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 zu 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

---

[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

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*).

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

---

[7] Es handelt sich hierbei um eine mögliche Implementierung dieser Hintertüren. Es gibt auch andere Implementierungsmöglichkeiten, die technisch jedoch nicht weniger problematisch sind.
[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

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 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

[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

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.

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)

---

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

Mit freundlichen Grüßen

Cathleen Berger
Lead, Global Governance and Policy Strategy

Mozilla
Schlesische Straße 27
10997 Berlin

UNTERZEICHNENDE (Stand: 12.06.2019 - 8:45 Uhr)

Industrie, Organisationen und Verbände

1. #cnetz e. V.
2. Bits of Freedom
3. Bundesverband IT-Sicherheit e. V. (TeleTrusT)
4. Bundesverband mittelständische Wirtschaft (BVMV) Unternehmerverband Deutschlands e. V.
5. Chaos Computer Club e. V. (CCC)
6. Chaos Computer Club Hansestadt Hamburg e. V.
7. Chaos Siegen e. V.
8. Chaos Computer Club Schweiz (CCC-CH)
9. Center for Internet and Human Rights (CIHR)
10. CIPHRON GmbH
11. D3 - Defesa dos Direitos Digitais
12. D64 – Zentrum für digitalen Fortschritt e. V.
13. Dataskydd.net
14. Deutsche Vereinigung für Datenschutz (DVD) e. V.
15. Digitalcourage e. V.
16. Digitale Gesellschaft e.V. (DigiGes)
17. Digitale Gesellschaft [Schweiz]
18. digitevo GmbH
19. eco Verband der Internetwirtschaft e. V.
20. Electronic Frontier Finland (Effi)
21. epicenter.works - for digital rights
22. European Digital Rights (EDRi)
23. eyeo GmbH
24. Föreningen för Digitala Fri- och Rättigheter (DFRI)
25. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
26. Frënn vun der Ënn A.S.B.L.
27. Friedrich-Naumann-Stiftung für die Freiheit
28. G DATA Software AG
29. Gesellschaft für Informatik e. V. (GI)
30. Hannover IT e. V
31. Hermes Center for Transparency and Digital Human Rights
32. HK2 Rechtsanwälte
33. Homo Digitalis
34. Human Rights Watch
35. Inhalt.com e. V.
36. Internet Society, German Chapter (ISOC.DE) e. V.
37. IT-Political Association of Denmark
38. kmb2 Abrechnungszentrum GmbH
39. La Quadrature du Net

40. Least Authority TFA GmbH
41. LOAD e.V.
42. Michael Wiesner GmbH
43. Mozilla
44. Nextcloud GmbH
45. No-Spy e. V.
46. Open Knowledge Foundation (OKF) Deutschland e. V.
47. ownCloud GmbH
48. p≡p foundation
49. Präsidiumsarbeitskreis für Datenschutz und IT-Sicherheit [Gesellschaft für Informatik e. V.]
50. Praemandatum
51. Privacy International (PI)
52. Reporter ohne Grenzen e. V. (ROG)
53. Schwarzes Glück
54. Stiftung Erneuerbare Freiheit
55. Stiftung Neue Verantwortung e. V. (SNV)
56. The Law Technologist
57. Think Tank iRights.Lab
58. UN-Hack-Bar e.V.
59. Wikimedia Deutschland e. V.
60. Wire
61. 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. Björn Assmann, Informatiker
3. Manuel Atug, Arbeitsgruppe KRITIS*
4. Dr. Asli Telli Aydemir, Association of Alternative Informatics*
5. André Behrschmidt, Behrschmidt IT*
6. Thorsten Benner, Global Public Policy Institute*
7. Danny Bruder, Künstler
8. Dr. Ulf Buermeyer, Gesellschaft für Freiheitsrechte*
9. Frédéric Dubois, Internet Policy Review (HIIG)*
10. Thomas Dullien, optimyze.cloud AG*
11. Dr. Michael Friedewald, Fraunhofer ISI und Forum Privatheit*
12. Peter Ganten, Open Source Business Alliance e.V. und Univention GmbH*
13. Kai Gärtner, Informatiker
14. Matthias Glaser, GLASER -isb cad- Programmiersysteme GmbH*
15. Prof. Dr.-Ing. Ulrich Greveler, Hochschule Rhein-Waal*
16. Raphael Das Gupta, HSR Hochschule für Technik Rapperswil*

