Offener Brief an den Rat der Europäischen Union, das Bundesministerium der Justiz und das Bundesministerium des Innern

Berlin, den 17. November 2020

Verschlüsselung von Messenger-Diensten nicht aushebeln!

Sehr geehrte Mitglieder des Rats der Europäischen Union,
sehr geehrte Frau Bundesministerin, sehr geehrter Herr Bundesminister,

angesichts der jüngsten Terroranschläge hat die deutsche Ratspräsidentschaft einen Resolutionsentwurf[1] vorgelegt, in dem „technische Lösungen“ gefordert werden, um „den zuständigen Behörden im Bereich der Sicherheit und des Strafrechts“ den Zugang zu verschlüsselter Kommunikation zu ermöglichen. Wir schreiben Ihnen, um unsere Besorgnis über die angestrebte Ausarbeitung eines Regulierungsrahmens zum Ausdruck zu bringen, der die Integrität von Ende-zu-Ende-verschlüsselten Messengerdiensten in Frage stellen und damit das Recht auf Privatsphäre und die Vertraulichkeit der Kommunikation von Journalistinnen und Journalisten und ihren Quellen gefährden würde.

Die im Resolutionsentwurf des Ministerrates benannte „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ ist ein Widerspruch in sich selbst. Verschlüsselung funktioniert entweder ausnahmslos, oder sie funktioniert gar nicht. Eine funktionierende Verschlüsselung, die nur für die Sicherheitsbehörden eine Ausnahme schafft, ist nicht denkbar und nicht möglich. Jedes technische Mittel des Zugriffs auf verschlüsselte Kommunikation würde die Vertraulichkeit der Daten aller Nutzerinnen und Nutzer schwächen und die Bürger und Dienste einem erhöhten Risiko von Angriffen durch Hacker und ausländische Geheimdienste aussetzen, selbst wenn die vorgeschlagene Lösung „den Prinzipien der Legalität, Transparenz, Notwendigkeit und Verhältnismäßigkeit“ entsprechen würde.

Es ist zu befürchten, dass der im Resolutionsentwurf vorgesehene Zugang zu Daten die Schaffung eines Nachschlüssels für „zuständige Behörden" bedeuten würde, mit Hilfe dessen die Behörden auf die Kommunikation der Bürger zugreifen könnten. Mit „zuständigen Behörden“ sind nicht nur Strafermittler gemeint, sondern offenbar auch die Nachrichtendienste. Eine Hintertür gäbe diesen Diensten die Möglichkeit nicht nur auf einzelne Chats einiger weniger Personen zuzugreifen und diese zu speichern, sondern den Kommunikationsstrom aller Nutzerinnen und Nutzer von Messengerdiensten auszuforschen.

Sollte dies umgesetzt werden, würde die Vertraulichkeit der Kommunikation von Journalistinnen und Journalisten gefährdet, ebenso wie der Schutz der Identität ihrer Quellen. Ende-zu-Ende-verschlüsselte Messengerdienste sind für Medienschaffende im digitalen Zeitalter ein wesentliches Recherche- und Kommunikationsinstrument, das nicht in Frage gestellt werden darf. Die wichtige Kontrollfunktion des Journalismus als unabhängige vierte Gewalt in einer Demokratie hängt von der Fähigkeit ab sicher und in voller Vertraulichkeit zu kommunizieren.

Wie mittlerweile bekannt ist, konnte der Anschlag nur passieren, weil der Verfassungsschutz in Österreich durchaus vorhandene Informationen über den Attentäter nicht verwendet hat. Nicht mehr Überwachungsbefugnisse, sondern bessere Arbeit der Behörden hätten den

[1] Draft Council Resolution on Encryption - Security through encryption and security despite encryption https://files.orf.at/vietnam2/files/fm4/202045/783284_fh_st12143-re01en20_783284.pdf

Anschlag verhindern können. Eben die Behörden, deren Versagen den Anschlag erst möglich machte, sollen jetzt noch weitere Kompetenzen erhalten.

Wir fordern daher den Rat der Europäischen Union, das Bundesinnenministerium und das Bundesjustizministerium auf, keine Anstrengungen zu unternehmen, die das Grundrecht auf Privatsphäre gefährden könnten. Die Beibehaltung der Ende-zu-Ende-Verschlüsselung ist für den Schutz der Pressefreiheit von entscheidender Bedeutung. Alle weiteren Diskussionen sollten in transparenter und offener Weise geführt werden und die Zivilgesellschaft mit einbeziehen.

Mit freundlichen Grüßen

Christian Mihr

Reporter ohne Grenzen

Julia Stein

Netzwerk Recherche