MEHR DATENSICHERHEIT UND SCHUTZ VOR MASSENÜBERWACHUNG

Politische Strategien

GERHARD SCHMID || Der Konflikt zwischen dem Schutz der Privatsphäre und Sicherheit ist alt, aber eine Debatte darüber ist hochaktuell. Der technische Fortschritt bei Großrechnern und in der Speichertechnologie, die zunehmende Nutzung sozialer Netzwerke im Internet und die Gesetzgebung nach 9/11 in den USA haben die Möglichkeiten einer Überwachung der privaten Kommunikation durch Nachrichtendienste dramatisch ausgeweitet. Die Geschichte der Fernmeldekontrolle lehrt, dass Nachrichtendienste in diesem Feld alles tun, was sie technisch können und was das Gesetz ihnen erlaubt. Darum muss die Verhältnismäßigkeit heutiger Überwachungsmöglichkeiten auf den Prüfstand gestellt werden.

HILFE ZUR SELBSTHILFE LEISTEN

Auf dem internationalen Datenhighway schützt niemand unsere Privatsphäre vor einem Zugriff der Dienste. Die Situation ist vergleichbar mit dem wilden Westen, wo draußen in der Prärie sich jeder selbst verteidigen musste. Da kam höchstens mal alle paar Wochen ein US-Marshal vorbei, aber in unserem Zusammenhang wäre der auch kein Hoffnungsträger. Es wurde schon viel über die Möglichkeiten gesprochen, wie der Einzelne seine elektronische Kommunikation mit Verschlüsselung schützen kann. Leider wird das viel zu wenig genutzt, und das ist kein Kostenproblem. Es gibt sehr gute und sichere Open-Source-Software kostenlos im Internet. Vielmehr handelt es sich um ein Schwellenproblem, die meisten kennen sich leider damit nicht aus. Der Staat hat da meiner Auffassung nach eine Verpflichtung, Hilfestellung zu leisten. Das Grundgesetz verpflichtet ihn zum Schutz der Bürger – und das schließt Prävention mit ein. Wenn ich mir ins Gedächtnis rufe, mit welchem Werbeaufwand zur Zeit einer möglichen Bedrohung durch die Schweinegrippe massiv dazu geraten wurde, sich möglichst nicht die Hände zu geben und vor allem mehrfach am Tag die Hände zu waschen – wo bleibt denn eine vergleichbare Initiative, die für Verschlüsselung der E-Mails wirbt? Es kann jedenfalls nicht sein, dass die ultimative Antwort der Politik sich auf die Kryptokurse der Piratenpartei beschränkt.

Mir ist durchaus klar, dass der Staat da in einer Klemme steckt. Einerseits sollen seine Sicherheitsorgane im Rahmen der Gesetze Kommunikation überwachen können und andererseits soll er Bürgern helfen, Kommunikation vor Zugriffen zu schützen. Das dafür zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) löst meiner Beobachtung nach den Konflikt so: Es versucht, die Kommunikationsinfrastruktur unserer Behörden zu schützen, und es berät vorrangig die Wirtschaft. Um fair zu sein: Wenn man sich als Bürger selber darum kümmert, bekommt man auch vom BSI durchaus brauchbare Hilfe. Aber von einer massenhaften Werbekampagne für Verschlüsselung ist das Amt meilenweit entfernt.

Letztlich ist das aber zu kurz gedacht. Weder den Kadern der Organisierten Kriminalität noch den Terroristen muss man Verschlüsselung beibringen – die können das schon! Ich erinnere mich gut daran, dass sich das BKA schon sehr früh darüber beklagt hat, dass die versprengten Reste der RAF nicht zu fassen waren, weil die Herrschaften ihre E-Mails mit dem Verschlüs-

selungsprogramm PGP verschlüsselt haben. Im Übrigen: Die Metadaten, das heißt die Information, wer mit wem wann kommuniziert hat – heutzutage der erste Ansatz beim elektronischen Ermitteln –, lassen sich naturgemäß nicht verschlüsseln. Es sei denn, jemand kommuniziert über Thor, aber wer tut das schon.

Fazit: Wenn der Staat dem normalen Bürger dabei helfen würde, seine Kommunikation sicherer zu gestalten, würde er in Wahrheit wenig auf der Sicherheitsseite einbüßen.

