Anti-Terror-Kampf in Europa : Verschlüsselung als erklärter Feind ?

Seit den terroristischen Anschlägen auf das Satire-Blatt "Charlie Hebdo" im Januar 2015 hat sich in Frankreich die Debatte um die Regulierung von Informantions- und Kommunikationstechnologien verschärft. Vor einem Jahr wurden den französischen Geheimdiensten per Gesetz umfangreiche Möglichkeiten zur Bespitzelung von Mobilfunk und Datenverkehr in dem Land eingeräumt. Unter dem Eindruck der weiteren Anschläge in Paris, Nice oder Rennes wird der Druck auf die Regierung immer höher. Weitere Maßnahmen für die Kommunkationsüberwachung werden aus verschiedenen politischen Reihen gefordert - unter anderem das Verbot von Verschlüsselungstechnologien. Jetzt hat auch Innenminister Bernard Cazeneuve eine internationale Initiative gegen Verschlüsselung versprochen. Morgen will er sich darüber mit seinem deutschen Kollegen unterhalten. Drei Experten aus Frankreich reagieren.

Es ist eine Tatsache : unsere Sicherheitslage ist kritisch. In zwanzig Monaten hat der internationale Terrorismus mehrere hunderte Opfer in unserem Land verursacht. In diesem Klima allgemeiner Unsicherheit ist die Versuchung stark, immer neue Aktionsmittel für die Terrorismusbekämpfung einzusetzen, auch wenn allein in Frankreich 16 Anti-Terror-Gesetze in den letzten dreißig Jahren verabschiedet wurden, und alle noch nicht vollständig umgesetzt wurden. Viele von ihnen haben wichtige netzpolitische Implikationen.

Der Erfolg von kryptierten Messenger-Dienste wie Whatsapp oder Telegram hat Verschlüsselung wieder einmal in das Visier der Sicherheitskräfte gebracht. Der französische Innenminister Bernard Cazeneuve hat am 12. August auf einer Pressekonferenz einen internationalen Aktionsplan gegen Verschlüsselung angekündigt. Die Idee mag attraktiv klingen. Niemand bestreitet nämlich, dass eine robuste Verschlüsselung die Arbeit von Ermittlern erschweren kann, vor allem die sogenannte Ende-zu-Ende-Verschlüsselung. Ende-zu-Ende bedeutet, dass der Dienstanbieter selbst nicht über die Entschlüsselungsschlüssel verfügt, sondern nur die Chat-Teilnehmer. So attraktiv die Idee auch klingen mag, solche Technologien zu begrenzen, sie ignoriert die konkrete Realität von Netzwerken und übersieht die wesentliche Bedeutung von IT-Sicherheit in einer immer umfassender digitalisierten Gesellschaft. Sie steht deswegen auch im Widerspruch zu anderen politischen Zielen und sogar Gesetzen, wie das kürzlich verabschiedete Gesetz “für eine digitale Republik”, in welchem die Förderung von datenschutzfreundliche Technologien wie Verschlüsselung eingeführt wurde.

Die Verschlüsselungsdebatte ist nicht neu und ist global. Schon seit 40 Jahren stehen sich Sicherheitsdienste und Verteidiger von Grundfreiheiten entgegen (“während den so genannten “Crypto Wars”). Frankreich blieb lange international isoliert: erst in den späten 1990er Jahre wurde Kryptographie nicht mehr ausschließlich als Kriegswaffe betrachtet. Nun scheint es, als wollten Politiker erneut diese Position auf europäischer Ebene vertreten, obwohl diese jahrelang die erfolgreiche Digitalisierung von Wirtschaft und Gesellschaft behindert hat. Heute kann es sich Europa aber nicht mehr leisten, in diesem Bereich hinterzuhinken. Man muss sich vorstellen, dass während Europe sich in endlosen

Diskussionen zur Ende-zu-Ende-Verschlüsselung verliert, China seinerseits schon den ersten Satelliten ins Orbit geschickt, der dank Quantenkryptographie eine komplett abhörsichere Kommunikation ermöglichen soll.

