WIKIPEDIA
Die freie Enzyklopädie

Hauptseite
Themenportale
Zufälliger Artikel

Mitmachen
Artikel verbessern
Neuen Artikel anlegen
Autorenportal
Hilfe
Letzte Änderungen
Kontakt
Spenden

Werkzeuge
Links auf diese Seite
Änderungen an verlinkten Seiten
Spezialseiten
Permanenter Link
Seiteninformationen
Artikel zitieren
Kurzlink
QR-Code herunterladen
Wikidata-Datenobjekt

Drucken/exportieren
Als PDF herunterladen
Druckversion

In anderen Sprachen
Gaeilge
Links bearbeiten

Client-Side-Scanning

Client-Side-Scanning (CSS) bezeichnet eine technische Verfahrensweise, bei der versendete oder empfangene Dateien lokal auf dem Endgerät einer Person auf bestimmte, in einer Datenbank hinterlegte Inhalte durchsucht werden, bevor diese weiter verschickt beziehungsweise verarbeitet werden. Dies geschieht beispielsweise bei Antivirenprogrammen, die Schadsoftware aufgrund vorher ermittelten Signaturen erkennen.[1] Im Speziellen ist mit CSS eine Methode zur Telekommunikationsüberwachung gemeint, bei der zu versendende Dateien bereits vor der Ende-zu-Ende-Verschlüsselung nach Inhalten überprüft werden. Kritiker sprechen in diesem Fall auch von **Chatkontrolle**.[2]

Umsetzungsgeschichte [Bearbeiten | Quelltext bearbeiten]

Europäische Union [Bearbeiten | Quelltext bearbeiten]

In der EU dürfen Unternehmen auf der Grundlage einer Ausnahmeregelung von der *Datenschutzrichtlinie für elektronische Kommunikation* eine Chatkontrolle durchführen. Diese Ausnahmeregelung läuft im August 2024 aus, eine Verlängerung ist vorgesehen. Die Europäische Kommission will die Chatkontrolle dauerhaft verpflichtend machen, hat aber Schwierigkeiten, die nötigen Mehrheiten zu erzielen. Das Vorhaben stößt auf breite Kritik.[3]

Am 11. Mai 2022 legte die Europäische Kommission einen Gesetzesentwurf für eine sogenannte Chatkontrolle vor, der die Betreiber von Messengern zum Scannen auf Kinderpornografie verpflichtet.[4] Eine genaue Technologie schreibt dieser nicht vor. Möglich sind das Aufweichen kryptografischer Protokolle oder eben Client-Side-Scanning, z. B. mittels Hashabgleich.[5]

Die Mitgliedsstaaten der EU waren in der Frage Stand Februar 2023 noch zwiegespalten: gegen die Chatkontrolle traten damals vor allem Deutschland, Frankreich und Slowenien ein sowie Österreich, die Niederlande und Lettland, eindeutig für die Chatkontrolle hingegen Spanien, Kroatien, Griechenland, Litauen und Zypern.[6] Im Mai 2023 positionierten sich in einem gemeinsamen Papier zehn Staaten für die Einführung: Belgien, Bulgarien, Zypern, Ungarn, Irland, Italien, Lettland, Litauen, Rumänien und Spanien.[7] Stand Juni 2023 war die eindeutige Mehrheit der Staaten für die Einführung, darunter nun auch Frankreich, Slowenien und Lettland.[8] In vielen Staaten, darunter Deutschland, kam es zu unterschiedlichen Meinungen innerhalb der Regierungskoalitionen: Oft steht ein die Pläne unterstützendes Innenministerium einem die Pläne ablehnenden Justizministerium gegenüber.[9] Dabei wurden im Koalitionsvertrag der Bundesregierung unter Olaf Scholz „allgemeine Überwachungspflichten, Maßnahmen zum Scannen privater Kommunikation und eine Identifizierungspflicht“ abgelehnt, und es wurde erklärt, dass „anonyme und pseudonyme Online-Nutzung“ gewahrt bleiben wird.[10]

Im Mai 2023 bezeichnete der Juristische Dienst des EU-Rats die Pläne als grundrechtswidrig und schloss sich damit anderen Juristen, den deutschen und europäischen Datenschutzbeauftragten sowie den Wissenschaftlichen Diensten von Bundestag und EU-Parlament an.[11]

Internetgiganten [Bearbeiten | Quelltext bearbeiten]

CSS als Mittel der Telekommunikationsüberwachung wurde erstmals im größeren Maße öffentlich diskutiert, nachdem Apple 2021 angekündigt hatte, die Endgeräte seiner Nutzer auf Darstellungen von Kindesmissbrauch zu durchsuchen. Dateien, die auf die iCloud hochgeladen werden, sollten auf kinderpornografische Inhalte überprüft werden, indem sie mit Einträgen einer Datenbank des National Center for Missing & Exploited Children abgeglichen würden. Nach Protesten wurde das Vorhaben verschoben.[12]

