erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

FIfF e. V. – Pressemitteilung

Aushebelung von Ende-zu-Ende-Verschlüsselung trifft die Falschen und leistet der IT-Sicherheit einen Bärendienst

10. November 2020 – *EU-Ministerrat strebt praktisch ein Verbot von Ende-zu-Ende-Verschlüsselung an, einem elementaren Baustein der vertrauenswürdigen digitalen Gesellschaft, dabei haben „haarsträubende Ermittlungsfehler bei den Behörden den Anschlag in Wien erst ermöglicht, nicht fehlende digitale Überwachungsbefugnisse" (Erich Möchel).*

Der EU-Ministerrat veröffentlichte am 6. November 2020 das überarbeitete Entwurfspapier „Draft Council Declaration on Encryption – Security through encryption and security despite encryption" [1]. Darin berichten die AutorInnen von der Absicht, einen gesetzlichen Rahmen zu schaffen, durch den AnbieterInnen von Messenger-Diensten wie Signal, Threema, Telegram,

Skype oder WhatsApp ihre Verschlüsselungsverfahren aufweichen müssten, indem quasi ein behördlicher Generalschlüssel hinterlegt werden soll.

Schon wieder die Mär vom „Going Dark"

Durch das Papier zieht sich dabei das Narrativ, man müsse eine „Balance" finden zwischen den Wünschen von BürgerInnen und Wirtschaft nach sicherer, datenschutzfreundlicher und privater Kommunikation einerseits und den Wünschen der Geheimdienste und der Ermittlungsarbeit von Strafverfolgungsbehörden [3] andererseits. In längst widerlegten Mustern argumentieren die AutorInnen des Papiers, ein effektiver Schutz vor organisierter Kriminalität, Darstellungen von sexualisierter Gewalt gegen Kinder und Terrorismus wäre ohne Zugang zu Kommunikationsinhalten aus verschlüsselten Messengerdiensten nicht möglich. Gerade vor dem Hintergrund der jüngsten Terroranschläge in Wien folgt diese Ansicht einem bekannten Schema: Dem Märchen des „Going Dark", also dem angeblichen Verschwinden von Terroristen und Straftätern vom Radar der Ermittlungsbehörden aufgrund verschlüsselter Kommunikation. Darum sei nun auch diese Einschränkung der Freiheitsrechte aller BürgerInnen notwendig. Tatsächlich verdichten sich aber auch in Wien die Hinweise, dass der Täter schon lange behördlich bekannt war – ganz ohne Generalschlüssel – die Behörden jedoch mehrfach gravierende Fehler gemacht haben.

Die „Balance", die von den AutorInnen eingefordert wird, ist jedoch ein Trugbild: Maßnahmen, die Ende-zu-Ende-Verschlüsselung um einen Generalschlüssel erweitern, führen zwangsläufig zu unsicherer Verschlüsselung, denn das Ende-zu-Ende-Prinzip wird durch die Zugriffsmöglichkeit Dritter unterminiert. Es ist schlicht mathematisch unmöglich, Verschlüsselung zugleich tatsächlich sicher und behördlich abhörbar zu gestalten, denn es gibt aus Sicht der Kryptographie keine „guten" oder „schlechten" AngreiferInnen.

> *„Entweder die VerfasserInnen des EU-Papiers kennen diesen prinzipiellen Widerspruch und die seit Jahrzehnten darum geführten wissenschaftlichen Debatten [2] nicht oder aber ihnen ist die Natur des Problems wohlbekannt, aber sie möchten in unsicheren Zeiten symbolpolitischen Aktionismus simulieren. Beide Optionen sind hinsichtlich demokratischer Prozesse besorgniserregend",*

bewertet Rainer Rehak vom FIfF den Vorstoß.

