Ein IMSI-Catcher ist das, was Carnivore für E-Mails und ein Key-Logger für den PC ist.

Oben die Abbildung einer Anlage, die als IMSI-Catcher funktioniert aus dem Dokument On the security of 3GPP networks von Michael Walker. Darunter ein IMSI-Catcher, wie ihn der Verfassungsschutz (2002) benutzt aus dem DuD-Artikel Der IMSI Catcher.

Laut dem Magazin "connect" wurden in Deutschland 1999 die Telefonanschlüsse von 12600 Personen abgehört, in den USA waren es im gleichen Zeitraum nach offiziellen Angaben 1190 Personen (Link). Nach der Tageszeitung "Die Welt", die sich auf Angaben des Justizministeriums und der Regulierungsbehörde für Telekommunikation und Post stützt, haben 1998 Richter fast 10.000 Telefonüberwachungen an 11.272 Anschlüssen angeordnet. Davon waren 6391 Mobiltelefon-Anschlüsse (Link).
Man sieht also eine deutliche Tendenz.

Zum Abhören von Mobilfunkgeräten, landläufig als "Handys" bekannt, werden von Strafverfolgungsbehörden und Geheimdiensten sogenannte "IMSI-Catcher" eingesetzt, wie u. a. das von deutschen Geheimdiensten benutzte Gerät "GA 090" der Firma Rohde & Schwarz. Das Kryptohandy, das von Siemens auf der Basis des S35i entwickelt wurde, hat Rohde & Schwarz aufgekauft und vertreibt es unter dem Produktnamen "TopSec GSM".

Das auch Verschlüsselung bei GSM Handys nichts nutzt, meldete im September 2003 das Magazin New Scientist im Artikel GSM phone encryption "can be cracked" und die Netzzeitung in ihrem Artikel GSM-Handys belauschbar. Darin wird von einer Man-in the-Middle Methode zum Brechen heutiger GSM Verschlüsselung berichtet, die vom Team um den bekannten Kryptologen Eli Biham unter Ausnutzung einer Sicherheitslücke im Verschlüsselungssystem aller bis heute (Stand Sept. 2003) verkauften GSM Handys (3G Handys sind nicht btroffen) entwickelt wurde. Die Methode bietet sich zum Einsatz in IMSI-Catchern an.

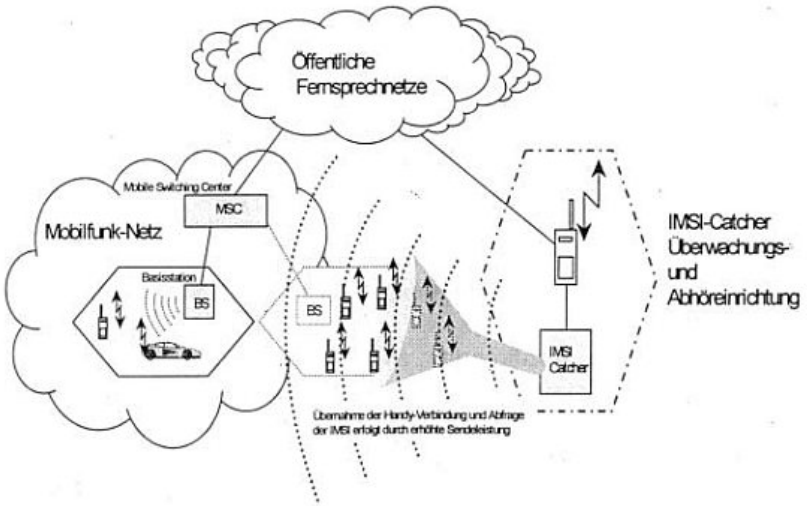
Bundestag legalisiert den Einsatz von IMSI-Catchern ohne weitere Beratung

Laut der Meldung des SPIEGL Online vom 08.06.2002 Bundestag erlaubt umstrittene Abhörmethode für Handys haben

> "...die Abgeordneten ohne weitere Beratung einen Gesetzesentwurf der rot-grünen Bundesregierung gebilligt, der den Einsatz des IMSI-Catchers bei "Straftaten von erheblicher Bedeutung" erlaubt (...) Das neue Gesetz erlaubt das Abhören nun nach einem richterlichen Beschluss. Am 21. Juni soll es im Bundesrat behandelt werden."

