Gerne betont die Politik die Wichtigkeit eines sicheren Informationsaustauschs im Internet. Die EU-Datenschutzgrundverordnung verpflichtet sogar explizit zum Einsatz entsprechender Verschlüsselungstechniken. Die Mitgliedsstaaten der Europäischen Union sehen die Sache nicht so verbissen und forcieren von langer Hand vorbereitete Pläne, Strafermittlern und Geheimdiensten Einblick in die über Messenger-Dienste wie WhatsApp und Signal verbreiteten Botschaften zu ermöglichen. Wie üblich liefert der internationale Terrorismus die Rechtfertigung für den massiven Eingriff in die Grund- und Freiheitsrechte – ganz konkret und ganz aktuell der jüngste Anschlag in Wien. Vier Tage danach schritt die deutsche Ratspräsidentschaft zur Tat. Von **Ralf Wurzbacher**.

Gelegenheit macht Diebe. Große politische, ökonomische oder soziale Krisen sind erfahrungsgemäß beste Gelegenheiten für die Eliten, Dinge durchzusetzen, die sich in Normalzeiten nicht so leicht durchsetzen ließen. Wie die Gegenwart eindrucksvoll beweist, gilt das allemal für Gesundheitskrisen. Welche für die Allgemeinheit mithin unerfreulichen Maßnahmen die Bundesregierung allein in den Hunderte Milliarden Euro schweren Corona-Rettungspaketen versteckt hat, wird sich wohl erst offenbaren, wenn es für Widerstand zu spät ist. Und was von den massiven und mannigfachen Grundrechts- und Freiheitseingriffen nach Ende der Pandemie zurückgenommen beziehungsweise bleiben wird, steht genauso in den Sternen. Zur Erinnerung: Die im Gefolge der Anschläge vom 11. September 2001 in Deutschland erlassenen sogenannten Sicherheitsgesetze sind zum großen Teil noch heute in Kraft.

Als noch günstiger erweisen sich die Gelegenheiten, bei denen gleich mehrere Krisen zusammentreffen. Während die Fieberkurve der öffentlichen Erregtheit wegen Corona ohnehin schon seit Monaten auf hohem Niveau verharrt und dieser Tage weiter nach oben ausschlägt, erlebt die Welt nun zeitgleich eine Wiederkehr des islamistischen Terrors: angefangen mit den bestialischen Morden in Frankreich, gefolgt von der Attacke eines schießwütigen jungen Mannes in Wien, dessen Amoklauf vier Menschenleben und 23 Verletzte kostete. Im Nachgang der Ereignisse in der österreichischen Hauptstadt vom 2. November zeichnet sich immer mehr ab, dass die Bluttat womöglich hätte verhindert werden können, wären im Vorfeld nicht diverse Ermittlungspannen und andere Fälle von Behördenversagen aufgetreten. Wegen der Schwere der Verdachtsmomente wurde inzwischen eine Untersuchungskommission zur Klärung der Hintergründe eingesetzt.

**EU-Parlament kaltgestellt?**

Auch auf Ebene der Europäischen Union (EU) zog der Fall inzwischen Konsequenzen nach sich, allerdings keine, die unbedingt naheliegend erscheinen. Wie am Montag zuerst der Österreichische Rundfunk (ORF) berichtete, haben sich die EU-Mitgliedsstaaten auf Antrag

der deutschen Ratspräsidentschaft darauf verständigt, ein Verbot sicherer Verschlüsselungen bei der Kommunikation im Internet zu erlassen. Laut einem geheimen Entwurf, aus dem der Sender zitierte, sollen Messenger-Dienste wie WhatsApp, Signal und Telegram dazu verpflichtet werden, Geheimdiensten und Strafverfolgern Einblick in die Schriftwechsel und Gespräche ihrer User zu ermöglichen. Auf seiner Webseite schrieb der ORF wörtlich, „der Terroranschlag in Wien wird im EU-Ministerrat dazu benützt“, die Neuregelung ins Werk zu setzen.

Tatsächlich datiert das fragliche Dokument auf den 6. November, womit die Urheber binnen nur vier Tagen nach der Wiener Mordserie Nägel mit Köpfen gemacht haben. In diesem Tempo geht es weiter. Tatsächlich soll das Papier „beschlussfertig“ sein, schon Anfang Dezember könnten die EU-Innen- und -Justizminister ihren Segen zu einer entsprechenden Verordnung geben. Laut ORF ist der weitere Fortgang programmiert, weil auf höchster Ebene abgekaspert. Im Rat der ständigen Vertreter der Mitgliedsländer (COREPER), der sich am 25. November mit der Sache befasst, habe die Ratsvorlage den Status eines I-Items, womit sie ohne weitere Diskussion passieren kann.

Ob das EU-Parlament, aus dem schon jetzt heftige Unmutsbekundungen nach außen dringen, in der Angelegenheit tätig werden wird, ist nicht ausgemacht. „Angesichts der offenbaren Einstimmigkeit wäre es im Ministerrat allerdings möglich, die geplante Regulation in ihrem Kern auch ohne Mitwirkung des Parlaments durchzuziehen“, heißt es beim ORF.