VERSCHLÜSSELUNG IST EIN GRUNDLEGENDES ELEMENT UNSERER SICHERHEIT

Wie jedes technische Innovation ist die Kryptographie gleichermaßen Gift oder Medizin, je nachdem, ob sie in gute oder schlechte Hände fällt. Die verschlüsselten Messenger-Dienste, die von Terroristen genutzt werden, werden auch sehr von Politikern, Angestellten der Ministerien, Unternehmen und Bürgern geschätzt! Und das aus gutem Grund: Verschlüsselung ist für unsere Sicherheit in der digitalen Welt von wesentlicher Bedeutung.

Jeden Tag schützen kryptographische Systeme Milliarden von Individuen gegen Cyber-Bedrohungen, die sich zunehmend verstärken. Sie sind das Rückgrat des Vertrauens in der digitalen Welt. Es sind Verschlüsselungstechnologien, die es uns ermöglichen, sicher eine Banküberweisung zu machen, oder unsere Gesundheitsdaten in einer elektronischen Gesundheitsakte zu speichern. Es sind auch diese Technologien, die die Untersuchungen der Panama Papers erlaubten, indem sie die Vertraulichkeit der Quellen gewährleisteten. Für Unternehmen sind sie heute der beste Schutz vor Wirtschaftsspionage. In Frankreich schätzt man, dass der durch Wirtschaftsspionage entstandene Schaden allein im Jahr 2013 sich auf mehr als 40 Milliarden Euro belaüft. Kleine und mittlere Unternehmen sind die ersten Opfer dieser Angriffe, weil sie sich eine robuste Verschlüsselung nicht leisten können.

VERSCHLÜSSELUNG EINSCHRÄNKEN BEDEUTET DIE SICHERHEIT ALLER NETZE SCHWÄCHEN

Ein Vorschlag, der regelmäßig aus Sicherheitskreisen befürwortet wird, ist Hersteller und Dienstleister zu zwingen, in ihre Systeme “Backdoors” gezielt einzuführen. Diese Backdoors sind geheime Passagen - oder Sicherheitslücken - die den Behörden zur Verfügung gestellt werden sollen, um einen Zugriff auf verschlüsselte Daten ohne Wissen des Benutzers zu ermöglichen. Die Idee ist zwar von gesundem Menschenverstand geprägt, besteht aber den Realitätstest nicht. Denn wie kann man sich hinter seiner Panzertür sicher fühlen, wenn man weiß, dass es einen Universalschlüssel gibt, der diese öffnen kann - auch wenn dieser Schlüssel nur im Besitz von Polizei oder Behörden wäre?

Experten - unter anderen die *Nationale Agentur für Sicherheit der Informationssysteme (ANSSI)* - sind sich einig: es ist technisch unmöglich sicherzustellen, dass ein solcher Zugang nur den berechtigten Personen zur Verfügung steht. Zu jeder Zeit können sie zu offenen Türen für kriminelle, mafiöse oder terroristische Organisationen werden. Die Verallgemeinerung von Backdoors wäre somit katastrophal für die Sicherheit und Freiheit aller Nutzer.

Darüber hinaus ist es sehr wahrscheinlich, dass diese Maßnahmen eine mehr als relative Effizienz für den Kampf gegen die Nutzung von Verschlüsselung für terroristtische Zwecke. Verschlüsselungstechnologien sind nämlich öffentlich und weltweit verbreitet, also frei zugänglich für alle kriminellen Vereinigungen. Wie also verhindern, dass Terroristen ihre eigenen verschlüsselten Anwendungen entwickeln und ungestört ein höheres Maß von Sicherheit genießen, während eine Mehrheit von berechtigten Nutzern ungeschützt bleibt?

Das allgemeine Beschränken von Verschlüsselung für die breite Öffentlichkeit bedeutet also, feindseligen Organisationen ein Monopol zur sicheren Kommunikation zu gewähren.

