DuD
Datenschutz und Datensicherheit

Der IMSI-Catcher

Dirk Fox

Seit 1997 geistert der „IMSI-Catcher“ durch die Medien. Damals veröffentlichte die DuD eine erste Beschreibung der technischen Funktionsweise des Geräts.[1] Mit der Verabschiedung des Terrorismusbekämpfungsgesetzes geriet der IMSI-Catcher erneut in die Schlagzeilen. Als Beitrag zur Versachlichung der Diskussion werden im Folgenden die technischen Möglichkeiten und Gefahren des Geräts zusammenfassend dargestellt.

Dipl.-Inform.
Dirk Fox

Security Consultant und Geschäftsführer der Secorvo Security Consulting GmbH. Arbeitsschwerpunkt: Public Key Infrastrukturen, Digitale Signaturen, Sicherheit in Netzen.
E-Mail: fox@secorvo.de

Einleitung

Mit der Entwicklung, Einführung und rasanten Verbreitung mobiler Kommunikationstechniken seit Anfang der 90er Jahre stehen Strafverfolgungsbehörden und Nachrichtendienste bei der Telekommunikationsüberwachung vor einer neuen Herausforderung. Denn der Bezugspunkt einer jeden Abhörmaßnahme, die eindeutige Kennung der von einem Tatverdächtigen benutzten Telekommunikationsanlage, ist im Zeitalter mobiler Kommunikationsendgeräte nicht mehr ohne weiteres feststellbar.

Solange observierte Personen das herkömmliche Telefonnetz (Festnetz) für ihre Kommunikation benutzen, lässt sich die für die Veranlassung einer Abhörmaßnahme oder die Ermittlung der Verbindungsdaten erforderliche Nummer des verwendeten Endgeräts unmittelbar aus dem Standort ableiten. Ist also der Aufenthalt eines Kommunikationsteilnehmers bekannt, können die Ermittlungsbehörden die Anschlusskennung und Verbindungsdaten bei Vorlage einer richterliche Anordnung und unter Mitwirkung des Netzbetreibers leicht gewinnen; auch eine „Fangschaltung“ kann so eingerichtet werden.

Anders bei mobilen Kommunikationsendgeräten: Vom Aufenthaltsort eines Handynutzers kann nicht mehr auf die Anschlusskennung geschlossen werden. Selbst wenn der Name des Nutzers bekannt ist, lässt sich darüber nicht zwangsläufig die für eine Abhörmaßnahme erforderliche Kennung ermitteln. Denn vorsichtige Kriminelle vermeiden tunlichst den Abschluss von Mobilfunkverträgen unter ihrem eigenen Namen.

1 Hintergrund

Um diese Beschränkung der polizeilichen Ermittlungsmöglichkeiten nicht ohnmächtig hinnehmen zu müssen, setzen Bundeskriminalamt (BKA) und Bundesgrenzschutz (BGS) seit 1998 „in außergewöhnlichen Polizeilagen und Fällen mit hohem Gefährdungsgrad zur Bekämpfung besonders schwerer Kriminalität (Produkterpresungen, Flucht von Serienmördern, Geiselnahmen und internationalem Rauschgifthandel)“ sogenannte „IMSI-Catcher“ ein. Insgesamt 35 Mal wurde nach Auskunft des BMI bisher (Stand: November 2001) ein IMSI-Catcher verwendet.

Bei diesem Gerät handelt es sich ursprünglich um ein Test- und Messsystem der Firma Rohde & Schwarz, dass für den Zweck der Bestimmung der Endgerätekennung eines Handys weiter entwickelt wurde. Dieses Gerät mit der Typenkennzeichnung „GA 090“ wurde vom Hersteller im Dezember 1996 Vertretern des BMWi und der drei Mobilfunknetzbetreiber D1/T-Mobile, D2/Vodafone, E-Netz/E-Plus in München vorgestellt.

Erstmalig „aktenkundig“ wurde der IMSI-Catcher im Zusammenhang mit der Diskussion eines Gesetzentwurfs der Bundesregierung für ein Begleitgesetz zum Telekommunikationsgesetz von 23.05.1997 im Bundesrat. In einem Änderungsvorschlag wollte der Bundesrat eine gesetzliche Ermächtigungsgrundlage für den Einsatz des erweiterten Modells „GA 900“ schaffen, das nicht nur die Feststellung der Gerätekennung, sondern auch ein Abhören abgehender Gespräche erlaubt.