**Augenwischerei vom Innenminister**

Konkret geht es bei dem Vorstoß um die sogenannte E2E-Verschlüsselung. Bei „End-to-End“ können nur der Absender und der Empfänger eine Nachricht auf ihren Geräten lesen, für unbefugte Dritte, staatliche Stellen und den Betreiber der Services sind die Inhalte nicht einsehbar. Ein „Verbot“ im strengen Sinne führen die Initiatoren nicht im Schilde. Die Technik soll nicht komplett aus dem Verkehr gezogen werden, sondern bei „Bedarf“ und mit Zutun der Plattformunternehmen ausgehebelt werden können. Diese wären verpflichtet, eine Art Generalschlüssel zu erzeugen und diesen bei den Behörden zu hinterlegen. Damit könnten sich diese dann jederzeit unerkannt in private Unterhaltungen und andere verschlüsselte Übertragungen einklinken. Von „Generalschlüssel“ bis „Generalverdacht“ ist es ein kurzer Weg, zumal sich sogenannte Terrorjäger und Strafverfolger mit politischer und richterlicher Rückendeckung inzwischen auf so ziemlich alles stürzen können, was irgendwie „gesinnungsmäßig“ aus der Reihe tanzt. Mitunter genügt schon ein falsches Wort (Bombe?) – und prompt steht der Staatsschutz vor der Tür.

Natürlich spielt besagter Resolutionstext die Tragweite des Vorhabens herunter. Ausdrücklich wird darin die Bedeutung der Verschlüsselung gewürdigt. Es müsse aber eine „bessere Balance“ zwischen dem Schutz der Privatsphäre einerseits und der Bekämpfung von organisierter Kriminalität und Terrorismus andererseits geschaffen werden. Die technischen Lösungen dafür müssten „den Grundsätzen der Rechtmäßigkeit, Transparenz, Notwendigkeit und Verhältnismäßigkeit“ entsprechen. Regierungen, Industrie, Forschung und Wissenschaft sollten zusammenarbeiten, „um dieses Gleichgewicht strategisch herzustellen“. Aus dem Bundesinnenministerium (BMI) verlautete, der Entwurf enthalte „keinerlei Lösungsvorschläge oder Forderungen nach Schwächung von Verschlüsselungssystemen“. Ziel sei es, „in einen dauerhaften Dialog mit der Industrie zu treten“, um einen „allgemeinen Konsens“ zu erzielen.

**Freier Zugang für „Five Eyes“**

Zurück zu den „guten Gelegenheiten“. Wie das „Heise“-Magazin schrieb, gab es zur neuesten Vorlage eine Vorversion vom 21. Oktober. War dort noch von Zugriff für Strafverfolgung und Justiz die Rede gewesen, sind diese nun – womöglich als Folge des Anschlags von Wien – unter „Competent Authorities“ subsumiert. Diese Gruppe schließt die Geheimdienste mit ein, also sämtliche Schlapphüte, egal ob im In- oder Ausland tätig. Sie sollen künftig ebenfalls ganz legal beim Chatten via WhatsApp, Threema und Co. mitlesen dürfen. Dazu passend ist auch die gewählte Methode zum Abschöpfen von Informationen namens „Exceptional Access“ oder „Man-in-the-Middle-Angriff“ eine Kopfgeburt der Schnüffler im Untergrund. Ersonnen wurde sie vom britischen Militärgeheimdienst GCHQ.

Es gibt weitere Hinweise, wer beim Verfassen der Ratsresolution die Feder führte. So ist Großbritannien neben den USA, Kanada, Australien und Neuseeland Teil der Geheimdienstallianz „Five Eyes“. Alle Beteiligten sind Vertragsparteien des multilateralen UKUSA-Abkommens, eines Vertrags über die gemeinsame Zusammenarbeit bei der Signalaufklärung. Vor genau einem Monat hatte sich „Five Eyes“ gemeinsam mit Regierungsvertretern Japans und Indiens mit einer Erklärung aus der Deckung gewagt. Darin forderten sie exakt das, was die EU nun hoppladihopp in die Tat umsetzen will: eine Hintertür (Backdoor) zu verschlüsselter End-to-End-Kommunikation. Demnach müssten Techfirmen den Strafverfolgungsbehörden Zugang zu Inhalten in einem lesbaren und nutzbaren Format ermöglichen, wenn dies legal erforderlich oder angemessen sei.

**Blaupause aus Deutschland**

Die Argumente, wie damit der öffentlichen Sicherheit gedient wird, lauten dabei wie folgt: Erstens verbauten sich die Plattformbetreiber durch Verschlüsselung die Möglichkeit, die

selbst gesetzten Gemeinschaftsregeln durchzusetzen. Zweitens könnten Strafverfolgungsbehörden auf diesem Wege Aktivitäten wie Gewaltverbrechen, terroristische Propaganda und Anschlagsplanung ermitteln. Außerdem verhindere eine Verschlüsselung, Kommunikationen automatisiert auf Kindesmissbrauch wie Cyber-Grooming zu analysieren. Man ist gerührt, wie sehr sich die Damen und Herren vom US-amerikanischen CIA oder beim britischen MI6 um das Wohl der Kleinsten sorgen, nachdem die US-Militärgeheimdienste in Afghanistan wiederholt das Auslöschen ganzer Hochzeitsgesellschaften befehligt haben.