VERSCHLÜSSELUNG IST KEIN UNÜBERWINDBARES HINDERNIS FÜR ERMITTLER

Es kann vernünftigerweise nicht behauptet werden, dass Verschlüsselung ein unüberwindliches Hindernis für Ermittler ist - obwohl auch nicht zu leugnen ist, dass sie den Zugang zu bestimmten Informationen erschweren kann. Erstens ist es meistens möglich, eine Verschlüsselung durch die Ausnutzung technischer Schwachstellen, Entzifferung oder durch direktes Einbrechen in die Ausrüstung der Zielperson zu umgehen. Zweitens bleiben Metadaten im Gegensatz zum Inhalt der Kommunikationen unverschlüsselt. Wer kommuniziert mit wem? Wann und wie lange? Wo war er oder sie lokalisiert? Diese Daten beantworten die wichtigsten Fragen rund um unsere Gewohnheiten, unsere Mitarbeiter, unsere Interessen, unsere Meinungen. Sie sind extrem empfindlich, und das ist auch der Grund, warum das letzte französische Anti-Terror-Gesetz, welches eine massive Sammlung von Metadaten ermöglicht, vielfach kritisiert wurde. Bevor eine neue Gesetzgebung in Betracht gezogen wird, sollte zunächst sichergestellt werden, dass Sicherheitsdienste die vielen Möglichkeiten, die ihnen schon geboten werden, vollständig nutzen.

Aus dieser Sicht sollte auf jeden Fall ein Verfahren bevorzugt werden, das die Zusammenarbeit mit Dienstanbietern für einen Zugriff auf Daten unter richterliche Kontrolle stellt. Es wäre in der Tat zweckmässig, die Regeln zur gerichtlichen Zusammenarbeit zu stärken, insbesondere die sogenannten *mutual legal assistance treaties (MLAT),* die den Austausch von Informationen und Daten während laufenden Ermittlungen erlauben - um Übertragungsverzögerungen zu reduzieren. Darin könnte der Sinn einer internationalen Initiative liegen.

VERSCHLÜSSELUNG TRÄGT ZUR WIDERSTANDSFÄHIGKEIT UNSEREN DIGITALEN GESELLSCHAFTEN BEI

Die zunehmende Digitalisierung unseres Alltags, sowie die erhöhte Rechenleistung und der anhaltende Rückgang der Kosten von Datenspeicherung machen Massenüberwachung weniger teuer. Es stellen sich also grundsätzliche Fragen überall auf der Welt, und in Frankreich sind wir in der glücklichen Lage, über die potenzielle Nützlichekit von dieser Art von Überwachung und die dadurch entstehenden Probleme zu diskutieren. Die Verantwortung ist historisch: Verschlüsselung - und die Grundfreiheiten, deren Ausübung sie ermöglicht - ist ein Schutzwall gegen möglichen Missbrauch staatlicher Gewalt. Sie ist auch ein Schutz gegen den zunehmenden Einfluss privater Konzerne auf unser digitales Leben.

Wir leben in einer Zeit der Unruhe und Unsicherheit. Die Versuchung kann stark sein, unseren Wunsch nach Sicherheit auf Kosten unserer wirtschaftlichen Entfaltungsmöglichkeiten und wesentlicher Grundlagen unserer Gesellschaft nachzugenen: Gleichheit, die Achtung von Grundrechten und Rechtsstaatlichkeit. Genau die Prinzipien, die Frankreich einst als Vorreiter verteidigt hat. Diejenigen, die uns angreifen, versuchen eine emotionale Reaktion hervorzurufen - keine rationale. Statt “stapelweise” Maßnahmen zu ergreifen, die im Notfall und unter dem Einfluss von Emotionen entschieden werden, sollten wir angesichts des Ausmaßes dieser Transformationen eine umfassende und kollektive Debatte führen. Es geht `hier um die Widerstandsfähigkeit unserer Gesellschaften.

Mounir MAHJOUBI, Unternehmer, Präsident des *Conseil national du numérique (französischer Digitalrat)*

Gilles BABINET, Digitaler Botschafter von Frankreich bei der Europäischen Kommission

Isabelle FALQUE-PIERROTIN, Präsidentin der *Commission Nationale de l'Informatique et des Libertés* (nationale Datenschutzbehörde Frankreichs)