Offener Brief an das Bundesministerium des Innern, für Bau und Heimat

AN:
Bundesministerium des Innern, für Bau und Heimat

IN KOPIE:
Auswärtiges Amt
Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Bundesamt für Sicherheit in der Informationstechnik

11. Juni 2019

Betreff: Geplanter Eingriff in Verschlüsselung von Messenger-Diensten hätte fatale Konsequenzen

Sehr geehrte Damen und Herren,

das Bundesministerium des Innern, für Bau und Heimat plant laut Medienberichten eine Gesetzesänderung, um es deutschen Polizei- und Sicherheitsbehörden künftig leichter zu machen, Zugriff auf die digitale Kommunikation von Verdächtigen zu erhalten. Dafür sollen Anbieter von Messenger-Diensten wie beispielsweise Whatsapp, Threema oder iMessage gesetzlich verpflichtet werden, ihre Verschlüsselungstechnik so umzubauen, dass Behörden bei Verdachtsfällen die gesamte Kommunikation von Nutzer:innen mitschneiden können.

Wir warnen ausdrücklich vor einem solchen Schritt und fordern eine sofortige Abkehr von diesem oder ähnlichen politischen Vorhaben auf deutscher wie europäischer Ebene. Die vorgeschlagene Reform würde das Sicherheitsniveau von Millionen deutscher Internet-Nutzer:innen schlagartig senken, neue Einfallstore für ausländische Nachrichtendienste und Internetkriminelle schaffen sowie das internationale Ansehen Deutschlands als führender Standort für eine sichere und datenschutz-orientierte Digitalwirtschaft massiv beschädigen. Statt bereits seit Jahren überholte Reform-Ideen umzusetzen, sollte das Bundesministerium des Innern, für Bau und Heimat aus unserer Sicht einen neuen sicherheitspolitischen Weg einschlagen und Vorschläge entwickeln, die die Arbeit der Polizei- und Sicherheitsbehörden verbessern, ohne dabei aber die Sicherheit von IT-Systemen und privater Kommunikation in Deutschland insgesamt verschlechtern.

Unsere Kritik im Detail:

Die deutsche Kryptopolitik

Ende Mai wurde bekannt, dass das Bundesministerium des Innern, für Bau und Heimat plant, die bestehende TKG-Regulierung auf verschlüsselte Messenger wie WhatsApp, Signal, Threema, Wire oder Telegram auszuweiten. Konkret bedeutet dies: Die Betreiber dieser Dienste müssen ihre Software so umgestalten, dass die Inhalte der Nachrichten unverschlüsselt an Sicherheitsbehörden weitergegeben werden können. Sollten die Betreiber dies ablehnen, so würden ihre Dienste in Deutschland gesperrt. Wie eine technische Umsetzung der Hintertüren in den Messengern aussehen könnte, beschreiben Vertreter:innen des britischen GCHQ in ihrem "Ghost Proposal"[1]. Dieser Vorschlag wurde erst vor Kurzem von einer internationalen Allianz aus Wirtschaft, Wissenschaft und Zivilgesellschaft in einem offenen Brief stark kritisiert.[2]

Der BMI-Vorschlag konterkariert 20 Jahre erfolgreiche Kryptopolitik in Deutschland[3]. In den Eckpunkten der deutschen Kryptopolitik aus dem Jahre 1999[4] einigte sich die damalige Bundesregierung auf ein Prinzip, das unter der Maxime "Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" bekannt wurde. Dieser Grundsatz wurde seitdem mehrfach von Seiten der nachfolgenden Bundesregierungen bestätigt. Noch 2014 wollte Deutschland sogar zum "Verschlüsselungsstandort Nr. 1"[5] in der Welt aufsteigen. Ein Bruch mit diesen Bekenntnissen würde der IT-Sicherheit Deutschlands in Verwaltung, Wirtschaft und Gesellschaft nachhaltig schaden.

