Überregionaler Pressespiegel 02.01.2012

TAZ l 02.01.2012 l Christian Rath

Wie man Handys Geheimnisse entlockt

Wenn die Sicherheitsbehörden Mobiltelefone überwachen wollen, verfügen sie über viele Möglichkeitenr. Hier sind sechs Methoden des Zugriffs.

Abhören: Wie ein Festnetztelefon kann auch ein Handy abgehört werden. Mit einem richterlichen Beschluss kann die Polizei vom Mobilfunkprovider Zugang zu den Gesprächen eines bestimmten Teilnehmers verlangen. Zur Strafverfolgung kann das Handy eines Verdächtigen oder einer Kontaktperson abgehört werden. Die Rechtsgrundlage ist jahrzehntealt (Paragraf 100a Strafprozessordnung, StPO). Auch zur Abwehr künftiger Gefahren dürfen Telefone in manchen Bundesländern (unter anderem Bayern) und beim BKA abgehört werden.

Mitlesen: Auf die gleichen Vorschriften kann sich die Polizei berufen, wenn sie SMS mitlesen will. Deshalb spricht sie heute weniger vom Abhören als allgemeiner von Telekommunikationsüberwachung (TKÜ). Bei einem internetfähigen Smartphone kann sie auch den E-Mail-Verkehr mitlesen. Wenn ein Handy beschlagnahmt wird, darf die Polizei zudem die darin gespeicherten SMS und E-Mails auswerten.

Kontakte: Bei Handys und Festnetztelefonen interessiert die Polizei, wer mit wem wann telefoniert hat. Die Polizei kann diese Daten mit richterlichem Beschluss zur Strafverfolgung (Paragraf 100g StPO) und teilweise zur Gefahrenabwehr beim Provider herausverlangen. So kann etwa festgestellt werden, mit wem ein Mordopfer zuletzt telefoniert hat oder mit wem ein frisch enttarnter Terrorist in letzter Zeit im Kontakt stand.

Die Vorratsdatenspeicherung sollte sicherstellen, dass diese Daten für die Polizei ein halbes Jahr zur Verfügung stehen. Derzeit ist in Deutschland aber umstritten, ob sie wieder eingeführt wird. Je nach Provider stehen die Telefonverbindungsdaten derzeit nur einige Stunden, Tage oder Wochen zur Verfügung.

Ortung: Ein Mobiltelefon kann der Polizei auch verraten, wo sich der Benutzer ungefähr aufhält. Wenn nicht telefoniert wird, gibt das Handy ungefähr einmal am Tag seine Location Area an. Seit 2008 darf die Polizei diese Daten abfragen. Wenn mit dem Handy telefoniert oder gesimst wird, meldet sich das Gerät bei einer konkreten Funkzelle an, dann kann es noch genauer geortet werden. Auf diese Daten hat die Polizei schon länger Zugriff (Paragraf 100g StPO).

Mit der Vorratsdatenspeicherung sollten auch die Standortdaten sechs Monate lang festgehalten werden, was derzeit aber nicht geschieht. Bei Telefonen, mit denen nicht oder nicht oft genug telefoniert wird, kann die Polizei "stille SMS" einsetzen, damit solche Verkehrsdaten erzeugt und abgefragt werden können. *(siehe Text oben)*

Ortung per Funkzellenabfrage: Hier fragt die Polizei nicht, bei welcher Funkzelle sich ein bekanntes Handy einwählt, sondern sie will wissen, welche Handys sich bei einer bekannten Funkzelle eingewählt haben (Paragraf 100g). So kann sie zum Beispiel herausfinden, welche Telefone in der Nähe eines Tatorts benutzt wurden. Bei Auseinandersetzungen um eine Nazidemonstration in Dresden hat die Polizei im vorigen Februar exzessiv Funkzellenabfragen durchgeführt und die Daten dann auch für unzulässige Zwecke eingesetzt.

Imsi-Catcher: Wenn die Polizei nicht weiß, mit welcher SIM-Karte ein Verdächtiger telefoniert, kann sie ihn weder abhören noch orten noch seine Kontakte kontrollieren. Mithilfe eines Imsi-Catchers, der eine Funkzelle simuliert, kann aber die Kartennummer

(International mobile subscriber identity = Imsi) herausgefunden werden (Paragraf 100i StPO).

Ist die Handynummer bekannt, kann der Imsi-Catcher auch zur genaueren Ortung genutzt werden, indem innerhalb der echten Funkzelle eine immer kleinere virtuelle Funkzelle erzeugt wird. Wenn die Zielperson in dieser Zeit nicht telefoniert, kann die Polizei wieder stille SMS einsetzen. Manche Imsi-Catcher könnten - ohne rechtliche Grundlage - auch Gespräche mithören.

http://www.taz.de/Handyueberwachung-in-Deutschland/!84775/
