Kurzinformation
Zum Brechen oder Umgehen von Ende-zu-Ende-Verschlüsselungen

1. Einleitung

Am 24. Juli 2020 präsentierte die Europäische Kommission die EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs von Kindern[1] als eine ihrer Sofortinitiativen zur Umsetzung der Strategie für die Sicherheitsunion.[2] Mittels dieser Strategie soll der sexuelle Missbrauch von Kindern[3] effizienter bekämpft werden.

Auf einer Informationsseite der Europäischen Union heißt es zum Hintergrund, in den letzten Jahren sei in der EU ein dramatischer Anstieg des sexuellen Missbrauchs von Kindern festgestellt worden.[4] Das Nationale Zentrum für vermisste und ausgebeutete Kinder der USA stelle einen Anstieg in der EU von 23.000 Berichte über sexuellen Kindesmissbrauch im Jahr 2010 auf mehr als 725.000 im Jahr 2019 fest. Darunter fänden sich mehr als 3 Millionen Bilder und Videos. Einen ähnlichen Anstieg stellt man weltweit fest: von einer Million Berichte im Jahr 2010 auf fast 17 Millionen im Jahr 2019, einschließlich fast 70 Millionen Bilder und Videos. Die überwiegende Mehrheit dieser Berichte stammten aus elektronischer Kommunikation.[5]

Auf den Internetseiten des Magazins „Politico“ ist ein Arbeitspapier zu finden, das technische Lösungen zur Detektion von sexuellem Kindesmissbrauch in Ende-Zu-Ende verschlüsselten

1 European Commission: EU strategy for a more effective fight against child sexual abuse; COM(2020) 607 final; https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf.

2 https://ec.europa.eu/commission/presscorner/detail/de/IP_20_1380.

3 European Commission: EU strategy for a more effective fight against child sexual abuse; COM(2020) 607 final; https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf.

4 https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1381.

5 Ebd.

WD 8 - 3000 – 089/20 (2. Dezember 2020)

Kommunikationsformen darstellt. Die Autoren und das Verfasserdatum sind unbekannt. Das Dokument wurde nicht von der Europäischen Kommission angenommen oder gebilligt und dient als Diskussionsgrundlage.[6] In der vorliegenden Kurzinformation werden zunächst die Einschätzungen von Wissenschaftlern zweier Forschungseinrichtungen (Ruhr-Universität Bochum und Technische Universität Dresden (TU Dresden)) zu diesem Diskussionspapier unter Berücksichtigung der Fragen nach den Unterschieden der angesprochenen Methoden und der Übertragbarkeit auf andere kriminelle Taten dargestellt. Im Anschluss wird auf das laufende Forschungsprojekt KISTRA der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) eingegangen.

2. Informationen einzelner wissenschaftlicher Einrichtungen

Nach Einschätzung von Wissenschaftlern sowohl der Ruhr-Universität Bochum[7] als auch der TU Dresden[8] liegt ein zentrales Problem des Diskussionsgrundlagen-Papiers „Technical solution to detect child abuse in end-to-end encrypted communications“ darin, dass die benannten methodischen Darstellungen nicht auf die tatsächlichen Implementierungen von Messenger-Diensten eingingen. Laut des Wissenschaftlers der TU Dresden unterschieden sich zwar die Methoden darin, wie datenschutzfreundlich sie seien; allerdings gingen alle davon aus, dass in gewisser Weise der Nutzer „mitspiele“, was bei bewussten kriminellen Vorgängen fraglich sein könne. Alle Methoden schließen das Gerät des Nutzers ein, von dem Informationen ausgesendet werde. Dabei sei zu erwarten, dass technisch Versierte dies umgehen werden. Damit ein Lösungsansatz in der Praxis sich bewähre, müssten Umgehungsmaßnahmen ausgeschlossen werden.

Der Wissenschaftler der Ruhr-Universität Bochum unterscheidet drei Kategorien von Messenger-Diensten in dem Papier:

(1) Dies seien zum einen unverschlüsselte Messenger-Dienste. Prinzipiell könnten hier die Strafverfolgungsbehörden an jeder ihr zugänglichen Datenverbindung mitlesen. Von den Internetanbietern könnten hier aufgrund einer zu schaffenden gesetzlicher Grundlage Abhörschnittstellen gefordert werden (wie es dies im Mobilfunk schon gibt).
(2) Bei nicht Ende-zu-Ende-verschlüsselten Messenger-Diensten (nur Transportverschlüsselung) bestünde bei Schaffung einer gesetzlichen Grundlage technisch ebenfalls die Möglichkeit, Abhörschnittstellen vom Anbieter des Dienstes zu fordern.
(3) Bei den Ende-zu-Ende-verschlüsselte Messenger kann der Anbieter nur Metainformationen (z.B. wer kommuniziert mit wem) liefern. Er kennt aber die übertragenen Daten selbst nicht. In dem Papier würden dazu zwei verschiedene Lösungsansätze angeboten: 1. Spionagesoftware auf Endgeräten oder 2. Einsatz homomorpher Verschlüsselung für E2EE. Der erste Ansatz (Spionagesoftware) entspreche ungefähr dem Einsatz des 'Bundestrojaners', der im Verdachtsfall auf das Endgerät eines Verdächtigen aufgebracht würde. Es würde vorgeschlagen, Hashwerte von Bildern an einen zentralen Server zu übertragen und dort mit einer Liste 'verbotener' Hashwerte zu vergleichen. Als Nachteile wird geäußert, dass prinzipiell alle Nutzer der Dienste unter Generalverdacht gestellt würden, Kriminelle nur

6 https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf.