Auswirkungen auf die IT-Sicherheit

Die geplante Verpflichtung der Messenger-Betreiber würde dazu führen, dass die Betreiber eine Schwachstelle in ihre Software einbauen müssten. Das erfordert einen tiefen Eingriff in die bestehenden komplexen Softwaresysteme der Betreiber. Diese Schwachstelle könnten von Nachrichtendiensten und Kriminellen ausgenutzt werden, um an sensible Informationen von Individuen, Behörden und Firmen zu kommen. Aktuelle Beispiele[6] zeigen, dass die Absicherung eines Messengers schon komplex genug ist, ohne dass dort zusätzlich gezielt Schwachstellen eingebaut werden und so die IT-Sicherheit zusätzlich gefährdet wird.

Gleichzeitig würde dieser Schwachstelle-Einbau es Mitarbeiter:innen bei den Betreibern ermöglichen, Kommunikationsinhalte einsehen zu können, was aktuell nicht möglich ist. Hierdurch erhöht sich nicht nur das Missbrauchspotenzial. Eine zentrale Ablage der dazu benötigten kryptographischen Schlüssel[7] würde auch ein primäres Ziel für Angreifer:innen darstellen, der im Fall eines erfolgreichen Angriffs zur Offenlegung der Kommunikation aller (!) Nutzer:innen führen könnte (*Single-Point-of-Failure*).

[1] Ian Levy, Crispin Robinson: Principles for a More Informed Exceptional Access Debate
[2] Coalition Letter: Open Letter to GCHQ
[3] Sven Herpig, Stefan Heumann: Encryption Debate in Germany
[4] Die Raven Homepage: Eckpunkte der deutschen Kryptopolitik
[5] Die Bundesregierung: Digitale Agenda 2014 - 2017
[6] Jürgen Schmidt: Kritische Sicherheitslücke gefährdet Milliarden WhatsApp-Nutzer und Marius Mestermann: Ernster iPhone-Bug: Apple schaltet FaceTime-Gruppenanrufe ab
[7] Es handelt sich hierbei um eine mögliche Implementierung dieser Hintertüren. Es gibt auch andere Implementierungsmöglichkeiten, die technisch jedoch nicht weniger problematisch sind.

Hinzu kommt, dass die neue Version des jeweiligen Messengers mit Hintertür als Softwareupdate eingespielt werden müsste. Hier würden dann entweder alle deutschen Nutzer:innen oder ausgewählte deutsche Nutzer:innen dieses mit der Hintertür versehene Update eingespielt bekommen. Dieser Vorgang würde das Vertrauen der Verbraucher:innen in Sicherheitsupdates erschüttern und sich damit nachhaltig negativ auf die IT-Sicherheit in Deutschland auswirken.

Sollten die Messenger-Betreiber die vorgesehene Maßnahme nicht umsetzen, sollen laut Plan des Innenministeriums ihre Dienste in Deutschland gesperrt werden. Das wäre auch die einzige Möglichkeit, wie die zuständigen Behörden mit Messengern umgehen könnten, deren Verschlüsselung ohne einen zentralen Betreiber auskommt und in die daher keine Hintertüren per Regulierung implementiert werden könnten (z. B. Pretty Good Privacy, Off-The-Record). Das würde unweigerlich dazu führen, dass es innerhalb Deutschlands keine sichere Messenger-Kommunikation mehr geben könnte. Eine technische Umsetzung wäre aber, vor allem für quelloffene Messenger wie Signal, faktisch unmöglich zu realisieren. Es würde eine dedizierte und stark in die Freiheitsrechte eingreifende IT-Infrastruktur brauchen, um das Umgehen dieser Sperren auszuschließen (inklusive Blockieren von Virtuellen Privaten Netzwerken [VPNs] und The Onion Router [TOR]), da Kriminelle die ersten wären, die dies versuchen würden.[8]

Betroffen wären davon allerdings nicht “nur” deutsche Behörden (u. a. Polizei, Feuerwehr, THW), Firmen und Bürger:innen im Allgemeinen, sondern auch Berufsgeheimnisträger:innen (z.B. Rechtsanwälte, Geistliche, Ärzte, Journalisten und Abgeordnete) und andere besonders schützenswerte Personengruppen.

