GESELLSCHAFT
FÜR INFORMATIK

Berlin, 9. Dezember 2020

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

zum Recht auf Verschlüsselung

Keine digitalen Nachschlüssel für Sicherheitsbehörden und Organisierte Kriminalität

Die Gesellschaft für Informatik (GI) fordert den zuständigen Bundesinnenminister Horst Seehofer der Bundesregierung als amtierende Ratsvorsitzende der Europäischen Union nachdrücklich auf, für ein starkes europäisches „Recht auf Verschlüsselung" einzutreten und sich vehement gegen eine Schwächung der (Ende-zu-Ende)-Verschlüsselung durch Nachschlüssel auszusprechen. Die Bekämpfung der internationalen Kriminalität (z.B. Terrorismus) darf nicht auf Kosten der Sicherheit der Nutzerinnen und Nutzer (Bürger, Unternehmen und Behörden) gehen.

Auch die Europäische Kommission und das Parlament sind aufgerufen, sich für den europäischen Datenschutz einzusetzen. Mit der Allgemeinen Datenschutzverordnung (GDPR) ist es der EU in den letzten Jahren gelungen, einen Standortvorteil für die europäische digitale Wirtschaft zu schaffen und die Grundlagen für ihre technologische Souveränität zu legen. Zum Beispiel wurden mit Art. 32 der GDPR speichernde Stellen ausdrücklich dazu verpflichtet, „personenbezogene Daten zu verschlüsseln".

Die Annahme, Terrorismus und andere Schwerkriminalität nur mit Hintertüren in verschlüsselten Kommunikationsdiensten bekämpfen zu können ist eine Illusion. Dies zeigen auch die jüngsten Auswertungen in Frankreich, Österreich, Deutschland.

Wer die Verschlüsselung schwächt, schwächt die IT-Sicherheit und damit die Souveränität als Ganzes. Ein „Master Key", wie er vom Ministerrat gefordert wird, untergräbt im Übrigen das Vertrauen in Verschlüsselung und gefährdet das Wachstum der europäischen IKT-Industrie und die europäische Technologiesouveränität. Kriminelle können natürlich auf Dienste ausweichen, die mit EU-Gesetzen gar nicht erreichbar sind, und Verschlüsselungsprodukte ohne einen solchen Master Key nutzen.

Hintergrund[1]

Auf Anregung der „Five Eyes"[2] bereiten die Regierungen der EU-Länder derzeit im Ministerrat eine Resolution mit dem Titel „Entwurf einer Entschließung des Rates über Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung"[3] vor. Sie zeigt deutliche Ähnlichkeit mit früheren Initiativen, die

1 Keys under doormats: mandating insecurity by requiring government access to all data and communications, Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter and Daniel J. Weitzner; Journal of Cybersecurity, 1(1), 2015, 69–79, DOI: 10.1093/cybsec/tyv009; https://academic.oup.com/cybersecurity/article/1/1/69/2367066

2 Abkommen zur weltweiten Überwachung elektronischer Kommunikation zwischen den USA und Großbritannien zur nachrichtendienstlichen Zusammenarbeit; später erweitert auf Australien, Kanada und Neuseeland (5 Eyes); beigetreten sind später Deutschland, Frankreich, Israel, Schweden, Italien, Japan, Norwegen, Südkorea, Türkei.

3 Council document 12143/1/20 REV1 "Draft Council Resolution on Encryption-Security through encryption and security despite encryption" https://www.heise.de/downloads/18/2/9/9/8/5/2/0/783284_fh_st12143-re01en20_783284.pdf, earlier version on https://www.heise.de/downloads/18/2/9/9/8/5/2/0/eu-council-draft-

Anbieter verschlüsselter Ende-zu-Ende-Kommunikation zwingen wollten, einen „Hauptschlüssel“ (Nachschlüssel) bereitzustellen, um „zuständigen Behörden“ den Zugang zu elektronischen Beweismitteln zu ermöglichen[4, 5].