UNTERSTÜTZUNG TECHNISCHER MAßNAHMEN

Die Datenpakete einer E-Mail werden heutzutage nicht auf dem geographisch kürzesten, sondern auf dem billigsten oder schnellsten Weg verschickt (geroutet). Eine E-Mail von Kloster Banz nach München kann also unter Umständen über London oder Amerika laufen. Nach den Enthüllungen von Snowden sind technische Vorschläge aufgetaucht, die Kommunikation wieder, wie in der Vergangenheit, auf dem kürzesten Weg im Lande zu halten. Die Bundesregierung will das nicht erzwingen (obwohl sie es könnte), sondern verweist darauf, dass es Anbieter dafür auf dem Markt gibt, z. B. die Deutsche Telekom. Ungeklärt ist bisher, ob die Netzkapazitäten in Deutschland dafür ausreichen. Sobald jemand aber einen der Internetdienste wie Twitter oder Facebook nutzt, deren Server in den USA stehen, nützt das wenig.

Ein weiterer Vorschlag zielt darauf ab, das Routing auf die Schengenstaaten zu begrenzen – damit wäre Großbritannien raus. Das wäre aber nicht mehr als weiße Salbe, weil nicht allein die USA und die Briten strategische Fernmeldekontrolle betreiben. Die meisten Schengenstaaten machen das auch, und zwar unter weniger strengen Auflagen, als wir sie für die Dienste in Deutschland haben.

Schließlich gibt es den Vorschlag, beim Aufbau von Kapazitäten für Cloud Computing in der EU (fälschlich in der Presse auch Schengen-Cloud genannt) politisch zu helfen. Das wäre in der Tat sinnvoll, weil Cloud Computing ökonomische Vorteile hat und die Betreiber von solchen Servern dem Europäischen Datenschutzrecht und nicht dem US-Recht unterliegen würden. Allerdings muss sichergestellt werden, dass Firmen mit Sitz in Drittstaaten, die in der EU Server betreiben, dies nur dann können, wenn das Recht am Ort der Betriebsstätte ihrem nationalen Recht vorgeht. Im Klartext: Der in den USA auch bei Gerichten verbreiteten Allmachtsphantasie, dass amerikanisches Recht für amerikanische Firmen global gelte, muss ein wirksamer und eindeutiger Riegel in der neuen EU-Datenschutzgrundverordnung vorgeschoben werden.

Außerdem gibt es Debatten darüber, ob man nicht so etwas wie Twitter oder Facebook auf europäischer Ebene aufbauen könnte.

NO-SPY-ABKOMMEN

In die deutsche politische Debatte über die Abhörpraktiken der NSA wurde letztes Jahr der Vorschlag eines bilateralen „No-Spy-Abkommens“ zwischen den USA und der Bundesrepublik Deutschland eingebracht. Er kam auf, als öffentlich wurde, dass die NSA das Mobiltelefon von Kanzlerin Merkel abgehört hatte. Die Diskussion wurde sehr emotional geführt und hat eines nicht bedacht: Staaten haben Interessen, aber keine Freunde. Sogar innerhalb eines Verteidigungsbündnisses können die sonstigen Interessen der Partner völlig verschieden sein. In Wahrheit ist es so: Staaten spionieren einander aus, um politische oder wirtschaftliche Vorteile zu erlangen, und es gibt da keinen Tabubereich, der durch Freundschaft abgegrenzt würde. Das Ganze war eine romantische deutsche Idee ohne eine echte Chance auf Verwirklichung. Staaten werden durch das Völkerrecht nicht vor Spionage geschützt, ausdrückliche Regeln oder Konventionen fehlen. Aber sie können sich mit Verschlüsselung, mit ihrem Strafrecht und mit einem geheimen Spionageabwehrdienst schützen. Meinem Urteil nach haben in der Vergangenheit deutsche Bundesregierungen den Verfassungsschutz nicht dazu angehalten, auch die Aktivitäten der Nachrichtendienste von westlichen Verbündeten und von Israel aufzuklären. Das Gegenteil soll der Fall gewesen sein. Es macht keinen Sinn, einem Nachbarn vorzuwerfen, dass er durchs Fenster in Schlafzimmer schaut, wenn man die Vorhänge nicht zuzieht.

