Nichts zu verbergen?

Sicher und vertraulich kommunizieren: Ein Grundrecht

Bild: Albert Hulm

Zum Recht auf informationelle Selbstbestimmung gehört auch vertrauliche Kommunikation. Angriffe auf dieses Grundrecht gibt es traditionell nicht nur von Kriminellen, sondern auch von Staaten – einschließlich solchen, die sich gern als freiheitlich-demokratisch einordnen. Jeder Einzelne kann viel tun, um vertraulich zu mailen, zu chatten und zu telefonieren. Oft ganz ohne Komfortverlust.

Von Jan Mahn

Deutschland ist ein freies Land – zu dieser Erkenntnis kommen seit Jahren auch die Politikwissenschaftler der unabgängigen Forschungsorganisation Freedom House. Sie machen sich alljährlich die Mühe, die Freiheit aller Staaten der Welt zu erforschen. Für jedes Land schreiben sie einen Bericht und vergeben Punkte in 25 Kategorien (siehe ct.de/ypbr). Darin geht es um Wahlen, Presse- und Demonstrationsfreiheit und auch um die Freiheit im Internet. Mit 94 von 100 möglichen Punkten schneidet Deutschland vergleichsweise gut ab, Österreich kommt auf 93 Punkte, die Schweiz auf 96.

In Kategorie D4 geht es in den Länderberichten um die Freiheit, keine Überwachung fürchten zu müssen. Diese Freiheit ist in Deutschland gesetzlich verankert: Das Grundgesetz kennt das Post- und Fernmeldegeheimnis, die Europäische Menschenrechtskonvention nennt in Artikel 8 das Recht auf Achtung des Privatlebens und den Schutz der Korrespondenz. Es ist also ein Grundrecht, vertraulich mit anderen kommunizieren zu können – auch dann, wenn sich die Gesprächspartner nicht gegenüber sitzen und ein elektronisches Medium die Übertragung übernimmt.

Vertrauliche Kommunikation ist nicht nur für die wenigen Berufsgruppen wichtig, die immer wieder genannt werden, wenn es um verschlüsselte Kommunikation geht: Journalisten, Whistleblower und Dissidenten in unfreien Staaten müssen natürlich besonders auf Vertraulichkeit achten, jeder andere sollte von seinem Grundrecht aber ebenfalls großzügig Gebrauch machen.

Denn auch als Normalbürger hat man eine Menge zu verlieren, wenn man sich auf die Vertraulichkeit des Geschriebenen nicht verlassen kann. Wer meint, er habe nichts zu verbergen, sollte am besten von einem Messenger direkt auf Twitter wechseln und die nächste Kneipentour nach der Pandemie mit Freunden in aller Öffentlichkeit planen und im Anschluss auch dort nachbesprechen. Spätestens, wenn man mit Kollegen oder Kunden über dienstliche Inhalte kommuniziert, ist Vertraulichkeit oft entscheidend. Wer mit Kundendaten fahrlässig umgeht, muss die DSGVO fürchten, wer Firmengeheimnisse ungeschützt übermittelt, muss Angst vor Industriespionen haben.

Es ist also ein Grundrecht, vertraulich mit anderen kommunizieren zu können.

Mühsame Angriffe

Die Gefahr, von staatlichen Stellen abgehört zu werden, wirkt in Europa nicht so groß. Doch auch Deutschland bekommt in dieser Kategorie von den Freedom-House-Forschern Punktabzüge unter anderem für die Quellen-Telekommunikationsüberwachung (TKÜ). Im Visier sind dabei vor allem die Messaging-Dienste. Strafverfolgungsbehörden dürfen auf richterliche Anordnung einen Trojaner auf dem Mobiltelefon einer verdächtigen Person installieren, der zum Beispiel Screenshots der Nachrichten aufzeichnet und diese an die Strafverfolger verschickt. Das Verfahren ist aber mühsam, meist muss ein Ermittler mehrere Minuten Zugriff auf das Telefon des Verdächtigen haben.