Der Entwurf erklärt: „Die Europäische Union unterstützt voll und ganz die Entwicklung, Umsetzung und Verwendung starker Verschlüsselung. Die Verschlüsselung ist ein notwendiges Mittel zum Schutz der Grundrechte und der digitalen Sicherheit von Regierungen, Industrie und Gesellschaft. Gleichzeitig muss die Europäische Union die Fähigkeit der zuständigen Behörden im Bereich der Sicherheit und des Strafrechts, z.B. der Strafverfolgungs- und Justizbehörden, gewährleisten, ihre rechtmäßigen Befugnisse sowohl online als auch offline auszuüben. „Der Schutz der Privatsphäre und der Sicherheit der Kommunikation durch Verschlüsselung und gleichzeitig die Aufrechterhaltung der Möglichkeit für die zuständigen Behörden im Bereich der Sicherheit und des Strafrechts, rechtmäßig auf relevante Daten für legitime, klar definierte Zwecke bei der Bekämpfung schwerer und/oder organisierter Kriminalität und des Terrorismus, auch in der digitalen Welt, zuzugreifen, sind äußerst wichtig. Alle Maßnahmen müssen diese Interessen sorgfältig gegeneinander abwägen“[6].

Doch während das Grundrecht auf Verschlüsselung für die Demokratien Europas unverzichtbar ist – so wie es das Post- und Telefongeheimnis in der analogen Welt war – lässt sich vertrauliche Kommunikation erfahrungsgemäß weder mit einem Generalschlüssel oder Nachschlüssel noch mit einem Verschlüsselungsverbot wirksam verhindern. Darüber hinaus eröffnen Hintertüren und verdeckte Kanäle einen ständigen Zugang für Sicherheitsbehörden und binnen Kurzem dann auch für die Organisierte Kriminalität. Kriminelle könnten darüber hinaus auf eigene Produkte mit unbeobachtbarer Kommunikation ausweichen.

Bereits Anfang der 1990er Jahre wollte die US-Regierung die internationale Nutzung US-amerikanischer Verschlüsselungsprodukte verbieten und verlangte von den Herstellern die Hinterlegung benutzter Schlüssel (Key Recovery[7]). Dies verhinderte zwar nicht die Verbreitung von Verschlüsselungssoftware, z. B. „Pretty Good Privacy“ (PGP)[8] –

declaration-against-encryption-12143-20.pdf, some background on https://blog.lukaszolejnik.com/the-policy-of-security-despite-encryption/

4 How a Crypto 'Backdoor' Pitted the Tech World Against the NSA, WIRED, https://www.wired.com/2013/09/nsa-backdoor/

5 Backdoors – A Few Thoughts on Cryptographic Engineering, Matthew Green, https://blog.cryptographyengineering.com/category/backdoors/

6 How a Crypto 'Backdoor' Pitted the Tech World Against the NSA, WIRED, https://www.wired.com/2013/09/nsa-backdoor/

7 Enterprise Key Recovery. Vertrauenswürdige Server mit skalierbarer Sicherheit zur Archivierung von Konzelationsschlüsseln. Pohl, H.; Cerny, D. Informatik Spektrum 22: 110-121 (1999) https://www.researchgate.net/publication/220351529_Enterprise_Key_Recovery_Vertrauenswurdige_Server_mit_skalierbarer_Sicherheit_zur_Archivierung_von_Konzelationsschlusseln

8 Why I Wrote PGP?, Philip Zimmermann, https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

verhinderte aber den Einsatz überlanger Schlüssel in diesem Produkt und schwächte so insgesamt die Möglichkeiten vertraulicher Kommunikation.