Mittlerweile argumentieren auch vermehrt ehemalige Geheimdienstchefs, dass gemessen an den Kosten, der Nutzen von umfassender Verschlüsselung (ohne Hintertüren) im Zeitalter von Cyber-Kriminalität, Datenlecks und Spionage den Verlust der Überwachungsfähigkeit mehr als aufwiege. Die strategischen Interessen wie die Stabilität des IT-Sektors und des IT-Ökosystems wiegen hier schwerer als die taktischen Interessen der Strafverfolger, so zum Beispiel der ehemalige NSA-Chef Michael Hayden und der ehemalige Chef des britischen Inlandsgeheimdienstes MI5.[9]

Empirischer Erkenntnisstand und Alternativen

Den Eckpunkten der Kryptopolitik folgend hat sich die Bundesregierung im Jahr 1999 entschieden, keine Schwächung der Verschlüsselung (inklusive Einbau von Hintertüren) vorzunehmen, sondern Schadsoftware (“Bundestrojaner”) zur Beschaffung von Daten vor/nach Verschlüsselung einzusetzen. Dieser Maßnahme wurde vom Bundesverfassungsgericht aus nachvollziehbaren Gründen hohe Hürden gesetzt. Anstatt auf Basis der bereits existierenden Überwachungsmaßnahmen eine dringend notwendige Bedarfsanalyse und die bereits vor vielen Jahren vom Bundesverfassungsgericht geforderte

[8] Matthias Schulze: Überwachung von WhatsApp und Co. Going dark?
[9] Michael Hayden: The Pros and Cons of Encryption and The Guardian: Ex-MI5 Chef warns against crackdown on encrypted messaging apps

Überwachungsgesamtrechnung[10] durchzuführen, soll nun eine Regulierung implementiert werden, die mehr als 20 Jahre wissenschaftliche Erkenntnisse in der IT-Sicherheitsforschung ignoriert[11].

Die oft angeführte These, dass Geheimdienste und Strafverfolgungsbehörden aufgrund von Verschlüsselung keinen Zugriff mehr auf relevante Daten haben (*Going Dark*), ist bisher nicht empirisch belegt.[12] Im Gegenteil haben die technologischen Entwicklungen der letzten Jahrzehnte dazu geführt, dass Strafverfolger:innen mehr Daten zur Verfügung stehen als je zuvor.[13] Strafverfolgungsbehörden dokumentieren bisher kaum, in wie vielen Fällen verschlüsselte Kommunikation tatsächlich zu einem Erliegen von Ermittlungen geführt hat. Auch liegt keine vollständige Übersicht vor, welche alternativen Möglichkeiten zur Erhebung der notwendigen Daten in Deutschland bereits legal sind und wo sich noch weiße Flecken befinden.[14]

Internationale Spillover-Effekte

Sollte dieser Vorschlag umgesetzt werden, hätte dies auch weit über die deutschen Grenzen hinaus negative Strahlkraft. Autoritäre Staaten würden sich auf diese Regulierung berufen und entsprechende Inhaltsdaten von den Messenger-Betreibern anfordern mit dem Verweis darauf, dass dies in Deutschland - und damit technisch - möglich sei. Hiervon wäre dann die Kommunikation von Menschenrechtsaktivist:innen, Journalist:innen und anderen verfolgten Personengruppen massiv betroffen – Personengruppen, die die deutsche Außen- und Entwicklungshilfepolitik bisher zu schützen versucht hat und jährlich in Milliardenhöhe fördert. Deutschland muss sich seiner Verantwortung in der Welt auch in diesem Bereich bewusst sein. Mit einer bewussten Schwächung von sicheren Messengern würde Deutschland seine außenpolitische Glaubwürdigkeit als Verfechter eines freien und offenen Internets auf Spiel setzen.[15] Das Netzwerkdurchsetzungsgesetz dient hier als mahnendes Beispiel dafür, welche Auswirkung eine deutsche Gesetzgebung in der Welt entfalten kann.[16]

