muss, inklusive natürlich verbundener Haftungsfragen.

Über die Siegel, das war ja nun oft genug schon Thema im Bundestag, auch die Planung des BSI, hin zu den Zertifikaten. Wir sind im Augenblick da dran, so schnell wie möglich die letzten Bestandteile dahin auf europäischer Ebene abzuschließen, dass wir in diesem Jahr noch damit beginnen können, Zertifizierer in Deutschland zu akkreditieren, die dann wiederum ein entsprechendes Datenschutzzertifikat – ähnliches müsste es natürlich in anderen Bereichen auch geben, wird ja auch entwickelt – zu geben. Damit jeder weiß, wenn er ein bestimmtes Produkt als Teil seiner Architektur einsetzt, dass dieses Produkt diese Zertifizierung zumindest besitzt. Da gibt es ja auch geförderte – durch Bundestag und Bundesregierung. Ich nehme mal als Beispiel das Auditor-Projekt für Cloud-Anwendungen, die möchten gern ein solcher Zertifizierer werden. Ich glaube übrigens, dass das auch für Produkte und Dienstleistungen aus Deutschland heraus ein Wettbewerbsvorteil werden kann. Weil ja oft gesagt wird, oh, Ihr macht das so kompliziert mit Euren Sicherheits- und Datenschutzvorgaben, ich glaube, es gibt einen Weltmarkt dafür. Überall

dort, wo Recht wie in Europa geschaffen wird, sowieso, weil es dort gemacht werden muss, und überall anders gibt es Menschen, die gerne dieses Recht hätten, nicht bekommen von ihrem Staat, aber wenigstens Produkte hätten, die das möglichst weit einhalten.

ZITiS, in der Tat, Sie erinnern sich wahrscheinlich,– 2017, auch die Kritik meiner Vorgängerin, nicht beratend beteiligt worden zu sein. Beratend beteiligen muss uns die Regierung nicht, wir haben eine Beratungspflicht, wenn wir gefragt werden, es gibt leider keine Pflicht sich beraten zu lassen. Wir sind damals eingeladen worden vom Innenminister, unsere Kontrollmöglichkeiten wahrzunehmen, die besitzen wir. ZITiS ist damals durch einen Erlass eingerichtet worden, hat natürlich ansonsten alle anderen rechtlichen Grundlagen zu berücksichtigen. Wir haben unseren ersten Informationsbesuch in 2018 gemacht und werden ZITiS natürlich auch im Rahmen von Kontrollbesuchen entsprechend bedienen, inklusive sämtlicher Abhilfemaßnahmen, die wir durch die Datenschutzgrundverordnung und JI-Richtlinie bekommen haben. Als ich gerade nochmal auf die Webseite gegangen bin, ist mir auch eine Kleinigkeit schon eingefallen, die Datenschutzerklärung sollte vielleicht noch beinhalten, dass wir auch die Datenschutzaufsichtsbehörde sind. Dass das fehlt, ist ein bisschen peinlich, aber das kann morgen abgestellt werden.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Und wir kommen abschließend zu Herrn Prof. Federrath.

SV **Prof. Dr. Hannes Federrath (**Gesellschaft für Informatik; Uni Hamburg): Vielen Dank. Zur Frage einer offenen Lösung und der etwaigen stufenweisen Verwässerung des Begriffs Ende-zu-Ende, wenn man etwa auf dem Endgerät eines Senders oder eines Empfängers, also der beiden Endpartner versucht mitzuhören: Diese Frage hängt sehr eng zusammen mit der Frage nach der Vertrauenswürdigkeit des jeweiligen Programmcodes, der auf der Datenquelle oder eben auf der Datensenke verwendet wird und insoweit muss man das eben auch eng mit genau dieser Frage der Codeüberprüfung sehen. Wenn ich mir Software installiere aus einem App-Store oder aus dem Internet runterlade oder auch beauftrage, etwa als Firma, dann habe ich häufig nicht die Möglichkeit – weder theoretisch noch praktisch – diesen Code zu überprüfen. Das mag einerseits an der Menge des Codes liegen, häufig aber auch an rechtlichen Fragestellungen, eben z. B. dass es keine Pflicht zur Offenlegung von Quellcodes gibt. Wenn es Quellcode gibt, der überprüfbar ist, weil er von vornherein offengelegt wird oder vielleicht weil es rechtlich zugesichert wurde durch den Auftraggeber, dann besteht sehr wohl die Möglichkeit, den Quellcode zu überprüfen. Quellcodeüberprüfungen dauern unter Umständen mehrere Wochen bis Monate und sind vor allem dann, wenn die Softwarehersteller, deren Quellcodes überprüft werden, kooperationsbereit sind, recht leicht möglich. Aber das Hauptproblem ist: Das ist nur ein statischer Zustand des Quellcodes, der überprüft wurde, und etwaige Software-Updates können Backdoors einbauen, können natürlich Sicherheitsschwächen enthalten und somit scheitert heute die Codeüberprüfung vor allem daran, dass man nur diesen statischen Zustand überprüft und eben nicht fortlaufend in der Lage ist, effizient Codes zu überprüfen.

Ende-zu-Ende-Verschlüsselung bedeutet konsequenter Weise, dass auf der gesamten Übertragungsstrecke niemand mitlesen kann, allerdings sind immer die Verkehrsdaten oder auch Metadaten offen. Somit ist Ende-zu-Ende-Verschlüsselung auch nicht alleine die Methode, die man anwenden müsste, wenn man wirklich versuchen wollte, sowohl das Recht auf informationelle Selbstbestimmung durchzusetzen, als auch – eben auf der anderen Seite – Betriebs- und Geschäftsgeheimnisse zu schützen. Ende-zu-Ende-Verschlüsselung muss immer kombiniert sein mit einer Verbindungsverschlüsselung oder Leitungsverschlüsselung oder welche Begriffe auch in dem Zusammenhang immer genannt werden. Also, es ist kein entweder/oder, sondern ein sowohl/als auch und somit werden zumindest Außenstehende daran gehindert, mitzulesen. Und ansonsten bleibt die Restproblematik, die mit der Codeüberprüfung angesprochen wurde. Gerade im Zusammenhang mit gutem Code möchte ich noch erwähnen, dass Regulierung in anderen Bereichen auf die Verfahren und Produkte zukommen wird und somit auch die Frage der Sicherheit von Kryptografie in dem Zusammenhang mit geprüft und reguliert werden könnte. Nehmen wir etwa Medizingeräte der Zukunft oder eben auch Fahrzeuge – seien sie nun vernetzt oder autonom – ohne Zulassung geht in diesen Bereichen gar nichts und in dem Zusammenhang könnte man sich vorstellen, dass etwa so wie KI-Bausteine in Zukunft vielleicht zulassungspflichtig werden,

eben auch Krypto-Bausteine zulassungspflichtig werden könnten oder anders gesagt, Produkte ohne solche Bausteine überhaupt keine Zulassung mehr erhalten könnten.

Vielleicht an der Stelle noch eine letzte Bemerkung. Erstens fällt mir auf, dass wir stark von dem eigentlichen Thema Kryptografie abgewichen sind hin zu einer Grundsatzdiskussion im Bereich Sicherheit. Das halte ich für richtig und gut. Und lassen Sie mich vielleicht noch an der Stelle sagen, wir haben ja so etwas wie den Schutz des Fernmeldegeheimnisses und das drückt im Wesentlichen aus, dass man, wenn man nicht Berechtigter ist, nicht hineinschauen darf in Kommunikation und nicht mitlesen darf. Wie wäre es denn, wenn genau dieses Fernmeldegeheimnis etwa alleine schon dadurch umgesetzt ist, dass man eben nicht mehr reinschauen kann, sprich, eben der Standard ist, dass Kommunikation im Interesse des Schutzes des Fernmeldegeheimnisses verschlüsselt ist. Somit hätten wir deutlich mehr erreicht für den Grundrechtsschutz, als wenn wir Verschlüsselung als optionale Add-on-Lösung mit allen Unsicherheiten und Risiken verankern. Ich bin sehr dafür, auch mal in diese Richtung nachzudenken. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann sind wir am Ende der zweiten Fragerunde und damit auch am Ende der öffentlichen Anhörung. Ich möchte mich bei allen Sachverständigen nochmal ausdrücklich bedanken und schließe die Sitzung um 15:54 Uhr. Dankeschön.

Schluss der Sitzung: 15:54 Uhr

Jochen Haug, MdB
Stellv. Vorsitzender

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 A

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 22.01.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Innenausschusses zum Thema

Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken

am 27. Januar 2020

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Verschlüsselung ist Grundrechtsschutz!

Seit Jahrzehnten wird kontrovers über die Auswirkungen der Nutzung kryptographischer Verfahren diskutiert. Die Eckpunkte der deutschen Kryptopolitik stammen bereits aus dem Jahr 1999, gelten inhaltlich gleichwohl fort. Die Kernfrage ist geblieben: Wie kann es gelingen, Kryptographie und Sicherheitsinteressen auszubalancieren? Sicherheit *durch* Verschlüsselung bei gleichzeitiger Sicherheit *trotz* Verschlüsselung?

Dies vorausgeschickt, unternimmt die vorliegende Stellungnahme nicht den Versuch einer Kommentierung der gesamten Kryptodebatte, sondern versteht sich als pointierte Positionierung in dieser fortwährenden Diskussion.

Die Haltung des Datenschutzes

Verschlüsselung ist die Basis für den Schutz der Privatsphäre eines jeden Einzelnen und fast jeder wirtschaftlichen Betätigung in der digitalen Welt. Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist es erforderlich, Daten wirkungsvoll vor Zugriffen Unberechtigter schützen zu können. Der Einsatz von Kryptographie ist hierbei ein ganz elementares Instrument.

Unsere Aufgabe muss es daher sein, die Nutzung der Verschlüsselung bestmöglich zu fördern. Wir brauchen einfache und sichere Lösungen für den Einsatz moderner kryptographischer Verfahren. Einfach zu bedienende Verschlüsselungsverfahren müssen ohne Einschränkungen für jedermann nutzbar sein. Die Bundesregierung selbst fordert im Koalitionsvertrag, eine „Ende-zu-Ende-Verschlüsselung für jedermann verfügbar“ zu machen, s. Zeilen 1979 ff. des Koalitionsvertrags der 19. Legislaturperiode des Bundestages.

Datenschutz und IT-Sicherheit sind wichtige Einflussfaktoren für eine kluge Industriepolitik. Eine verantwortungsbewusste und sinnvolle technologische Weiterentwicklung ist ohne Datenschutz und IT-Sicherheit undenkbar. Wir sind deshalb gut beraten, in Deutschland und Europa den Einsatz von Verschlüsselungstechnologien zu forcieren und ihre (Weiter-)Entwicklung zu unterstützen. Eine generelle Herabsenkung des Kryptoniveaus unterwandert das Vertrauen in die digitale Welt. Sie ist deshalb zwingend zu verhindern.

Die Forderung nach einer rechtlichen Verankerung eines Rechts auf Verschlüsselung ist vor diesem Hintergrund zu begrüßen.

1. Recht auf Verschlüsselung – Verschlüsselung ist als technisch-organisatorische Maßnahme bereits rechtlich verankert

Gemäß Artikel 5 Abs. 1 lit. f) Datenschutzgrundverordnung (DSGVO) sind personenbezogene Daten in einer Weise zu verarbeiten, die eine angemessene Sicherheit dieser Daten ge-

währleistet. Dies schließt auch den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen mit ein („Integrität und Vertraulichkeit“).

Wie in Art. 34 Abs. 3 lit. a) DSGVO erläuternd dargestellt wird, zielt Verschlüsselung darauf ab, Daten für Unbefugte unzugänglich zu machen. Damit erfüllt sie eine unmittelbar grundrechtsdienende Funktion, die bereits vom Bundesverfassungsgericht in seiner Entscheidung zum „Volkszählungsurteil“ statuiert wurde: Sie schafft einen Freiraum für die freie persönliche Entscheidungen eines jeden Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Mit Art. 32 Abs. 1 DSGVO wird den Verantwortlichen und Auftragsverarbeitern die Pflicht auferlegt, geeignete technische und organisatorische Maßnahmen zur Sicherung personenbezogener Daten zu treffen. Die DSGVO nennt explizit die Verschlüsselung als Maßnahme, um Datenschutzrisiken zu reduzieren und ein angemessenes Schutzniveau zu gewährleisten, vgl. Art. 32 Abs.1 lit. a).

Risikobezogen ist die Verschlüsselung stets unter Berücksichtigung der Umstände der konkret bezweckten Verarbeitung mit in Betracht zu ziehen. Verschlüsselung ist damit mehr als eine unverbindliche Empfehlung. Denn immer dann, wenn hohe Risiken für die Rechte und Freiheiten natürlicher Personen bestehen und es zu Schutzverletzungen kommt, werden Verantwortliche die kritische Frage beantworten müssen, warum auf eine erforderliche Verschlüsselung verzichtet wurde.

Geeignete technische und organisatorische Maßnahmen sind nach Art. 25 DSGVO auch erforderlich, um den Grundsätzen und Anforderungen des „Datenschutzes durch Technikgestaltung“ zu genügen. Zwar lässt der Gesetzgeber weitgehend offen, welche konkreten Schutzmaßnahmen dies umfasst, zumindest aber die Verschlüsselung ist hierzu zu zählen.

Dabei müssen die eingesetzten Sicherheitsverfahren selbstverständlich stets dem Stand der Technik entsprechen und auch tatsächlich zu einem geeigneten Schutzniveau führen. Um diese Schutzwirkung nicht zu konterkarieren, dürfen keine Hintertüren in die Verschlüsselungssysteme eingebaut werden, die ansonsten einen unbefugten Informationszugang ermöglichen könnten. Dies gilt für eine potentielle Nutzung eingebauter Schwachstellen durch berechtigte Stellen ebenso wie für eine Nutzung durch (kriminelle) Dritte.

2. Recht auf Verschlüsselung

Die Vertraulichkeit der Kommunikation ist ein verfassungsrechtlich verbrieftes Grundrecht. Es wird in das Grundrecht des Art. 10 Grundgesetz (GG) eingriffen, wenn gesetzliche Rege-

lungen hinsichtlich der geschützten Kommunikationsformen die Möglichkeit zur Verschlüsselung von Kommunikationsinhalten einschränken (BeckOK Grundgesetz/Ogorek GG Art. 10 Rn. 53). Es muss den Kommunikationsteilnehmern anheimgestellt bleiben, wie sie die Vertraulichkeit des Informationsaustausches gewährleisten wollen und wer von dem Inhalt Kenntnis erlangen soll (BeckOK Grundgesetz/Ogorek GG Art. 10 Rn. 53 m.w.N.).

Aber auch nach Abschluss der laufenden Kommunikation – also, wenn der Schutzbereich des Art. 10 GG endet – sind Betroffene nicht schutzlos. So stellte das Bundesverfassungsgericht unmissverständlich klar, dass das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst (BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07). Eine heimliche Infiltration eines informationstechnischen Systems, mit der die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist daher verfassungsrechtlich nur in engen Grenzen zulässig (sog. Online-Durchsuchung). Hierfür müssen im Einzelfall tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.

Diesem erheblichen grundrechtlichen Schutzbedürfnis würde es nicht entsprechen, wenn Selbstschutzmöglichkeiten – wie die Verschlüsselung – durch staatliche Aktivitäten konterkariert würden. Der Staat muss vielmehr eine möglichst ungehinderte Persönlichkeitsentfaltung ermöglichen, indem er diese Schutzmöglichkeiten bestmöglich ausbaut, etwa durch eine positivrechtliche Statuierung eines Rechts auf Verschlüsselung.

