NEWS

Chatkontrolle: Strafverfolgung um jeden Preis?

Artikel von Dr. Datenschutz · 8. Mai 2023

Nachtigall, ick hör dir trapsen. Seit über einem Jahr schleicht sich der Gesetzgeber Schritt für Schritt an die Einführung der sogenannten Chatkontrolle heran. Die Überwachung von Chat-Kommunikation wird derzeit wieder heiß diskutiert – Grund genug für uns, ein Update über den Stand der Dinge zu geben.

Der Inhalt im Überblick

Altes Thema, neue Diskussion

Bereits vor einem Jahr haben wir über die Chatkontrolle berichtet. Nach wie vor handelt es sich bei den „Maßnahmen zum Scannen privater Kommunikation" um ein hochaktuelles Thema, das sowohl auf nationaler als auch auf europäischer Ebene intensiv diskutiert wird.

Die derzeit regierende rot-gelb-grüne Koalition streitet sich. Ein wenig erinnert das Ganze an die Vorratsdatenspeicherung. Jahrelang gab es Bestrebungen und Gegenbestrebungen, bis der EuGH sich der Sache angenommen und der Vorratsdatenspeicherung grundsätzlich einen Riegel vorgeschoben hat (freilich nicht ausnahmslos).

Dieses mal geht es aber um den Entwurf einer „Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern" (Child-Sexual-Abuse-Verordnung, CSA-VO). Im Mai 2022 hat die EU-Kommission jene umstrittene Verordnung vorgeschlagen, die von Bürgerrechtlern um den EU-Parlamentarier Patrick Breyer „Chatkontrolle" getauft wurde.

Worum geht es nochmal?

Zur Aufdeckung von Straftaten und unter generalpräventiven Gesichtspunkten sollen sowohl E-Mail und Messenger-Chats als auch Dateien in Cloudspeichern flächendeckend gescannt werden. Besteht eine Anordnung durch eine nationale Behörde, soll ein Provider dem Entwurf der Kommission zufolge künftig beispielsweise Bilder der Nutzer anhand bestehender Hash-Datenbanken auf strafbare Treffer hin überprüfen. Daneben sollen KI-gestützte Systeme proaktiv Darstellungen unbekleideter Kinder und Grooming-Versuche in Textnachrichten finden. Kern des Kommissionsvorschlags sind Aufdeckungsanordnungen, auf deren Basis Anbieter auch verschlüsselter Messenger-Dienste wie WhatsApp, Signal oder Threema nach bekannten und neuen Darstellungen sexuellen Kindesmissbrauchs suchen müssten.

Welche Positionen gibt es?

Die Beteiligten an der hiesigen Diskussion sind erneut die Damen und Herren aus dem Bundesinnenministerium rund um Frau Nancy Faeser (SPD), die Bürgerrechte-Fraktion rund um die FDP und die Herren Buschmann und Wissing (FDP) rund um das Bundesministerium für Digitales und das BMJ. Am 05. April 2023 legte die Bundesregierung nun

Dr. Datenschutz
intersoft consulting services

> „Ausschluss von Maßnahmen, die zu einem Scannen privater verschlüsselter Kommunikation führen".

Maßnahmen,

> „die zu einem Bruch, einer Schwächung, Modifikation oder einer Umgehung von Ende-zu-Ende-Verschlüsselung führen", [müssten] durch konkrete technische Anforderungen im Verordnungsentwurf [ausgeschlossen werden]."

Damit ist die umstrittene Umgehung von Ende-zu-Ende-Verschlüsselung vom Tisch. Auch das sogenannte Client-Side-Scanning auf dem Endgerät der Anwender soll von der Verordnung ausgeschlossen werden. Solche Client-Side-Scanner könnten zu einer Verpflichtung von Messenger-Diensten wie WhatsApp oder Signal führen, auf mobilen Endgeräten aller Nutzer alle Texte und alle Bilder zu scannen. Chats könnten so vor und nach der Verschlüsselung abgegriffen werden. Allerdings hält sich die Bundesregierung im Hinblick auf Client-Side-Scanning sowie Metadaten-Kontrolle Hintertürchen auf.

Daneben prüft die Regierung weiterhin die

> „Zulässigkeit sowie etwaiger Umfang serverseitiger Aufdeckungsmaßnahmen in unverschlüsselten Telekommunikations- sowie (Cloud-) Speicherdiensten".

Die Bundesregierung lehnt demnach Maßnahmen zum Scannen privater Kommunikation auf EU-Ebene grundsätzlich nicht ab, obwohl das wörtlich so im Koalitionsvertrag steht:

> „Allgemeine Überwachungspflichten, Maßnahmen zum Scannen privater Kommunikation und eine Identifizierungspflicht lehnen wir ab."

Die Bundesregierung will sich aber eben nicht gegen das massenhafte, verdachtsunabhängige Durchleuchten unverschlüsselter Kommunikation auf Servern aussprechen. Diese Positionierung dürfte die meisten E-Mails sowie Chats etwa per Facebook-Messenger und Instagram sowie Dienste von Microsoft und Google betreffen, die noch keine Ende-zu-Ende-Verschlüsselung implementiert haben. Der CCC kritisiert den Bruch des Koalitionsvertrags. Sprecherin Elina Eickstädt kommentiert auf Netzpolitik.org:

> „Der Bundesregierung scheint das Thema allgemeine Überwachungspflichten auf EU-Ebenen vollkommen egal zu sein. FDP und Grüne tragen den von Nancy Faeser angestifteten Bruch des Koalitionsvertrag wohlweislich mit. Diese Pseudo-Einigung ist mehr eine Erklärung zum Bruch des Koalitionsvertrags als alles andere."