Aufmerksam geworden durch die Erwähnung des Geräts in der Begründung des Bundesrates zu diesem Änderungsvorschlag (BR-Drs. 369/1/97 = BT-Drs. 13/8016) veröffentlichte damals die DuD eine erste Beschreibung der Funktionsweise des „GA 090“ sowie des erweiterten Modells „GA 900“ [Fox_97]. Die sich anschließende öffentliche Aufregung legte sich allerdings wieder, nachdem der Änderungsvorschlag des Bundesrats nicht in die Endfassung des BegleitG (veröffentlicht im Bundesgesetzblatt vom 23.12.1997) aufgenommen worden war. In ihrer Erwiderung auf den Vorschlag des Bundesrats machte die Bundesregierung allerdings deutlich, dass der Einsatz des „GA 090“ im Rahmen der polizeilichen Ermittlungstätigkeit vorgesehen sei.

[1] Siehe Fox, DuD 9/1997 [Fox_97].

Seit Sommer 2001 hat der IMSI-Catcher nun wieder Konjunktur: In seiner Ausgabe vom 13.08.2001 berichtete das Nachrichtenmagazin „Der Spiegel“ über den Einsatz des IMSI-Catchers zur Verfolgung von Straftaten durch den Bundesgrenzschutz (BGS).[2] Diese Darstellung führte zu einer Kleinen Anfrage im Bundestag durch Abgeordnete der FDP-Fraktion.[3] Nur wenige Wochen später geriet der IMSI-Catcher bei der Diskussion des schließlich am 01.01.2002 in Kraft getretenen Terrorismusbekämpfungsgesetzes[4] erneut ins Rampenlicht: Mit der Aufnahme eines neuen Absatz 4 im § 9 Bundesverfassungsschutzgesetz (BVerfSchG) wurden nun auch der Verfassungsschutz und der MAD zur Nutzung des IMSI-Catchers ermächtigt.

Bild: IMSI-Catcher (Quelle: Verfassungsschutz)

2 Funktionsumfang des IMSI-Catchers

Verfolgt man die Diskussion in den Medien und im Umfeld der Gesetzgebung stößt man immer wieder auf erhebliche Missverständnisse und Fehleinschätzungen bei der Darstellung der Funktionsweise und der Bewertung der (möglichen) Auswirkungen des IMSI-Catchers. Das Gerät besitzt drei in diesem Zusammenhang wichtige Funktionen: Die Ermittlung der IMSI, die Bestimmung der IMEI und die Lokalisierung eines mobilen Endgeräts (Handys). Die Modellvariante GA 900 erlaubt zusätzlich ein Mithören abgehender Gespräche.

2.1 Ermittlung der IMSI

Die zentrale Eigenschaft des „IMSI-Catchers“, der er auch seine Bezeichnung verdankt, ist die Möglichkeit, die IMSI (*International Mobile Subscriber Identity*) eines eingeschalteten Handys in seinem Einzugsbereich zu ermitteln.

Diese IMSI ist eine weltweit eindeutige Kennung, die den Teilnehmer (Vertragspartner eines Netzbetreibers) eindeutig identifiziert. Die IMSI ist auf der Chipkarte (SIM – *Subscriber Identity Module*) gespeichert, die ein Mobilfunkteilnehmer bei Abschluss eines Vertrags erhält. Die ersten Ziffern der IMSI bezeichnen den Netzbetreiber; anhand der weiteren Ziffern kann über die beim Netzbetreiber gespeicherten Bestandsdaten der Mobilfunkteilnehmer ermittelt werden. Mit Hilfe der IMSI kann nicht nur die Identität des Teilnehmers, sondern auch dessen Mobilfunk-Telefonnummer bestimmt werden; dazu ist ebenfalls ein Zugriff auf die Bestandsdaten des Netzbetreibers erforderlich.