Kontraproduktiv ist es, wenn Gesetzesinitiativen den gegenteiligen Weg beschreiten, indem sie versuchen, das Sicherheitsniveau des Art. 32 DSGVO abzusenken. Beispielsweise sollen mit einer aktuellen Anpassung der Abgabenordnung auch sensible Daten der Bürgerinnen und Bürger auf Basis einer Einwilligung mit einer unverschlüsselten E-Mail von den Finanzbehörden übermittelt werden können. Die sichere Verarbeitung personenbezogener Daten ist aber gerade nicht disponibel. Sie kann deshalb auch nicht durch eine Einwilligung eingeschränkt werden.

Ebenso kritisch ist die – leider regelmäßig auch in Deutschland diskutierte – Bestrebung, für Nutzer Herausgabepflichten für verwendete Schlüssel oder Passwörter einer Verschlüsselung vorzusehen. Ein entsprechendes Vorgehen verstößt gegen den Grundsatz der Selbstbelastungsfreiheit (nemo-tenetur-Grundsatz). Dieser Grundsatz wird in der Rechtsprechung als selbstverständlicher Ausdruck einer rechtsstaatlichen Grundhaltung bezeichnet, der auf dem Leitgedanken der Achtung vor der Menschenwürde beruht (BVerfG NJW 1981, 1431).

Auch ist es abzulehnen, Diensteanbieter zur Herausgabe von Schlüsseln, Passwörtern etc. zu verpflichten. Dies würde in der Eingriffsintensität einer Online-Durchsuchung gleichkommen, ohne jedoch gleichzeitig die dort notwendigen technischen und organisatori-

schen Maßgaben einhalten zu können, mit der diese Maßnahme kontrollierbar gestaltet werden kann. Zu den technischen und organisatorischen Maßnahmen, die Anbieter nach Art. 32 DSGVO zur Datensicherheit zu treffen haben, gehört auch die sicher verschlüsselte Speicherung und Übermittlung von Passwörtern. Technisch gesehen werden gesetzeskonform arbeitende Anbieter die Passwörter folglich ohnehin als Hash speichern. Sie könnten die gewünschten Informationen daher gar nicht herausgeben. Eine Pflicht zur Speicherung der Zugangsdaten in einer durch Dritte leicht aufhebbaren Verschlüsselung oder gar im Klartext würde die Datensicherheit und den Datenschutz massiv konterkarieren.

3. Ende-zu-Ende-Verschlüsselung von Kommunikationsdiensten

Die fehlende Vertraulichkeit einer unverschlüsselten E-Mail-Kommunikation ist allseits bekannt. Unverschlüsselte E-Mails entsprechen im Hinblick auf den Schutz der Vertraulichkeit dem Versand per Postkarte. Wenn Informationen also im Falle eines Postversands nicht per Postkarte, sondern nur in einem verschlossenen Umschlag verschickt werden würden, dann sollten sie auch beim elektronischen Versand in einer verschlüsselten E-Mail übermittelt werden.

Zwar muss nicht zwangsläufig jedwede Übermittlung personenbezogener Daten auf elektronischem Wege per Ende-zu-Ende Verschlüsselung erfolgen. Die Ende-zu-Ende-Verschlüsselung stellt aber eine mögliche, bei Datenübermittlungen wichtige Maßnahme dar, ein angemessenes Schutzniveau zu gewährleisten. Grundsätzlich sollte daher beispielsweise bei der Übermittlung von E-Mails immer eine Ende-zu-Ende-Verschlüsselung angestrebt werden und somit den Standardanwendungsfall darstellen. Dies gilt insbesondere für E-Mails mit besonders sensiblen Inhalten (s.o.). Nutzer und Anbieter sollten deshalb die notwendigen technischen Voraussetzungen schaffen, um eine verschlüsselte Ende-zu-Ende-Kommunikation durchführen zu können. Mit einer zunehmenden Zahl von Nutzern, wird sich der verschlüsselte Versand dann auch zwischen Privatpersonen zügig verbreiten.

Da es in der Praxis aber in absehbarer Zeit noch immer nicht durchgängig möglich sein wird, eine Ende-zu-Ende-Verschlüsselung durchzusetzen, sollte wenigstens eine Transportverschlüsselung implementiert werden. Diese kann mittel- und langfristig eine Ende-zu-Ende-Verschlüsselung nicht ersetzen, aber kurzfristig einige Risiken bei der Nutzung von E-Mails reduzieren.

Eine proaktive, sichere und damit vertrauenswürdige Technikgestaltung setzt auch voraus, sich bereits bei Standardisierungsprozessen aktiv um ein Höchstmaß an Sicherheit zu bemühen (privacy by design). Hierzu zählt unter anderem der nachdrückliche Einsatz für eine standardmäßige Ende-zu-Ende-Verschlüsselung in neuen Telekommunikationstechnologien, wie dies z.B. bei der Spezifikation von 5G-Netzen versäumt wurde.

4. Plädoyer für eine standardisierte Informationsweitergabe von IT-Sicherheitslücken

Die Digitalisierung durchdringt alle Lebensbereiche. Der Cyber- und Informationssicherheit kommt hierbei eine herausragende Bedeutung zu. Die Sammlung von Informationen über IT-Sicherheitslücken, aber auch Schadprogrammen und IT-Sicherheitsvorfällen ist für ein Gesamtlagebild von enormer Bedeutung. Es ist gut, wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) weiter zu einer Informationsdrehscheibe für IT-Sicherheit in Deutschland ausgebaut wird. Insbesondere staatliche Behörden sollten daher verpflichtet sein, IT-Sicherheitslücken unverzüglich an das BSI zu melden.

Zu berücksichtigen ist aber auch, dass IT-Sicherheit und Datenschutz unmittelbar miteinander verzahnt sind. IT-Sicherheit soll den Missbrauch, unberechtigten Zugang und die unberechtigte Nutzung personenbezogener Daten ausschließen. IT-Sicherheitsrisiken sind damit regelmäßig auch Datenschutzrisiken. Insoweit ist die Domäne der datenschutzrechtlichen Aufsichtsbehörden betroffen. Es ist daher wichtig, dass das BSI derartige Informationen unmittelbar an alle relevanten Behörden weiterleitet.

5. IT-Sicherheit und Datenschutz als Standortfaktor ausbauen

Datenschutz und IT-Sicherheit sind wichtige Differenzierungsmerkmale in einer digitalisierten Welt. Der Einsatz von Verschlüsselungstechnologien spielt hierbei eine herausragende Rolle. Sie ist auch und gerade wichtig, um einen effektiven Schutz vor Spionage, (Cyber-)Sabotage und Datendiebstahl zu gewährleisten. Es ist deshalb richtig, wenn im Koalitionsvertrag gefordert wird, dass „sicherheitsrelevante Schlüsseltechnologien […] besser vor einem Ausverkauf oder einer Übernahme geschützt werden [sollen], vgl. s. Zeilen 1979 ff. des Koalitionsvertrags der 19. Legislaturperiode des Bundestages.

Jegliche gesetzliche Beschränkungen oder Verbote kryptographischer Sicherheitssysteme sind kontraproduktiv und fahrlässig.

Eine besondere Bedeutung hat die Nutzung von frei verfügbaren, offenen und einfach handhabbaren Protokollen und Verschlüsselungsstandards. Mit ihrer Transparenz tragen sie dazu bei, ihre Überprüfbarkeit zu sichern und ihre Kontrolle zu erleichtern. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden.

6. Keine grundsätzliche Schwächung des Kryptoniveaus

Sicherheits- oder Strafverfolgungsbehörden tragen seit Jahren vor, aufgrund eines zunehmenden „Going Dark-Effektes“ ihre Aufgaben nicht mehr effektiv wahrnehmen zu kön-

nen. Paradoxerweise steigen zwar die Datenmengen der berechtigen Stellen, gleichzeitig können die Informationen aber wegen der Verschlüsselung nicht im Klartext ausgewertet werden. Es wird schwieriger, Inhalte und Strukturen in den Daten zu erkennen und relevantes von nicht relevantem zu unterscheiden.

Dennoch lassen sich auch aus verschlüsselten Kommunikationsinhalten werthaltige Ermittlungsansätze generieren, etwa mit Blick auf Verbindungsdaten, die Beziehungsgeflechte offenbaren. Auch solche Auswertungen stellen bereits erhebliche Eingriffe in die Privatsphäre der betroffenen Menschen dar.

Soweit Sicherheits- und Strafverfolgungsbehörden heimlich in Datenbestände eingreifen, ist die Rechtsprechung des Bundesverfassungsgerichts zur sog. Online-Durchsuchung zu beachten. Eingriffe sind nur unter den dort dargestellten Voraussetzungen zur Abwehr konkreter Gefahren für überragend wichtige Rechtsgüter zulässig. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Bereits in der Vergangenheit hat es diverse Ansätze gegeben, auf dem Weg der Regulierung bzw. des Verbotes den kryptographischen Schutz von Kommunikation zu schwächen. Ein Beispiel dafür sind die US-Exportbeschränkungen für (damals) „starke“ Kryptographie, die in den Anfangstagen des World Wide Web dazu geführt haben, dass fast alle Internetnutzerinnen und -nutzer mit einem ungenügenden Schutz ihrer Kommunikation leben mussten. Letztlich führen alle diese Ansätze dazu, dass die Sicherheit *aller* Nutzerinnen und Nutzer geopfert wird, um auf die Kommunikation *einiger weniger* Akteure zugreifen zu können.

Bei der Frage, ob Ansätze wie ein Verbot sicherer Verschlüsselung oder das Einbauen von Hintertüren bzw. Schwachstellen in Kommunikationsinfrastruktur dem Gebot der Verhältnismäßigkeit genügen, wird somit die Antwort nicht nur aus grundsätzlichen, sondern auch aus praktischen Gesichtspunkten in der Regel ein klares „Nein“ sein.

7. Digitale Verwaltung – der Staat als Vorbild

Der Staat muss seiner Vorbildfunktion nachkommen. Richtigerweise wird daher auch in dem aktuellen Koalitionsvertrags gefordert, dass Bürgerinnen und Bürgern es ermöglicht werden soll, mit der Verwaltung über gängige Standards verschlüsselt zu kommunizieren (PGP/SMIME), s. Zeilen 1980 ff. des Koalitionsvertrags der 19. Legislaturperiode des Bundestages. Dies wäre ein erster wichtiger Schritt.

Die Sensibilisierung für den Einsatz von Verschlüsselungstechnologien ist eine weitere wichtige Aufgabe, bei der staatliche Stellen Mehrwerte schaffen können. Zusätzlich ist hier

aber ein gesamtgesellschaftliches Engagement von Politik, Wirtschaft und Gesellschaft insgesamt erforderlich. Ziel muss es sein, eine Kultur der *grundsätzlichen* Verschlüsselung zu verankern. Auch vor diesem Hintergrund wäre eine positivrechtliche Festschreibung eines Rechts auf Verschlüsselung sinnvoll.

Der Bundesregierung kommt nach alledem die herausragende Rolle zu, die richtigen Rahmenbedingungen für eine positive Entwicklung eines sicheren und vertrauenswürdigen digitalen Raums zu schaffen. Und Verschlüsselung ist hierfür nach meiner festen Überzeugung ein wesentlicher Erfolgsfaktor.

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 B

Stellungnahme zum Antrag "Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken"

Prof. Dr. rer. nat. Rüdiger Weis, Diplom-Mathematiker, Berlin

Stellungnahme zum Antrag "Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken" des Ausschusses für Inneres und Heimat des Deutschen Bundestages im Rahmen der Öffentlichen Anhörung des Ausschusses für Inneres und Heimat am Montag, dem 27. Januar 2020 zum Antrag der Fraktion der FDP "Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken" - BT-Drucksache 19/5764

- Prof. Dr. rer. nat. Rüdiger Weis, Diplom-Mathematiker, Berlin
- Zusammenfassung Stellungnahme: "Recht auf Verschlüsselung"

Bei der Analyse der Sicherheit von Computernetzwerken geht man in der theoretischen Modellbildung von sehr mächtigen Angreifern aus, die alle Nachrichten mitlesen und verändern kann. Da das Internet auf der Grundphilosophie von offenem Zugang gründet, ist der Schutz von Daten Aufgabe der Kryptographie. Die in der Praxis eingesetzen kryptographischen Algorithmen haben die interessante Eigenschaft, daß Sie entweder für Niemanden oder nahezu für jeden Motivierten brechbar ist. Diese Eigenschaft verbietet eine Schwächung der Kryptographie. Kryptographie ist in vielerlei Hinsicht das einzig wirksame Werkzeug die Digitalisierung im Geiste einer freiheitlich demokratischen Grundordnung mitzugestalten. Die Grundlagenforschung insbesondere in den Bereichen Kryptographie und sicheres Systemdesign ist auszubauen. Anknüpfend an weltweit anerkannte Initiativen (beispielsweise GNU-Privacy Guard) soll die Förderung von Open Source Lösungen weitergerführt, erweitert und intelligent verstetigt werden.

Sicherheitslücken können mit Hilfe von Angriffswerkzeugen ausgenutzt werden, bei denen es sich um kopierbare Programme handelt. Diese gefährlichen digitalen Waffen können selbst aus halbwegs engagierten Einzelpersonen mächtige Angreifer ganzer Wirtschaftssysteme machen. Im Falle von WannaCry ist die Weltwirtschaft nur wegen der diletantischen Programmierung, von einem katastrophalen Schaden bewahrt worden. Aus diesen Gründen scheint seit wenigen Tagen der US-amerikanische Nachrichtendienst NSA seine Veröffentlichungspraxis zu ändern.

Die in Deutschland durch die Gründung des BSI bisher angestrebte Trennung von Schutz der Bevölkerung und der Entwicklung von digitalen Angriffswaffen hat zu einer im Vergleich zu anderen Staaten höheren Vertrauensbildung geführt. Ausdrücklich lobend erwähnt sei die vertrauensbildende Arbeit des BSI im Falle Huawei. Diese hat im Bereiche der aufziehenden Handelskrieges zu einer Deeskalation beigetragen. Dieses Vertrauen sollte in einer immer instabileren Weltlage nicht aufs Spiel gesetzt werden, sondern gepflegt, ausgebaut und auch institunell verstetigt werden.

- Das Nichtschließen von Sicherheitslücken bedroht angesichts der weiter fortschreitenden Vernetzung in den Bereichen Industrie und der kritischen Infrastruktur nicht mehr nur im digitalen Sinne Heimat und innere Sicherheit.

Übersicht

In dieser Stellungnahme soll der Einsatz von Kryptographie von der mathematischen und der informatischen Sicht diskutiert werden. Im weiteren Text werden, nach einer Analyse der Bedrohungslage mit einen Schwerpunkt auf die konkreten Gefahren für die innere Sicherheit durch die fortschreitende Vernetzung von Industrie und kritischer Infrastruktur, Handlungsempfehlungen insbesondere im Bereich der Open Source Software gegeben.

Kryptographie als Gestaltungsmittel

Da das Internet auf der Grundphilosophie von offenem Zugang gründet, ist der Schutz von Daten Aufgabe der Kryptographie. Die in der Praxis eingestzen kryptographischen Algorithmen haben die interessante Eigenschaft, daß Sie entweder für Niemanden oder für jeden Engagierten brechbar ist. Diese Eigenschaft verbietet eine Schwächung der Kryptographie. Kryptographie ist in vielerlei Hinsicht das einzig wirksame Werkzeug die Digitalisierung im Geiste einer freiheitlich demokratischen Grundordnung mitzugestalten. Die Grundlagenforschung insbesondere in den Bereichen Kryptographie und sicheres Systemdesign ist auszubauen. Anknüpfend an weltweit anerkannte Initiativen (beispielsweise GNU-Privacy Guard) soll die Förderung von Open Source Lösungen weitergerführt, erweitert und intelligent verstetigt werden.

