Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)255 D

Stellungnahme

Dr. Aleksandra Sowa
Datenschutzbeauftragte, Datenschutzauditorin und Buchautorin, u. a. „Digital Politics“

zu den Anträgen der Fraktion DIE LINKE (19/7705) „Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors“ der Fraktion der FDP (19/7698) „Digitalisierung ernst nehmen – IT-Sicherheit stärken“ und der Fraktion BÜNDNIS 90/DIE GRÜNEN (19/1328) „IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern“.

im Rahmen der Öffentlichen Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 8. April 2019.

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

ich bedanke mich für die Einladung als Sachverständige und möchte zu den o. g. Anträgen wie folgt Stellung beziehen:

IT-Sicherheit stärken, Freiheit erhalten, Privatsphäre stärken, effektive Maßnahmen einführen, hinreichende Ressourcen bereitstellen, Ende-zu-Ende-Verschlüsselung als Recht gewährleisten: Tolle Anträge mit guten Ideen, Lösungsansätzen und Vorschlägen, wie man IT-Sicherheit – diese „Achillesferse des Informationszeitalters“[1] – in Deutschland und Europa stärken solle.

Vielen Dank dafür.

Ein Déjà-vu-Effekt setzt dennoch ein: Backdoor, Recht auf Verschlüsselung, Hackbacks und die Rolle der Bundeswehr bei all dem, Cyber-Abwehr und die Ausgründung (oder Neugründung) einer unabhängigen Behörde mit Zuständigkeit Digitales und/oder IT-Sicherheit, Überwachungs-Software und ihre Exporte – all das ist schon einmal da gewesen. Oder gar mehrmals. Seit mehr als 20 Jahren wird debattiert, Argumente und Gegenargumente werden ausgetauscht, Experten angehört und Lösungen vorgeschlagen: ob im Virtuellen Ortsverein, der Möglichkeiten des Internets für die politische Arbeit erproben wollte, in der Enquete-Kommission, ob anlässlich der Beinahe-Verhaftung von Phil Zimmermann, Erfinder von Pretty Good Privacy, PGP, wegen illegaler Exporte von Verschlüsselungs-Software, zu den Stellungnahmen namhafter Kryptologen und IT-Sicherheitsexperten zu Backdoor (u. a. mit dem Paper: *Keys und Doormats*[2]) oder zuletzt anlässlich des Widerstandes von Apple, den US-Behörden Zugriff auf das iPhone des San-Bernardino-Attentäters einzuräumen.

Das Ziel des Krieges sei Sieg – und nicht die Fortsetzung von Kriegsoperationen, klärte Sun Tzu auf. Um es mit dem chinesischen Kriegsherrn zu halten:

Der Bundestag wird endlich entscheiden müssen!

Denn dafür, wo Deutschland in den nächsten Jahren zu dem wichtigsten Thema steht, egal, ob es um Digitalisierung, Industrie 4.0 oder lernende Algorithmen und Künstliche Intelligenz geht – dafür, wie sich Deutschland zu dem Thema IT-Sicherheit positioniert, wird der Gesetzgeber verantwortlich sein.

---

[1] BT Drs 19/7698, S. 1.
[2] https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf (7.7.2015).

1. „Anonymes Surfen – das brauche man nicht in einer Demokratie“, erklärte der Innensekretär Günter Krings der *Süddeutsche Zeitung*[3] . Das Gegenteil davon ist richtig: Gerade in einem freien Land, in einer Demokratie, braucht man Anonymität im Internet – nicht weniger als im Allgemeinen. Nicht ohne Grund sind die Wahlen in einer Demokratie anonym. Anonymität – ob in trauter Heimarbeit oder mithilfe moderner Technologien – darf kein Luxus sein. Anonymität ist legitim. Sie ist … vollkommen normal.

   Tatsächlich können Straftaten in Computernetzen „nur vermieden werden, wenn die Vertraulichkeit der Kommunikation mittels sicherer Verschlüsselung gewährleistet ist“[4]. Dies wurde bereits im Jahr 1998 im Schlussbericht der Enquete-Kommission festgehalten.

   Während es technisch und organisatorisch relativ einfach ist, kompatible, verschlüsselte E-Mail-Kommunikation in kleinen, autarken Organisationen wie Unternehmen oder Behörden zu implementieren, sind die Etablierung und Einführung von Lösungen, die ganze Gesellschaften umfassen, weit weniger trivial. Die von Phil Zimmermann erfundene Pretty Good Privacy (PGP) ist ein Beispiel für Technologie, die relativ verbreitet und relativ nutzerfreundlich sowie weitgehend kostenlos ist. Damit Technologien wie diese zum Masseneinsatz kommen, erfordert es Unterstützung und Förderung. Ja, es wird Geld kosten. Ja, es wird Förderung bedürfen. Und ja, Politik und Staat müssen beteiligt sein.