Zur Ermittlung der IMSI simuliert ein IMSI-Catcher die Basisstation einer regulären Funkzelle eines Mobilfunknetzes.[5] Eingeschaltete Handys („Stand-By-Betrieb“) im Einzugsbereich dieser vermeintlichen „Basisstation“ und mit einer SIM des simulierten Netzbetreibers buchen sich nun automatisch beim IMSI-Catcher ein.[6] Durch einen speziellen „IMSI Request“ der Basisstation (ein Kommando, das sonst üblicherweise nur im Fehlerfall benötigt wird) kann die Herausgabe der IMSI vom Handy erzwungen werden.

Ist der von einer observierten Person genutzte Netzbetreiber nicht bekannt, muss diese Suche ggf. für Basisstationen aller vier Netzbetreiber (T-D1, D2 Vodafone, E-Plus, Viag Interkom) durchgeführt werden. In Funkzellen mit vielen Teilnehmern kann es außerdem erforderlich sein, mehrere Messungen durchzuführen, bis die gesuchte IMSI aus der Vielzahl gesammelter Daten herausgefiltert werden kann.

2.2 Ermittlung der IMEI

Da ein Endgerät mit verschiedenen SIM-Karten (und damit unterschiedlichen IMSIs) genutzt werden kann, kann für ein Ermittlungsverfahren auch die Bestimmung der eindeutigen Geräte- oder Seriennummer eines Handys, der IMEI (*International Mobile Equipment Identity*), von Bedeutung sein. Diese Handy-Seriennummer wird durch den IMSI-Catcher auf technisch ähnliche Art wie die IMSI ermittelt.

2.3 Lokalisierung eines Handy-Nutzers

Der IMSI-Catcher GA 090 erlaubt außerdem eine vergleichsweise genaue Feststellung der Position eines Handys (Ortung). Damit kann der Aufenthaltsort einer observierten Person eingegrenzt und so z. B. ein polizeilicher Zugriff ermöglicht werden.

Üblicherweise ist der Basisstation eines Netzbetreibers der Standort eines eingebuchten Mobilfunkgeräts nur „zellgenau“ und daher sehr grob bekannt, denn eine Mobilfunkzelle kann in einem der D-Netze leicht einen Durchmesser von mehreren Kilometern besitzen. Da der IMSI-Catcher

[2] „Der Spiegel“, Heft 33/2001, S. 54 f.

[3] Kleine Anfrage: BT-Drs. 14/6827; Antwort der Bundesregierung: BT-Drs. 14/6885 vom 10.09.2001.

[4] Siehe Rublack, in diesem Heft.

[5] Bei Angriffen dieser Art spricht man auch von einer „Maskerade-Attacke“.

[6] Handys, mit denen zum Zeitpunkt der Observierung Gespräche geführt werden, können von einem IMSI-Catcher nicht erfasst werden.

üblicherweise eine Funkzelle mit geringer Leistung (< 1 Watt) und damit erheblich geringerer Ausdehnung simuliert, kann so der Aufenthaltsort eines eingeschalteten Handys ziemlich stark eingegrenzt und damit quasi „implizit“ geortet werden.

Von Rohde & Schwarz wird jedoch auch technisches Equipment zur Peilung eines Handys angeboten:[7] Durch drei Messungen von verschiedenen Standorten kann so der Aufenthaltsort exakt bestimmt werden.[8]

Die „implizite“ Ortungs-Funktion des IMSI-Catchers setzt in jedem Fall voraus, dass

- das von der observierten Person genutzte Mobilfunknetz und die IMSI bekannt sind,
- sich das Handy der observierten Person im Stand-by-Betrieb befindet, und
- der IMSI-Catcher das Handy der observierten Person „gefangen“ hat.

Ohne Vorabkenntnis der IMSI des benutzten Handys und eine grobe Kenntnis des Aufenthaltsorts der gesuchten Person ist eine Ortung mit dem IMSI-Catcher nicht möglich.

2.4 Abhören von Gesprächen

Nach verfügbaren Informationen ist der von Rohde & Schwarz entwickelte und vertriebene Gerätetyp „GA 090“ nur in der Lage, IMSI- und IMEI-Kennungen eingeschalteter Handys im Einzugsbereich des Geräts zu „sammeln“. Technisch ist jedoch durch vergleichsweise geringe Änderungen in der Betriebssoftware eine Variante des Geräts möglich, die von einem „gefangenen“ Handy abgehende Gespräche mitschneiden kann.