Grundlagenforschung Kryptographie und Systemdesign

Die Grundlagenforschung insbesondere in den Bereichen Kryptographie und sicheres Systemdesign ist auszubauen. Anknüpfend an weltweit anerkannte Initiativen (beispielsweise GNU-Privacy Guard) soll die Förderung von Open Source Lösungen weitererführt, erweitert und intelligent verstetigt werden.

Post-Quantum Kryptographie zwingend notwendig

- Mathematischen Grundlagenforschung im Bereich der Post-Quantum-Kryptographie ist die einzige praktische Herangehensweise für mittel bis langfristige sichere Verschlüsselung und Signierung.

Systemrelevante Open-Source Softwareprojekte

Die genannten Open-Source Projekte stellen systemrelevante Sicherheitssoftware für den Erhalt der digitalen Souveränität dar. Eine nachhaltige Sicherung dieser Projekte ist wichtig für die digitale Souveränität und damit auch Aufgabe staatlicher Stellen. Aufgrund der vielen ehrenamtlichen Projektteilnehmer sind die entstehenden Kosten gering. Die Offenen Lizenzen garantieren die Nachhaltigkeit

- VeraCrypt: Festplattenverschlüsselung

Firmengeheimnisse und andere vertrauliche Daten sollten immer verschlüsselt gespeichert werden – vor allem, auf mobilen Geräten, die leicht gestohlen werden können. Das früher vielfach genutzte Truecrypt wird offiziell nicht mehr weiterentwickelt, aber die offene Lizenz erlaubte eine Weiterentwicklung unter dem Namen Veracrypt.

- Open SSH: Kommunikations-Sicherheit

Open SSH dient unter anderem der abhör- und fälschungssicheren Übermittlung von Steuerinformationen an eingebettete Systeme oder Internetserver.

- Open SSL: Datentransport-Sicherheit

TLS (Transport Layer Security) ist das im Internet am meisten genutzte Sicherheitsprotokoll. Leider gibt es immer wieder Sicherheitslücken im TLS-Protokoll, oder in einzelnen TLS-Bibliotheken. Open SSL ist die meistgenutzte und deshalb wichtigste TLS-Bibliothek.

- GNU Privacy Guard: Anwendungs-Sicherheit

Der GNU Privacy Guard wurde zum Versenden von verschlüsselten und unterschriebenen E-Mails nach dem Open PGP Standard entwickelt. GnuPG ist auch wichtig, um die Herkunft und Echtheit von Sicherheitsupdates zu überprüfen.

- Das TOR Projekt: Anonym Surfen

Mit Hilfe des TOR-Browsers kann man im Netz surfen, ohne seine Identität zu verraten. Das TOR Projekt wird momentan vorwiegend vom US Verteidigungsministerium finanziert.

Anmerkungen zur Pflicht zur Herausgabe von Passwörtern in § 15 TMG Entwurf

Zur Diskussion des Spannungsverhältnis zwischen Entwurf TMG und der DGSVO sei aus der Stellungnahme der Digitalen Gesellschaft e.V. an das Bundesministerium der Justiz und für Verbraucherschutz zum Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität zitiert.

> "Die Bestimmung in § 15a TMG n.F. umfasst dem Wortlaut nach eine Pflicht zu Herausgabe von Passwörtern. Zum einen ist nicht ersichtlich, welchen legitimen Nutzen die Herausgabe von Passwörtern für die Strafverfolgungsbehörden haben kann. Sofern bestimmte Informationen, die auf einem Account gespeichert sein könnten, von Interesse für die Strafverfolgung sind, können diese herausverlangt werden. Ob der Erhalt von Passwörtern etwa zum verdeckten Weiterbetrieb eines Accounts durch Behörden führen soll, für den keine Rechtsgrundlage ersichtlich ist, oder zum Ausprobieren für andere Accounts der betreffenden Person – solche denkbaren Verwendungen der Passwörter wären verfassungswidrig. Passwörter dürfen nach der DSGVO nicht im Klartext gespeichert werden, um Integrität und Vertraulichkeit zu gewährleisten. Gespeichert sind demnach bei Anbietern, die ihre datenschutzrechtlichen Pflichten einhalten, in der Regel Hashwerte von Passwörtern, mittels derer ermittelt werden kann, ob ein eingegebenes Passwort richtig ist, die jedoch nicht auf das Passwort als solches zurückgerechnet werden können. Deshalb stellt sich auch die Frage der Vereinbarkeit der vorgeschlagenen Regelung mit europäischem Datenschutzrecht."

Änderung einer Zahl macht Passwortermittlung unmöglich

Auch an diesem Beispiel kann man einfach die Macht von kryptographischen Lösungen erkennen. Das kryptographische Modell geht von der praxisnahen Annahme aus, daß ein Angreifer zumindest lesenden Zugriff auf die Zugangsinformationsdatei erhält.

Sichere Speicherung von Zugangsinformationen

Das gängigste Verfahren zur Anmeldung bei Internetdiensten ist die Verwendung der Kombination Nutzername und Passwort. Es ist unmittelbar nachvollziehbar, daß eine Datei, die Nutzernamen und Passwörter im Klartext enthält für Angreifer ein sehr lohnendes Ziel wäre.

- Die Kenntnis des Inhaltes dieser einen Passwortdatei würde das gesamte Zugriffssystem komplett kompoimitieren. Aus diesem Grund ist es eine strikte Anforderung der Sicherheitsforschung stattdessen nur einen Wert zu Speichern, welcher durch Verwendung einer Einwegfunktion (in der Praxis durch kollissionsresitente Hashfunktionen realisiert) auf das Passwort und einem zusätzlichen Zufallswert (Salt) berechnet wird. Andere Vorgehensweise entsprechen nicht dem Stand der Technik sind sind somit zum Bearbeiten von persönlichen Daten nicht rechtskonform.

- DGSVO treue Anbieter besitzen keine gespeicherten Passwörter.

Wiederholungszähler

Um dem Angreifer trotz der Kenntnis der Zugangsdatei das Errechnen der eigentliche Passworte zu erschweren, verwendet man in der Praxis vereinfacht gesprochen meist einen Zähler, welcher das Berechnen der Einwegfunktion durch mehrfache Ausführung schwerer macht. Setzt man diesen DGSVO-konform auf den Stand der Technik, können auch Ermittlungsbehörden die gewünschten Passworte nicht mit vertretbarem Aufwand bestimmen.

Für Mathematiker und Forscher im Bereiche der IT-Sicherheit ist es eine sehr spannende Beobachtung, daß die lange Zeit als zu theoretisch und paranoid kritisierten Sicherheitsmodelle die realistischste Einschätzung der aktuellen Sicherheitslage darstellen.

Akademisches Sicherheitsmodell

Bei der Analyse der Sicherheit von Computernetzwerken geht man in der theoretischen Modellbildung von sehr mächtigen Angreifern aus, die alle Nachrichten mitlesen und verändern kann. Da das Internet auf der Grundphilosophie von offenem Zugang gründet, ist der Schutz von Daten Aufgabe der Kryptographie. Die in der Praxis eingesetzen kryptographischen Algorithmen haben die interessante Eigenschaft, daß Sie entweder für Niemanden oder faktisch für jeden Engagierten brechbar ist. Aus diesem Grunde verbietet eine Schwächung der Kryptographie. Kryptographie ist in vielerlei Hinsicht das einzig wirksame Werkzeug die Digitalisierung im Geiste einer freiheitlich demokratischen Grundordnung mitzugestalten.

Praktisches Sicherheitsmodell

- Siehe letzten Abschnitt.

Auch aus rein technischer Sicht zeigt die Tatsache, dass gespeicherte Daten in der real existierenden IT-Welt (2020) nicht gesichert werden können, die Notwendigkeit eines verfassungsrechtlichen Schutzes.

- Grundannahme: Jeder Technische Schutz für Daten versagt eines Tages.

Generelle Hackbarkeit

Bedeutend für eine gesellschaftliche Einschätzung ist auch die Tatsache, dass neben den Diensten fremder Staaten auch Privatpersonen und Firmen in der Praxis recht einfach (in der Regel rechtswidrigen) Zugriff auf die heutigen Computersysteme erlangen können. Es haben sich hier Online-Marktplätze für ausnutzbare Sicherheitslücken (Zero-Days) gebildet, an denen sich in rechtlich problematischer Weise auch deutsche Dienste beteiligen. Die Preise sind schwankend, allerdings meist für Einzelpersonen mit höhere Einkommen und kleinere Firmen durchaus finanzierbar. Inzwischen gibt es bereits frei

verfügbare Werkzeuge, die nur geringe Anforderungen an die Computerkenntnisse des Angreifers stellen.

Cyberwaffen sind kopierbar

Die Ausnutzung von Sicherheitslücken hat die Eigenschaft, dass die Angriffswerkzeuge kopierbare Programme sind. Diese gefährlichen digitalen Waffen können selbst aus halbwegs engagierten Einzelpersonen mächtige Angreifer ganzer Wirtschaftssysteme machen. Im Falle von WannaCry ist die Weltwirtschaft nur wegen der diletantischen Programmierung, von einem katastrophalen Schaden bewahrt worden. Aus diesen Gründen scheint seit wenigen Tagen der US-amerikanische Nachrichtendienst NSA seine Veröffentlichungspraxis zu ändern.

Die in Deutschland durch die Gründung des BSI bisher angestrebte Trennung von Schutz der Bevölkerung und der Entwicklung von digitalen Angriffswaffen hat zu einer im Vergleich zu anderen Staaten höheren Vertrauensbildung geführt. Ausdrücklich lobend erwähnt sei die vertrauensbildende Arbeit des BSI im Falle Huawei. Diese hat im Bereiche der aufziehenden Handelskrieges zu einer Deeskalation beigetragen. Dieses Vertrauen sollte in einer immer instabileren Weltlage nicht aufs Spiel gesetzt werden, sondern gepflegt, ausgebaut und auch institutionell verstetigt werden.

- Das Nichtschließen von Sicherheitslücken bedroht angesichts der weiter fortschreitenden Vernetzung in den Bereichen Industrie und der kritischen Infrastruktur nicht mehr nur im digitalen Sinne Heimat und innere Sicherheit.

Sicherheitsproblem Industrievernetzung: Gefahren über die Digitale Welt hinaus

Die Sicherheitslage ist im Bereich des Internet-of-Things (IoT) aus einer Reihe von Gründen deutlich schlechter als in der klassischen Computerindustrie. Viele Geräte adressieren einen Markt mit sehr geringen Stückpreisen oftmals im einstelligen Eurobereich. Ein organisiertes Netzsicherheitsmanagement, welches die PC-Industrie über viele Jahre mit erheblichem Aufwand aufbaute, ist im Massenanlagenbau meist nicht zu finden. Oftmals bestehen nicht einmal ausreichende Update-Möglichkeiten. Verschärft wird dies durch eine im niedrigpreisigen Gerätemarkt geringere Kundenbindung der Hersteller, so dass die Verbraucher nicht befriedigend über nötige Sicherheitsupdates informiert werden. Weiterhin haben viele eingebettete Systeme eine weit längere Einsatzzeit als persönliche Computersysteme. Diese kann beispielsweise bei smarten Heizungssteuerungen viele Jahre betragen. Schließlich ist auch bei vielen Verbrauchern oft nicht einmal das Wissen vorhanden, dass das wegen seiner Funktion angeschaffte Gerät einen wartungsintensiven Internet-Teilnehmer darstellt.

Industriesteuerungen

Von unsicheren IoT Geräten gehen Gefahren nicht nur für die digitale Welt aus. So können Störungen in industriellen Anlagen Katastrophen auslösen. Auch innerhalb der Hausvernetzungen liegen etwa bei der Heizungssteuerung nicht zu unterschätzende Gefahrenpotentiale vor. Zahlreiche Autoren demonstrierten, wie Angreifer bestimmte IoT-Geräte dazu bringen können, eine Infektion durch ein Schadprogramm weiterzugeben. Innerhalb weniger Minuten können sich Zehntausende von ungeschützten IoT-Geräten in einer Stadt zu einem einzigen, von den Angreifern kontrollierten Botnetz zusammenschließen.

Haftung für Schäden

Die seit geraumer Zeit vermehrt auftretenden Angriffe mit Millionen übernommener IoT Geräte zeigen eine neue Dimension des Problems. Für den Verbraucher entsteht unter anderem auch das Problem, dass mit übernommenen Geräten angerichtete Schäden die IP-Adresse des Besitzers als Angriff-

sherkunft hinterlassen. Dies kann sowohl juristische Folgen, als auch Folgen für die technischen Systeme haben. Abwehrmaßnahmen der angegriffenen Systeme können zu Störungen der unwissend für Angriffe missbrauchten IoT Systemen führen.

- Aus Sicht des Verbraucherschutzes ist eine Klärung der Haftung für von IoT Geräten verursachte Schäden und eine stärkere Inverantwortungnahme der Hersteller herbeizuführen.
- Umgekehrt muss von Verbrauchern verlangt werden, dass Sie für Geräte, die die Sicherheit der Allgemeinheit gefährden, die Verantwortung übernehmen und zumindest die Sicherheitsupdates der Hersteller auch einspielen, so es welche gibt.

Sicherheitsupdates und Nachhaltigkeit

Die Erfahrung der letzten Jahre lehrt, dass alle Kommunikationsgeräte zu einer Gefahr für ihre Nutzer und für die Allgemeinheit werden können, wenn nicht regelmäßig entdeckte Sicherheitslücken durch Sicherheitsupdates geschlossen werden. Ein wichtiger Grundsatz ist deshalb, dass während der gesamten Lebenszeit eines Gerätes Sicherheitsupdates geschrieben und installiert werden müssen. Eingebettete und IoT Geräte sind da keine Ausnahme. In der Praxis ist die Einhaltung dieses Grundsatzes ein Problem. Erstens haben die Hersteller, wenn sie ihre Geräte einmal verkauft haben, oft kein ökonomisches Interesse an einer weiteren Pflege und dem Erstellen vom Sicherheitsupdates. Zweitens ist, vor allem bei kleinen Herstellern, nicht klar, wie lange dieser Hersteller am Markt sein wird, bzw. wie lange es eine verantwortliche Firma gibt, die Sicherheitsupdates erstellen kann. Um dieses Problem zu lösen, schlagen wir das Folgende vor.

Handlungsvorschläge IoT-Sicherheit

- Hersteller sind während der gesamten Lebenszeit eines IoT Gerätes dazu verpflichtet, Sicherheitsupdates zu schreiben und an die Nutzer zu verbreiten.
- Wollen die Hersteller sich, nach Ablauf einer angegebenen Lebenszeit, dieser Verpflichtung entziehen, müssen sie spätestens zu diesem Zeitpunkt ihre Quelltexte als Open-Source veröffentlichen. Damit soll sichergestellt werden, dass zumindest Dritte das Schreiben und ggf. Verbreiten von Sicherheitsupdates übernehmen können.
- Soweit die Quelltexte der Hersteller anfänglich nicht Open-Source sind, müssen sie bei einem Treuhänder hinterlegt werden. Kommt ein Hersteller den genannten Verpflichtungen nicht nach oder existiert der Hersteller nicht mehr, sorgt der Treuhänder für die Veröffentlichung der Quelltexte als Open-Source.

Die Notwendigkeit der Datensparsamkeit

Beginnend mit dem Volkszählungsurteil des Bundesverfassungsgerichts (1983) hat sich in Deutschland ein weltweit beachtetes Datenschutzrecht in Gesetzgebung und Rechtsprechung entwickelt. Datensparsamkeit ist die verfassungsrechtlich und höchstrichterlich geforderte einzuhaltende Norm.

