Offener Brief aus dem zivilgesellschaftlichen Bereich vom 17. April 2024

Massenhafte Überwachung und Unterminierung von Verschlüsselung – immer noch auf dem Tisch des Rats der Europäischen Union (EU)

Sehr geehrte Justiz- und Innenminister der EU-Mitgliedsstaaten,
sehr geehrte Ständige Vertreter (Botschafter) bei der EU,
sehr geehrte Vertreter der EU-Mitgliedsstaaten bei der Arbeitsgruppe Rechtsdurchsetzung (Law Enforcement Working Party – LEWP),

als eine Koalition von 50 zivilgesellschaftlichen Organisationen und 26 einzelnen Experten fordern wir Sie auf, dem Standpunkt des EU-Rates zur Verordnung über sexuellen Kindesmissbrauch (Child Sexual Abuse Regulation – CSA) nicht zuzustimmen, solange noch so viele kritische Fragen offen sind. Die grundlegenden Mängel des Gesetzentwurfs der Kommission und früherer Ratstexte – einschließlich der Massenüberwachung und der ernsthaften Bedrohung der Verschlüsselung – wurden durch die jüngsten Texte des belgischen Ratsvorsitzes nicht behoben.

Im Zuge dieses EU-Legislativvorschlags wurden von Tausenden von Experten aus den Bereichen Menschenrechte, Cybersicherheit, (digitale) Kinderrechte, Kinderschutz-Hotlines, Polizeikräfte, Datenschutz und mehr erhebliche Bedenken geäußert.

Diese Bedenken wurden unter anderem von den Regierungen Deutschlands, Polens, Frankreichs, Österreichs, der Niederlande, Estlands und Finnlands aufgegriffen, die gegen mehrere der großen rechtlichen und technischen Mängel des Vorschlags votiert haben. Wir weisen warnend darauf hin, dass diese kritischen Punkte in dem neuen Konzept immer noch präsent sind.

Insbesondere enthält der neue Vorschlag keine wesentlichen oder sinnvollen Änderungen zum Schutz der Grundrechte. Er kann Anbieter nach wie vor dazu zwingen, die Ende-zu-Ende-Verschlüsselung ihrer Dienste zu untergraben, um einer Aufdeckungsanordnung nachzukommen, und er kann sie nach wie vor dazu verpflichten, Nutzer zu überwachen, ohne dass ein Zusammenhang mit einer Straftat der CSA-Verordnung besteht.

Es geht darum, das Recht auf Privatsphäre, Datenschutz, freie Meinungsäußerung und die Unschuldsvermutung der Menschen in der EU und darüber hinaus im Kern zu wahren.

Trotz einiger formalen Änderungen des Rahmens für die Risikokategorisierung erlaubt der neue Vorschlag nach wie vor die Anwendung von Aufdeckungsanordnungen auf breiter Basis und ohne gezielte Ausrichtung (im Sinne eines direkten oder indirekten Zusammenhangs, wie er vom Europäischen Gerichtshof (EuGH)[1] ausgelegt wird).

Die vom Juristischen Dienst des Rates der EU geäußerten Bedenken hinsichtlich der Unvereinbarkeit mit der Menschenrechtsrechtsprechung, die eine allgemeine Überwachung verbietet, bleiben bestehen. Aufdeckungsanordnungen sind daher weiterhin anfällig für eine Nichtigerklärung durch den EuGH.

Es geht darum, eines der wichtigsten Instrumente zum Schutz der digitalen Kommunikation, die wir in der Welt haben, nämlich die Ende-zu-Ende-Verschlüsselung, nicht zu unterminieren.

Der neue Vorschlag macht zwar einige Andeutungen, dass der Schutz von Verschlüsselung notwendig sei, verhindert aber nur, dass Anbieter gezwungen werden, verschlüsselte Kommunikation zu „verändern“ oder selbst zu „entschlüsseln“. Die Verwendung von Client-Side-Scanning (CSS)-Techniken bleibt auf dem Tisch. Es wird nicht verhindert, dass Anbieter gezwungen werden, die Sicherheit oder Integrität ihrer Dienste generell zu schwächen oder zu untergraben.

Anfang dieses Jahres hat der Europäische Gerichtshof für Menschenrechte (EGMR) ein wegweisendes Urteil gefällt, in dem er die Bedeutung der Verschlüsselung für den Schutz des Rechts auf Privatsphäre hervorhob.[2] Dieser wichtige Aspekt spiegelt sich in dem neuen Ansatz des Rates nicht wider. Es würden daher neben den Vorgaben des EuGHs wahrscheinlich auch die des EGMR verletzt.

Unabhängig von der Zielrichtung des Gesetzes geht es darum sicherzustellen, dass diejenigen, deren Sicherheit von einer sicheren Online-Kommunikation abhängt, nicht übermäßig beeinträchtigt werden.