Grafiken zur Funktionweise des IMSI-catchers

Schaubild aus dem SPIEGEL (33/2001) Artikel "Wahre Wunderbox"



Aufbauschema des IMSI-Catchers aus Handys - Komfort nicht ohne Risiko

Funktionsweise

Gespräche, die mit Handys [*Anm.: nach GSM Standard*] geführt werden, sind grundsätzlich abhörbar. Das mag zunächst verwunderlich erscheinen, da die Netzbetreiber und Gerätehersteller lange Zeit gerade mit der Verschlüsselung für diese neue Kommunikationstechnik geworben haben. In diesem Zusammenhang wurde jedoch nicht erwähnt, daß Netzbetreiber durch einen Befehl die Verschlüsselung ausschalten können. Diese Funktion ist notwendig, da in einigen europäischen Ländern nur eine unverschlüsselte Kommunikation möglich ist. Ob verschlüsselt oder unverschlüsselt übertragen wird, wird auf den Handys bislang nicht angezeigt.

Im Rahmen der Beratungen über ein Begleitgesetz zum Telekommunikationsgesetz wurde erörtert, Nachrichtendiensten und Strafverfolgungsbehörden den Einsatz von Geräten (sog. IMSI-Catcher) zu erlauben, die gezielt **bei einzelnen** Handys die Verschlüsselung ausschalten können und damit das Mithören und Aufzeichnen von Gesprächen ermöglichen. Daneben sollten diese Geräte dazu genutzt werden, die netzinternen Rufnummern von Mobiltelefonen, die sogenannten **IMSI** (International Mobile Subscriber Identity - netzinterne Teilnehmerkennung, die zu einem bestimmten Mobilfunknetz gehört) zu ermitteln, um treffsicher auf einzelne Handys zugreifen zu können.

Aufbau des IMSI-Catchers

Das Grundgerät ist nicht größer als ein durchschnittlicher PC. Die Steuerung erfolgt durch ein handelsübliches Laptop. Der IMSI-Catcher kann in zwei Betriebsmodi (fangen, abhören) arbeiten. Geräte zum Fangen und Abhören sind identisch; zum Abhören ist zusätzlich lediglich eine

Softwareergänzung und ein nachgeschaltetes Handy nötig. IMSI-Catcher können in verschiedenen Funknetzen (D1, D2, E-Plus) eingesetzt werden. Der Betrieb kann aus einem PKW heraus erfolgen. Damit ist ein schneller Ortswechsel unproblematisch.

IMSI-Catcher im Fangmodus

Um gezielt abhören zu können, ist in aller Regel die Kenntnis der Rufnummer erforderlich. Die Abhörgeräte simulieren dafür eine Basisstation, indem sie eine zusätzliche eigene Funkzelle [*Anm.: **eines** Mobilfunknetzes, also D-1 oder E-Plus usw.*] aufbauen, die sich genau wie eine Originalzelle verhält. Weil die Abhörgeräte mit einer etwas stärkeren Leistung arbeiten, melden sich alle Geräte in dieser neuen Funkzelle und nicht bei der eigentlichen Basisstation an. Über diese Station laufen dann alle Verbindungsanfragen der Handys. Die Nutzerinnen und Nutzer bemerken von diesem "Fangen" nichts. Von **allen** in seiner Reichweite befindlichen Handys [*Anm.: **sämtliche** Mobiltelefone im Umkreis von etwa 100 Metern*] kann das Abhörgerät neben der IMSI auch die **IMEI** (International Mobile Station Equipment Identity - Endgerätekennung) abrufen. Technisch bedingt kann während dieser Prozedur [*Anm.: ein paar Minuten*] niemand mit dem betroffenen Handy Gespräche führen oder empfangen. Selbst Notrufe zu Polizei, Feuerwehr oder ärztlichem Notdienst sind von keinem der in der neuen Funkzelle eingebuchten Handys möglich.

IMSI-Catcher im Abhörmodus

Im Abhörmodus nutzen IMSI-Catcher die Möglichkeit, die Verschlüsselung auszuschalten. Wenn also die Gespräche **eines Handys** abgehört werden sollen, wird beim Verbindungsaufbau die Verschlüsselung ausgeschaltet, so daß die Gesprächsinhalte zwar nach wie vor in digitaler Form, jetzt aber unverschlüsselt und mit entsprechender Software abhörbar vorliegen und aufgezeichnet werden können. Solange das Abhörgerät in diesem Modus arbeitet, kann mit keinem gefangenen Handy im Einflußbereich des Abhörgerätes eine Verbindung aufgebaut werden. Lediglich **abgehende Gespräche des abgehörten Handys** sind möglich.

Die Datenschutzbeauftragten des Bundes und der Länder haben den Einsatz der IMSI-Catcher insbesondere deshalb abgelehnt, weil bei der Feststellung der Rufnummer und beim Abhören der Betroffenen mit einer bisher noch nicht dagewesenen Intensität das Recht auf unbeobachtete Kommunikation unbeteiligter Dritter beeinträchtigt wird.