Im April 2022 erklärte Meta Platforms, an Ende-zu-Ende-Verschlüsselung als Langzeitziel festzuhalten. In der von Meta zitierten Untersuchung *Human Rights Impact Assessment – Meta's Expansion of End-to-End Encryption* der Organisation „Business for Social Responsibility“ heißt es, dass eine sichere Ende-zu-Ende-Verschlüsselung grundlegende Menschenrechte wie Meinungsfreiheit und Privatsphäre bewahrt und Individuen vor repressiven Regimen schützt. Auch der Datenschutz sei ein grundlegendes Menschenrecht. Der Einsatz von clientseitigen Scan-Techniken untergrabe aber die Integrität von Ende-zu-Ende-Verschlüsselung. Um gesellschaftliche Probleme wie Kriminalität und Kindesmissbrauch zu bekämpfen, seien Präventionsstrategien wie die Auswertung von Metadaten und Verhaltensanalysen, aber auch Nutzeraufklärung und eine „robuste Benutzerberichterstattung“ geeigneter.[13]

Kritik [Bearbeiten | Quelltext bearbeiten]

Kritiker sehen CSS als schweren Eingriff in die Privatsphäre der Nutzer und als mögliche Methode der Massenüberwachung. Leicht ließen sich auch andere, nicht-illegale Inhalte überwachen. Die Überwachungs- und Kontrollmöglichkeiten von CSS könnten leicht von feindlichen staatlichen Akteuren, Kriminellen oder Intimpartnern der Benutzer missbraucht werden.[2] Die Möglichkeit solcher Angriffe wurde von Forschern der TU Darmstadt am Beispiel von Apples CSS-Algorithmus *NeuralHash* zur Detektion von kinderpornografischem Material empirisch nachgewiesen. Während das CSS-System und die damit einhergehende Detektion von illegalem Material mit einfachen Bildänderungen umgangen werden konnte, ließen sich Bilder mit unsensiblem Material in einer Art und Weise manipulieren, dass diese vom System fälschlicherweise als kinderpornografisches Material erkannt wurden. Dies könne zur fälschlichen Markierung unschuldiger Nutzer durch das System führen, bis hin zu einer möglichen politischen Verfolgung sozialer Gruppen.[14]

Der Chaos Computer Club sieht die Umsetzungsversuche der Europäischen Kommission im Mai 2022 vor Veröffentlichung des Gesetzesentwurfs als einen Angriff auf die Grundfesten jeglicher vertraulicher Kommunikation. Die Chatkontrolle sei ein „überbordender Ansatz, leicht zu umgehen“ und setze an der „völlig falschen Stelle an“. Kriminelle würden gar nicht über Messenger ihr Material austauschen. Auch kleinste Fehlerquoten würden bei einer halben Milliarde pro Tag versendeten Nachrichten den Behörden mehrere tausend Bilder am Tag zusenden, von denen keiner wisse, wer sie betrachte, ob sie gelöscht würden und ob sie nicht wiederum missbraucht würden. Die Chatkontrolle setze mit dem Fernmeldegeheimnis und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gleich zwei fundamentale Grundrechte außer Kraft. Sie missachte zwei Bedingungen für vertrauliche Kommunikation, nach denen das eigene Gerät integer sein müsse und Inhalte nicht an Dritte ausleiten dürfe und die Verschlüsselung sicher sein müsse, so dass man nicht dem Netz vertrauen müsse. Daher sei die Chatkontrolle „als fundamental fehlgeleitete Technologie grundsätzlich abzulehnen“.[15]

Die Präsidentin der Stiftung des Signal-Messengers Meredith Whittaker kritisiert, dass Client-Side-Scanning das ganze Grundprinzip von Ende-zu-Ende-Verschlüsselung mit einer höchst unsicheren Technologie untergräbt und der Regierung die Möglichkeit geben würde, buchstäblich jede Äußerung zu kontrollieren, bevor sie veröffentlicht wird.[16]

Der Wissenschaftliche Dienst des Deutschen Bundestages sieht bei der Chatkontrolle einen erheblichen Eingriff „in das Recht auf Privatsphäre, in den Datenschutz sowie unter anderem in die Grundrechte der EU-Grundrechtecharta“[17] Im März 2023 lehnten alle 9 Sachverständige in einer Anhörung des Ausschusses für Digitales im Deutschen Bundestag die geplante den EU-Vorschlag ab; eine Totalüberwachung im Internet als auch eine Überforderung der Strafverfolgungsbehörden mit Falschmeldungen wurde befürchtet.[18] Im selben Monat bezweifelte der Bundesdatenschutzbeauftragte sowohl Verhältnismäßigkeit als auch Grundrechtskonformität des Entwurfes, der außerdem kaum Schutz für Kinder biete.[19]