17. Marit Hansen, Informatikerin und Landesbeauftragte für Datenschutz Schleswig-Holstein*
18. PD Dr. Jessica Heesen, Internationales Zentrum für Ethik in den Wissenschaften und Forum Privatheit*
19. Prof. Dr. Jeanette Hofmann, Alexander von Humboldt Institut für Internet und Gesellschaft*
20. Mirko Hohmann, Mercator Kolleg für Internationale Aufgaben*
21. Viktoria Jost, Privatperson
22. Sven Philipp Kalweit, Kalweit ITS GmbH*
23. Prof. Dr. Wolfgang Kleinwächter, Global Commission on Stability in Cyberspace*
24. Ronja Kniep, Wissenschaftszentrum Berlin für Sozialforschung*
25. Frank Knischewski, DTS Systeme und Hannover IT*
26. Marek Kreul, Forensik und Incident Response Spezialist
27. Caroline Krohn, VINDLER GmbH*
28. Henning Christian Lahmann, Völkerrechtler
29. Daniel Lengies, Michael Wessel Informationstechnologie GmbH*
30. Torsten Lengies-Nalasek, Informatiker
31. Bundesministerin a. D. Sabine Leutheusser-Schnarrenberger, Friedrich-Naumann-Stiftung für die Freiheit*
32. Prof. Dr. Klaus-Peter Löhr, Freie Universität Berlin*
33. Klaus Marwede, Datenschutzbeauftragter*
34. Prof. Dr.-Ing. Peter Merz, Hochschule Hannover*
35. Natanael Mignon, Informatiker
36. Staatssekretär Digitalisierung Stefan Muhle, Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung*
37. Dr. Bettina Müller LL.M. - Privatgelehrte
38. Prof. Dr. Claudia Müller-Birn, Freie Universität Berlin*
39. Maxi Nebel, Universität Kassel*
40. Prof. Dr. Karl-Heinz-Niemann, Hochschule Hannover*
41. Amadeus Peters, Alexander von Humboldt Institut für Internet und Gesellschaft*
42. Dr. Jörg Pohle, Alexander von Humboldt Institut für Internet und Gesellschaft*
43. Prof. Dr. Lutz Prechelt, Freie Universität Berlin*
44. Tim Richter, Internet Governance Forum Deutschland und Deutsche Gesellschaft für die Vereinten Nationen e.V. (DGVN)*
45. Thomas Reinhold, cyber-peace.org*
46. Ulf Riechen, Berater Informationssicherheit für KRITIS-Unternehmen und Informationssicherheitsbeauftragter*
47. Prof. Dr.-Ing. Volker Roth, Freie Universität Berlin*
48. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D. Peter Schaar, Europäische Akademie für Informationsfreiheit und Datenschutz (EAID)*
49. Alexander Scheel, ArkonIT Consulting*
50. Prof. Dr. Björn Scheuermann, Alexander von Humboldt Institut für Internet und Gesellschaft und Humboldt-Universität zu Berlin*

51. Dr. Thomas Schmaltz, Ingenieur und Innovationsforscher
52. Christian Schmitz, ownCloud Foundation / Up2University.eu*
53. Phillipp Schoppmann, Humboldt-Universität Berlin*
54. Dr. Matthias Schulze, Stiftung Wissenschaft und Politik (SWP)*
55. Stefan Schumacher, Informatiker
56. Sergio Siccha, Mathematiker und Informatiker
57. Matthias Spielkamp, AlgorithmWatch*
58. Isabel Skierka, Politikwissenschaftlerin
59. Stephan Springer, IT-Beratung Springer*
60. Prof. Dr.-Ing. Robert Tolksdorf, Informatiker
61. Sven Uckermann, Pentester und IT-Security Experte
62. Dr. Ben Wagner, Vienna University of Economics and Business*
63. Peter Zoche, Freiburger Institut für angewandte Sozialwissenschaft e. V.*
64. Christoph Zurheide, Deutsche Post DHL Group*
65. Philip Zimmermann, Pretty Good Privacy (PGP) und Delft University*

*ZUGEHÖRIGKEITEN DIENEN AUSSCHLIEßLICH DER BESSEREN ZUORDNUNG

Möchten Sie diesen offenen Brief als Unterzeichner:in unterstützen?
Senden Sie eine Email an sherpig@stiftung-nv.de