Die weltweite Initiative der Sicherheitsbehörden gefährdet nicht nur die informationelle Selbstbestimmung der EU-Bürger, sondern auch den Schutz von Betriebs- und Geschäftsgeheimnissen deutscher und europäischer Unternehmen und damit die dringend notwendige Digitalisierung der europäischen Wirtschaft. Hinzu kommt die Notwendigkeit einer zuverlässigen, vertraulichen Kommunikation für die politische Willensbildung und die Schaffung einer freien Gesellschaft, die durch eine solche Schwächung der Verschlüsselung ebenfalls gefährdet werden.

Die Verschlüsselung trägt dazu bei, die Werte auf unseren IKT-Systemen angemessen zu schützen und damit in eine sichere und vertrauenswürdige digitale Zukunft zu gehen. Eine Schwächung der Verschlüsselung bedeutet eine Gefährdung der Digitalisierung in der EU. Deshalb ist es wichtig, das Vertrauen in die IKT zu fördern – und nicht zu verringern.

Technische Illusion

Die „Balance", die Verschlüsselung sicher und gleichzeitig offiziell brechbar zuzulassen, ist eine Illusion. Und aus kryptographischer Sicht gibt es keine „guten" oder „schlechten" Angreifer. Daher sind sich die zuständigen Cybersicherheitsbehörden einig, dass und absichtlich eingebaute Hintertüren in eine ursprünglich starke Verschlüsselungstechnologie den Prinzipien der Kryptographie völlig widersprechen – sichere (starke) Verschlüsselung bedeutet, dass nur diejenigen die Daten kontrollieren, die auf sie zugreifen können[9, 10]. Den Sicherheitsbehörden stehen bereits jetzt Werkzeuge wie Online-Trojaner zur Verfügung, die ihnen einen vollständigen Einblick in die verschlüsselte Kommunikation am jeweiligen Endpunkt geben.

Im Entwurf des Vorschlags des Europäischen Rates wird nicht angegeben, wie die Zugriffswerkzeuge und die abgerufenen Daten geschützt werden sollen. Der Schutz solcher Tools und der abgerufenen Daten ist jedoch ein sehr sensibles Thema, da viele Parteien daran interessiert sein dürften. Im digitalen Bereich bieten Sicherheitslücken wie Hintertüren und verdeckte Kanäle - anders als im analogen Bereich – die Zugriffsmöglichkeit auch auf alle anderen gespeicherten Daten. Dies ist z. B. in sozialen Netzwerken relevant. Dies bietet also die Möglichkeiten für den unkontrollierten Zugriff unzähliger Verbraucher und Sicherheitsbehörden aus dem In- und Ausland auf die Kommunikation zwischen deutschen und EU-Bürgern und Unternehmen. Eine

9 The Importance of Strong Encryption to Security, Bruce Schneier, Schneier on Security, https://www.schneier.com/blog/archives/2016/02/the_importance_.html

10 ENISA's Opinion Paper on Encryption: Strong Encryption Safeguards our Digital Identity, European Union Agency for Network and Information Security (ENISA), https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption

Schwächung oder gar Beseitigung einer angemessenen Verschlüsselung gefährdet eine große Zahl privater, kommerzieller und behördlicher Nutzer – unter sehr vielen anderen auch Journalisten und Menschenrechtsaktivisten.

Lösungen mit Hintertüren, Generalschlüssel oder Nachschlüssel widersprechen dem „Stand der Technik“ und gefährden den (liberalen) Rechtsstaat. Wenn Nachschlüssel in „falsche Hände“ geraten, würde dies zu einer Katastrophe führen. Die Beseitigung starker Ende-zu-Ende-Verschlüsselung schafft Sicherheitslücken, die nicht nur von deutschen und EU-Behörden genutzt werden, sondern auch von jedem anderen – einschließlich Hackern, Cyberkriminellen und ausländischen Regierungen inklusive kommerzieller Unternehmen – mit der technischen Fähigkeit, diese absichtlich geschaffenen Hintertüren zu nutzen, missbraucht werden können.

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist mit rund 20.000 persönlichen und 250 korporativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum und vertritt seit 1969 die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Gesellschaft und Politik. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.