Dazu gibt sich die vermeintliche „Basisstation“, die der IMSI-Catcher simuliert, gegenüber der nächsten erreichbaren Basisstation des Netzbetreibers, über den der Verbindungsaufbau erfolgen soll, ihrerseits als Handy aus und leitet die von dem gefangenen Handy ausgehenden Datenpakete an diese weiter (und umgekehrt). Der IMSI-Catcher realisiert damit einen sogenannten „Man-in-the-middle“-Angriff.

Damit die Inhaltsdaten des Gesprächs, die üblicherweise mit einem nur einer echten Basisstation bekannten geheimen Schlüssel verschlüsselt werden, belauscht werden können, schaltet der IMSI-Catcher zuvor den Verschlüsselungsmodus aus. Diese Möglichkeit der netzseitigen Unterdrückung der Verschlüsselung auf der „Luftschnittstelle“, d. h. während der Funkübertragung, ist der Tatsache zu verdanken, dass im GSM-Standard mit Rücksicht auf Staaten, in denen eine Verschlüsselung unzulässig oder genehmigungspflichtig ist, die Verschlüsselung lediglich optional vorgesehen wurde. Das Abhören von Gesprächen ist allerdings technisch auf eine einzige, von einem „gefangenen“ Handy aus aufgebaute Gesprächsverbindung beschränkt.

Tatsächlich bietet die Firma Rohde & Schwarz ein Gerät mit der Typbezeichnung GA 900 als Exportversion an, das über diese zusätzliche Abhörfähigkeit verfügt. Nach Auskunft des BMI ist diese Geräteversion weder beim BKA noch beim BGS im Einsatz; lediglich das Bundesamt für Sicherheit in der Informationstechnik (BSI) besitzt zu „wissenschaftlichen Erprobungszwecken“ ein Exemplar dieses Gerätetyps.

Größere Erfahrung aus dem Einsatz der Exportversion gibt es offenbar in europäischen Nachbarstaaten. Auch wenn die Verkaufszahlen von Rohde & Schwarz nicht offengelegt sind, wird von unterschiedlicher Seite berichtet, dass diese Gerätevariante, deren Preis angeblich bei 200-300 T€ liegt, ein „Exportschlager“ sei.

3 Bewertung

Aus technischer Sicht sind drei Kriterien zur Bewertung des IMSI-Catchers wesentlich: die Wirksamkeit der technischen Lösung, die mit seinem Einsatz verbundenen Störungen und die Missbrauchsgefahr. Auf diese drei Merkmale wird im Folgenden näher eingegangen.[9]

3.1 Wirksamkeit

Grundsätzlich ist der IMSI-Catcher geeignet, durch Bestimmung der IMSI eines Mobilfunkgeräts eine Abhörmaßnahme oder die Auswertung der Verbindungsdaten eines Verdächtigen zu ermöglichen und damit das eingangs beschriebene Handicap der Strafverfolgungsbehörden in nicht-terrestrischen Telekommunikationsnetzen zu kompensieren. Allerdings unterliegt diese Vorgehensweise einer Reihe von technischen Einschränkungen:

- So muss der Aufenthaltsort einer observierten Person auf wenige Kilometer genau bekannt sein.
- Das observierte Gerät muss zum Zeitpunkt des Einsatzes des IMSI-Catchers eingeschaltet sein („Stand-by-Betrieb“), und es darf keine Kommunikationsverbindung bestehen.
- Der vom Verdächtigen genutzte Netzbetreiber muss bestimmt werden.
- Aus der – abhängig von Ausdehnung und Lage der simulierten Funkzelle – möglicherweise großen Anzahl erfasster IMSIs ist die richtige herauszufiltern; dafür können mehrere Messungen erforderlich sein.
- Hinzu kommt, dass der IMSI-Catcher aus mehreren Messgeräten, einer leistungsfähigen Antenne und einem Steuerrechner besteht und daher nur mit einem gewissen Aufwand (z. B. in einem Fahrzeug) mobil eingesetzt werden kann (siehe Bild).