Selbst wenn diese Abhörgeräte zwar von Nachrichtendiensten und Strafverfolgungsbehörden zunächst nicht eingesetzt werden sollen, bleiben die beschriebenen Risiken für die Nutzerinnen und Nutzer von Handys jedoch bestehen. Einerseits ist nicht auszuschließen, daß diese Geräte beispielsweise für den Export produziert werden. Andererseits dauert es erfahrungsgemäß nicht lange, bis Bauanleitungen für einzelne Komponenten oder für das gesamte Gerät veröffentlicht werden. Es wäre verwunderlich, wenn das, was erhältlich ist, nicht auch von irgend jemand zum Einsatz gebracht würde.

Es wird deutlich, daß nur ein ausgeschaltetes Handy einen wirklich sicheren Schutz vor mißbräuchlicher Nutzung garantiert. Damit wird aber gerade der Zweck der Handynutzung, der in der ständigen Erreichbarkeit liegt, unterlaufen. Den Nutzerinnen und Nutzern von Handys müssen die hier beschriebenen Risiken jedoch bekannt sein, damit sie für sich selbst bewußt entscheiden können, ob und wie lange sie bei welchen Gelegenheiten ihr Handy einschalten. Schön wäre es, wenn Mobilfunkgeräte so weiterentwickelt und der Netzbetrieb so ausgestaltet würden, daß Mißbrauchsmöglichkeiten von vornherein so weit wie möglich ausgeschlossen sind. Gerätehersteller und Netzbetreiber sind aufgefordert, im Rahmen des geltenden Rechts durch geeignete Maßnahmen dafür zu sorgen, daß ihre Kundinnen und Kunden vertraulich miteinander kommunizieren können. Solange dies nicht sichergestellt ist, bedarf es auch von ihrer Seite der offenen und umfassenden Aufklärung der Kundschaft über die Risiken für die vertrauliche Kommunikation in Mobilfunknetzen.

Aus Handys - Komfort nicht ohne Risiko
der Landesbeauftragten für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

"GSM Interceptor" für Regierungsbehörden des Spy World Shops im Jahr 2007.

Rechtliche Zulässigkeit von so genannten IMSI-Catchern

Kleine Anfrage vom 23.08.2001 der Abgeordneten Dr. Edzard Schmidt-Jortzig, Jörg van Essen, Rainer Funke, Dr. Wolfgang Gerhardt und der Fraktion der F.D.P. [BT Drucksache 14/6827] mit den Antworten der Bundesregierung vom 06.09.2001 [BT Drucksache 14/6885]

Laut Bericht des Nachrichtenmagazins DER SPIEGEL vom 13. August 2001 (Heft 33/2001 S. 54f.) setzt der Bundesgrenzschutz zur Verfolgung von Straftaten so genannte IMSI-Catcher ein. Dabei handelt es sich um ein technisches Gerät, mit dem u. a. die Gerätenummer von Mobiltelefonen festgestellt und somit eine eindeutige Lokalisierung des Benutzers vorgenommen werden kann.
Die Strafverfolgungsbehörden begründen den Einsatz dieser Geräte mit der anscheinend vermehrt zu beobachtenden Tatsache, dass Tatverdächtige schwerer Straftaten, vor allem im Bereich der Organisierten Kriminalität (OK), zur Verschleierung ihre Mobiltelefone und Telefonkarten häufig wechseln und somit aufgrund immer neuer Rufnummern von der Polizei kaum mehr zu überwachen seien. Bei der aktuell gewordenen Überwachungsmethode wird durch den IMSI-Catcher eine Basisstation, in die sich die Mobiltelefone zur Herstellung von Funkverbindungen zu ihrem Netzbetreiber einloggen müssen, in der Nähe des Verdächtigen simuliert, so dass die Gerätedaten der Mobiltelefone direkt in den polizeilichen Apparat übertragen werden. Dies hat im Übrigen auch technische Nebenfolgen. Zum einen führt es zu einem zeitweiligen Ausfall der Basisstationen der Mobilfunkbetreiber und zum anderen zur Übermittlung der Geräte- und ggf. Rufnummern auch aller anderen Mobilfunknutzer in der näheren räumlichen Umgebung. Streitig ist nun, ob die geltenden Vorschriften, insbesondere der Strafprozessordnung (StPO) den Einsatz solcher Geräte überhaupt decken. Vergleichbare Probleme bestehen bei der Frage des auf Gerätenummern bezogenen Abhörens.