7 Persönliche Auskunft aus der Ruhr-Universität Bochum vom 23. November 2020.

8 Persönliche Auskunft aus der TU Dresden vom 19. November 2020.

minimale Bildveränderungen veranlassen müssten, um es gegen Erkennung zu schützen und Diensteanbieter eine Fülle neuer Informationen über ihre Nutzer erhielten da alle Bilder als Hashwerte an den Anbieter übertragen werden. Der zweite Ansatz (Homomorphe Verschlüsselung) sei sehr rechenaufwändig und werde derzeit im Messenger-Umfeld nicht eingesetzt. Es bleibe in dem Papier unklar, wie durch diesen Ansatz im Detail das angestrebte Ziel erreicht werden solle.

Prinzipiell seien Lösungsansätze durchaus von dem benannten Bereich des Kindermissbrauchs auf andere Kriminalfelder zu übertragen. Allerdings stelle sich die Frage – so der Wissenschaftler der TU Dresden – inwiefern sich andere Delikte automatisiert beurteilen ließen. Während Bilder recht gut automatisiert zu beurteilen seien, sei ggf. bei anderen Delikten eine Schlüsselwort-Listung notwendig oder auch andere Instrumente.[9]

3. Informationen der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)

Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) ist eine nicht rechtsfähige Bundesanstalt im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat und als Dienstleister für die Sicherheitsbehörden in Deutschland tätig. Die ZITiS wurde am 6. April 2017 im Erlasswege errichtet.[10] Die Arbeitsfelder des ZITiS erstrecken sich über die Bereiche „Digitale Forensik“, „Telekommunikationsüberwachung“, Kryptoanalyse“ und „Big Data Analyse“.

Seit Juli 2020 läuft am ZITiS das Forschungsprojekt KISTRA (Einsatz von KI zur Früherkennung von Straftaten). Ziel dieses Projekts ist „die Erforschung der Möglichkeiten und Rahmenbedingungen für den ethisch und rechtlich vertretbaren Einsatz von Künstlicher Intelligenz durch Sicherheitsbehörden zur frühzeitigen Erkennung und Prävention von Straftaten der Hasskriminalität.“

Das ZITiS schreibt zur Durchführung der Forschungsarbeit: „An dem dreijährigen Projekt beteiligt sich ein Konsortium aus neun Partnern, geleitet von der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS). KISTRA zeichnet sich durch die interdisziplinäre Einbindung von Wissenschaft, Wirtschaft und Endanwendern aus. Neben ZITiS und dem Bundeskriminalamt (BKA), das zugleich Partner und Endanwender ist, sind sieben weitere Partner am Projekt beteiligt: die Johannes Gutenberg-Universität Mainz, die Ludwig-Maximilians-Universität München, Munich Innovation Labs GmbH, die RWTH Aachen University, die Technische Universität Berlin, die Technische Universität Darmstadt und die Universität Duisburg-Essen. Das Forschungsprojekt verfügt über ein Gesamtbudget von 2,98 Millionen Euro.

Die Ergebnisse von KISTRA werden sowohl sozialwissenschaftliche, ethische und rechtliche Gutachten umfassen sowie technische Lösungen, zum Beispiel Softwaredemonstratoren. Neben der direkten Anwendung beim BKA können auch weitere Behörden mit Sicherheitsaufgaben von den Ergebnissen profitieren: einerseits über die Funktion der ZITiS als zentrale Stelle mit dem

9 Ebd.

10 Der Errichtungserlass ist im gemeinsamen Ministerialblatt der Bundesministerien am 20.4.2017 veröffentlicht (GMBl Nr.15, 2017, Seite 274, ISSN 0939-4729).

Auftrag, die deutschen Sicherheitsbehörden durch die Erforschung und Entwicklung von Werkzeugen im digitalen Raum zu unterstützen, andererseits über die Zentralstellenfunktion des BKA für die Polizeien des Bundes und der Länder.

Das Vorhaben fußt auf der „Schutz vor Kriminalität und Terrorismus“-Initiative des nationalen Sicherheitsforschungsprogrammes beim Bundesministerium für Bildung und Forschung (BMBF) und will die Entwicklung rechtskonformer KI und Verfahren zur Erfassung und Bewertung sicherheitsrelevanter Inhalte im Internet voranbringen.

KISTRA erforscht die mögliche Anwendung von KI in Sicherheitsbehörden in einem ganzheitlichen Ansatz. Zu den übergeordneten Zielen gehören unter anderem:

- die Betrachtung der Rechtmäßigkeit und der ethischen Vertretbarkeit der angestrebten KI-Lösungen und daraus resultierender Methoden für Sicherheitsbehörden,
- die Erkennung und sozialwissenschaftliche Betrachtung politisch motivierter Hassreden und „Hasskriminalität“ im Internet,
- die Erarbeitung und Implementierung von adaptiven KI-Methoden zur Unterstützung der polizeilichen strafrechtlichen Bewertung von Vorgängen, die Hasskriminalität betreffen, sowie
- die ganzheitliche Betrachtung der einzelnen technischen Komponenten und wissenschaftlichen Ergebnisse und deren Übertragung in eine technische Gesamtlösung (Framework).“[11]

Auf den Internetseiten der ZITiS finden sich weitere Forschungsprojekte, die am Rande eine Erkennung und/oder effektive Verfolgung von Straftaten behandeln.[12]

***

11 https://www.zitis.bund.de/DE/ZITiS/Forschungsprojekte/forschungsprojekte_node.html.

12 Ebd.