   Diese IT-Sicherheit, die Verschlüsselung, so liest und hört man, die Schaffung sicherer Kommunikationskanäle, der Integrität und Vertraulichkeit der Informationen – das alles kostet Geld und ist im Grunde genommen unnötig – und wenn etwas passiert, kann man immerhin eine Anzeige erstatten. Man lebe letztendlich in einem Rechtsstaat.

   So einfach verhält es sich nicht.

   Politik muss involviert sein, forderte der Silicon-Valley-Aktivist Mat Ceglowski. Politik muss involviert sein, um Lösungen wie Ende-zu-Ende-Verschlüsselung zu gewährleisten, die jedermann zugänglich sind – und auf die man vertrauen kann. Erstens muss die Prämisse Privacy-as-a-Right und Security-as-a-Right heißen – und nicht etwa Privacy- oder Security-as-a-Service. Zweitens ist eine **konsequente** Positionierung hinsichtlich der Frage der Backdoors – Hintertüren – erforderlich:

   Die Fraktion der FDP fordert,
   „sich gegen gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme auszusprechen;
   den Einsatz von sogenannten Backdoors zu verurteilen und eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken abzulehnen“[5].
   Dies sind zweifelsohne gute Vorschläge. Möglicherweise aber nicht hinreichend: Sie schließen bspw. Unterbeauftragung und/oder Outsourcing an privatwirtschaftliche Organisationen/Unternehmen nicht aus.

---

[3] https://www.sueddeutsche.de/digital/tor-netzwerk-darknet-demokratie-1.4363329.

[4] BT Drs. 13/1104. 1998. Schlussbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft*) zum Thema Deutschlands Weg in die Informationsgesellschaft, http://dip21.bundestag.de/dip21/btd/13/110/1311004.pdf, S. 16 (172).

[5] BT Drs. 19/5764.

Dezidierter:

Die Forderung der Fraktion DIE LINKE lautet, *„den Einsatz von Staatstrojanern zu unterbinden und Sicherheitslücken wie Backdoors oder Zero-Day-Exploits weder zu nutzen noch anzuschaffen“*[6].

Noch besser: deren Einsatz zu sanktionieren. Wie? Hierbei kann man sich von der DSGVO inspirieren lassen.

2. „Ist ein Land, in dem man nicht zwischen Tor und Bundestrojaner wählen darf, noch frei?“, fragte einer der Internet-Diskussionsteilnehmer anlässlich des *SZ*-Statements von Günter Krings.

   IT-Sicherheit hilft zweifellos auch Kriminellen. Technologien wie Ende-zu-Ende-Verschlüsselung oder starke Kryptografie können gewiss auch Terroristen nutzen. Aber keine IT-Sicherheit bedeutet für alle Nichtkriminellen mehr Kriminalität. Insofern gefährdet ein Staat, der vermeintliche Sicherheit vor IT-Sicherheit setzt, seine Schutzfunktion gegenüber den Bürgern.

   Um des Weltfriedens willen ist es vermutlich viel wichtiger, sichere Plattformen für die Kommunikation zu besitzen, als wenn gelegentlich ein Krimineller nicht geschnappt werden kann. Im Fall eines begründeten Verdachts kann die Ermittlungsbehörde immer noch auf die Kommunikation des Verdächtigen zugreifen – im hinreichend begründeten Verdachtsfall und unter hinreichender Beachtung der Rechteabwägung.

   Auch wenn es im Einzelfall gute Gründe geben kann, eine (vorhandene) Hintertür zu nutzen, spricht aus der gesamtgesellschaftlichen Perspektive alles dagegen. Da wäre zuerst die Frage, für wen die Hintertüren geschaffen werden sollten und wer (und wann) Zugriff darauf erhalten sollte. Nur für die Regierungen des Herstellerlandes? Oder sollen importierte Produkte mit Backdoors für die Sicherheitsbehörden des jeweiligen Importlandes ausgestattet werden? Wie stellt man sicher, dass der Zugriff auf Backdoors nicht weitergegeben wird? Der US-Sicherheitsguru Bruce Schneier konstatierte Folgendes: Wenn man Hintertüren einbaut oder für etwaige Gegenangriffe offenhält, sollte man dafür sorgen, dass nur die „guten Jungs“ sie nutzen, und zwar nur dann, wenn sie es sollen. Die Welt wäre allerdings viel sicherer, wenn es sie gar nicht gäbe.[7]

   Und da wir zwar im Informationszeitalter, aber zugleich auch in einer Ära sehr niedriger Effizienz der Regierungen leben, hätten Unternehmen zahlreiche Möglichkeiten, solche nationalen Regulierungen zur Backdoor-Pflicht zu umgehen und bspw. ihren Standort nach Indien zu verlegen (die meisten Geräte werden ohnehin in Asien gefertigt, inklusive Software). Kunden würden ggf. den Erwerb nichtdeutscher Produkte vorziehen. Denn: Wer kauft schon gerne ein Produkt mit eingebauter Backdoor?