Der Kinderschutzbund sprach sich gegen anlassloses Scannen als „unverhältnismäßig und nicht zielführend“ aus.[20]

Die Leiterin der Beschwerdestelle des eco – Verbands der Internetwirtschaft Alexandra Koch-Skriba, die Beschwerden zu Missbrauchsbildern im Netz entgegennimmt, betrachtet die von der EU-Kommission vorgelegten Pläne mit Sorge, denn sie untergrüben „jede Form der vertraulichen und sicheren Kommunikation im Netz“, der Entwurf habe „das Potenzial, einen Freifahrtschein für staatliche Überwachung zu schaffen“, dies sei „ineffektiv und illegal“.[21]

heise online sieht es als nicht zufällig an, dass das für die Chatkontrolle geplante EU-Zentrum im selben Gebäude in Den Haag angesiedelt werden soll, welches auch die EU-Polizeibehörde Europol beherbergt, es scheine ein reger Datenaustausch zwischen Prüfern und Strafverfolgern gewollt zu sein.[22]

Laut heise online kann, auch wenn die deutsche Regierung dagegen ist, Deutschland im Ministerrat überstimmt werden.[23] Nach Einschätzung von heise ist in den anderen EU-Mitgliedsstaaten kein ähnlich lauter Protest gegen die Verordnung zu hören wie in Deutschland.[24]

Weblinks [Bearbeiten | Quelltext bearbeiten]

- Alexander Lehmann: *Kampagnenvideo gegen Chatkontrolle* auf YouTube

Einzelnachweise [Bearbeiten | Quelltext bearbeiten]

1. ↑ *Fact Sheet: Client-Side Scanning.* In: *Internet Society.* 24. März 2020, abgerufen am 22. Mai 2022 (amerikanisches Englisch).
2. ↑ a b Markus Reuter: *Client-Side-Scanning: Berühmte IT-Sicherheitsforscher:innen warnen vor Wanzen in unserer Hosentasche.* 16. Oktober 2021, abgerufen am 25. März 2022 (deutsch).
3. ↑ netzpolitik.org, abgerufen am 23. Januar 2024.
4. ↑ ec.europa.eu
5. ↑ heise.de
6. ↑ *So stehen die EU-Länder zur Verschlüsselung.* In: *netzpolitik.org.* 9. Februar 2023, abgerufen am 12. Februar 2023.
7. ↑ *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse − Common position of the like-minded group (LMG) of Member States.* Abgerufen am 22. Mai 2023.
8. ↑ netzpolitik.org, abgerufen am 13. Juni 2023.
9. ↑ *Justizminister Buschmann mobilisiert EU-Kolleg:innen.* In: *netzpolitik.org.* 12. Mai 2023, abgerufen am 12. Mai 2023.
10. ↑ spd.de
11. ↑ *Chatkontrolle ist grundrechtswidrig und wird scheitern.* Abgerufen am 22. Mai 2023.
12. ↑ Markus Reuter, Holly Hildebrand: *Nach Protesten: Apple verschiebt Pläne zur Durchsuchung von Dateien auf iPhones.* 3. September 2021, abgerufen am 25. März 2022 (deutsch).
13. ↑ Wiedergegeben nach: https://www.heise.de/news/Meta-haelt-an-Ende-zu-Ende-Verschluesselung-als-Langzeitziel-fest-6662912.html
14. ↑ Lukas Struppek, Dominik Hintersdorf, Daniel Neider, Kristian Kersting: *Learning to Break Deep Perceptual Hashing: The Use Case NeuralHash*. In: *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAccT)*. 2022 (arxiv.org [PDF; abgerufen am 10. Juni 2022]).
15. ↑ linus: *EU-Kommission will alle Chatnachrichten durchleuchten.* Chaos Computer Club, 9. Mai 2022, abgerufen am 10. Mai 2022.
16. ↑ https://edri.org/our-work/signals-meredith-whittaker-voices-edris-concerns-with-the-csa-regulation/
17. ↑ netzpolitik.org
18. ↑ Benjamin Hilbricht: *Alle gegen Chatkontrolle.* In: *Behörden Spiegel.* 9. März 2023, abgerufen am 24. März 2023 (deutsch).
19. ↑ Markus Reuter: *Jahresbericht: Bundesdatenschutzbeauftragter watscht Chatkontrolle ab.* 15. März 2023, abgerufen am 24. März 2023 (deutsch).
20. ↑ br.de
21. ↑ heise.de
22. ↑ heise.de
23. ↑ heise.de
24. ↑ heise.de