SCHUTZ DURCH RECHT

Der Schutz der Privatsphäre von Bürgern vor Eingriffen des Staates beruht auf rechtlichen

Regelungen. Die Privatheit der Kommunikation gehört zu den elementaren Menschenrechten und deshalb ist er in Demokratien Bestandteil der Verfassungen. Bei uns regelt das Artikel 10 des Grundgesetzes. Mögliche Eingriffe der Polizei oder eines Nachrichtendienstes dürfen nur auf der Grundlage eines Gesetzes für diese genau beschriebenen Fälle und Zwecke erfolgen, wobei der Grundsatz der Verhältnismäßigkeit stets gilt. Ein Abhören oder das Öffnen von Briefen muss von einer unabhängigen Person, z. B. von einem Richter, genehmigt werden, der die Angemessenheit prüft. Die den Staat einschränkenden Vorschriften gelten aber nur für die eigenen Staatsbürger oder für Personen, die sich gerade im Staatsgebiet aufhalten. Sie gelten nicht für den Rest der Menschheit.

Damit sind wir beim Kern des Problems. Die Kommunikation hat sich heutzutage globalisiert, der Schutz gilt aber nur innerhalb des Nationalstaates. Bedrohungen haben sich auch im nichtmilitärischen Bereich internationalisiert und oft liefert nur Kommunikationsüberwachung die einzigen Informationen darüber. Die Aktivitäten einer Terrorzelle, die sich im Gebiet eines nicht funktionsfähigen oder nicht zur Zusammenarbeit bereiten Staates angesiedelt hat, ist ein Beispiel. Die Geldwäscheoperationen der Internationalen Organisierten Kriminalität ein anderes. Aber all das darf nicht dazu führen, dass der Schutz der Privatsphäre auf dem internationalen Datenhighway völlig verloren geht.

Derzeit gibt es fast keinen wirksamen Schutz der Privatsphäre durch internationales Recht. Das UN-Abkommen zum Schutz ziviler und politischer Rechte zielt mit dem Art. 17 auf den Schutz der Privatsphäre. Aber es ist in der Praxis nicht justiziabel und damit wertlos. Die Charta der Menschenrechte der Europäischen Union ist auf das Verwaltungshandeln von Mitgliedstaaten außerhalb des Bereichs der Anwendung von EU-Recht nicht anwendbar. Der einzige grenzüberschreitend wirksame Schutz der Menschenrechte geht von der Europäischen Menschenrechtskonvention des Europarates aus. Die dort formulierten Menschenrechte sind nicht an die Nationalität gebunden, sondern müssen von den Unterzeichnerstaaten allen Bürgern auch der anderen Unterzeichnerstaaten gewährt werden.

Das zu lösende Problem ist kein europäisches und kann deshalb allein innerhalb Europas nicht gelöst werden. Aber der Ansatz des Europarates könnte als Blaupause für ein künftiges internationales Abkommen dienen, das die folgenden Elemente aufweisen müsste:

- Es sollte ein Abkommen zwischen demokratischen Nationalstaaten sein, das von ihren Parlamenten ratifiziert wird. Eine Koalition von „Willing States“ sollte beginnen und weitere Staaten zur Teilnahme einladen.
- Die Privatsphäre einer Person, die im Hoheitsgebiet der Unterzeichnerstaaten lebt, sollte genauso geschützt werden wie die eines Staatsbürgers.
- Im Rahmen dieses Abkommens werden Staatsangelegenheiten nicht als Teil der Privatsphäre eines Bürgers betrachtet.
- Die Entscheidung über das Mitschneiden einer privaten Kommunikation durch die Polizei oder einen Nachrichtendienst setzt die Genehmigung durch eine unabhängige Person, z. B. einen Richter, voraus.
- Die Suchbegriffe für die strategische Fernmeldekontrolle müssen ebenfalls einer entsprechenden Kontrolle unterliegen.
- Ein Gerichtshof wird eingerichtet, an den sich Bürger wenden können.
- Die Vertragsstaaten passen ihre nationale Gesetzgebung, die Befugnisse der Polizei und der Nachrichtendienste regelt, dem Abkommen an.

Dieser Ansatz verwirklicht nur Minimalstandards, aber mehr wird nicht zu erreichen sein. Ein solches Abkommen hat nur dann eine Chance auf Verwirklichung, wenn sich die bisher eher national organisierten Bürgerbewegungen für den Datenschutz internationalisieren. Die Nachrichtendienste werden zunächst dagegen sein, weil es ihre Arbeit komplizierter macht. Aber sie sollten bedenken, dass die ganze Fernmeldekontrolle irgendwann von weltweiten Bürgerprotesten hinweggefegt werden wird, wenn nicht rechtsstaatliches Streben auch international einbezogen wird.

DR. GERHARD SCHMID

Vizepräsident des Europäischen Parlaments a. D., Regensburg