Wirtschaftsstandort Deutschland

Verwaltung, Wirtschaft und Verbraucher:innen müssen sich darauf verlassen können, dass bei der Nutzung digitaler Produkte und Dienstleistungen die Voraussetzungen zum Schutz ihrer Daten und zur Integrität ihrer Systeme erfüllt sind. Gerade für Unternehmen spielt das bei der Wahl ihres Produktionsstandortes eine große Rolle. Sie siedeln sich dort an, wo sie ihre Geschäftsgeheimnisse und Kundendaten geschützt wissen.

---

[10] Constanze Kurz: Überwachungsgesamtrechnung: Vorratsdatenspeicherung ist der Tropfen, der das Fass zum Überlaufen bringt

[11] Danielle Kehl, Andi Wilson, Kevin Bankston: DOOMED TO REPEAT HISTORY? Lessons from the Crypto Wars of the 1990s

[12] Matthias Schulze, Going Dark? Dilemma zwischen sicherer, privater Kommunikation und den Sicherheitsinteressen von Staaten.

[13] Peter Swire, The FBI Doesn't Need More Access: We're Already in the Golden Age of Surveillance und Matthias Schulze: Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016

[14] Sven Herpig: A Framework for Government Hacking in Criminal Investigations

[15] Matthias Schulze: Verschlüsselung in Gefahr und Cathleen Berger: Is Germany (involuntarily) setting a global digital agenda?

[16] Reporter ohne Grenzen: Russland kopiert Gesetz gegen Hassbotschaften

Sabotage und Wirtschaftsspionage verursachten in den Jahren 2016/2017 alleine im Industriesektor einen Schaden von 43 Mrd. Euro.[17] Es ist davon auszugehen, dass eine Schwächung der Verschlüsselung diese Zahlen weiter in die Höhe treibt, da eingebaute Hintertüren auch von ausländischen Nachrichtendiensten und Kriminellen missbraucht werden können. Wenn Deutschland ein innovationsfreundlicher und wettbewerbsfähiger Wirtschaftsstandort sein möchte, müssen technische Hintertüren, die Zugriffe für Dritte ermöglichen, weiterhin ausgeschlossen bleiben.

Dazu kommt, dass Deutschland auch ein Standort für IT-Sicherheitsunternehmen u. a. mit Fokus auf Verschlüsselungstechnologien ist. Die Vertrauenswürdigkeit dieser Unternehmen im Speziellen würde durch das geplante Vorhaben massiv gefährdet. Damit würde Deutschland als Standort für die IT-Sicherheitsindustrie auch als Ganzes geschwächt werden, was den industriepolitischen Zielen Deutschlands und Europas direkt widerspricht.

Wir warnen ausdrücklich vor dem geplanten Vorhaben des Bundesministeriums des Innern, für Bau und Heimat zur Regulierung von Messenger-Diensten und fordern eine sofortige Abkehr von diesem oder ähnlichen politischen Vorhaben auf deutscher wie europäischer Ebene. Darüber hinaus wäre eine offizielle Einschätzung folgender Stellen erforderlich:

- des Bundesministeriums für Wirtschaft und Energie (Fokus: möglicher Schaden für die deutsche Industrie sowie die Digitalwirtschaft)
- des Auswärtigen Amts (Fokus: *Spillover*-Effekte, v. a. in autoritären Staaten, Ansehensverluste Deutschlands als etablierter Rechtsstaat)
- des Bundesministeriums der Justiz und für Verbraucherschutz (Fokus: Vertrauensverlust von Verbraucher:innen)
- und des Bundesamts für Sicherheit in der Informationstechnik (Fokus: Gefährdung der IT-Sicherheit in Deutschland für Staat, Wirtschaft und Gesellschaft)

Mit freundlichen Grüßen

[17] bitkom: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie

UNTERZEICHNENDE (Stand: 13.06.2019 - 17:00 Uhr)

