Die Ohren weit geöffnet: Lawful Interception

Alle Staaten der Welt haben ein Interesse daran, unter bestimmten Umständen auf die Kommunikation der eigenen BewohnerInnen zugreifen zu können. Dabei ist nicht nur relevant, was gesprochen wird, sondern auch, wer mit wem wann redet. Manchmal möchten Staatsorgane auch darüber Bescheid wissen, was an Gesprächen aus dem eigenen in ein fremdes Land läuft oder gar über Kommunikation, die sich ganz außerhalb des eigenen Territoriums abspielt.

Abgehört wird aus Gründen der Durchführung oder Bekämpfung z.B. von Terrorismus, verfassungsfeindlichen Bestrebungen, Kinderpornografie, Internetkriminalität, Drogenhandel, Datenklau und Spionage. Mit den Überwachungsmaßnahmen werden Beweise gesichert, anlassunabhängige Kontrollen durchgeführt oder einfach nur abgeschreckt und eingeschüchtert.

Abgehört wird potenziell jede Form der Kommunikation, vom Festnetz- und Mobiltelefon über Fax, Mail, Chat, Zugriffe auf Webseiten bis hin zu ganz normalen Gespächen („großer Lauschangriff"). Wie das technisch auszusehen hat, schreibt in der BRD die Regulierungsbehörde für Post und Telekommunikation vor[1] .Den rechtlichen Rahmen hingegen geben etliche Gesetze vor, an denen in den letzten Jahren im Windschatten der Terrorhysterie eifrig herumgeschraubt wurde; zu erwähnen sind hier in erster Linie:

- Terrorismusbekämpungsgesetz
- Telekommunikationsüberwachungsverordung
- Bundesverfassungsschutzgesetz
- Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
- Polizeigesetze
- BND-Gesetz

Diese Gesetze regeln unter anderem, wer was abhören darf, welcher „Bedarfsträger" also in welchem Umfang auf Kommunikationsdaten Zugriff nehmen darf. Beispiele für solche Bedarfsträger sind die Polizeien (mit Bundesgrenzschutz als Bundespolizei), der Verfassungsschutz als Inlands- und der BND als Auslandsgeheimdienst, aber auch der Zoll oder sogar die Bundesagentur für Arbeit.

Eine Kontrolle der Abhörmaßnahmen findet nur sehr unzureichend statt. Zuständig sind die Datenschutzbeauftragten und die für die Kontrolle der Geheimdienste verantwortliche parlamentarische Kontrollkommission – beides Stellen, die nicht eben für ihre üppige Ausstattung (bzw. im Fall der PKK ihr bürgerrechtliches Engagement) bekannt sind.

Wie funktioniert das Abhören?

Die Überwachungsschnittstellen befinden sich an wichtigen Infrastrukturpunkten der Diensteanbieter (z.B. bei Internetprovidern und Telefonieanbietern). Die Bedarfsträger kontrollieren die Spionageeinheiten zumeist per Fernzugriff, wobei ein Bedarfsträger in der Regel nicht weiß (wissen sollte), was der andere tut. Selten sind sie auf die Hilfe von MitarbeiterInnen des Diensteanbieters angewiesen. Die Bedienung ist für abfragende Personen einfach und ohne technische Kenntnisse durchführbar.

Damit das Ausforschen der BürgerInnen durch die verschiedenen Bedarfsträger reibungslos klappt und nichts verloren geht, sind die Kommunikations- und Abhöreinrichtungen standardisiert. In Deutschland werden die Standards des ETSI (European Telecommunications Standards Institute) angewendet und mit entwickelt[2] . Dieses ETSI übrigens definiert unser Thema, die Lawful Interception, so:

> „Abhören: Verfügbar machen (gesetzlich fundiert) von bestimmten Informationen, durchgeführt von einem Netzwerkoperator, Zugangsanbieter oder Diensteanbieter (NWO/AP/SvP) und Weiterreichen dieser Daten an die Überwachungseinheit (Law Enforcement Monitoring Facility) der staatlichen Bedarfsträger."