Berücksichtigt werden müssen Journalisten über jugendliche Aktivisten bis hin zu Menschen, die Informationen über Sexualität oder reproduktive Gesundheit suchen. Der jüngste Vorschlag und der dazugehörige Anhang schreiben weiterhin riskante Altersüberprüfungsinstrumente vor und fördern andere Formen einer umfassenden und invasiven Offenlegung persönlicher Daten. Zusammengenommen würde dies die Online-Anonymität

nahezu unmöglich machen. Dies kann schwerwiegende Folgen für die digitalen Freiheiten und die Sicherheit der Menschen haben.
Darüber hinausgehend haben die neuen vorgeschlagenen Risikokategorien zur Folge, dass die Dienste, die die Privatsphäre und die Sicherheit ihrer Nutzer schützen, als hochriskant eingestuft werden. Umgekehrt werden diejenigen, deren Geschäftsmodelle auf der Ausbeutung und Monetarisierung der Daten ihrer Nutzer beruhen und die keine sicheren Kommunikationskanäle anbieten, standardmäßig als weniger riskant eingestuft. Dies steht im Widerspruch zu den Grundsätzen eines „eingebauten Datenschutzes“ (Privacy by Design) und eines „Datenschutzes durch Voreinstellung“ (Privacy by Default), wie sie in der europäischen Datenschutz-Grundverordnung (DSGVO) festgelegt sind.
Wie der Europäische Datenschutzbeauftragte kürzlich betonte, besteht bei der CSA-Verordnung die Gefahr, dass die EU den Rubikon überschreitet. Mit diesem jüngsten Versuch des Ratsvorsitzes, die Verhandlungen freizugeben, würde der Rat allgemeine Überwachungs- und Verschlüsselungsmaßnahmen billigen, die sicherlich weltweit Wirkung entfalten.
Wir, die Unterzeichner, fordern Sie als Vertreter Ihres Landes auf, unsere Rechte und Freiheiten zu schützen, indem Sie diese neue Ausrichtung des Rates ablehnen.

Unterzeichnende zivilgesellschaftliche Organisationen:
Europäische Union: • European Digital Rights (EDRi) • The Centre for Democracy and Technology Europe • European Network for the Promotion of the Rights and Health among Migrant Sex Workers (TAMPEP) • Access Now
• Civil Liberties Union for Europe • Defend Democracy • Wikimedia Europe
Österreich: • epicenter.works - for digital rights
Dänemark: • IT-Pol Denmark
France: • La Quadrature du Net
Germany: • Digitale Gesellschaft • Gesellschaft für Informatik e.V. • Deutsche Vereinigung für Datenschutz e.V. (DVD) • SUPERRR Lab • D64 – Zentrum für Digitalen Fortschritt • Digitalcourage
Griechenland: • Homo Digitalis
Italien: • Comitato per i Diritti Civili delle Prostitute APS
Niederlande: • Bits of Freedom • Privacy First • PIC
Portugal: • AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação • ISOC Portugal • ANSOL - Associação Nacional para o Software Livre • D3 - Defesa dos Direitos Digitais
Slowenien: • Državljan D / Citizen D
Spanien: • Xnet, Institute for Democratic Digitalisation (Spain)
Schweden: • Red Umbrella Sweden
International/global: • Electronic Frontier Foundation (EFF) • Fundación Cibervoluntarios • Internet Society • The Tor Project • Aspiration • ARTICLE 19 • Committee to Protect Journalists (CPJ)
International und Regionen: • Internet Society Catalan Chapter (ISOC-CAT) • CIPESA (Africa) • Bangladesh NGOs Network for Radio and Communication(BNNRC)! • Tech for Good Asia • Internet Society - Brazil Chapter • Electronic Frontier Norway • Fight for the Future (United States) • Privacy & Access Council of Canada • JCA-NET(Japan) • Big Brother Watch (United Kingdom) • Electronic Frontiers Australia • Defend Digital Me (United Kingdom) • STAR - The First Sex Workers Collective in the Balkans (North Macedonia) • European Sex Workers' Rights Alliance (ESWA) (Europe and Central Asia) • The Law and Technology Research Institute of Recife (IP.rec) (Brazil)
sowie Einzelpersonen u.a. aus Wissenschaft, Technik, Recht.

Die englischsprachige Originalfassung des Offenen Briefes finden Sie unter:
https://edri.org/wp-content/uploads/2024/04/48-NGOs-and-26-experts-warn-Mass-surveillance-and-undermining-encryption-still-on-table-in-EU-Council.pdf.

[1] EuGH Urteil v. 21.12.2016 – C-203/15 u. C-698/15 (Tele 2), Rn. 111.
[2] EGMR, Podchasov v. Russia (no. 33696/19) at the European Court of Human Rights (ECtHR).