Industrie, Organisationen und Verbände

1. #cnetz e. V.
2. .riess applications gmbh
3. Algoright
4. bitkomplex UG
5. Bits of Freedom
6. Blockchain Bundesverband e. V.
7. Bundesverband Deutsche Startups e. V.
8. Bundesarbeitsgemeinschaft Digitales & Medien von Bündnis'90 / DIE GRÜNEN
9. Bundesverband IT-Sicherheit e. V. (TeleTrusT)
10. Bundesverband mittelständische Wirtschaft (BVMV) Unternehmerverband Deutschlands e. V.
11. Chaos Computer Club e. V. (CCC)
12. Chaos Computer Club Darmstadt e.V.,
13. Chaos Computer Club Hansestadt Hamburg e. V.
14. Chaos Siegen e. V.
15. Chaos Computer Club Schweiz (CCC-CH)
16. Center for Internet and Human Rights (CIHR)
17. CIPHRON GmbH
18. D3 - Defesa dos Direitos Digitais
19. D64 – Zentrum für digitalen Fortschritt e. V.
20. Dataskydd.net
21. Deutsche Vereinigung für Datenschutz (DVD) e. V.
22. dieDatenschützer Rhein Main
23. Digitalcourage e. V.
24. Digitale Gesellschaft e.V. (DigiGes)
25. Digitale Gesellschaft [Schweiz]
26. digitevo GmbH
27. eco Verband der Internetwirtschaft e. V.
28. Electronic Frontier Finland (Effi)
29. epicenter.works - for digital rights
30. ESR Pollmeier GmbH
31. ETES GmbH
32. European Digital Rights (EDRi)
33. eyeo GmbH
34. flipdot e. V.
35. Förderverein Freie Netze Bodensee e.V.
36. Föreningen för Digitala Fri- och Rättigheter (DFRI)
37. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
38. Freifunk Dreiländereck e. V.
39. Frënn vun der Ënn A.S.B.L.
40. Friedrich-Naumann-Stiftung für die Freiheit
41. G DATA Software AG
42. Gesellschaft für Informatik e. V. (GI)
43. GnuPG e. V.
44. Hannover IT e. V

45. Hermes Center for Transparency and Digital Human Rights
46. HK2 Rechtsanwälte
47. Homo Digitalis
48. Human Rights Watch
49. Inhalt.com e. V.
50. Initiative Digitale Freiheit
51. Internet Society, German Chapter (ISOC.DE) e. V.
52. IT-Political Association of Denmark
53. kmb2 Abrechnungszentrum GmbH
54. Kopano GmbH
55. La Quadrature du Net
56. Least Authority TFA GmbH
57. LOAD e.V.
58. LUKi e. V.
59. Michael Wiesner GmbH
60. Mozilla
61. neXenio GmbH
62. Nextcloud GmbH
63. No-Spy e. V.
64. Open Knowledge Foundation (OKF) Deutschland e. V.
65. ownCloud GmbH
66. p≡p foundation
67. Präsidiumsarbeitskreis für Datenschutz und IT-Sicherheit [Gesellschaft für Informatik e. V.]
68. Praemandatum
69. Privacy International (PI)
70. Reporter ohne Grenzen e. V. (ROG)
71. Schwarzes Glück
72. Secomba GmbH
73. Selbstbestimmt.Digital e. V.
74. Stiftung Datenschutz
75. Stiftung Erneuerbare Freiheit
76. Stiftung Neue Verantwortung e. V. (SNV)
77. The Law Technologist
78. Think Tank iRights.Lab
79. TRUSTpact GmbH
80. UN-Hack-Bar e.V.
81. Uniki GmbH
82. Wikimedia Deutschland e. V.
83. Wire
84. Zwiebelfreunde e. V.