Vorratsdatenspeicherung

Informationen darüber, wer wann mit wem telefoniert hat, welche Webseiten besucht wurden, an wen Mails

gingen, die so genannten Verbindungsdaten, werden im Rahmen der Vorratsdatenspeicherung verdachtsunabhängig und flächendeckend gespeichert, etwa, um Widersprüche gegen Telefonrechnungen bearbeiten zu können. Im Bereich der Telefonie werden Daten dieser Art gegenwärtig für ein halbes Jahr vorgehalten, bei Internetverbindungen ist die Praxis noch uneinheitlich.

Die Kommunikationsprofile, die sich mit diesen Daten mit minimalem Aufwand konstruieren lassen, sind für die Bedarfsträger natürlich äußerst interessant - per Knopfdruck lässt sich mit ihnen bei Bedarf die Struktur ganzer Szenen im Handumdrehen rekonstruieren. Solche Begehrlichkeiten spiegeln sich in der gegenwärtig auch auf EU-Ebene geführten Diskussion wider, sämtliche Diensteanbieter zur Speicherung von Verbindungsdaten für drei bis fünf Jahre zu verpflichten.

Umfang der Überwachung

Es ist nicht einfach, einen Überblick darüber zu gewinnen, wie viel Überwachung tatsächlich stattfindet. Ein Grund ist die erwähnte Schwäche der die Bedarfsträger kontrollierenden Stellen, ein anderer, dass auch Dienste, die nicht einmal dieser Kontrolle unterliegen, munter abhören, etwa das globale Abhörnetzwerk Echelon[3] oder das von der EU betriebene Enfopol[4] .

Halbwegs verlässliche Zahlen gibt es für die polizeilichen „Maßnahmen". Im Jahr 2002 etwa gab es rund 4000 richterliche Überwachungsanordnungen für Festnetztelefone und etwa 18000 Anordnungen für Mobiltelefone. Hinter jeder dieser Anordnungen verbergen sich im Schnitt rund 1500 Gespräche, so dass man mit gegen 30 Millionen abgehörten Gesprächen rechnen muss. Die weit überwiegende Zahl dieser Anordnungen betraf Bereiche wie Betäubungsmittelmissbrauch oder Mord und Totschlag.

Der Staatschutzbereich ist darin vergleichsweise gering vertreten. Wie viel die Geheimdienste, insbesondere der Verfassungsschutz, abhören, ist unbekannt -- würden diese ihre Zahlen veröffentlichen müssen, wären es ja keine Geheimdienste mehr.

Gibt es ein Entkommen?

Wie können wir uns dieser Kontrolle entziehen, bzw. den Lauschern die Ohren verstopfen?

Solange wir überwachungsfähige Kommunikation benutzen (und das ist alles außer eventuell Telepathie), entstehen immer Verbindungsdaten. Dagegen können wir wenig tun. Wohl aber ist es uns möglich, den Inhalt der Gespräche zu verbergen.

Im Emailverkehr kann PGP (Pretty good Privacy; „ziemlich gute Privatsphäre") eingesetzt werden, im WWW können Anonymisierproxies und die Verwendung des verschlüsselten https-Protokolls (das alle verbreiteten Browser, aber nur wenige Webserver unterstützen) helfen.

Verschlüsseltes Telefonieren, etwa über ein Cryptophone[5] oder mit PGPfone, ist technisch seit geraumer Zeit auch kein großes Problem mehr, ist aber angesichts der geringen Verbreitung der nötigen Programme gegenwärtig eher unrealistisch.

Zum Schluss noch ein Verweis auf ein Interview, in dem die Hacker-Legende Wau Holland über illegales Verhalten, Kontrolle und Staubsauger spricht: „Mit Geheimdiensten kann man nicht spielen".[6]

Datenschutzgruppe der Roten Hilfe Heidelberg

Per Email: datenschutzgruppe@rotehilfe.de

Per Briefpost: Rote Hilfe Heidelberg, Datenschutzgruppe, Postfach 103162, 69021 Heidelberg

Unser PGP-Fingerabdruck: A3D8 4454 2E04 6860 0A38 A35E D1EA ECCE F2BD 132A

[1] http://www.regtp.de/tech_reg_tele/start/in_06-09-00-00-00_m/index.html

[2] http://www.heise.de/tp/deutsch/special/enfo/9306/1.html

[3] http://kai.iks-jena.de/miniwahr/echelon-index.html

[4] http://kai.iks-jena.de/miniwahr/enfopol.html

[5] http://www.cryptophone.de

[6] http://www.chscene.ch/ccc/ds/75/001.htm