Die beschwerliche Quellen-TKÜ ist für die Strafverfolger auch nur eine Notlösung – das Problem für alle, die vertrauliche Kommunikation mitlesen wollen, ist die Ende-zu-Ende-Verschlüsselung. Sie stellt sicher, dass nur die Gesprächspartner einen Schlüssel besitzen, um die Nachrichten lesen zu können. Alle anderen auf dem Weg, also der Betreiber des WLANs, die Internetanbieter, Knotenpunkte, abzapfende Geheimdienste, aber auch zum Beispiel die Betreiber der Messenger selbst, sehen nur verschlüsselten Datensalat. Ende-zu-Ende-Verschlüsselung schützt die Kommunizierenden nicht nur vor individueller Überwachung. Vor allem schützt sie zuverlässig vor der Massenüberwachung ganzer Gesellschaften. Eine solche haben unter anderem die Geheimdienste der USA und Großbritanniens weltweit eingerichtet, indem sie an Internetknotenpunkten große Teile des Internetverkehrs ausleiten und auswerten. Gegen Ende-zu-Ende-verschlüsselte Nachrichten kommen aber auch BND, GCHQ und NSA nicht an.

Das liegt schlicht daran, dass Ende-zu-Ende-Verschlüsselung durch die einzigen Gesetze geschützt wird, die Geheimdienste nicht beugen und Politiker nicht durch Verordnungen aushöhlen können: durch die Gesetze der Mathematik. Die stellen sicher, dass es beim Knacken der Verschlüsselung aktuell keine Abkürzungen gibt und man auch mit viel teurer Hardware nicht effizient entschlüsseln

kann, wenn man den Schlüssel nicht kennt. Warum Ende-zu-Ende-verschlüsselte Übertragung kryptografisch sicher ist und was es mit Selbstheilung und Abstreitbarkeit auf sich hat, erfahren Sie auf Seite 60. Wie verschiedene Messenger-Anbieter die Ende-zu-Ende-Verschlüsselung umsetzen und welche Auswirkungen das auf den Komfort hat, lesen Sie ab Seite 56.

Schwere Geschütze

Mit diesem für Überwacher unbefriedigenden Zustand wollen sich auch in Deutschland einige Politiker aber nicht abfinden – allen voran das CSU-geführte Innenministerium. Zusammen mit den europäischen Amtskollegen haben sie eine Resolution auf den Weg gebracht, in der sie Zugriffe für Strafverfolger und zuständige Stellen auf verschlüsselte Kommunikation fordern. Ausführlich berichtet haben wir darüber Mitte Dezember 2020 [1]. Wie die Zugriffe auf die Nachrichten technisch aussehen sollen, ist mehr als unklar. Funktionieren kann das nur, indem man Lücken in die Software einbauen lässt, die Ende-zu-Ende-Verschlüsselung stellenweise deaktiviert, die Kommunikationspartner aber nicht darüber informiert. Ein mathematischer oder informationstechnischer Weg, Verschlüsselung nur ein bisschen zu brechen, existiert nicht. Problematisch sind solche Zugriffe unter anderem rechtlich: In Deutschland muss man keine Strafverfolgung fürchten, wenn man den ungarischen Ministerpräsidenten Viktor Orbán als Diktator und Faschisten bezeichnet, in Ungarn sieht das möglicherweise anders aus. Gäbe es nun eine richterliche Anordnung aus Ungarn an einen Messenger-Betreiber, die Inhalte einer Unterhaltung von zwei Deutschen offenzulegen und die Verschlüsselung zu umgehen – wer sollte entscheiden, welches Recht jetzt schwerer wiegt? Was, wenn die Unterhaltung von einem Deutschen und einem Ungarn geführt wurde?

Davon lassen sich Seehofer und seine Kollegen aber nicht abhalten und sprechen von einem Dialog mit den Anbietern, der nötig sei, um technische Lösungen zu finden. Sollten sie mit ihren Grundrechtseinschnitten im EU-Parlament und später in den nationalen Parlamenten durchkommen, müssten die Messenger-Anbieter dem auch Folge leisten. Tun sie das nicht, droht ihnen der Rauswurf aus den Stores von Apple und Google. Das trifft allerdings vor allem die Mehrheit der Bürger, deren Grundrecht beschnitten wird. Kriminelle würden dann auf andere Kanäle ausweichen. Mit solchen Hintertüren wäre außerdem nicht nur die gezielte Überwachung von Verdächtigen auf richterliche Anordnung möglich. Auch Massenüberwachung, wie sie Europa in den USA immer scharf kritisiert hat, wäre dann technisch kein Problem mehr. Die Geschichte der Hintertüren und Zweitschlüssel zeigt leider: Noch nie ist ein solches Instrument langfristig nur einem kleinen Kreis zugänglich geblieben. Zu den größten Fehlgriffen zählten die Hintertüren, die Netzwerkausrüster Juniper in seine Geräte auf Veranlassung der NSA einbauen musste. Genutzt wurden sie schnell auch vom chinesischen Geheimdienst.