Vertreter:innen aus der deutschen und europäischen Wirtschaft, Wissenschaft und Zivilgesellschaft

1. Prof. Dr. Florian Adamsky, Hochschule für Angewandte Wissenschaften Hof*
2. Leon Andrae, Informatiker in Ausbildung
3. Björn Assmann, Informatiker
4. Manuel Atug, Arbeitsgruppe KRITIS und defensivecon.org*
5. Dr. Asli Telli Aydemir, Association of Alternative Informatics*
6. Zahra Rahmani Azad, Universität Köln*
7. Prof. Dr. Andrej Bachmann, Hochschule Hof – University of Applied Sciences*
8. Kai Baumgartner, Privatperson
9. André Behrschmidt, Behrschmidt IT*
10. Thorsten Benner, Global Public Policy Institute*
11. Peter Berlich, Dozent IT Security
12. Michael Binzen, Informatiker
13. Privatdozent Dr.-Ing. Roland Bless, Karlsruher Institut für Technologie (KIT)*
14. Tamas Blummer, IT Unternehmer im Ruhestand
15. Michael Borggräfe, Leibniz-Universität Hannover*
16. Prof. Dr. Achim Brucker, University of Exeter*
17. Danny Bruder, Künstler
18. Dr. Ulf Buermeyer, Gesellschaft für Freiheitsrechte*
19. Prof. Dr. Christina B. Class, Ernst-Abbe-Hochschule Jena*
20. Frédéric Dubois, Internet Policy Review (HIIG)*
21. Daniel Duda, rehm Datenschutz GmbH*
22. Thomas Dullien, optimyze.cloud AG*
23. Lukas Engelhardt, Informatiker in Ausbildung
24. Jörn Erbguth, Legal Tech, Blockchain, Smart Contract and Data Protection Consultant
25. Dennis Felsch, Ruhr-Universität Bochum*
26. MdB a. D. Dr. Ute Finckh-Krämer, Mathematikerin
27. Dr. Michael Friedewald, Fraunhofer ISI und Forum Privatheit*
28. Peter Ganten, Open Source Business Alliance e.V. und Univention GmbH*
29. Kai Gärtner, Informatiker
30. Prof. Dr. Peter Gerwinski, Hochschule Bochum*
31. Matthias Glaser, GLASER -isb cad- Programmiersysteme GmbH*
32. Prof. Dr. Max von Grafenstein LL.M., Universität der Künste Berlin und Alexander von Humboldt Institut für Internet und Gesellschaft*
33. Prof. Dr.-Ing. Ulrich Greveler, Hochschule Rhein-Waal*
34. Raphael Das Gupta, HSR Hochschule für Technik Rapperswil*
35. Patrick Hähnel, Offensive Security und CSIRT KRITIS*
36. Sascha Hanse, Software Architekt
37. Marit Hansen, Informatikerin und Landesbeauftragte für Datenschutz Schleswig-Holstein*
38. Ernst Härtl, Digital4TRESS*
39. Marc Hauer, TU Kaiserslautern*
40. PD Dr. Jessica Heesen, Internationales Zentrum für Ethik in den Wissenschaften und Forum Privatheit*
41. Dr. Marc Herbstritt, Albert-Ludwigs-Universität Freiburg*
42. Prof. Dr. Dominik Herrmann, Universität Bamberg*