Datenverzicht

Heute müssen sich Datenschutzexperten daher auch in hoch konfliktäre Diskussionen einbringen. Das hier leider vorherrschende politische Diskussionsklima schreckt dabei verständlicherweise viele Wissenschaftler ab. Dennoch gebietet es die gesellschaftliche Verantwortung, darauf hinzuweisen, wenn technische Entwicklungen, wie eine allumfassende Überwachung oder die praktische Angreifbarkeit von Computersystemen, juristische Datenschutzsicherungen praktisch unwirksam werden lassen. In der Computer-Sicherheitsforschung herrscht die Meinung vor, dass Daten auf vernetzten Computersystemen generell als hackbar anzusehen sind.

- Wenn man nicht bereit ist, das Risiko einer möglichen Veröffentlichung von vertraulichen Daten einzugehen, darf man die Daten gar nicht erst speichern.

Daten von besonders gefährdeten Personengruppen

Wer Daten speichert, oder eine Verpflichtung zum Speichern bestimmter Daten einführt, muss die Vorteile, die sich aus einer Speicherung ergeben, mit den Nachteilen, die sich aus einer Veröffentlichung der Daten ergeben würden, abwägen – selbst wenn eine Veröffentlichung der Daten nicht vorgesehen ist. Es genügt keinesfalls, die Daten nur rechtlich zu sichern (also, ihre Veröffentlichung zu verbieten bzw. unter Strafe zu stellen). Es genügt nicht einmal, die Daten, zusätzlich zu dem juristischen Schutz auch technisch zu schützen, mit Maßnahmen, die dem Stand der Technik entsprechen. Denn nicht einmal die Kombination von rechtlichen und technischen Sicherungsmaßnahmen gibt eine Garantie dafür, dass die Daten auf Dauer geheim bleiben. Erwachsen aus einer möglichen Veröffentlichung besonders schwere Nachteile für die Betroffenen, oder sogar eine Gefahr für Leib und Leben, müssen die Vorteile einer Speicherung diesen Nachteilen und Gefahren gegenübergestellt werden.

Geschlossene Systeme und Systemsicherheit

Die Frage, ob geschlossene oder offene Systeme hinsichtlich der Systemsicherheit vorzuziehen sind, ist zentral innerhalb der Informatik. Während geschlossene Systeme im günstigen Falle durch eine ausreichende Qualitätskontrolle einige Angriffe verhindern können, ist, falls die Qualitätskontrolle versagt, der Schaden vom Nutzer selbst nur schwer abwehrbar. Neben der Trusted Computing Infrastruktur verbaut Intel in zahlreichen seiner Prozessoren eine eigene Sicherheitsarchitektur. Diese ist ein geschlossenes Konzept, welches höchst problematische Eigenschaften aufweist. Daher ist eine grundsätzliche Deaktivierung der Intel Active Management Technology (AMT) zu empfehlen.

Alternative Vertrauensanker

Es ist zwingend notwendig, Alternativen zum Vertrauensanker von Microsoft zur Verfügung zu stellen. Aus technischen Gründen ist dies sogar deswegen notwendig, weil Microsoft teilweise mit einer Schlüssellänge von 2048 bit arbeitet, welche vom BSI nicht für langfristige Sicherheit empfohlen wird.

- Für den staatlichen Bereich könnte beispielsweise die Bundesnetzagentur eine führende Position einnehmen. Hier sind im Zusammenhang mit dem Signaturgesetz schon erhebliche Vorarbeiten vorgenommen worden.

- Für nichtstaatliche Bereiche erscheint eine gemeinnützige Stiftung außerhalb der USA die bessere Lösung. Als Beispiele könnten hier die Reformen bei ICANN und das verteilte Erzeugen von DNSSEC-Rootzonenschlüssel dienen.

Quellenhinweis

Teile dieser Stellungnahme enthalten aktualisierte Vorschläge und Analysen, welche im Rahmen der Studie

- Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen der Bundesministeriums für Justiz und Verbraucherschutz
- Juni 2017
- Technologien für und wider Digitale Souveränität
- Rüdiger Weis, Stefan Lucks, Volker Grassmuck
- `https://www.svr-verbraucherfragen.de/wp-content/uploads/Weis_Lucks_Grassmuck_Studie_.pdf`

erstellt und veröffentlicht wurden. Diese fachübergreifende Studie enthält weitere Empfehlungen, Analysen der Auswirkung der Digitalisierung und ein ausführliches Quellenverzeichnis und sei zur zusätzlichen Lektüre empfohlen.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 C

Rheinische
Friedrich-Wilhelms-
Universität Bonn

Institut für Informatik

Prof. Dr. Michael Meier
Lehrstuhl IT-Sicherheit

Prof. Dr. Michael Meier
Universität Bonn · Institut für Informatik

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Per E-Mail: innenausschuss@bundestag.de

Bonn, 23. Januar 2020

Stellungnahme zum Antrag der Fraktion der FDP „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“ – Drucksache 19/5764

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Bundestagsabgeordnete,

vielen Dank für die Gelegenheit zur Stellungnahme zum oben genannten Antrag und für die Einladung zur Sitzung des Ausschusses am 27. Januar 2020.

Stellungnahme zum Antrag der Fraktion der FDP:

Den im Antrag unter I. getroffenen Feststellungen schließe ich mich an.

IT-Sicherheit, also die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, hinreichend durchzusetzen ist aufgrund verschiedener Ursachen (u.a. komplexitätsbedingten Fehlern in Soft- und Hardware sowie Seiteneffekten von Soft- und Hardware) eine große Herausforderung. Gleichzeitig werden IT-Systeme zunehmend zum Fundament von Wirtschaft und gesellschaftlichem Leben. Für den Schutz der Vertraulichkeit innerhalb von IT-Systemen stehen mit Verschlüsselungsverfahren, sofern konsequent und korrekt eingesetzt, wirksame Werkzeuge zur Verfügung.

Zu den unter II. aufgestellten Forderungen an die Bundesregierung nehme ich im Folgenden Stellung:

1. *… sich zum Schutz der Privatsphäre und zur Erhöhung der IT-Sicherheit für ein Recht auf Verschlüsselung einzusetzen;*

Diverse, teilweise im Antrag aufgeführte, Grundrechte korrespondieren mit einem Recht auf Vertraulichkeit. Verschlüsselung ist das wesentliche Werkzeug zur wirksamen Durchsetzung von Vertraulichkeit. Ohne Verschlüsselung kann ein Recht auf Vertraulichkeit heute nicht wirksam durchgesetzt werden. Entsprechend ergibt sich aus dem Recht auf Vertraulichkeit ein Recht auf Verschlüsselung.

2. *… in diesem Sinne Telekommunikations- und Telemedienanbieter zu verpflichten, ihre Kommunikationsdienste nach einer Übergangsfrist für zukünftige technische Systeme als Standard abhörsicher (Ende-zu-Ende verschlüsselt) anzubieten;*

Für Betreiber von Telekommunikationsnetzen und -diensten ergeben sich aus § 109 TKG Plichten zur Umsetzung technischer Schutzmaßnahmen, für die die Bundesnetzagentur einen Katalog von Sicherheitsanforderungen[1] aufgestellt hat. Darin heißt es:
„Wer Telekommunikationsnetze betreibt oder öffentliche Telekommunikationsdienste erbringt sollte sich mit diesem Thema auseinandersetzen und bei entsprechender Gefährdungslage an geeigneter Stelle eine Verschlüsselung der Daten vornehmen."
Aus meiner Sicht ist heute im Regelfall von einer entsprechenden Gefährdungslage auszugehen.

Im Telemediengesetz ist in §13 (7) formuliert:
„Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens."
In der BSI-Veröffentlichung zur „Absicherung von Telemediendiensten nach Stand der Technik" (Stand 2016)[2] ist Verschlüsselung als Basismaßnahme für alle Provider-Typen (Content-, Host- und Access-Provider) vorgesehen.

Aus meiner Sicht entspricht eine Ende-zu-Ende-Verschlüsselung dem heutigen Stand der Technik, sodass sich die Forderung durch die oben genannten Regelungen ergibt. Unabhängig davon, ob hier eine Rechtsanpassung notwendig ist, trägt die Umsetzung der Forderung zu einer sinnvollen Verbesserung der IT-Sicherheit bei und ist ein Beitrag zum erklärten Ziel der Bundesregierung Deutschland zum Verschlüsselungsstandort Nr. 1 zu machen.

3. *… die Weiterentwicklung von Verschlüsselungstechnologien, der Sicherheit von Speichersystemen und von qualifizierten Zugriffs- und Berechtigungslogiken konsequent voranzutreiben;*

Oben genannte Herausforderungen bei der Durchsetzung von IT-Sicherheit bei gleichzeitiger Intensivierung der IT-Nutzung in unserem Land machen eine umfangreiche Weiterentwicklung von IT-Sicherheitstechnologien zwingend erforderlich. Neben der Weiterentwicklung von Technologien bedarf es auch der Entwicklung und Umsetzung von Ansätzen und Konzepten mit denen Sicherheitstechnologien wie Verschlüsselung in eine breite Anwendung gebracht werden. Zu letztgenanntem Aspekt sehe ich großen Nachholbedarf.

4. *… sich gegen gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme auszusprechen;*

Verschlüsselung ist das einzige wirksame Mittel zum Vertraulichkeitsschutz. Jegliche Beschränkung der Nutzung oder Beeinträchtigung der Wirksamkeit bzw. Sicherheit etwa durch Verwaltung zusätzlicher Schlüsselkopien für staatliche Stellen etc. sind der IT-Sicherheit abträglich und mit verheerenden Auswirkungen verbunden. Dadurch würde jegliches Recht auf Vertraulichkeit ausgehöhlt.

[1] Bundesnetzagentur: Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG), 2016, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf
[2] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_125.pdf

5. *… den Einsatz von sogenannten Backdoors zu verurteilen und eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken abzulehnen;*

Sicherheitslücken gefährden unsere Digitale Gesellschaft und müssen schnellst möglich geschlossen werden. Versuche Sicherheitslücken offen zu halten, um sie ausnutzen zu können, sind unverantwortlich und abzulehnen.

Eine staatliche Beteiligung an Märkten für Sicherheitslücken sollte jedoch differenzierter betrachtet werden. So kann eine Beteiligung an diesen Märkten ausschließlich zum Zweck der Aufklärung dort (und damit bei Angreifern) verfügbarer Informationen zu Sicherheitslücken sinnvoll sein, um hiervon ausgehend Empfehlungen und Warnungen in Richtung von IT-Nutzern auszusprechen, um Gefahren durch entsprechende Sicherheitslücken zu reduzieren.

6. *… alle staatlichen Behörden zu verpflichten, IT-Sicherheitslücken unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Das BSI muss diese nach dem marktüblichen Standard der „Coordinated/Responsible Disclosure“ veröffentlichen;*

Aus bereits angeführten Gründen unterstütze ich diese Forderung.

7. *… die Verwendung von frei verfügbaren, offenen und einfach handhabbaren Protokollen sowie Verschlüsselungsstandards wie z. B. GPG voranzutreiben.*

Ich unterstütze diese Forderung: Das Beispiel der Ende-zu-Ende-Verschlüsselung von E-Mails (z.B. mittels S/MIME oder GPG) zeigt, dass trotz grundsätzlich verfügbarer Technologie die Nutzung begrenzt ist, da erforderlichen Infrastrukturen und Schlüsselverteilmechanismen fehlen. Innerhalb von Organisationen wird durch den zentralen Betrieb solcher Infrastrukturen die einfache und weitgehend transparente Nutzung von Ende-zu-Ende-Verschlüsselung ermöglicht. Für die Nutzung von Ende-zu-Ende-verschlüsselter E-Mail-Kommunikation über Organisationsgrenzen hinweg und im privaten Umfeld sind spürbare Hürden zu überwinden, da entsprechende Schlüssel-Infrastrukturen und Verzeichnisdienste kaum verfügbar sind oder, im Falle von GPG, nur durch IT-affine Anwender sicher benutzbar sind. Hier sind zusätzliche Anstrengungen von staatlicher Seite erforderlich um IT-Sicherheit und Datenschutz durch breite standardmäßige Nutzung von Ende-zu-Ende-Verschlüsselung zu erhöhen und Deutschland tatsächlich zum Verschlüsselungsstandort Nr. 1 zu machen.

Abschließende Anmerkungen zu verwandten aktuellen Diskussionen:

Aufgrund der für 5G vorgesehenen kryptographischen Sicherheitsmechanismen werden im Endausbau des 5G-Netzes klassische IMSI-Catcher (zur Erfassung von Mobiltelefonen im Umfeld) nicht mehr funktionieren. Allerdings sehe ich konzeptionell keine Hindernisse für die Entwicklung von 5G-fähigen IMSI-Catchern, die u.U. in Zusammenarbeit mit den Mobilfunkbetreibern zu entwickeln und zu betreiben wären. Grundsätzlich handelt es sich bei diesen Geräten jedoch um Dual-Use-Aufklärungswerkzeuge, die auch von Kriminellen genutzt werden können. Anstatt auf die Entwicklung derartiger Werkzeuge zu setzen, erscheint mir die Realisierung hoheitlicher Aufklärungs- und Ermittlungsaufgaben über die Mitwirkung von Mobilfunk-Providern geeigneter.

Die Spionagemöglichkeiten durch 5G-Ausrüster werden intensiv diskutiert. Diesen kann mit Verschlüsselung effektiv begegnet werden. Eine weitere Aufweichung der Sicherheits- insbesondere Verschlüsselungsmechanismen innerhalb von 5G (tatsächlich bleiben die Verfahren hinter dem heute möglichen und sinnvollen zurück) muss verhindert werden. So ist etwa die im Zusammenhang mit der Überwachung ausländischer Handynutzer vorgesehene pauschale (egal ob tatverdächtig oder nicht)

Weitergabe von (zur Transportverschlüsselung genutztem) Schlüsselmaterial in das Besuchsland allein zum Zweck einer möglichen Entschlüsselung zur Überwachung höchst kritisch zu betrachten, und schwächt die Sicherheit des gesamten Systems und damit aller Nutzer. Hierdurch werden zusätzliche Angriffspunkte für Angreifer geschaffen.

Kritisch zu sehen ist auch der im Rahmen des Entwurfs des Gesetzes zur Bekämpfung von Rechtsextremismus und der Hasskriminalität unternommene Vorstoß alle Telemedienanbieter zu verpflichten vertrauliche Passwortinformationen (nach Stand der Technik in der Regel Passwort-Hashes) auf Anforderung an Sicherheitsbehörden zu übermitteln.

Vertrauliche Passwortinformationen und kryptographische Schlüssel sind grundlegend für die IT-Sicherheit und den Datenschutz und müssen maximal geschützt werden. Dies schließt derartige Zugriffsmöglichkeiten für Dritte wie z.B. Sicherheitsbehörden aus.