Ein Problem stellen auch ausländische Handys dar: Zwar kann ein IMSI-Catcher auch deren IMSI bestimmen; für die Durchführung einer Abhörmaßnahme wird jedoch die Anschlusskennung (Mobiltelefonnummer) benötigt – und für deren Bestimmung ist die Mitwirkung des ausländischen Netzbetreibers zwingend erforderlich.

Die Nutzung des IMSI-Catchers als Ortungsgerät unterliegt ebenfalls technischen Einschränkungen: So müssen die IMSI bekannt und das Handy eingeschaltet sein (Stand-by-Betrieb). Zudem muss der Aufenthaltsort des Nutzers so gut eingegrenzt werden können, dass der IMSI-Catcher in geographischer Nähe der Zielperson betrieben werden kann.

Auch für den Einsatz der Gerätevariante GA 900, die zusätzlich ein Abhören von Gesprächen ermöglicht, gilt eine wichtige technische Einschränkung: Der IMSI-Catcher erlaubt nur das Abhören eines einzigen Gesprächs, und der gleichzeitige Betrieb eines zweiten GA 900 ist zumindest für dieselbe Funkzelle nicht möglich.

3.2 Störungen

Sorgen bereiten den Netzbetreibern die durch den Einsatz eines IMSI-Catchers verursachten Störungen des Netzbetriebs. Wird ein Handy von einem IMSI-Catcher „gefangen“, können bis zur „Freigabe“ an eine echte Basisstation mit diesem Handy

[7] Das erforderliche Messinstrumentarium füllt einen kleinen Bus.

[8] Siehe Pütz, DuD 8/1998 [Pütz_98].

[9] Auf eine rechtliche Bewertung des IMSI-Catchers wird hier verzichtet; siehe dazu z. B. Rublack, in diesem Heft.

weder Gespräche empfangen noch Verbindungen aufgebaut werden. Davon sind unterschiedslos alle Handys betroffen, die sich im Einzugsbereich des IMSI-Catchers befinden – auch Notrufnummern können von diesen Mobiltelefonen in diesem Zeitraum nicht angewählt werden.

Die tatsächlich verursachten Störungen werden von Netzbetreibern und der Bundesregierung allerdings sehr unterschiedlich eingeschätzt.

> So geht das BMI davon aus, dass es beim Einsatz des IMSI-Catchers für höchstens zehn Sekunden – das ist die Zeit, die für die Erfassung von IMSI und IMEI eines Handys maximal benötigt wird – zu Einschränkungen kommt.

Unmittelbar darauf werde das Handy wieder an die originale Basisstation zurückverwiesen. Zudem werde der IMSI-Catcher ohnehin nur in unmittelbarer Nähe einer Zielperson eingesetzt, allein schon, um die Menge der erfassten und zu überprüfenden IMSIs klein zu halten. Auch würde üblicherweise versucht, vorab das von der observierten Person genutzte Mobilfunknetz zu ermitteln.

> Die Netzbetreiber befürchten hingegen, dass die durch einen IMSI-Catcher verursachte Störung weit länger dauert als der für die Erfassung einer einzelnen IMSI erforderliche Zeitraum: Nach Auskunft des Herstellers Rohde & Schwarz können während des gesamten Einschaltzeitraums im Einzugsbereich des IMSI-Catchers keine Gespräche aufgebaut werden – und der läge eher bei 5-10 Minuten.

In diesem Zeitraum können zudem die Netzbetreiber in dieser Funkzelle ihrer lizenzrechtlichen Versorgungspflicht, einen erreichbaren Notrufdienst anzubieten, nicht genügen.

Auch eine weiter gehende generelle Beeinträchtigung des Netzbetriebs im „Einzugsbereich“ eines IMSI-Catchers wird von den Netzbetreibern befürchtet: Durch Interferenzen der simulierten Basisstation mit den Funksignalen der echten Basisstation seien im Überlappungsbereich Übertragungsstörungen und Gesprächsabbrüche unvermeidlich. Schließlich sei der IMSI-Catcher für eine Sendeleistung von bis zu 20 Watt ausgelegt – eine Leistung, mit der eine Funkzelle von der Fläche einer mittleren deutschen Großstadt ausgeleuchtet werden könne. Würde diese maximale Leistung z. B. zur Ortung eines Handys mit bekannter IMSI genutzt, dann wäre eine erhebliche Anzahl von Handy-Nutzern von Störungen betroffen.