   Stattdessen fordert das Bundeskriminalamt (BKA) wieder neue Gesetze: TOR, Darknet, „eigene Strafbarkeit“ für Administratoren und Moderatoren der als „illegal“ bezeichneten

[6] BT Drs. 19/7705.
[7] https://www.schneier.com/blog/archives/2011/10/fbi-sponsored_b.html (letzter Zugriff: 5.3.2018).

Plattformen etc.[8] Wer aber die IT-Sicherheit einer vermeintlichen Sicherheit opfert, erntet nicht Sicherheit, sondern Kriminalität. Mehr Kriminalität. Es ist bedauerlich, dass sich diese banale Erkenntnis auch nach über 20 Jahren der damaligen Enquete noch immer nicht als Allgemeingut durchgesetzt hat. Nichts daran ist falsch. Im Gegenteil. Auch aus diesem Grund ist die Herauslösung des BSI aus dem BMI in der Tat vordringlich – wie es zuvor die Herauslösung des BSI aus dem BND war.

3. Bisweilen erwecken das politische Sinnieren über den Cyber-Krieg und das Ersinnen fantastischer digitaler Gegenangriffsszenarien gegen Hacker aus fernen Ländern den Eindruck, von anderen, viel gewichtigeren Problemen abzulenken: „Zu lange hat die Bundesregierung die im Mittelpunkt stehenden Fragen der IT-Sicherheit der Selbstregulierung der Wirtschaft überlassen und eine Politik verfolgt, die die Interessen von Sicherheitsbehörden vor den effektiven Schutz von Grundrechten und sichere digitale Angebote stellt“[9], kritisiert die Fraktion Bündnis 90/Die Grünen in ihrem Antrag. Ein lässiger Umgang mit IT-Sicherheit, veraltete Technologien, keine Kontrollen und kaum Sanktionen gegen notorische Sicherheitssünder (vgl. u. a. § 14 BSIG[10]) sind das Ergebnis. Dass ein digitaler Gegenschlag im Notfall tatsächlich „wirken“ würde, ist noch nicht erwiesen, obwohl es auch darauf ankommt, welches Ergebnis die Bundesregierung als „wirksam“ bezeichnet.

   Unterschiedlich gehen die Fraktionen mit dem Problem der Attribution um:

   Die Fraktion BÜNDNIS 90/DIE GRÜNEN schlägt die Einrichtung einer unabhängigen Organisationseinheit zur „*Bewertung einer etwaigen Zurechenbarkeit von Angriffen*“ vor.

   Die Fraktion der FDP fordert: „*Die Bundesregierung soll […] die weitere Prüfung zur Schaffung einer rechtlichen Grundlage für Hack Backs umgehend einstellen.*“

   Die Forderung der Fraktion DIE LINKE geht am weitesten: Die Bundesregierung solle *„sogenannte Hackbacks durch staatliche Institutionen“* ausschließen und ächten.

   Statt Strategien für Kriege der Zukunft zu entwickeln, sollten Unternehmen und Behörden ihre Systeme und Netzwerke angemessen – gemäß dem Stand der Technik – absichern, in Firewalls und Perimeter-Sicherheit und in gut ausgebildete sowie erfahrene Spezialisten investieren, damit externe Angreifer nicht mehr mit gewohnter Nonchalance in die Systeme eindringen können. Und nicht auf den Hinweis der Geheimdienste warten, ob sie eventuell doch Opfer einer Cyber-Attacke geworden sind.

   Im Zeitalter sinkender Effektivität der Regierungen sind freiwillige Verpflichtungen kaum eine Alternative zu verpflichtenden Standards, Mindestanforderungen oder obligatorischen Zertifizierungen. An der Hochschule für Telekommunikation Leipzig (HfTL) arbeitet Frau Prof. Sabine Radomski an methodischen Grundlagen und einer Definition quantifizierbarer Qualitätsbegriffe für ein IT-Gütesiegel für Software-Sicherheit (Definition von objektiven, messbaren Indikatoren, Metriken) in Bezug auf die Sicherheit von Anfang an. Denn: Die Sache beginnt am Beginn.