Angemerkt sei auch, dass mit einer breiteren Akzeptanz der aktuell vorangetriebenen FIDO2-Technologie zur Authentifikation von Nutzern bei Web-Diensten, seitens Dienstanbieter keine entsprechenden Passwortinformationen oder Vergleichbares mehr vorhanden sein werden.

gez. Prof. Dr. Michael Meier

Hochschule des Bundes
für öffentliche Verwaltung

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 D

POSTANSCHRIFT HS BUND, POSTFACH 40527, 10063 BERLIN

Deutscher Bundestag
- Ausschuss für Inneres u. Heimat -

via E-Mail

Prof. Dr. Jan-Hendrik Dietrich
HAUSANSCHRIFT Habersaathstr. 51, 10115 Berlin
POSTANSCHRIFT Postfach 40527, 10063 Berlin
TEL 030 – 22 00 89 – 86341
EMAIL jan-hendrik.dietrich@fhbund-muc.de

DATUM Berlin, 26.01.2020

BETREFF **Schriftliche Stellungnahme zur Sachverständigenanhörung vor dem Ausschuss für Inneres und Heimat des Deutschen Bundestages am 27.01.2020**

über

den Antrag der Abgeordneten Jimmy Schulz, Stephan Thomae, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP

Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken

BT-Drs. 19/5764

Zu den im o.g. Antrag aufgeworfenen Rechtsfragen nehme ich vor der mündlichen Anhörung aus verfassungs- und verwaltungsrechtlicher Sicht folgendermaßen Stellung:

I. „Recht auf Verschlüsselung“?

Ein „Recht auf Verschlüsselung“ kennt die deutsche Rechtsordnung nicht. Ein entsprechendes Grundrecht ist weder ausdrücklich im Grundgesetz geregelt noch der Rechtsprechung des BVerfG zu entnehmen. Einfachgesetzlich ist es bisher nicht hin-

terlegt. Dafür besteht auch kein Bedarf. Denn „Verschlüsselung“ ist nichts anderes als ein **schutzbereichsrelevantes Verhalten im Rahmen der Gewährleistung bekannter Grundrechte**.[1] Soweit gesetzliche Pflichten bestehen, Inhalte von elektronischer Kommunikation „verschlüsselt“ zu übertragen (Vgl. etwa § 5 Abs. 3 S. 2 De-Mail-Gesetz), bei Datenübermittlungen Vorkehrungen zum Schutz „gegen den unbefugten Zugriff Dritter“ (Vgl. z.B. § 21a S. 1 BZRG) zu treffen oder elektronische Überwachungsinstrumente „nach dem Stand der Technik gegen unbefugte Nutzung zu schützen (Vgl. § 49 Abs. 2 S. 2 BKAG), wird lediglich das grundrechtliche Schutzniveau konkretisiert.

1. „Verschlüsselung“ in der abwehrrechtlichen Dimension der Grundrechte

Grundrechte fungieren zu allererst als Abwehrrechte von Bürgerinnen und Bürgern gegenüber staatlichen Eingriffen.[2] „Verschlüsselung“ kann in diesem Zusammenhang ein Verhalten darstellen, das vom Schutzbereich eines Grundrechts erfasst ist. So kann Verschlüsselung etwa vom **Schutz des Fernmeldegeheimnisses i.S.v. Art. 10 Abs. 1 GG** umfasst sein. Das Fernmeldegeheimnis schützt die Vertraulichkeit der räumlich distanzierten Kommunikation. Die Verwendung von Verschlüsselungstechniken soll diesen Schutz stärken. Ganz vergleichbar ist die Verwendung eines Briefumschlags zur Wahrung des Briefgeheimnisses.[3] Insofern stellt „Verschlüsselung“ ein geschütztes Verhalten im Schutzbereich von Art. 10 Abs. 1 GG dar. Schutzbereichsverstärkend kann sich hierbei auswirken, dass es auch Gegenstand der Meinungsäußerungsfreiheit i.S.v. Art. 5 Abs. 1 S. 1 Hs. 1 GG sein kann, eine Meinung „codiert“ zu äußern.[4] Der Grundrechtsträger ist bei der Wahl der Form der Meinungsäußerung frei.

---

[1] Siehe ausführlich dazu *Gerhards*, (Grund-) Recht auf Verschlüsselung?, 2010, S. 123 ff.

[2] Vgl. BVerfGE 7, 198 (204); 50, 290 (337); 68, 193 (205)

[3] Vgl. *Voßhoff/Büttgen*, ZRP 2014, 232 (232).

[4] Vgl. *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 202 ff.; in diese Richtung wohl auch *Gusy*, nach dessen Auffassung die Nutzung von Verschlüsselungstechniken allgemein dem Schutzbereich von Art. 5 Abs. 1 S. 1 GG unterfallen soll. Siehe *Gusy*, in: v. Mangoldt/Klein/Starck, GG, Bd. 1, 7. Aufl. 2018, Art. 10 Rn. 66.

Die Nutzung von Verschlüsselungstechniken kann zudem dem Schutz des **allgemeinen Persönlichkeitsrechts i.S.v. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG** unterfallen. Das vom BVerfG aus dem allgemeinen Persönlichkeitsrecht abgeleitete **Recht auf informationelle Selbstbestimmung** vermittelt dem Grundrechtsträger das Recht, über die Verwendung seiner personenbezogenen Daten grundsätzlich selbst zu entscheiden. Dies umfasst zweifellos das Recht, solche Daten zu verschlüsseln. Darüber hinaus hat das BVerfG in seiner Entscheidung zur „Online-Durchsuchung" dem allgemeinen Persönlichkeitsrecht den Teilgehalt eines **Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme** entnommen.[5] Geschützt ist dabei das Interesse des Nutzers, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.[6] Die Vertraulichkeits- und Integritätserwartung lässt sich insbesondere über Verschlüsselungsmechanismen erreichen. Sie bilden die entscheidende technische Hürde gegen Ausspähung, Überwachung oder Manipulation. Mit Blick auf die zunehmende Digitalisierung des Alltags und faktisch bestehenden Grenzen eines staatlich vermittelten Schutzes vor Bedrohungen im „World Wide Web" muss der Einzelne berechtigt sein, die Vertraulichkeit und Integrität seiner informationstechnischen Systeme selbst in die Hand zu nehmen.[7] Der Einsatz von Verschlüsselung unterfällt demgemäß dem Schutzbereich von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Schließlich kann die Nutzung von Verschlüsselung von der **grundrechtlichen Gewährleistung wirtschaftlicher Betätigung** nach Art. 12 Abs. 1 GG und Art. 14 Abs. 1 S. 1 GG umfasst sein. Die Berufsfreiheit gem. Art. 12 GG schützt u.a. die Berufs*ausübungs*freiheit. Vom Schutzbereich erfasst alles, was eine berufliche Tätigkeit ausmacht (insb. Form, Mittel, Umfang und Inhalt der Betätigung).[8] Bei bestimmten Berufsgruppen ist ein besonderes Vertrauensverhältnis besonders charakteristisch für die berufliche Tätigkeit. Angesprochen sind sog. Berufsgeheimnisträger, wie etwa

---

[5] BVerfGE 120, 274 (313 ff.).

[6] BVerfGE 120, 274 (314).

[7] In diesem Sinne *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 183.

[8] Siehe *Manssen*, in: v. Mangoldt/Klein/Starck (Hrsg.), GG (Fn. 4), Art. 12 Rn. 67; *Mann*, in: Sachs (Hrsg.), GG, 8. Aufl. 2018, Art. 12 Rn. 79.

Ärzte, Geistliche oder Strafverteidiger. Das diese Berufe kennzeichnende Vertrauensverhältnis wird gesetzlich besonders geschützt (Vgl. z.B. § 53 Abs. 1 StPO, § 62 BKAG, § 203 Abs. 1 StGB).[9] Die Wahrung des Berufsgeheimnisses zählt damit untrennbar zur beruflichen Betätigung. Jedes Verhalten, das der Gewährleistung des typischen Vertrauensverhältnisses dient, unterfällt insofern dem Schutzbereich von Art. 12 GG.[10] So liegt es im Fall der Verwendung von Verschlüsselungstechniken. Zudem kann der Schutzbereich der Eigentumsfreiheit i.S.v. Art. 14 Abs. 1 GG eröffnet sein. Dies ist jedenfalls anzunehmen, soweit es um den Schutz betriebsbezogener Daten geht, die bereits zu einem Vermögenswert geworden sind.[11] Namentlich Betriebs- und Geschäftsgeheimnisse können ohne Verschlüsselungsvorkehrungen nicht vor unbefugter fremder Kenntnisnahme bewahrt werden.[12]

Der Einsatz von Verschlüsselungstechniken wird nach alledem von verschiedenen Grundrechten geschützt. Der grundrechtliche Schutz wird allerdings nicht schrankenlos gewährleistet. Der Staat kann „Verschlüsselung“ in Konkretisierung jeweils einschlägiger grundrechtlicher Gesetzesvorbehalte regulieren. Als solche **Grundrechtseingriffe** kommen verschiedene Maßnahmen in Betracht. Der denkbar schwerste Eingriff wäre ein **grundsätzliches Verbot von Verschlüsselungstechniken**, wie es zur Zeit in den USA diskutiert[13] und in manchen Staaten bereits praktiziert wird[14]. Unterhalb der Verbotsschwelle sind **mildere gesetzliche Beschränkungen** denkbar. Hierzu würde etwa zählen, Diensteanbieter zur Wahrung von staatlichen Sicherheitsinteressen zum **Einbau von sog. „Backdoors“** oder zur **Hinterlegung von Schlüsseln** zu verpflichten. Schließlich könnte der Gesetzgeber für Diensteanbieter, bei denen Verschlüsselungsoptionen gewählt werden können, eine

---

[9] Zur Schutzbedürftigkeit von Berufsgeheimnisträgern siehe jüngst BVerfGE 141, 220 (Rn. 255) sowie *Löffelmann*, GSZ 2019, 190 (193).

[10] Siehe näher *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 253 ff.

[11] Vgl. *Jarass/Pieroth*, GG, 15. Aufl. 2018, Art. 14 Rn. 17.

[12] Vgl. *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 233 ff.

[13] Näher *Geller*, POLITICO v. 27.06.2019, https://www.politico.com/story/2019/06/27/trump-officials-weigh-encryption-crackdown-1385306 (Stand: 20.01.2020).

[14] So z.B. in Saudi-Arabien. In anderen Staaten steht der Einsatz von Verschlüsselungstechniken unter Genehmigungsvorbehalt (z.B. im Iran, in China oder Russland). Nachweise bei *Schulze*, APuZ 46-47/2017, 23 (25 f.); *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 117 ff.

gesetzliche Pflicht zur Herausgabe von Schlüsseln oder Passwörtern an Sicherheitsbehörden vorsehen, wenn im Einzelfall eine bestimmte Gefahren- oder Verdachtslage besteht und ein Gericht die Herausgabe anordnet. Auf die Zulässigkeit solcher Beschränkungsmaßnahmen wird unten eingegangen (siehe unten III.).

2. „Verschlüsselung" und grundrechtliche Schutzpflichten

Die Grundrechte vermitteln nicht nur abwehrrechtliche Schutzansprüche des Einzelnen. Sie verkörpern in ihrer Gesamtheit eine **objektive Werteordnung**.[15] In diesem Sinne wirken sie sich auf die Gestaltung und Anwendung des einfachen Rechts durch alle drei Gewalten aus, indem sie objektiv-rechtlich **staatliche Schutzpflichten** begründen[16], d.h. sie verlangen vom Staat ein positives Tun, die grundrechtlich verbrieften Rechtsgüter des Einzelnen vor Eingriffen Dritter zu schützen.[17] In Bezug auf den Einsatz von Verschlüsselungstechniken ist fraglich, ob den Staat eine grundrechtliche Schutzpflicht trifft, Diensteanbieter gesetzlich hierzu zu verpflichten (dazu sogleich unter II.).

II. Gesetzliche Verpflichtung zum Einsatz von „Ende-zu-Ende"-Verschlüsselung

Im o.g. Antrag wird die Bunderegierung aufgefordert,

> „Telekommunikations- und Telemedienanbieter zu verpflichten, ihre Kommunikationsdienste nach einer Übergangsfrist für zukünftige technische Systeme als Standard abhörsicher (Ende-zu-Ende verschlüsselt) anzubieten".

Es stellt sich die Frage, ob der deutsche Gesetzgeber hierzu im Wege grundrechtlicher Schutzpflichten verpflichtet ist. Eine Schutzpflicht, die gesetzgeberische Handlungsaufträge vermittelt, ist grundsätzlich in Bezug auf alle Grundrechte denkbar.[18]

---

[15] Siehe nur BVerfGE 7, 198 (205).

[16] Vgl. BVerfGE 39, 1 (41 f.); 53, 30 (57); 56, 54 (73); 88, 203 (232, 251); 115, 118 (152).

[17] Siehe *Groß*, JZ 1999, 236 (331).

[18] Siehe *Ronellenfitsch*, DuD 2018, 110 (111); *Roßnagel*, ZRP 1997, 26 (28), *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 321; *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten und Drittwirkung im Internet, 2014, S. 48.

Eine gesetzliche Verpflichtung von Diensteanbietern zum Einsatz von Ende-zu-Ende-Verschlüsselungen könnte sich aus der Schutzpflichtendimension des Fernmeldegeheimnisses i.S.v. Art. 10 Abs. 1 GG ergeben.[19] Diesbezüglich hat das BVerfG ausdrücklich festgestellt, dass Art. 10 Abs. 1 GG (auch) einen Auftrag an den Staat begründet, **„Schutz insoweit vorzusehen, als private Dritte sich Zugriff auf die Kommunikation verschaffen“**.[20]

Hieraus folgt zunächst, dass eine akute Gefährdungslage hinsichtlich der Vertraulichkeit der räumlich distanzierten Kommunikation bestehen muss.[21] Die drohende – oder sogar schon eingetretene – Rechtsgutverletzung müsste dabei von dritter Seite herrühren und auf den Mangel einer Verschlüsselung zurückzuführen sein. Dem soll am Beispiel der E-Mail-kommunikation nachgegangen werden: es spricht einiges dafür, dass von den Milliarden E-Mails, die jährlich in Deutschland verschickt werden, immer noch ein gewisser Anteil nicht verschlüsselt wird. Im Jahr 2015 wurde in nur 16% aller Fälle eine Verschlüsselungssoftware verwendet.[22] Eine Gefährdungslage hinsichtlich des Rechtsguts aus Art. 10 Abs. 1 GG ist demnach nicht auszuschließen, denn ohne Verschlüsselungstechnik ist die E-Mail-Kommunikation gegen Hacking-Angriffe oder andere Formen des unbefugten Zugriffs nur unzureichend geschützt. Insoweit ist eine aus Art. 10 Abs. 1 GG resultierende Schutzpflicht anzunehmen.

Es stellt sich allerdings die Frage, ob die Schutzpflicht so weit reicht, dem Gesetzgeber die Einführung einer verpflichtenden Ende-zu-Ende-Verschlüsselung aufzuerlegen. Denn dem Staat kommt bei der Erfüllung der Schutzpflichten ein sehr **weiter Einschätzungs-, Wertungs- und Gestaltungsspielraum** zu.[23] Dieser Spielraum wird lediglich durch das sog. **Untermaßverbot** beschränkt.[24] Eine Handlungspflicht

---

[19] Daneben sind auch Schutzpflichten aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG denkbar, die in dieser Betrachtung unberücksichtigt bleiben.

[20] BVerfG NJW 2002, 3619 (3620); NJW 2007, 3055 (3055).

[21] Siehe zur Schutzpflichtendogmatik *Möstl*, Die staatliche Garantie für öffentliche Sicherheit und Ordnung, 2002, S. 93 ff.; *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten (Fn. 18), S. 47 ff.

[22] *Schulze*, APuZ 46-47/2017, 23 (23); *Voßhoff/Büttgen*, ZRP 2014, 232 (232).

[23] BVerfGE 77, 170 (214 f.); 88, 203 (262).