Kriminelle können ausweichen, BürgerInnen und Wirtschaft nicht

Verschlüsselungsmethoden zu unterbinden ist zudem nicht wirksam, da es stets Möglichkeiten gibt, derartige Verbote zu umgehen. Vielmehr haben Kriminelle ausreichend Anreize und Ressourcen, um auch komplexe und verbotene Verfahren anzuwenden – rechtstreue BürgerInnen und legal agierende Wirtschaftsunternehmen hingegen bleiben hier außen vor. Weichen also die etablierten Messengerdienste wie vorgeschlagen ihre Verschlüsselung auf, steigen die organisierte Kriminalität sowie TerroristInnen in der Folge auf andere wirklich abhörsichere Kommunikationskanäle um. Eine derartige gesetzliche Regelung würde also nur dazu führen, dass der Großteil der Bevölkerung unsicher kommuniziert – und damit anfälliger für Kriminalität wäre, während ein kleiner Teil der Gesellschaft, auf den die in dem Papier beschriebenen Maßnahmen abzielen, leicht den Mehraufwand investieren kann, um auch weiterhin verdeckt kriminell zu agieren – die Maßnahme träfe also nur die Falschen. Bemerkenswert ist dabei auch, dass der nun geforderte technische Ansatz ursprünglich aus der Feder des britischen Geheimdienstes GCHQ stammt, der mit vergleichbaren Praktiken bereits aus den Snowden-Enthüllungen bekannt ist.

> *„Die organisatorische, juristische und technische Infrastruktur [4], die nötig wäre, um die postulierten Zugriffsmöglichkeiten (Backdoors) zu ermöglichen, stünden dabei zwangsläufig Behörden aus allen europäischen Mitgliedsstaaten zur Verfügung – auch denen, die in den letzten Jahren zunehmend in autokratische Fahrwasser gelangt sind",*

warnt Alexander Prehn vom FIfF. Und auch in Deutschland gilt: Überwachungsmaßnahmen, die wir heute für Behörden schaffen und einer Bundesregierung anvertrauen, sind nur eine Wahl davon entfernt, von weniger demokratischen Parteien genutzt zu werden. Darüber hinaus ist fest damit zu rechnen, dass Befugnisse, die heute für schwerste Straftaten eingeführt werden, später auch für weitere Zwecke zur Anwendung kommen.

Digitale Freiheitsrechte sind die Zukunft für Demokratie und Wirtschaft

Die EU hat sich gerade in Bezug auf die digitalen Freiheitsrechte nicht erst seit der Datenschutz-Grundverordnung (DSGVO) eine Signalfunktion in der Welt erarbeitet. Wenn also hierzulande Technologiefirmen gezwungen werden sollten, Ende-zu-Ende-Verschlüsselung zurückzubauen, dann verlieren nicht allein die BürgerInnen der EU: MenschenrechtsInnen und UmweltaktivistInnen, AnwältInnen, ÄrztInnen, BürgerrechtlerInnen und JournalistInnen – sie alle sind für ihre Arbeit auf sichere Kommunikationskanäle angewiesen. *„Das politische Signal aus der EU muss daher klar sein: Es kann keine Kompromisse bei Ende-zu-Ende Verschlüsselung geben"*, schließt Alexander Prehn.

Referenzen

[1] Council of the European Union (2020): Draft Council Resolution on Encryption, https://files.orf.at/vietnam2/files/fm4/202045/783284_fh_st12143-re01en20_783284.pdf

[2] Etwa Schneier et al. (2016): Don't Panic: Making Progress on the „Going Dark" Debate, Berkman Center for Internet & Society, Harvard University, 1.2.2016, https://cyber.harvard.edu/pubrelease/dont-panic/

[3] Moechel, Erich (2020): Auf den Terroranschlag folgt EU-Verschlüsselungsverbot, https://fm4.orf.at/stories/3008930/

[4] Wahrscheinlichste technische Umsetzung ist das exceptional-access-Verfahren des GCHQ, https://www.lawfareblog.com/evaluating-gchq-exceptional-access-proposal