Ende-zu-Ende-Verschlüsselung verhindert zuverlässig die Massenüberwachung ganzer Gesellschaften.

Im Freedom-House-Index dürften solche gesetzlich vorgeschriebenen Hintertüren zu massivem Punktabzug führen, Deutschland und die EU, einst Vorreiter bei der Freiheit, würden ins Mittelfeld abrutschen. Gleichzeitig schwächt man damit auch Argumente für die eigene Weltsicht: Unternehmen werden von der DSGVO aktuell dazu gebracht, personenbezogene Daten nur in Europa zu verarbeiten und nicht in den USA – dort erlaubt es der Cloud Act den Geheimdiensten, auf die Daten in den Rechenzentren zuzugreifen. An diesem Streitpunkt scheiterte zuletzt das Datenschutzabkommen Privacy Shield und Europa konnte immer aus der Position moralischer Überlegenheit argumentieren. Mit eigenen Hintertürgesetzen wäre damit Schluss.

Andere Wege

Möchte man auch dann noch abhörsicher kommunizieren, wenn die Innen- und Sicherheitspolitiker mit ihrer Grundrechtseinschränkung erfolgreich waren, kann man auf dezentrale Kommunikationssysteme umsteigen. Bei der populärsten dezentralen Kommunikationslösung gibt es keinen Anbieter, den man per Gesetz zu Hintertüren zwingen kann: Die gute alte E-Mail wird seit Jahrzehnten aber meist unverschlüsselt verschickt. Das liegt daran, dass Ende-zu-Ende-Verschlüsselung nicht Teil der Protokolle ist, nicht jeder Mailclient mitspielt und die Einrichtung durchaus mit Komfortverlusten verbunden ist. Auf Seite 54 erfahren Sie, was trotzdem möglich ist und wie Sie vertrauliche E-Mails versenden.

Vertraulichkeit ist nicht nur beim geschriebenen Wort oft wünschenswert. Telefonate sind schon seit vielen Jahrzehnten im Fokus von Mithörern. Was Sie tun können, um möglichst große Teile der Verbindung zwischen Ihrem Telefonhörer und dem Hörer Ihres Gesprächspartners zu verschlüsseln, und ob es wahre Ende-zu-Ende-Verschlüsselung bei Telefonaten überhaupt gibt, erfahren Sie ab Seite 58.

Datenbeiwerk

Nicht nur die Inhalte der Nachrichten sind für alle Arten von Mithörern interessant. Strafverfolger, Geheimdienste, aber auch die Werbewirtschaft interessieren sich brennend dafür, wer mit wem zu welcher Uhrzeit und von welchem Gerät kommuniziert. Mit solchen Metadaten kann man, sofern man genug davon hat, eine Menge über Personen, Netzwerke und Beziehungen erfahren. Scrollen Sie einfach mal durch Ihre letzten Chatverläufe, achten nur auf die Uhrzeiten und überlegen Sie, welche Schlüsse man allein daraus über Sie und Ihre Gesprächspartner ziehen könnte, wenn man diese Informationen systematisch auswertet. Wenn man dann noch einbezieht, wer mit wem in welcher Gruppe ist, wird das Bild komplett.

In den folgenden Artikeln geht es daher nicht nur um die reine Verschlüsselung der Inhalte, sondern auch um den Schutz und die Vermeidung von Metadaten. Das Recht auf private Korrespondenz beschränkt sich schließlich nicht nur auf die reinen Gesprächsinhalte.

(jam@ct.de) **c't**

Literatur

[1] Jan Mahn, Niemand hat die Absicht ..., Innenminister wollen Verschlüsselung umgehen, c't 26/2020, S. 16

Länderberichte von Freedom House:
ct.de/ypbr