[24] In der Rechtsprechung des BVerfG ist dies bisher kaum konturiert worden. Siehe BVerfGE 88, 203 (254). Näher dazu *Möstl*, Garantie für öffentliche Sicherheit und Ordnung, S. 103 ff.

des Staates erwächst allein dann, wenn das Untermaßverbot verletzt ist.[25] Davon kann hier keine Rede sein. Zur Gewährleistung des Schutzes der Vertraulichkeit der Distanzkommunikation hat der Gesetzgeber mittlerweile zahlreiche Regelungen getroffen. Im Mittelpunkt steht die einfachgesetzliche Verpflichtung der Diensteanbieter auf das Fernmeldegeheimnis durch § 88 TKG sowie daraus abzuleitende technische Konsequenzen i.S.v. § 109 Abs. 1 TKG. Eine Verletzung des Fernmeldegeheimnisses ist nach § 206 StGB strafbewehrt. Hinzu kommen weitere strafrechtliche Vorschriften, die mittelbar den Schutz der Vertraulichkeit der Kommunikation bezwecken (z.B. §§ 202a, 202b StGB). Im Mai 2011 ist zudem das De-Mail-Gesetz[26] in Kraft getreten, das De-Mail-Diensteanbieter auf die Nutzung von Signatur- und Verschlüsselungstechniken verpflichtet.[27] Schutzverstärkend wirken darüber hinaus Regelungen der sog. eIDAS-Verordnung[28] sowie der DS-GVO[29]. Art. 32 DS-GVO verpflichtet etwa Unternehmen in Verbindung mit Art. 33, 34 DS-GVO zur Verschlüsselung von E-Mails, die personenbezogene Daten enthalten, da bei Verstößen gegen Sicherheitsverpflichtungen bei der Datenverarbeitung Geldbußen in Millionenhöhe drohen.[30] Zu den gesetzgeberischen Anstrengungen treten zahlreiche administrative Initiativen wie die Empfehlungen und Services des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die Kombination der geschilderten Maßnahmen kann unmöglich eine Wirkung abgesprochen werden. Vor allem werden Bürgerinnen und Bürger in die Lage versetzt, **wirkungsvollen Selbstschutz** dort zu betreiben, wo – infolge der Internationalität des Internets – ohnehin nur eingeschränkt staatliche Zugriffsmöglichkeiten beste-

---

[25] *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten (Fn. 18), S. 51.

[26] De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), zuletzt geändert durch Artikel 14 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626).

[27] Siehe dazu *Roßnagel*, NJW 2011, 1473 (1473 ff.)

[28] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257 vom 28.8.2014, S. 73-114.

[29] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 vom 4.5.2016, S. 1-88.

[30] Vgl. *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2017, Art. 32 Rn. 14.

hen[31]. Eine **Verengung der Erfüllung der staatlichen Schutzpflicht** auf lediglich ein einziges Mittel, ist demnach **nicht vertretbar**.[32] Eine gesetzliche Verpflichtung von Diensteanbietern zum Einsatz von Ende-zu-Ende-Verschlüsselungen lässt sich insofern nicht aus der objektiv-rechtlichen Dimension von Art. 10 Abs. 1 GG ableiten.[33]

III. Zulässigkeit gesetzlicher Verschlüsselungsverbote oder -beschränkungen

Mit dem gegenständlichen Antrag wird die Bundesregierung u.a. aufgefordert, „sich gegen gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme auszusprechen“ und „den Einsatz von sogenannten Backdoors zu verurteilen“.

Hinter Verschlüsselungsverboten oder -beschränkungen steht in der Regel der Zweck, die sicherheitsbehördliche Arbeit nicht zu be- oder verhindern. Strafverfolgungsbehörden und Nachrichtendienste warnen vor einem **„Going Dark-Problem“**: die verbreitete Nutzung von Verschlüsselungstechnik führe dazu, dass klassische Telekommunikationsüberwachungsinstrumente zunehmend an Grenzen stießen.[34] Neu sind solche Überlegungen keineswegs. Die Anfänge der sog. **„Kryptokontroverse“** reichen bis in die 1990er Jahre zurück.[35] Seitdem hat sich die Lage aber weiter verschärft. Im Bereich der Kinderpornographie etwa stellte EUROPOL fest:

> „The use of end-to-end encrypted platforms for sharing media, coupled with the use of largely anonymous payment systems, is facilitating an escalation in the live streaming of child abuse. Offenders target regions where there are high levels of poverty, limited domestic child protection measures and easy access to children.[36]“

---

[31] Vgl. dazu *Hoffmann-Riem*, JZ 2008, 1009 (1011).

[32] In diesem Sinne wohl auch *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten (Fn. 18), S. 104.

[33] Auch in Bezug auf Schutzpflichten anderer Grundrechte ergibt sich kein anderes Ergebnis.

[34] Näher *Schulze*, APuZ 46-47/2017, 23 (24 ff.).

[35] Siehe ausführlich *Bizer*, in: Hammer (Hrsg.), Sicherungsinfrastrukturen – Gestaltungsvorschläge für Technik, Organisation und Recht, S. 179 (179 ff.).

[36] EUROPOL, Internet Organised Crime Threat Assessment 2016, S. 10.

Auch im jüngsten „Internet Organised Crime Threat Assessment 2019“ warnte die Behörde eindringlich vor versiegenden Informationsquellen der Strafverfolgungsbehörden:

> „Encryption, while recognised as an essential element of our digitised society, also facilitates significant opportunities for criminals. Investigative techniques, such as lawful interception, are becoming increasingly ineffective (or even impossible) as criminals exploit encrypted communication services, applications and devices. Similarly, criminals can deny forensic investigators access to critical evidence by encrypting their data. The criminal abuse of encryption technologies, whether it be anonymisation via VPNs or Tor, encrypted communications or the obfuscation of digital evidence (especially in cases of CSEM), was a significant threat highlighted by respondents to this year's IOCTA survey.[37]“

Es liegt auf der Hand, dass es der deutsche Staat nicht akzeptieren kann, wenn der Vollzug geltender Gesetze infolge missbräuchlicher Verwendung von Verschlüsselungstechnik derart erschwert oder unmöglich gemacht wird. Vielmehr ist er verfassungsrechtlich verpflichtet, die **exekutive Einlösung der Staatsaufgabe „Sicherheit“** auch im Internet zu effektuieren. Einhergehend mit der Digitalisierung des Alltags müssen daher die Sicherheitsbehörden in die Lage versetzt werden, ihrem gesetzlichen Auftrag „trotz Verschlüsselung“ nachzukommen. In dieser Hinsicht motivierte gesetzliche Regelungen zur Einschränkung von Verschlüsselungen würden in die Schutzbereiche mehrerer Grundrechte (s.o.) eingreifen und bedürften einer verfassungsmäßigen Rechtfertigung.

Der schwerste denkbare Grundrechtseingriff bestünde in einem **generellen Verbot jeglichen Einsatzes von Verschlüsselungstechniken**. Eine entsprechende gesetzliche Regelung wäre indes **unzweifelhaft verfassungswidrig**. Unabhängig davon, dass einiges dafür spricht, dass eine absolute Verbotsnorm sogar den Wesensgehalt der Grundrechte antasten würde[38], würde sie sich jedenfalls als unverhältnismäßig erweisen. Denn es fehlte ihr schon an der Geeignetheit, die Erfüllung des staatlichen Sicherheitsauftrags zu fördern. Verschlüsselungssoftware wäre trotz eines Verbotes in Deutschland weiterhin anderenorts auf der Welt verfügbar. Ob sie im Einzelfall

---

[37] EUROPOL, Internet Organised Crime Threat Assessment 2019, S. 56 f.

[38] Näher *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 139 ff.

eingesetzt wird, ließe sich kaum sinnvoll überprüfen.[39] Verstößen gegen ein absolutes Verschlüsselungsverbot stünden zudem keine wirksamen Sanktionsinstrumente entgegen.

Demzufolge kommen allein gesetzliche Beschränkungen unterhalb der Schwelle eines generellen Verschlüsselungsverbots in Betracht. Eine solche Beschränkung bestünde in einer gesetzlichen Verpflichtung von Herstellern und/oder Diensteanbietern zum **Einbau von sog. „Backdoors"**. Damit sind planmäßige Sicherheitslücken in Software oder Geräten angesprochen, die in der Regel aufwendig versteckt werden müssen.[40] Aus verfassungsrechtlicher Sicht bestehen **Zweifel an der Verhältnismäßigkeit** einer gesetzlichen Verpflichtung. Bei Abwägung der schutzwürdigen verfassungsrechtlichen Positionen zeigt sich, dass einem Eingriff von großer Streubreite kaum nennenswerte Sicherheitsgewinne gegenüberstehen. Im Gegenteil: über das (notwendige) Gesetz, das zur Einführung der Hintertür anhält, würde die Existenz einer Sicherheitslücke öffentlich bekannt. Für Hackergruppierungen aus der ganzen Welt böte sich damit ein lohnendes Ziel, eine „Backdoor" aufzuspüren und auf dem internationalen Markt für „Zeroday-Exploits"[41] gewinnbringend an solche zu veräußern, die noch weniger Gutes im Schilde führen.[42] Zudem erscheint im Hinblick auf die Transnationalität des Internets fraglich, inwieweit eine gesetzliche Verpflichtung überhaupt wirksam vollzogen werden könnte.

Der Einsatz von Verschlüsselungstechnik ließe sich schließlich im Wege gesetzlicher **Pflichten zur Schlüsselherausgabe** einzelfallbezogen einschränken. Der damit verbundene Grundrechtseingriff muss verfassungsmäßig gerechtfertigt werden können. Entscheidend ist hierbei, dass sich die Herausgabepflicht an den richtigen Adressaten richtet und im übrigen verfahrensmäßige Sicherungen bestehen, die den Eingriff unter Verhältnismäßigkeitsgesichtspunkten einhegen. Denkbar erscheint zunächst, im Falle offener Ermittlungen von Strafverfolgungsbehörden eine gesetzliche

---

[39] Vgl. *Schulze*, APuZ 46-47/2017, 23 (25).

[40] Siehe näher *Schulze*, APuZ 46-47/2017, 23 (24 f.).

[41] Hierzu ausführlich *Brunst*, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, V § 7 Rn. 99.

[42] So wohl auch *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 273; *Blechschmitt*, MMR 2018, 361 (365).

Herausgabepflicht an Beschuldigte selbst zu adressieren. Die Beschuldigten würden gesetzlich auf diese Weise zu einem aktiven Tun angehalten werden. Gerade dies ist aber mit dem verfassungsrechtlich hinterlegten **„nemo-tenetur"-Grundsatz[43] nicht zu vereinbaren**, wonach niemand gezwungen werden kann, sich selbst zu belasten. Ein Zwang zur Selbstbezichtigung würde die Würde des Menschen berühren, dessen Aussage als Mittel gegen ihn selbst verwendet wird.[44] Eine **gesetzliche Herausgabepflicht** von Beschuldigten wäre demzufolge **verfassungswidrig**.

Möglich ist dagegen, die **Herausgabe von Schlüsseln und Passwörtern von privaten Dritten** (z.B. Systemadministratoren oder Diensteanbietern) zu verlangen. Verfassungsrechtlich bestehen hiergegen grundsätzlich keine Bedenken, solange das Zusammenspiel aus tatbestandlichen Eingriffsschwellen für behördliche Maßnahmen (z.B. Anhaltspunkte eines Verdachts für schwere Straftaten) und verfahrensmäßigen Sicherungen (z.B. ein Richtervorbehalt) der Intensität des Grundrechtseingriffs gerecht wird. Teilweise sind Herausgabepflichten für Diensteanbieter bereits gesetzlich geregelt worden. § 8 Abs. 3 der Telekommunikations-Überwachungsverordnung (TKÜV)[45] verpflichtet Anbieter von Telekommunikationsdiensten, Schlüssel aufzuheben und den Sicherheitsbehörden bereitzustellen, wenn die Telekommunikation netzseitig – durch den Dienstanbieter selbst – verschlüsselt wird. Eine teilnehmerautonome Verschlüsselung wird von der Norm allerdings nicht erfasst, ebenso wenig die Internet-Telefonie.[46] Hinzu kommt, dass nach einer jüngsten Entscheidung des EuGH E-Mail-Dienste (wie etwa GMail, GMX), die keinen Internetzugang vermitteln, keinen „elektronischen Kommunikationsdienst" im europarechtlichen Sinne darstellen[47]. Infolgedessen können sie auch nicht im Wege des Telekommunikationsgesetzes (TKG)[48] und der TKÜV verpflichtet werden. Einen

---

[43] Grundlegend zum „nemo tenetur se ipsum accusare"-Prinzip BGHSt 38, 214 (214 ff.).

[44] BVerfGE 38, 105 (114 f.); 56, 37 (42).

[45] Telekommunikations-Überwachungsverordnung i. d. Fassung der Bekanntmachung vom 11. Juli 2017 (BGBl. I S. 2316), zuletzt geändert durch Art. 27 d. Gesetzes v. 20.11.2019 (BGBl. I S. 1724).

[46] Vgl. *Gerhards*, Recht auf Verschlüsselung? (Fn. 1), S. 302.

[47] EuGH NVwZ 2019, 1118 (1120).

[48] Telekommunikationsgesetz vom 22.06. 2004 (BGBl. I S. 1190), zuletzt geändert d, Art. 1 des G. vom 5.11.2019 (BGBl. I S. 2005).

Ausweg soll eine Änderung des § 15a Telemediengesetz (TMG) versprechen. Nach § 15a TMG in der Fassung des Referentenentwurfs[49] sollen Anbieter zur Auskunft über Bestandsdaten verpflichtet werden, „mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird“. Angesprochen sind damit z.B. Passwörter von E-Mailkonten oder von Cloud-Diensten. Tatsächlich kollidiert diese Regelung mit bestehenden Verpflichtungen aus der DS-GVO, denn die Anbieter sind grundsätzlich gehalten, Passwörter nicht im Klartext zu speichern. Sie verfügen lediglich über Hashwerte, die aber wiederum den Sicherheitsbehörden nichts nützen. Insofern hätte § 15a TMG n.F. wohl lediglich geringe praktische Relevanz.

IV. Behördliche Meldepflicht und Ankauf von IT-Sicherheitslücken

Im gegenständlichen Antrag wird die Bunderegierung aufgefordert,

> „alle staatlichen Behörden zu verpflichten, IT-Sicherheitslücken unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden“ sowie
>
> „(…) eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken abzulehnen“.

Beide Forderungen sind in einer Gesamtschau in den Blick zu nehmen. Eine allgemeine behördliche Meldepflicht ist zunächst vor dem Hintergrund von § 7 BSIG zu sehen. Danach ist das BSI befugt, zur **Erfüllung seiner gesetzlichen Aufgaben vor Sicherheitslücken und Schadprogrammen warnen**. Dabei steht dem BSU ein Ermessen zu, ob und in welchem Umfang es warnt. In eine Abwägung sind einerseits die Interessen der IT-Anwender einzustellen.[50] Ihnen würde durch die behördliche Warnung die Möglichkeit evtl. eröffnet, eigene Schutzmaßnahmen zu ergreifen. Andererseits muss das BSI berücksichtigen, ob durch die Veröffentlichung einer Schutzlücke schon deshalb ein Schaden entsteht, weil diese nicht so schnell geschlossen werden kann und gerade deshalb ein Angriffsziel darstellt. Möglicherweise kann eine Warnung auch unterbleiben, wenn ein Hersteller die Sicherheitslücke be-

[49] Siehe https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_ BekaempfungHatespeech. pdf?blob=publicationFile&v=1 (Stand: 22.01.2020).