43. Marcel Hesselbach, Kommunikationsinformatiker
44. Prof. Dr. Jürgen Heym, Hochschule für Angewandte Wissenschaften Hof*
45. Prof. Dr. Jeanette Hofmann, Alexander von Humboldt Institut für Internet und Gesellschaft*
46. Prof. Dr. Thorsten Holz, Ruhr-Universität Bochum*
47. Mirko Hohmann, Mercator Kolleg für Internationale Aufgaben*
48. Prof. Dr.-Ing. Tibor Jager, Universität Paderborn*
49. Prof. Dr. Martin Johns, Technische Universität Braunschweig*
50. Viktoria Jost, Privatperson
51. Niklas Kahlstadt, Informatiker in Ausbildung
52. Sven Philipp Kalweit, Kalweit ITS GmbH*
53. Dr. Nils Kammenhuber, Unternehmer
54. Prof. Dr. Wolfgang Kleinwächter, Global Commission on Stability in Cyberspace*
55. Sebastian Kliem, Wirtschaftsinformatiker und Politikwissenschaftler
56. Ronja Kniep, Wissenschaftszentrum Berlin für Sozialforschung*
57. Frank Knischewski, DTS Systeme und Hannover IT*
58. Enrico Koltermann, Privatperson
59. Michael Körfer, IT-Security Consultant
60. Michael Kranawetter, Microsoft Deutschland GmbH*
61. Normen Kraner, BADENmgzn.eu*
62. Alexandra Krause, Physikerin
63. Marek Kreul, Forensik und Incident Response Spezialist
64. Caroline Krohn, VINDLER GmbH*
65. Jens Kühn, Privatperson
66. Prof. Dr. Herbert Kuchen, Universität Münster*
67. Henning Christian Lahmann, Völkerrechtler
68. Paula Landes, Digital Media Women e.V. / Rhein-Main*
69. Prof. Dr. Tanja Lange, Eindhoven University of Technology*
70. Daniel Lengies, Michael Wessel Informationstechnologie GmbH*
71. Torsten Lengies-Nalasek, Informatiker
72. Bundesministerin a. D. Sabine Leutheusser-Schnarrenberger, Friedrich-Naumann-Stiftung für die Freiheit*
73. Prof. Dr. Klaus-Peter Löhr, Freie Universität Berlin*
74. Daniel Lücking, Journalist
75. Niels Mache, Struktur AG und Nextcloud GmbH*
76. Konstantin Macher, Queen's University Belfast*
77. Klaus Marwede, Datenschutzbeauftragter*
78. Prof. Dr.-Ing. Peter Merz, Hochschule Hannover*
79. Natanael Mignon, Informatiker
80. Staatssekretär Digitalisierung Stefan Muhle, Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung*
81. Dr. Bettina Müller LL.M. - Privatgelehrte
82. Prof. Dr. Claudia Müller-Birn, Freie Universität Berlin*
83. Dr. Michael Münch, Informatiker und m-cubed.de*
84. Dr. Michael Naehrig, Microsoft*
85. Maxi Nebel, Universität Kassel*
86. Dr. Peter Neuhaus, Informatiker
87. Prof. Dr. Karl-Heinz-Niemann, Hochschule Hannover*