---

[8] Vogt, Dr., Sabine 2017. „Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus“ der Kriminellen?“. In: Die Kriminalpolizei Nr. 2/2017, S. 4–7.

[9] BT-Drucksache 19/1328, Antrag *IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern.* 21.3.2018 (http://dipbt.bundestag.de/dip21/btd/19/013/1901328.pdf).

[10] BSI-Gesetz, https://www.buzer.de/gesetz/8987/a193775.htm (letzter Zugriff 3.5.2018).

Die steigende Komplexität der Systeme ist der größte Feind der Sicherheit. In einer aktuellen Studie der Gesellschaft für Informatik e. V., „*Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren*“[11], wurden zwei zentrale Methoden identifiziert, die die Transparenz algorithmischer Entscheidungen „signifikant erhöhen“: Testing und Audit.[12] Damit diese effektiv eingesetzt werden können, fehlen noch geeignete Standards, die den Bewertungen und Prüfungen zugrunde gelegt werden können. Neben den gesetzlichen Grundlagen, so das Ergebnis der Studie, fehlen an vielen Stellen Standards oder die konsequente Legitimation relevanter Instrumente wie Prüfungen, Tests oder Zertifikate durch den Gesetzgeber.

Die Einführung genereller Meldepflichten[13] für Sicherheitsvorfälle nach dem Vorbild der DSGVO – für alle Branchen und Organisationen, unabhängig von der Größe und ob der Vorfall einmalig ist – ist sehr interessant und kann als eine Ergänzung detektiver IT-Sicherheit für u. a. bessere Transparenz dienen – wobei Transparenz hier als eine notwendige Bedingung der Prüfbarkeit und Kontrolle gesehen wird.

Fazit:

Ein „schlüssiges Konzept einer einheitlichen Strategie für mehr digitale Sicherheit“[14] wird im Antrag der Fraktion DIE LINKE gefordert. Tatsächlich verhält es sich mit den Vorschlägen und Lösungsansätzen zur IT-Sicherheit ein wenig wie in dem Dürrenmattschen Hörspiel *Herkules und der Stall des Augias:*

EINE STIMME:
Bilden wir eine Oberkommission!
ALLE:
Beschlossen schon: Wir bilden eine Oberkommission![15]

Digitalministerium, ZITIS, CAZ, BSI, Ausgründung oder Neugründung, Zentralisierung der Kompetenzen kontra Dezentralisierung, mit mehr oder weniger Kompetenzen und Ressourcen – der Bundestag wird eine grundsätzliche Entscheidung treffen müssen: Möchte man weiterhin Technologien fördern, die Überwachung, Lebens- und Arbeitskontrolle stärken – oder möchte man in Technologien investieren, die neue Lebens- und Arbeitsentwürfe ermöglichen, Freiheit und Demokratie stärken – und so seine Schutzfunktion gegenüber den Bürgern ausfüllen.

Dafür ist es notwendig, die richtige Perspektive zu wählen und die Strategie für IT-Sicherheit danach auszurichten. Wenn man beispielsweise die Sicherheit in einem selbstfahrenden Auto aus der Perspektive des Fahrers gestaltet, sieht das Ergebnis anders aus, als wenn man die Sicherheit aus der Perspektive der Fußgänger und/oder Radfahrer modelliert. Nichts anderes gilt für die IT-Sicherheit.

Der deutsche Politologe Thomas Meyer warnte davor, die tatsächlichen absoluten Grundrechte wie die Freiheit mit Rechten von instrumentellem Wert, wie etwa Sicherheit, zu verwechseln:

---

[11] Fachgruppe Rechtsinformatik der Gesellschaft für Informatik e. V. (GI). 2018. Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren (Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen). Berlin: Oktober 2018, S. 6.
[12] Ebenda, S. 7.
[13] Hanßen, H. und Sowa, A. 2018. „Meldepflichten nach DSG-VO, ITSiG und NIS-Richtlinie“. In <*kes*> 4/2018 (36), S. 74–78.
[14] BT Drs. 19/7705.
[15] Dürrenmatt, F. 1964, „Herkules und der Stall des Augias“ (4. Auflage), Arche Zürich, S. 47.

„Der relative Wert der Sicherheit verkehrt sich in eine substanzielle Gefahr, sobald er den Rang der wirklichen Grundrechte usurpiert oder gar diese übertreffen soll.“[16]

[16] Meyer, T. 2013. „Falsche Sicherheit – Die Verwirrung der Begriffe“. In: *Neue Gesellschaft – Frankfurter Hefte* 9/2013, S. 14, http://www.frankfurter-hefte.de/upload/Archiv/2013/Heft_09/PDF/2013-09_meyer.pdf.