28. Mai 2024

Gemeinsame Erklärung zu den Gefahren des Kompromissvorschlags des EU-Rates von Mai 2024 zur geplanten Verordnung über sexuellen Kindesmissbrauch (child sexual abuse material (CSAM)

Die unterzeichnenden Organisationen, Unternehmen und Cybersicherheitsexperten, von denen viele Mitglieder der Global Encryption Coalition sind, erklären Folgendes als Reaktion auf den jüngsten Kompromissvorschlag der belgischen Ratspräsidentschaft vom Mai 2024 zur Verordnung über sexuellen Kindesmissbrauch (Child Sexual Abuse – CSA):

Sexueller Kindesmissbrauch und seine Verbreitung im Internet ist ein schweres Verbrechen, das nur dann wirksam bekämpft werden kann, wenn die EU-Mitgliedsstaaten einen maßvollen, auf Expertenwissen basierenden Ansatz verfolgen. Das EU-Parlament hat dies bereits getan, indem es beschloss, Dienste mit Ende-zu-Ende-Verschlüsselung vom Anwendungsbereich der Verordnung auszunehmen. Wir begrüßen diese Anerkennung der Bedeutung der Verschlüsselung für die Gewährleistung der Sicherheit und die Garantie der Menschenrechte und Grundfreiheiten. Mit diesem positiven Ansatz des EU-Parlaments schützt die wichtige Ende-zu-Ende-Verschlüsselungs-Technologie Erwachsene, Kinder, Unternehmen und Regierungen davor, Opfer böswilliger Akteure zu werden.

Wir sind besorgt, dass der Rat der EU nicht den gleichen Weg einschlägt. Der belgische Ratsvorsitz setzt sich weiterhin für den Einsatz von Scanning-Technologien für verschlüsselte Nachrichtendienste sowie für andere unverhältnismäßige Einschränkungen der digitalen Rechte ein. Die Erkennung von Inhalten ist bei einer Reihe von EU-Mitgliedsstaaten umstritten, die sich bisher gegen Client-seitige Scanning-Technologien gewehrt haben. Diese sind zu Recht der Meinung, dass dies ernsthafte Sicherheits- und Datenschutzrisiken schafft, eine allgemeine Überwachung ermöglicht und die Menschenrechte untergräbt. Wir danken den Ministern im Rat dafür, dass sie die Bedeutung der Verschlüsselung anerkennen und sich für deren Schutz einsetzen.

In dem Bemühen, eine Lösung zu finden, hat die belgische Präsidentschaft den Überwachungs-Ansatz auf „Upload-Moderation“ umgetauft. Bei dieser rein kosmetischen Änderung werden die von Experten vorgebrachten Sicherheits- und Rechtsbedenken in Bezug auf das clientseitige Scannen weiterhin nicht berücksichtigt. Das Scannen am Upload-Punkt unterläuft das Ende-zu-Ende-Prinzip der starken Verschlüsselung, kann leicht umgangen werden und schafft neue Sicherheitslücken, die von Dritten ausgenutzt werden könnten. Kurz: das Problem der Online-Verbreitung von Material über sexuellen Kindesmissbrauch wird dadurch nicht gelöst. Vielmehr entstünden erhebliche Sicherheitsrisiken für alle Bürger, Unternehmen und Regierungen.

Der jüngste Kompromisstext der belgischen Präsidentschaft versucht durch folgenden Vorschlag einen Konsens zu finden:

1. Das clientseitige Scannen soll nur auf visuelle Inhalte (Fotos und Videos) und URLs angewendet werden; und
2. Die Nutzer von Kommunikationsdiensten müssten ihre Zustimmung zum Scannen geben, andernfalls würde es ihnen nicht gestattet, Fotos und Videos über den Dienst hochzuladen oder zu teilen.

In der heutigen digitalen Gesellschaft ist der Austausch von Fotos und Videos eine Standardaktivität. Wenn ein Nutzer keine wirkliche Wahl hat, sich zur Einwilligung gezwungen fühlt oder bei Nichteinwilligung faktisch von einem Dienst ausgeschlossen wird, wird eine Einwilligung nicht freiwillig erteilt. Eine erzwungene Einwilligung ist nicht freiwillig. Zudem ist der Vorschlag untauglich. Er kann leicht dadurch umgangen werden, dass Fotos oder Videos in eine andere Art von Datei, z. B. in ein Textdokument oder eine Präsentation, eingebettet werden.

Wir fordern die Minister im Rat der EU auf, alle Scan-Vorschläge abzulehnen, die mit dem Prinzip der Ende-zu-Ende-Verschlüsselung unvereinbar sind, einschließlich des clientseitigen Scannens und der Upload-Moderation. Der Schutz der digitalen Rechte ist im gesamten Vorschlag zu gewährleisten. Die invasiven Techniken würden nur die Sicherheit und die Rechte der Internetnutzer gefährden.

Fragen zu dieser Erklärung können an den Lenkungsausschuss der Global Encryption Coalition gerichtet werden unter ge-admin@globalencryption.org.

Unterzeichnende Organisationen (Stand 31. Mai 2024):

Internet Society, Center for Democracy & Technology, Internet Freedom Foundation, Mozilla, Global Partners Digital, Signal, Access Now, Aspiration, Privacy International (PI), Article 19, Tuta, SecureCrypt, Privacy & Access Council of Canada, Big Brother Watch, The Centre for Democracy and Technology Europe, Sjard Braun, epicenter.works – for digital rights, Elektronisk Forpost Norge (EFN), JCA-NET(Japan), INSPIRIT Creatives NGO, Privacy First, The Commoners, ISOC Germany, Alternatif Bilisim (Alternative Informatics Association), Danes je nov dan, Defend Democracy, Defend Digital Me, **Deutsche Vereinigung für Datenschutz e.V. (DVD)**, Digital Rights Ireland, Irish Council for Civil Liberties, ISOC Switzerland Chapter, ISOC.DE e.V., Iuridicum Remedium, Majal.org, Proton, SimpleX Chat, Surfshark, Edvina AB, Law and Technology Research Institute of Recife – IP.rec, Dataföreningen väst, Bits of Freedom, D3 – Defesa dos Direitos Digitais, fairkom, ISOC Portugal, ISOC UK, ApTI, Gate 15, Electronic Frontier Foundation (EFF), Daniel Törmänen, Državljan D (Citizen D), Politiscope, European Digital Rights (EDRi), Global Partners Digital, Aivivid AB, Irene Promussas, Chairwoman Lobby4kids, IT-Pol Denmark, Electronic Frontiers Australia, ISOC-CAT Catalan Internet Society Chapter, U-YOGA UGANDA, eco – Association of the Internet Industry, Electronic Frontier Finland – Effi ry, OpenMedia, Studio Legale Fabiano – Fabiano Law Firm

sowie viele Einzelpersonen.

Der englischsprachigen Originaltext der Erklärung ist im Internet abrufbar unter

https://www.globalencryption.org/2024/05/joint-statement-on-the-dangers-of-the-may-2024-council-of-the-eu-compromise-proposal-on-eu-csam/