[50] Zum Folgenden ausführlich *Buchberger*, GSZ 2019, 183 (187 f.).

reits erkannt hat und an Abhilfe arbeitet. Schließlich kann der Adressatenkreis der Warnung nach § 7 Abs. 1 S. 4 BSIG insbesondere beschränkt werden, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern.[51]

Eine **allgemeine behördliche Meldepflicht von Sicherheitslücken** würde das BSI darin unterstützen, seiner Warnfunktion besser nachkommen zu können. Gleichwohl darf nicht übersehen werden, dass Strafverfolgungsbehörden und Nachrichtendienste u.U. ein Interesse daran haben können, dass Sicherheitslücken nicht sofort geschlossen werden, um sie für eigene Zwecke – etwa zur Durchführung einer Quellen-Telekommunikationsüberwachung oder einer sog. Online-Durchsuchung – zu nutzen.[52] Der Bedarf an einer Ausnutzung von Sicherheitslücken steigt: wie gezeigt stoßen klassische Überwachungsinstrumente infolge zunehmender Verbreitung von Verschlüsselungstechniken zunehmend an ihre Grenzen. Gleichzeitig erweisen sich gesetzliche Beschränkungen von Verschlüsselungen als unzulässig oder kaum durchsetzbar (s.o.). Die Sicherheitsbehörden müssen demgemäß in die Lage versetzt werden, ihrem gesetzlichen Auftrag **auf anderem Wege** nachzukommen. Dazu gehört auch, im Einzelfall Sicherheitslücken auf dem freien Markt zu erwerben, wenn anders der Schutz überragend wichtiger Rechtsgüter nicht sichergestellt werden kann.

Es geht damit um eine **(Schutz-) Pflichtenkollision**. Den Sicherheitsbehörden obliegt der Schutz der Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht sowie der von ihm zu gewährleistenden Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit.[53] Auf der anderen Seite stehen grundrechtlich geschützte Rechtspositionen des einzelnen IT-Anwenders. Diese Pflichtenkollision lässt sich nicht mit einer einseitigen allgemeinen behördlichen Meldepflicht für Sicherheitslücken lösen. Auch das grundsätzliche Verbot eines behördlichen Ankaufs von Sicherheitslücken ist kontraproduktiv. Vielmehr bedarf es **flexibler gesetzlicher**

---

[51] Siehe *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2018, BSIG § 7 Rn. 7.

[52] Zum „Wettlauf um Zeroday-Exploits“ siehe *Brunst*, in: Dietrich/Eiffler (Hrsg.), HdbRdN (Fn. 41), V § 7 Rn. 97 ff.

[53] BVerfGE 120, 274 (319).

Konfliktschlichtungsformeln in den Gesetzen der Sicherheitsbehörden.[54] Danach würde etwa die jeweilige Behörde selbst zur Abwägung ermächtigt, ob eine Weitergabe von Informationen an das BSI erfolgen sollte. Es versteht sich von selbst, dass sich das eingeräumte Ermessen umso mehr reduziert, je gefährlicher sich eine Sicherheitslücke auswirken kann. So wäre etwa bei einer Gefährdung der IT-Sicherheit sog. Kritischer Infrastrukturen (z.B. Atomkraftwerke) das behördliche Ermessen auf null reduziert. Vorbildcharakter für eine gesetzliche Regelung könnte § 7 Abs. 4a des Artikel-10-Gesetzes (G10) entfalten. Danach *darf* der Bundesnachrichtendienst (BND) personenbezogene Daten aus der Telekommunikationsüberwachung an das BSI übermitteln, „wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes oder zur Sammlung und Auswertung von Informationen über Sicherheitsrisiken auch für andere Stellen und Dritte“.

[redacted]
(Prof. Dr. Jan-Hendrik Dietrich)

[54] So wohl auch *Derin/Golla*, NJW 2019, 1111 (1115).

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

GESELLSCHAFT FÜR INFORMATIK

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 E

STELLUNGNAHME

Öffentliche Anhörung des Innenausschusses zum Thema „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“ am 27. Januar 2020

Prof. Dr. Hannes Federrath
Universität Hamburg, Fachbereich Informatik
Präsident der Gesellschaft für Informatik e.V. (GI)

27. Januar 2020

Kurzfassung

In den vergangenen Jahrzehnten hat die Bundesregierung mehrfach bestätigt, „dass es bei der uneingeschränkten Freiheit der Nutzer bei der Auswahl und dem Einsatz von Verschlüsselungssystemen bleibt“, wie es im Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik [BT1999, IMK2002] von 1999 heißt. Dies ist nachdrücklich zu begrüßen und sollte so beibehalten werden, da sich die Rahmenbedingungen zumindest aus technischer Sicht seitdem nicht verändert haben.

Die verfügbaren kryptographischen Algorithmen sind seit Jahren so ausgereift, dass ihr breiter Einsatz problemlos möglich ist. Die EU-Datenschutzgrundverordnung (DSGVO) [DSGV2016] verpflichtet in Art. 32 explizit zur „Verschlüsselung personenbezogener Daten“. Die Umsetzung solcher technischen und organisatorischen Maßnahmen zum Schutz der informationellen Selbstbestimmung ist dementsprechend unabdingbar.

In diesem Sinn ist es sowohl für den Schutz von Betriebs- und Geschäftsgeheimnissen als auch zur Durchsetzung des Rechts auf informationelle Selbstbestimmung aus technischer Sicht möglich und mit Blick auf die Risiken der Digitalisierung geboten, ein Recht auf Verschlüsselung für Wirtschaft, Verwaltung und Bürgerinnen und Bürger zu verankern und – noch weitergehend – eine Pflicht des Diensteanbieters zur Datenverschlüsselung zu etablieren, soweit dies technisch möglich und zumutbar ist.

Unwirksame und schlimmstenfalls gefährliche Kryptoregulierung

Zuletzt bestätigt wurde die Position der Bundesregierung zum freien Einsatz von Kryptographie zumindest im Jahr 2015: „Die Entwicklung und durchgängige Verwendung vertrauenswürdiger IT-Sicherheitstechnologien ist von entscheidender Bedeutung für Unternehmen, Verwaltung und Bürger in unserer heutigen Informationsgesellschaft. Daher wird die gezielte Schwächung oder Regulierung von Verschlüsselungstechniken von der Bundesregierung nicht verfolgt.“ [BT2015]

An diesen Eckpunkten sollte weiter festgehalten werden, da sich die technischen Rahmenbedingungen, die gegen eine Kryptoregulierung sprechen, seither kaum geändert haben. Im Wesentlichen gilt die wichtige, bereits 1997 formulierte Aussage [Fed1998] fort, dass die gesetzliche Einschränkung von Verschlüsselung oder gar das Verbot von Verschlüsselung nicht durchsetzbar und nicht kontrollierbar sind.

Erstens existieren mit steganographischen Verfahren zahlreiche technische Alternativen, deren Verwendung durch Kriminelle (bei richtigem technischen Einsatz) nicht einmal mehr erkennbar ist. Steganographie schützt sowohl die Vertraulichkeit des Inhalts einer Nachricht als auch deren Existenz. Steganographie wäre für textbasierte Kommunikation heute grundsätzlich genauso effizient und bequem einsetzbar, wie wir es von gängigen Messenger-Diensten kennen. Sie wäre in moderne Messenger-Apps leicht integrierbar und ist in Verbindung mit existierenden Anonymisierungsverfahren wie etwa dem TOR-System dazu geeignet, geheime Kommunikation noch effektiver zu schützen als wir es von heutigen Produkten kennen. Bisher existieren allerdings keine bzw. wenn überhaupt nur wenige für Endnutzer geeignete Apps zur steganographischen Kommunikation. Eine Kryptoregulierung würde die Entwicklung und die Verbreitung von solchen Schutzsystemen vorantreiben. Dies könnte die Aufklärung von Straftaten sogar schwerer machen als bisher.

Zweitens erfordern die in heutigen Kommunikationsnetzen notwendigen Schutzmaßnahmen den zwingenden Einsatz von Kryptographie. Verfahren zur rechtsverbindlichen Kommunikation (Elektronische Signatur) und zum Schutz vor unbemerkten oder unerlaubten Veränderungen von Nachrichten und Dokumenten sind ohne Kryptographie nicht denkbar. Sehr eindringlich hat dies bereits 1998 Ronald Rivest gezeigt, indem er mit Hilfe eines Verfahrens zum Schutz der Integrität (Message Authentication Codes) gezeigt hat, wie damit vertrauliche Nachrichten sicher und ohne Verschlüsselung übermittelt werden können [Riv1998].

Im Ergebnis läuft somit eine etwaige Einschränkung von Kryptographie leer, schwächt sowohl die Wirtschaft als auch das Recht auf informationelle Selbstbestimmung und erschwert schlimmstenfalls sogar die Strafverfolgung.

Einsatz von starker Verschlüsselung

Die meisten verfügbaren und heute praktisch genutzten kryptographischen Verschlüsselungsalgorithmen, etwa der Advanced Encryption Standard (AES) [NIST2001] sind seit Jahren gut untersucht, technisch ausgereift, kostengünstig einsetzbar und werden vermutlich noch für viele Jahre (mindestens 20 Jahre) ausreichenden Schutz auch gegen starke Angreifer bieten.

Durch die Fortschritte bei der Entwicklung von Quantencomputern werden vermutlich einige der weit verbreiteten Algorithmen in einigen Jahren nicht mehr einsetzbar sein (z.B. das Verfahren von Rivest, Shamir, Adleman [RSA1078]) und müssen durch sichere Alternativen ersetzt werden. Das amerikanische NIST (National Institute of Standards and Technology) hat bereits 2016 die Standardisierung von sog. Post-Quantum-Kryptographie initiiert [NIST2016], so dass zu erwarten ist, dass auch in Zukunft langfristig sichere Verfahren zur Verfügung stehen.

Eine verpflichtende Verbindungsverschlüsselung, bei der einzelne Teilabschnitte der Kommunikation zwischen den beteiligten Endgeräten, Routern und Servern abgesichert werden, wird trotz der jahrelangen technischen Verfügbarkeit, der geringen Kosten und des sehr wirksamen Schutzes vor Outsidern (Angreifer auf den Kommunikationsverbindungen) selten in den technischen Standards und bisher überhaupt nicht in der Rahmengesetzgebung zur Telekommunikation gefordert.

Obwohl die verfügbaren kryptographischen Algorithmen seit Jahren offene Standards sind und zudem sehr ausgereift sind, wurden in den standardisierten, offenen Kommunikationsprotokollen des Internet, etwa dem Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) und dem Internet Message Access Protocol (IMAP) über die Jahre hinweg kaum Fortschritte beim obligatorischen Einsatz von Verschlüsselung erzielt.

Zwar können offene Sicherheitsstandards wie OpenPGP/GnuPG (Pretty Good Privacy) und S/MIME (Secure Multipurpose Internet Mail Extensions) als optionale Verfahren zur Ende-zu-Ende-Verschlüsselung eingesetzt werden, bei der zwischen den Endgeräten der beteiligten Kommunikationspartner alle übertragenen Inhalte wirksam vor Outsidern (Angreifer auf den Kommunikationsverbindungen) als auch Insidern (Kommunikationsnetzbetreiber) geschützt sind. Allerdings ist dies für die Endbenutzer aufgrund der aufwendigen Installation von Software (GnuPG) und/oder Konfiguration (sowohl OpenPGP/GnuPG als auch S/MIME) sehr mühsam und fehleranfällig.

Selbst breit etablierte Lösungen wie etwa die Ende-zu-Ende-Verschlüsselung von https-Webseiten, die auf technisch ausgereifte Standards wie TLS (Transport Layer Security) zurückgreifen, sind nur optional. Noch immer sind viele Webangebote als unverschlüsselte http-Webseiten verfügbar.

Förderung frei verfügbarer, offener Krypto-Protokolle und Standards

Quelloffene und benutzerfreundliche Implementationen kryptographischer Protokolle und Verschlüsselungsstandards dienen der Allgemeinheit, da sie allen Menschen kostengünstigen Zugang zu kryptografischen Funktionen bieten. Durch die Offenlegung der zugrunde liegenden Techniken besteht die Möglichkeit, frühzeitig Sicherheitsschwächen zu finden und Verbesserungsvorschläge einzubringen.

TLS (Transport Layer Security) ist ein Beispiel für ein standardisiertes kryptographisches Protokoll, welches omnipräsent ist und die komplette Kommunikation zwischen Browser und Webserver durch Ende-zu-Ende-Verschlüsselung schützt. Ohne TLS wären Onlineshopping und Onlinebanking unsicher, könnten keine Anmeldedaten sicher übertragen werden, wäre nicht garantiert, dass Transaktionen unverändert und vertraulich zwischen Bürgerinnen und Bürgern und Staat bzw. Kunden und Händlern ablaufen.

Dennoch existieren auch in TLS systematische Schwächen in der Umsetzung (etwa die Möglichkeit, die TLS-Verschlüsselung durch Man-in-the-Middle-Angriffe und durch „on-the-fly“ erzeugte Schlüsselzertifikate aufzubrechen), die den Schutz von Geschäfts- und Firmengeheimnissen und personenbezogenen Daten gegenüber starken Angreifern (Insider, z.B. Kommunikationsnetzbetreiber; Outsider, z.B. Nachrichtendienste) nicht ausreichend gewährleisten. Im Kern hat sich die derzeit übliche Beglaubigung von Schlüsselmaterial nach dem X.509-Standard [ITU1988] und deren Überprüfung auf Echtheit nicht bewährt. Hier ist dementsprechend Forschungs- und Entwicklungsbedarf.

Paradoxerweise haben Messenger-Apps und (Bild)-Telefon-Software wie etwa iMessage, FaceTime (beide Apple), WhatsApp (Facebook), Signal und OTR innerhalb weniger Jahre gezeigt, dass eine nahtlose und sichere Integration von Ende-zu-Ende-Verschlüsselung in proprietäre Apps möglich ist. Diese existierenden Lösungen sind nur mit der App des jeweiligen Anbieters nutzbar und nicht miteinander kompatibel.

Die hohe Sicherheit und der Anwendungskomfort solcher proprietären Apps gehen somit zu Lasten der Interoperabilität und zumeist auch zu Lasten einer Offenlegung des Quellcodes, die eine Überprüfbarkeit der fehlerfreien Implementierung ermöglicht. Quelloffene Krypto-Bibliotheken sind durch unabhängige Stellen überprüfbar und stellen eine sehr kostengünstige Möglichkeit dar,

aktuelle kryptographische Techniken in diversen Kommunikationsplattformen anzuwenden. Ein Beispiel dafür ist das Signal-Protokoll, das sowohl im Signal-Messenger als auch im Messenger WhatsApp zum Einsatz kommt und so die Kommunikation von Millionen Menschen schützt.

Insbesondere für die sichere E-Mail-Kommunikation besteht Forschungs- und Entwicklungsbedarf. Während private Kommunikation zumeist mit geeigneten Messenger-Apps heute ausreichend gesichert werden kann, ist die E-Mail-Kommunikation für die Wirtschaft und Verwaltung vermutlich auch auf längere Sicht unverzichtbar. Daher ist es notwendig, Protokolle zur einfach anwendbaren, standardisierten und automatischem E-Mail-Verschlüsselung endlich umzusetzen. Hierbei ist GnuPG eines von vielen prominenten Beispielen für quelloffene Implementationen. Es muss jedoch bei der Entwicklung und Verbesserung quelloffener kryptographischer Implementationen und Protokolle auch ein Fokus auf eine extrem einfache Anwendbarkeit für die Endnutzer gelegt werden. Insbesondere die bereits angesprochene Problematik der vertrauenswürdigen Schlüsselzertifikate ist noch nicht ausreichend gelöst. Vielversprechende Initiativen wie etwa die vom Fraunhofer-Institut für Sichere Informationstechnologie (SIT) entwickelte und in Partnerschaft mit der Gesellschaft für Informatik e.V. (GI) vorangetriebene Volksverschlüsselung [VV2016, GI2017, GI2018] müssen gestärkt werden, zumal dort die komplizierte Zertifikatsbeantragung und die Übertragung der Schlüssel in die lokalen Anwendungsprogramme der Nutzer zumindest ansatzweise verbessert wird. Allerdings ist auch diese Lösung noch weit von einer breiten und leicht anwendbaren Lösung entfernt.