Wir fragen daher die Bundesregierung:

1. Teilt die Bundesregierung die Auffassung des Bundesministeriums des Innern, wonach der Einsatz

von so genannten IMSI-Catchern durch die geltende StPO hinreichend gedeckt sei?

Der Einsatz des IMSI-Catchers GA 090 im strafprozessualen Bereich ist durch die §§ 100a ff., 161 StPO gedeckt. Gleichwohl prüft die Bundesregierung aus Gründen der Rechtssicherheit und -klarheit die Schaffung einer ausdrücklichen Rechtsgrundlage in der StPO.

2. Wenn ja, in welchen Vorschriften der StPO sieht die Bundesregierung diese Ermächtigungsgrundlage?

   Auf die Antwort zu Frage 1 wird verwiesen.

3. Wie bewertet die Bundesregierung den Beschluss der Justizministerkonferenz vom 11. bis 13. Juni 2001 in Trier (TOP II.4), wonach die gesetzlichen Grundlagen im Bereich der Telekommunikationsüberwachung besonders im Falle von gerätebezogener Überwachung angepasst werden müssten?

   Die Bundesregierung prüft entsprechend dem Beschluss der Justizministerkonferenz vom 11. bis 13. Juni 2001 in Trier (TOP II, 4), ob es angesichts der veränderten technischen Gegebenheiten auf dem Gebiet der Telekommunikation, insbesondere im Mobilfunk, klarstellender Regelungen zur gerätebezogenen Überwachung von Mobiltelefonen sowie zum Bewegungsprofil bedarf.
   So hat der Ermittlungsrichter des Bundesgerichtshofs in der Gerätenummer eines Mobiltelefons (IMEI-Nummer) eine "andere Kennung" im Sinne des § 100b Abs. 2 Satz 1 StPO gesehen und als zulässigen Bezugspunkt für eine Telekommunikationsüberwachung erachtet (Beschluss vom 7. September 1998 - 2 BGs 211/98). Dies ist allerdings nicht unumstritten.
   Unstreitig ist dagegen, dass im Verlauf einer Telekommunikation auch die Daten über den "Standort" (Funkzelle), in der sich ein Mobiltelefon gerade befindet, nach den §§ 100a, 100b StPO erhoben werden dürfen. Umstritten ist jedoch die Rechtslage, wenn das Handy lediglich aktiv geschaltet ist, eine Telekommunikation aber nicht stattfindet. Der Ermittlungsrichter des Bundesgerichtshofs (Beschluss vom 21. Februar 2001 - 2 BGs 42/2001) hat im Einklang mit der Rechtsprechung verschiedener Landgerichte (LG Ravensburg, NStZRR 1999, 84; LG Aachen, StV 1999, 590; LG Dortmund, NStZ 1998, 577) auch in diesen Fällen unter Zugrundelegung des § 100a StPO die Erhebung der Positionsdaten für zulässig gehalten.

4. Wie verhält sich die Bundesregierung zur Argumentation, die Zulässigkeit des Einsatzes von IMSI-Catchern sei im Bereich der Repression durch Verweis auf den rechtfertigenden Notstand (§ 34 Strafgesetzbuch - StGB) möglich?

   Es wird auf die Antwort zu den Fragen 1 und 2 verwiesen. Eines Rückgriffs auf den rechtfertigenden Notstand nach § 34 StGB bedarf es danach nicht.

5. Wie stellt sich die Bundesregierung zu der Tatsache, dass die Vorschrift des § 34 StGB nach ganz herrschender Meinung nur individuelles Handeln rechtfertigt, aber nicht zu hoheitlichem Vorgehen ermächtigen kann, sich allenfalls in Ausnahmefällen bei tatsächlicher Gefährdung höchster Rechtsgüter überwinden lässt, aber folglich niemals zur standardisierten Zulassung einer repressiven Maßnahme verwendet werden kann?

   Auf die Antwort zu Frage 4 wird verwiesen.

6. Ist die Bundesregierung ebenso wie die Justizministerkonferenz in ihrem Beschluss zu TOP II.4 der Tagung vom 11. bis 13. Juni 2001 der Auffassung, dass auch "Bewegungsprofile", für deren Erstellung die bloße Aktivierung des Mobiltelefons ausreicht, einer ausdrücklichen gesetzlichen Regelung bedürfen?

   Auf die Antwort zu Frage 3 wird verwiesen.