Auch Sperranordnungen, die sich an Internet-Zugangsanbieter richten, sollen als letztes Mittel zulässig sein. Und zwar, wenn Maßnahmen gegen den Verantwortlichen nicht durchführbar oder nicht Erfolg-versprechend sind, die Sperrungen technisch möglich und zumutbar sind, keine Überwachungspflichten damit verbunden sind und etwaige HTTPS-Verschlüsselung gewahrt bleiben.

Lieber Libe (sic!)

Am 19.04.2023 wurde ein Bericht des LIBE-Ausschusses veröffentlicht, auch bekannt als Ausschuss für bürgerliche Freiheiten, Justiz und Inneres. Dies ist ein Ausschuss des Europäischen Parlaments, der sich mit Fragen der Freiheit, Sicherheit und Justiz in der Europäischen Union befasst. Er hat seine Rechtsgrundlage in der Geschäftsordnung des Europäischen Parlaments sowie in den Verträgen der Europäischen Union. Konkret basiert die Arbeit des Ausschusses auf Artikel 14 des Vertrags über die Europäische Union (EUV) sowie auf Artikel 68 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Dieser spricht sich zwar auch dafür aus, die Ende-zu-Ende-Verschlüsselung beizubehalten, schlägt aber vor, "freiwillige Aufdeckungsanordnungen" und das Scannen von Metadaten hinzuzufügen. Provider sollen demnach ermächtigt werden, private Kommunikation und Daten unverdächtiger Bürger „freiwillig" durchsuchen zu dürfen, auch wenn keine Chatkontrolle angeordnet ist. Insgesamt kommentiert die Piratenpartei den Entwurf als

> „in Teilen noch fataler als der Entwurf der EU-Kommission."

Beim Libe-Ausschuss handelt es sich um Neusprech par excellence.

Das fliegende Brathendl – Ein Blick auf die Technik

Zwar lehnt die Ampelkoalition „Maßnahmen zum Scannen privater Kommunikation" ab. Doch die Bundesregierung prüft die Zulässigkeit einer „serverseitigen" Chatkontrolle. Client-Side-Scanning und eine Umgehung der Ende-zu-Ende-Verschlüsselung werden abgelehnt. Nicht durchsucht werden soll Audiokommunikation (z. B. Sprachnachrichten). Allmählich scheint der Gesetzgeber die Grundsätze der Technik zu verstehen, wenn auch nicht lückenlos. Sichere, verschlüsselte Kommunikation und Massenüberwachung sind miteinander unvereinbar. Dadurch ist eine Strafverfolgung um jeden Preis nicht möglich. Gleichzeitig können aber rechtschaffende Bürger und Bürgerinnen den Missbrauch ihrer Privatsphäre verhindern. Private Daten sind interessant für Verbrecher, Werbetreibende und andere Nutznießer. Und der Gesetzgeber ist einfach nicht von der Vorstellung abzubringen, dass sich Missstände allein durch technische Lösungen wegwischen lassen. Die bei der Fehleranfälligkeit zu erwartenden exorbitanten falsch-positiven Verdächtigungen verhindern am Ende effektive Strafverfolgung, da sie die Strafverfolgungsbehörden auf der falschen Seite überlasten.

Es ist alles gesagt, nur noch nicht von jedem (?)

Insgesamt bleibt die Chatkontrolle ein komplexes Thema, das weiterhin intensiv diskutiert wird. Einerseits als notwendiges Mittel zur Sicherheit und Verbrechensbekämpfung betrachtet, sehen andere die Chatkontrolle als Bedrohung für die Freiheitsrechte und die Privatsphäre. Es ist zu erwarten, dass das Thema auch in Zukunft in den Medien und der Politik präsent bleiben wird, da neue Technologien und Herausforderungen entstehen, und die Gesetze entsprechend angepasst werden müssen.

Mehr zum Thema

- Die Chatkontrolle – EU-Kommission auf Abwegen
- Crypto Wars: EU & USA fordern „Lawful Access by Design“
- 31. Tätigkeitsbericht des Bundesdatenschutzbeauftragten
- Datenschutz – Jahresrückblick 2022 – Teil 2

Autor:in

Dr. Datenschutz
intersoft consulting services AG

Diesen Beitrag teilen

Datenschutz-Folgenabschätzung

Datenschutz & Microsoft 365: DSGVO-konformer Einsatz möglich?
Fachbeitrag · 23. Januar 2024

Top 5 DSGVO-Bußgelder im Dezember 2023
News · 3. Januar 2024

Microsoft 365 Copilot unter datenschutzrechtlicher Betrachtung
Fachbeitrag · 12. Dezember 2023

Mehr zum Thema

Messenger

DMA: Welche Probleme kommen auf WhatsApp und Co. zu
Fachbeitrag · 11. Juli 2022

Die Ende-zu-Ende-Verschlüsselung bei WhatsApp
Fachbeitrag · 6. Januar 2022

Recht auf Verschlüsselung und Daten für das FBI
News · 8. Dezember 2021

Mehr zum Thema

Beitrag kommentieren

Fehler entdeckt oder Themenvorschlag? Kontaktieren Sie uns anonym hier.

Klicken Sie hier, um den Kommentarbereich anzuzeigen.