Das, was nun in Windeseile und im Windschatten von Corona und Terrorismus an neuen Überwachungsmaßnahmen und Grundrechtseingriffen durchgedrückt werden soll, wurde laut ORF seit 2015 in einer ganzen Serie von Kampagnen vorbereitet. Immer mit dabei: „Five Eyes“, Europol und das US-amerikanische FBI. Bisher waren die Vorstöße aber stets am Widerstand von Datenschützern und Messenger-Diensten oder am Einspruch von Fachpolitikern gescheitert. Jetzt stehen die Dinge anders. Vor drei Wochen erst beschloss das Bundeskabinett so etwas wie eine Blaupause dessen, was auf EU-Ebene geplant ist. Danach sollen Geheimdienste in Zukunft Gespräche und Botschaften über verschlüsselte Messenger-Dienste belauschen und mitlesen dürfen – „selbstredend“ nur mit richterlicher Anordnung. Wer soll das glauben beim Blick auf die Profiteure: der Verfassungsschutz in Bund und Ländern, der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD). Außerdem sieht der Gesetzentwurf des Bundesinnenministers einen erweiterten Austausch von Informationen zwischen dem MAD und den Verfassungsschutzbehörden vor. Zudem werden die Hürden für die Beobachtung von Einzelpersonen durch den Verfassungsschutz gesenkt, wie Medien berichten.

**Datenschützer protestieren**

Immerhin: Ganz ohne Reibungen werden die Staatenlenker und ihre klandestinen Einflüsterer ihre Planspiele wohl doch nicht durchboxen. Für den Vorsitzenden des Bundestagsausschusses Digitale Agenda, Manuel Höferlin (FDP), kommt das Vorhaben „im Prinzip der Möglichkeit zur flächendeckenden Onlinedurchsuchung von Endgeräten gleich“ und sei deshalb „unverhältnismäßig“. Sein Parteikollege im EU-Parlament, Moritz Körner, beklagte ein „typisches Muster nach jedem Terroranschlag“. Eine Generalschlüssel-Lösung sei ein „sinnloser Angriff auf die Bürgerrechte“, während Terroristen andere Wege fänden, um sicher zu kommunizieren. Sein Urteil:

> „Ein Verschlüsselungsverbot wäre ein Terroranschlag auf die Bürgerrechte in der EU und würde jede private Kommunikation unsicher machen.“

Auch Thilo Weichert vom Netzwerk Datenschutzexpertise glaubt nicht daran, „dass die Entschlüsselung nur unter rechtsstaatlicher Kontrolle zum Einsatz käme“. Vielmehr drohten digitale Grundrechte „zum Totalverlust zu werden“.

Aus Sicht der Gesellschaft für Informatik (GI) gefährdet die Initiative nicht nur die informationelle Selbstbestimmung der Bürger, sondern desgleichen den Schutz von Betriebs- und Geschäftsgeheimnissen. „Auch für die politische Willensbildung und Gestaltung einer freien Gesellschaft brauchen wir eine verlässlich vertrauliche Kommunikation“, mahnte GI-Präsident Hannes Federrath. Kriminelle könnten dagegen auf unbeobachtbare Kommunikation mit Steganographie ausweichen.

**Klassisches Eigentor**

Vor einem klassischen Eigentor warnte Karsten Bartels vom Bundesverband IT-Sicherheit. Wenn Nachschlüssel in größerer Zahl in die falschen Hände fielen, könnte dies zu einer Katastrophe führen. Dennis-Kenji Kipker vom Bremer Institut für Informationsrecht beanstandete, dass immer wieder einzelne tragische Vorfälle herausgegriffen würden, „um sicherheitspolitische Vorhaben konsensfähig zu machen“. So werde aus einem Abwägen schnell eine „einseitige Sicherheitsrhetorik“, die nicht zwangsläufig zu einem verfassungskonformen Gesetz führe.

Sehr treffend kommentierte auch Erich Moechel, Verfasser des ORF-Beitrags, prämierter Investigativjournalist und Mitbegründer der österreichischen BigBrotherAwards: Bewillige der Rat den Resolutionsentwurf, dann könne das österreichische Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT), „das es nicht einmal schafft, einen Terroristen auszuschalten, der von zwei anderen Diensten zweimal auf dem Silbertablett serviert wird, künftig auch in Chatverläufen wochenlang nicht ermitteln“. Nun ließe sich sagen, damit befindet sich das BVT in schlechter Gesellschaft mit den deutschen „Nichtausschaltern“ des Attentäters vom Weihnachtsmarkt an der Berliner Gedächtniskirche vor vier Jahren. Aber lieber nicht – sonst hört noch jemand mit.

Titelbild: BeeBright/shutterstock.com