7. **Kann die Bundesregierung die Aussage des Bundesdatenschutzbeauftragten, Dr. Joachim Jacob, bestätigen, dass es zurzeit keine materielle Rechtsgrundlage für den telekommunikationsrechtlichen Betrieb von IMSI-Catchern gebe, da die Versuchsfunkgenehmigung 1999 ausgelaufen sei und die Regulierungsbehörde für Telekommunikation und Post bislang keine neue Genehmigung erteilt habe?**

   Ja

8. Wie schätzt die Bundesregierung die Gefahr durch missbräuchliche Verwendung von IMSI-Catchern durch Dritte ein, um an geheime Informationen von staatlichen Stellen oder Wirtschaftsbetrieben zu gelangen?

   Die Bundesregierung sieht die Gefahr als gering an.

9. Plant die Bundesregierung Gegenmaßnahmen zur Verhinderung von Straftaten mittels IMSI-Catchern?
   Wenn ja, welche?

   Das Bundesamt für Sicherheit in der Informationstechnik nimmt sich dieser Problematik an.

10. Denkt die Bundesregierung hierbei an eine erneute Ausweitung der Eingriffsmöglichkeiten nach dem G-10-Gesetz?

    Nein

11. Wie bewertet die Bundesregierung die Möglichkeiten zur Bestimmung des Aufenthaltsorts von Handynutzern oder die Erstellung von Bewegungsprofilen durch den Einsatz spezieller Software, die beispielsweise durch Peilung innerhalb von Funkzellen und Kenntnisse über die spezifische Ausbreitung der Signale eine Standortbestimmung ermöglichen.

    Der Bundesregierung ist bekannt, dass die Netzbetreiber zurzeit neue Dienstleistungen entwickeln, für die Voraussetzung ist, dass der Standort des Mobilfunkgeräts genauer bestimmt wird, als dies bisher der Fall ist. Sie beobachtet diese Entwicklungen aufmerksam.

12. Ist die Bundesregierung der Auffassung, dass eine gerätebezogene Überwachung von Mobiltelefonen an Hand der so genannten IMEI-Nummern von § 100a StPO gedeckt ist, weil es sich dabei um eine andere "Kennung" des TK-Anschlusses im Sinne von § 100b Abs. 2 Satz 1 StPO handelt?

    Der Ermittlungsrichter des Bundesgerichtshofs hat diese Frage in seinem Beschluss vom 7. September 1998 (2 BGs 211/98) in einer - aus Sicht der Bundesregierung - gut nachvollziehbaren Weise bejaht.

13. Wie schätzt die Bundesregierung die Gefahr ein, dass während des Einsatzes eines IMSI-Catchers von keinem der "gefangenen" Handys Gespräche geführt oder empfangen werden können, einschließlich Notrufe zur Polizei, der Feuerwehr oder dem ärztlichen Notdienst?

    Lediglich für die Mobilfunkgeräte, die ohne aktiven Netzbetrieb ("stand-by-Betrieb") im Wirkbereich des GA 090 sind, gibt es eine temporäre Beeinträchtigung (von max. 10 Sekunden), in der keine Verbindung zum Mobilfunknetz besteht, und somit auch kein Notruf möglich ist. Diese Beeinträchtigung, die sich aus Sicht des Mobilfunkteilnehmers wie eine kurzzeitige Versorgungslücke darstellt, ist jedoch mit den bekannten temporären Störungen in diesen Netzen vergleichbar und nach Auffassung der Bundesregierung hinzunehmen. Zu einer Beeinträchtigung der Basisstation des Mobilfunkbetreibers kommt es - anders als in der Vorbemerkung dargestellt - nicht.

14. Welche Rolle hat der Einsatz von IMSI-Catchern bei der Neuregelung der Frequenzzuteilungsverordnung, insbesondere bei deren § 4 gespielt?

    Der Einsatz des IMSI-Catchers ist bei der Formulierung des § 4 Abs. 1 Satz 2 der Frequenzzuteilungsverordnung (FreqZutV) berücksichtigt worden.

15. Hat es nach Kenntnis der Bundesregierung für den Einsatz von IMSI-Catchern entsprechende Anträge gegeben, und wenn ja, wie sind diese beschieden worden?

    Nach Auslaufen der Versuchsfunkgenehmigung sind zwei Anträge auf Verlängerung gestellt worden, die von der Regulierungsbehörde für Telekommunikation und Post abschlägig beschieden wurden.

Links:

- ZDnet
  Zahl der überwachten Handy-Gespräche in Deutschland enorm hoch
- Datenschutz und Datensicherheit (DuD 4/2002)
  Der IMSI-Catcher
- de.internet.com
  Wie der BND illegal Handynutzer abhört [20.08.01]
- 2001 Kongress Chaos Computer Club
  Vortrag "IMSI-Catcher - GSM Unsicherheit"

[Inhalt | Top]