88. Dr.-Ing. Stefan Nürnberger, CISPA Helmholtz Center for Information Security und Universität des Saarlandes*
89. Amadeus Peters, Alexander von Humboldt Institut für Internet und Gesellschaft*
90. Dr. Jörg Pohle, Alexander von Humboldt Institut für Internet und Gesellschaft*
91. Dr. Julia Pohle, Wissenschaftszentrum Berlin für Sozialforschung*
92. Dirk Pohlscheidt, MIT-Troisdorf und MEDIATA GmbH*
93. Prof. Dr. Lutz Prechelt, Freie Universität Berlin*
94. Claas Reiner, Privatperson
95. Ralf Reinhardt, Technische Hochschule Nürnberg und Technische Hochschule Deggendorf*
96. Thomas Reinhold, cyber-peace.org*
97. Marcus Richter, Journalist
98. Tim Richter, Internet Governance Forum Deutschland und Deutsche Gesellschaft für die Vereinten Nationen e.V. (DGVN)*
99. Ulf Riechen, Berater Informationssicherheit für KRITIS-Unternehmen und Informationssicherheitsbeauftragter*
100. Prof. Dr. Konrad Rieck, Technische Universität Braunschweig*
101. Raymond Roemke, Bildjournalist
102. Anne Roth, Referentin für Netzpolitik
103. Prof. Dr.-Ing. Volker Roth, Freie Universität Berlin*
104. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D. Peter Schaar, Europäische Akademie für Informationsfreiheit und Datenschutz (EAID)*
105. Tim Philipp Schäfers, Internetwache.org*
106. Robert Scheck, Informatiker
107. Alexander Scheel, ArkonIT Consulting*
108. Prof. Dr. Jörg Scheidt, Hochschule für Angewandte Wissenschaften Hof*
109. Dr. Florian Scheuer, Informatiker
110. Prof. Dr. Björn Scheuermann, Alexander von Humboldt Institut für Internet und Gesellschaft und Humboldt-Universität zu Berlin*
111. Jan Hendrik Scheufen, Monax*
112. Prof. Dr. Sebastian Schinzel, Fachhochschule Münster*
113. Dr. Annette Schaper, Leibniz-Institut Hessische Stiftung Friedens- und Konfliktforschung (HSFK)*
114. Dr. Thomas Schmaltz, Ingenieur und Innovationsforscher
115. Kai Schmidt, IT-Consultant und PenTester
116. Stephan Schmidt, Rechtsanwalt
117. Christian Schmitz, ownCloud Foundation / Up2University.eu*
118. Detlef Schmitz, Oberarzt
119. Prof. Dr. Johannes Schöning, Universität Bremen*
120. Phillipp Schoppmann, Humboldt-Universität Berlin*
121. Alfred Schröder, Open Source Business Alliance e.V. und GONICUS GmbH*
122. Dr. Matthias Schulze, Stiftung Wissenschaft und Politik (SWP)*
123. Stefan Schumacher, Informatiker
124. Daniel Schwerd, Informatiker und IT-Unternehmer
125. Sergio Siccha, Mathematiker und Informatiker
126. Matthias Spielkamp, AlgorithmWatch*
127. Isabel Skierka, Politikwissenschaftlerin
128. Gero Sprafke, MBSR-Trainer

129. Stephan Springer, IT-Beratung Springer*
130. MdA Dirk Stettner, Mitglied des Abgeordnetenhauses von Berlin*
131. Peter Birko Stich, Informatiker und Sachverständiger IT-Security / IT-Forensic
132. Michael Stresau, Universitätsmedizin Main*
133. Jan A. Strunk, Rechtsanwalt und Externer Datenschutzbeauftragter
134. Prof. Dr.-Ing. Robert Tolksdorf, Informatiker
135. Sven Uckermann, PenTester und IT-Security Experte
136. Steffen Unger, Hochschule für Angewandte Wissenschaften Hof*
137. Wolfram Volke, Heimrich & Hanot GmbH*
138. Dr. Ben Wagner, Vienna University of Economics and Business*
139. Kai Wagner, Jolocom GmbH*
140. Sebastian Walk, Verfahrensmechaniker
141. Sebastian Wiesendahl, Informatiker
142. Benedikt Wildenhain, Hochschule Bochum*
143. Martin Wolf, IT-Consultant und Autor
144. Prof. Dr. Andreas Zeller, CISPA Helmholtz Center for Information Security und Universität des Saarlandes*
145. Philip Zimmermann, Pretty Good Privacy (PGP) und Delft University*
146. Peter Zoche, Freiburger Institut für angewandte Sozialwissenschaft e. V.*
147. Christoph Zurheide, Deutsche Post DHL Group*

*ZUGEHÖRIGKEITEN DIENEN AUSSCHLIEßLICH DER BESSEREN ZUORDNUNG

Abgeordnete des Deutschen Bundestags

1. MdB Dr. Danyal Bayaz, Bündnis 90/Die Grünen
2. MdB Anke Domscheit-Berg, DIE LINKE.
3. MdB Saskia Esken, SPD
4. MdB Manuel Höferlin, FDP
5. MdB Andrej Hunko, DIE LINKE.
6. MdB Dieter Janecek, Bündnis 90/Die Grünen
7. MdB Dr. Konstantin von Notz, Bündnis 90/Die Grünen
8. MdB Konstantin Kuhle, FDP
9. MdB Tabea Rößner, Bündnis 90/Die Grünen
10. MdB Jimmy Schulz, FDP
11. MdB Dr. Petra Sitte, DIE LINKE.