Ausnutzung von unbekannten Sicherheitslücken

Zum Schutz der Allgemeinheit und im Interesse des Staates, seine Bürgerinnen und Bürger zu schützen, muss bei der Entdeckung von Sicherheitslücken (Backdoors) von höchster Priorität sein, diese an die verantwortlichen Stellen zu melden und sie zu schließen.

Eine Backdoor stellt eine verwundbare Stelle in einem System dar, die Angreifer dazu benutzen können, in das System einzudringen um vertrauliche Daten zu lesen, sie zu verändern oder sie zu zerstören. Backdoors entstehen entweder beabsichtigt, indem sie die Softwarehersteller gezielt einbauen oder unbeabsichtigt, indem die Sicherheitslücke selbst als Backdoor fungiert.

Sicherheitsschwächen in Kryptographie und Sicherheitslücken in Software können selten und im besten Fall zur Aufklärung von Straftaten genutzt werden, überwiegend schwächen sie jedoch massenhaft gesetztestreue Bürgerinnen und Bürger, Wirtschaft und Verwaltung, da sie auf dem Schwarzmarkt angeboten werden und nicht nur Hackern und inländischen staatlichen Stellen zum Kauf angeboten, sondern insbesondere auch durch ausländische Staaten angekauft

werden und somit schlimmstenfalls auch gegen Deutschland und andere EU-Staaten eingesetzt werden können.

Gerade vor dem Hintergrund der Vermeidung von Hintertüren in sicherheitsrelevanter Software ist die Offenlegung des Quellcodes – zwecks Überprüfbarkeit durch die Öffentlichkeit oder zumindest durch Experten – eine zwingende Voraussetzung für die Vertrauenswürdigkeit von Sicherheitstechnologie.

Verankerung eines Rechts auf Verschlüsselung

Zahlreiche Sicherheitsfunktionen, die nicht notwendigerweise unmittelbar als Verschlüsselung im engeren Sinn wahrgenommen werden, nutzen Verschlüsselungstechnologien. Die sichere Überprüfung von Passwörtern ist beispielsweise ohne kryptographische Verfahren heute undenkbar. Kryptographie ist somit eine wichtige Basistechnologie der Digitalisierung.

In der Vergangenheit hat der Gesetzgeber durchaus proaktiv dazu beigetragen, den Schutz von Bürgerinnen und Bürgern und Wirtschaft im Internet zu stärken. So hat etwa der Diensteanbieter nach § 13 Abs. 6 des Telemediengesetzes (TMG) „die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.“ In Anlehnung an den § 13 Abs. 6 TMG wäre es daher möglich und zur Stärkung des Schutzes geboten, eine analoge Vorschrift zum Angebot von Verschlüsselungsdiensten (nicht notwendigerweise im TMG) zu erlassen.

Die Durchsetzung des Rechts auf informationelle Selbstbestimmung in der digitalen Gesellschaft basiert ebenso wie die praktische Umsetzung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auf der Verfügbarkeit wirksamer kryptographischer Verfahren. Über die EU-Datenschutzgrundverordnung (DSGVO) [DSGV2016] sind die verantwortlichen Stellen gemäß Art. 32 explizit zur „Verschlüsselung personenbezogener Daten“ verpflichtet.

Weiterhin ist ein Recht auf Verschlüsselung auch für die freie Berufsausübung notwendig. Hierzu zählen etwa der Schutz vor Industriespionage und der Schutz journalistischer Berufe und ihrer Quellen. Freie Anwendbarkeit von Verschlüsselung und ein Recht auf Verschlüsselung schützen in diesem Sinn auch die Pressefreiheit.

Fazit

Die Forderungen des Antrags „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken“ [BT2020] sind in vollem Umfang aus informatisch-technischer Perspektive zu begrüßen.

Literaturverzeichnis

[BT1999] Bundesregierung: Eckpunkte der deutschen Kryptopolitik. 1999. Originalquelle beim BMWI nicht mehr vorhanden, Kopie unter https://hp.kairaven.de/law/eckwertkrypto.html (letzter Abruf am 24.01.2020)

[BT2015] Bundesregierung: BT-Drucks. 18/5144 vom 11.06.2015, S. 4. http://dipbt.bundestag.de/dip21/btd/18/051/1805144.pdf (letzter Abruf am 24.01.2020)

[BT2020] Deutscher Bundestag: Antrag der Fraktion der FDP: Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken. BT-Drucks. 19/5764 vom 13.11.2018. http://dip21.bundestag.de/dip21/btd/19/057/1905764.pdf (letzter Abruf am 24.01.2020)

[DSGV2016] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 (letzter Abruf am 24.01.2020)

[Fed1998] Hannes Federrath: Steganographie -- Vertrauliche Kommunikation ohne Kryptographie. in: Rainer Hamm, Klaus Peter Möller (Hrsg.): Datenschutz durch Kryptographie -- ein Sicherheitsrisiko? Nomos Verlagsgesellschaft, Baden-Baden 1998, 42-51.

[GI2017] Gesellschaft für Informatik: Volksverschlüsselung muss kommen. Pressemitteilung vom 02.02.2017. https://gi.de/meldung/volksverschluesselung-muss-kommen (letzter Abruf am 24.01.2020)

[GI2018] Gesellschaft für Informatik: GI begrüßt Forderung nach einem Recht auf Verschlüsselung und fordert Anstrengungen von Webdiensten. Pressemitteilung vom 04.12.2018. https://gi.de/meldung/gi-begruesst-forderung-nach-einem-recht-auf-verschluesselung-und-fordert-anstrengungen-von-webdiensten/ (letzter Abruf am 24.01.2020)

[IMK2002] Innenministerkonferenz: Anlage zum Bericht der Bundesregierung zu den Auswirkungen der Nutzung kryptografischer Verfahren auf die Arbeit der Strafverfolgungs- und Sicherheitsbehörden (Ziffer 4 der Eckpunkte der deutschen Kryptopolitik vom 2. Juni 1999)

„Verschlüsselungsbericht. 2002. https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2002-06-06/anlage-15.pdf?__blob=publicationFile&v=2 (letzter Abruf am 24.01.2020)

[ITU1988] International Telecommunication Union (ITU): Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. 1988-2019. https://www.itu.int/rec/T-REC-X.509/en (letzter Abruf am 24.01.2020)

[NIST2001] National Institute of Standards and Technology: Advanced Encryption Standard. NIST FIPS PUB 197, 2001.

[NIST2016] National Institute of Standards and Technology: Post-Quantum Cryptography. 2016, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography (letzter Abruf am 24.01.2020)

[Riv1998] Ronald L. Rivest: Chaffing and Winnowing: Confidentiality without Encryption. MIT Lab for Computer Science, March 22, 1998. http://people.csail.mit.edu/rivest/chaffing-980701.txt (letzter Abruf am 24.01.2020)

[RSA1978] Ronald L. Rivest, Adi Shamir, Leonard Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, February 1978. https://doi.org/10.1145/359340.359342 (letzter Abruf am 24.01.2020)

[VV2016] Volksverschlüsselung. Offene Initiative für Ende-zu-Ende-Sicherheit. https://volksverschluesselung.de (letzter Abruf am 24.01.2020)

Danksagung

Für die fachliche Zuarbeit bei der Erstellung dieser Stellungnahme danke ich meinen wissenschaftlichen Mitarbeiterinnen und Mitarbeitern Christian Burkert, Matthias Marx, Johanna Nehring-Ansohn, Monina Schwarz sowie den Mitarbeitern der GI-Geschäftsstelle Nikolas Becker und Daniel Krupka.

Kontakt

Prof. Dr. Hannes Federrath
Präsident der Gesellschaft für Informatik e.V. (GI)

Universität Hamburg, Fachbereich Informatik,
Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)
Web: svs.informatik.uni-hamburg.de
E-Mail: federrath@informatik.uni-hamburg.de

Gesellschaft für Informatik e.V. (GI)

Geschäftsstelle Berlin
im Spreepalais am Dom
Anna-Louisa-Karsch-Str.2, 10178 Berlin
Tel.: +49 30 7261 566-15
Mobil: +49 163 8694216
Fax: +49 30 7261 566-19
E-Mail: berlin@gi.de

Geschäftsstelle Bonn
im Wissenschaftszentrum
Ahrstr. 45, 53175 Bonn
Tel.: +49 228 302-145
Fax: +49 228 302-167
E-Mail: bonn@gi.de

Web: www.gi.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)434 F

Freie Universität Berlin

Fachbereich Mathematik und Informatik
ID-Management

Prof. Dr. Marian Margraf
Takustraße 9
14195 Berlin

+49 30 838 75-245
marian.margraf@fu-berlin.de

Innenausschuss des
Deutschen Bundestages

nur per E-Mail

Betr.: Öffentliche Anhörung zum Antrag der Fraktion der FDP "Recht auf Verschlüsselung - Privatsphäre und Sicherheit im digitalen Raum stärken"

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur öffentlichen Anhörung. Gern übersende ich Ihnen vorab meine Stellungnahme in schriftlicher Form.

Den unter I. aufgeführten Feststellungen schließe ich mich an. Zu den unter II. aufgeführten Vorschlägen nehme ich wie folgt Stellung.

1) **… sich zum Schutz der Privatsphäre und zur Erhöhung der IT-Sicherheit für ein Recht auf Verschlüsselung einzusetzen**

Ein Recht auf Verschlüsselung, also der technischen Umsetzung des Schutzziels Vertraulichkeit, leitet sich meines Erachtens aus dem Recht auf informationelle Selbstbestimmung ab, das nach Rechtsprechung des Bundesverfassungsgerichts ein Grundrecht ist.

2) **… in diesem Sinne Telekommunikations- und Telemedienanbieter zu verpflichten, ihre Kommunikationsdienste nach einer Übergangsfrist für zukünftige technische Systeme als Standard abhörsicher (Ende-zu-Ende verschlüsselt) anzubieten**

Die Forderung, dass Telekommunikations- und Telemedienanbieter ihre Kommunikationsdienste standardmäßig Ende-zu-Ende sicher anbieten sollen, begrüße ich. Allerdings ist zu beachten, dass damit wesentliche sicherheits-technische Anforderungen, insbesondere zum Schlüsselmanagement, auf die Nutzer*innen verlagert werden. Hierzu gehören beispielsweise Schlüsselgenerierung, Schlüsselspeicherung, Schlüsselverteilung, aber auch Maßnahmen zur Schlüsselwiederherstellung, sollte z.B. das Gerät, in dem der Schlüssel gespeichert wurde, verloren gehen. Die unter I. aufgeführte Feststellung, dass nur ca. 15% der Nutzer*innen Ende-zu-Ende sichere Technologien zur Verschlüsselung ihrer Kommunikation nutzen, ist auch darin begründet, dass diese Lösungen häufig

Usability-Probleme haben. Hier müssen Technologien entwickelt werden, die es auch technisch nicht versierten Nutzer*innen ermöglichen, diese Maßnahmen benutzbar umzusetzen, ohne die Sicherheit zu schwächen.

3) … die Weiterentwicklung von Verschlüsselungstechnologien, der Sicherheit von Speichersystemen und von qualifizierten Zugriffs- und Berechtigungslogiken konsequent voranzutreiben

Technologien zur Umsetzung von IT-Sicherheit müssen fortwährend weiterentwickelt werden, um auch gegen zukünftige Bedrohungen resistent zu sein, aber auch, um die Benutzbarkeit der Lösungen weiter zur erhöhen und damit eine breite Nutzung zu ermöglichen. Zum Thema Benutzbarkeit siehe die Ausführungen unter Punkt 2). Eine weitere Herausforderung ist die voraussichtliche Entwicklung von Quanten-computern, die erhebliche Auswirkungen auf die heute eingesetzte Kryptographie, insb. auf Verfahren zum sicheren Schlüsselaustausch haben. Hier muss die Entwicklung sogenannter quantencomputerresistenter kryptographischer Verfahren vorangetrieben werden. U.a. mit den aktuell laufenden Projekten zur BMBF-Ausschreibung "Post-Quanten-Kryptografie" im Rahmen des Forschungsrahmen-programms der Bundesregierung zur IT-Sicherheit "Selbstbestimmt und sicher in der digitalen Welt 2015 bis 2020“ gibt es in diesem Bereich laufende Aktivitäten. Solche Programme sind zu begrüßen und sollten weitergeführt werden (auch für weitere Themen der IT-Sicherheit).

4) … sich gegen gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme auszusprechen

Gesetzliche Beschränkungen oder Verbote kryptographischer Verfahren zur Umsetzung der Informationssicherheit würden das recht auf informationelle Selbstbestimmung massiv einschränken und müssen daher abgelehnt werden.

5) … den Einsatz von sogenannten Backdoors zu verurteilen und eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken abzulehnen

Die Geheimhaltung gefundener Sicherheitslücken mit dem Ziel, diese z.B. von staatlichen Stellen zur Kriminalitätsbekämpfung auszunutzen, kann erhebliche Auswirkungen auf die Sicherheit haben. Es kann davon ausgegangen werden, dass diese Sicherheitslücken nicht nur von staatlichen Stellen, sondern auch von Kriminellen gefunden und ausgenutzt werden. Davon ist nicht nur das Grundrecht auf informationelle Selbstbestimmung betroffen. Diese können auch zu großen wirtschaftlichen Schäden führen. In unserer zunehmend vernetzten Gesellschaft haben solche Sicherheitslücken also erhebliche Auswirkungen und müssen unverzüglich nach Bekanntwerden geschlossen werden.

Backdoors sind vor diesem Hintergrund nichts anderes als Sicherheitslücken, die ebenfalls von Kriminellen ausgenutzt werden können und sind damit abzulehnen. Auch die Forderung, Passwörter oder kryptographische Schlüssel an Ermittlungs-

behörden herauszugeben, ist vor diesem Hintergrund kritisch zu sehen. Setzt man die Sicherheitsmaßnahmen korrekt um, so ist eine Herausgabe von kryptographischen Schlüsseln und Passwörtern gar nicht möglich. Bei der Umsetzung von Ende-zu-Ende Sicherheit verbleiben die kryptographischen Schlüssel bei den Nutzer*innen, die Dienstanbieter haben hierauf gar keinen Zugriff. Zusätzlich werden Passwörter, bei richtiger Umsetzung, nicht im Klartext bei den Dienstanbietern gespeichert, sondern nur in einer Form, die es erlaubt, die Korrektheit des Passwortes zu prüfen, ohne das der Dienstanbieter das Passwort ermitteln kann.

6) **… alle staatlichen Behörden zu verpflichten, IT-Sicherheitslücken unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Das BSI muss diese nach dem marktüblichen Standard der „Coordinated/Responsible Disclosure" veröffentlichen**

Diese Forderung begrüße ich ebenfalls. IT-Sicherheitslücken müssen unverzüglich an das BSI gemeldet werden, damit entsprechende Gegenmaßnahmen schnell entwickelt und umgesetzt werden können.

7) **… die Verwendung von frei verfügbaren, offenen und einfach handhabbaren Protokollen sowie Verschlüsselungsstandards wie z. B. GPG voranzutreiben**

Auch diese Forderung begrüße ich. Allerdings müssen, wie unter 2) aufgeführt, vor allem Technologien entwickelt werden, die eine benutzerfreundliche Verwendung dieser Lösungen auch für technisch nicht affine Anwender*innen ermöglichen. Zusätzlich sollten staatliche Stellen dabei unterstützt werden, diese offenen Standards zur Kommunikation mit Bürger*innen anzubieten.

Mit freundlichen Grüßen

Prof. Dr. Marian Margraf