Eine verlässliche Aussage über die von einem IMSI-Catcher verursachten Störungen ließe sich erst nach systematischen Feldversuchen treffen. Bislang wurden solche Feldversuche jedoch offenbar nicht durchgeführt.

3.3 Missbrauch

Eine nicht zu unterschätzende Missbrauchsgefahr geht zudem von der Tatsache aus, dass beide Modelle des IMSI-Catchers, sowohl der GA 090 als auch der GA 900, legal erworben werden können. Zwar gibt es keine Betriebsgenehmigung der Regulierungsbehörde für Post und Telekommunikation für die Nutzung des Geräts in Deutschland.[10] Allerdings kann der unzulässige Einsatz technisch nicht festgestellt werden: Weder lässt sich die Simulation einer Basisstation durch einen IMSI-Catcher aufdecken, noch können Störungen des Netzbetriebs auf einen IMSI-Catcher zurückgeführt werden.

Daher kann nicht ausgeschlossen werden, dass insbesondere das Modell GA 900 von kriminellen oder ausländischen Geheimdiensten zum gezielten Abhören sensibler Handy-Gespräche in Deutschland eingesetzt wird. Derzeit untersucht das BSI im Auftrag des BMI dieses Risikopotenzial und erwägt technische Möglichkeiten, um den Einsatz eines IMSI-Catchers detektierbar zu machen.[11]

4 Fazit

Mit der Verabschiedung des Terrorismusbekämpfungsgesetzes und der damit einher gehenden Erweiterung der Befugnisse der Verfassungsschutzbehörden und des MAD ist in Zukunft mit einem verstärkten Einsatz des IMSI-Catchers bei Ermittlungsbehörden zu rechnen.

Dabei irritiert, dass offenbar bislang keine Feldversuche zur Feststellung des Störpotenzials durchgeführt wurden, obwohl die Netzbetreiber ihrerseits wiederholt ihre Mitwirkung angeboten haben.

Zusätzlich drängt sich der Eindruck auf, dass die Gefährdung, die von einer freien Verfügbarkeit des IMSI-Catchers GA 900 ausgeht, erheblich unterschätzt wird. Es erscheint nicht ausgeschlossen, dass der Gewinn an erweiterten Ermittlungsmöglichkeiten der Strafverfolgungsbehörden durch die Schaffung eines neuen Hilfsmittels zur Begehung von Straftaten überkompensiert wird.

Schließlich ist zu beobachten, dass Diskussionen über die insbesondere rechtliche Bewertung der Nutzung des IMSI-Catchers oft mit bestenfalls rudimentären Kenntnissen der technischen Möglichkeiten geführt werden – das gilt sogar für Formulierungen in Begründungen einschlägiger Gesetzgebungsentwürfe.

Allerdings könnte es sein, dass sich die gesamte Diskussion schon in Bälde erledigt: Sollte sich entgegen den derzeitigen Zweifeln an der Wirtschaftlichkeit des Netzaufbaus die UMTS-Technologie durchsetzen, wäre auch der IMSI-Catcher vom Tisch. Denn das UMTS-Protokoll arbeitet mit einer gegenseitigen Authentifikation[12] – das ist das Ende von Maskerade- und Man-in-the-Middle-Angriffen à la IMSI-Catcher.

Literatur

[Fox_97] Fox, Dirk: *IMSI-Catcher*. Gateway, Datenschutz und Datensicherheit (DuD), 9/1997, S. 539. Eine überarbeitete Fassung des Beitrags vom 07.10.1997 findet sich im Internet unter `http://www.datenschutz-und-datensicherheit.de/jhrg21/imsicatc.htm`

[PüSM_01] Pütz, Stefan; Schmitz, Roland; Martin, Tobias: *Security Mechanisms in UMTS*. Datenschutz und Datensicherheit (DuD), 6/2001, S. 323-332.

[Pütz_98] Pütz, Stefan: *Peilung und Ortung*. Gateway, Datenschutz und Datensicherheit (DuD), 8/1998, S. 462.

[10] Die Versuchsfunkgenehmigung der RegTP für den Testbetrieb lief 1999 aus. Ein Antrag auf dauerhafte Frequenzzuteilung wurde im Juli 2000 von der RegTP abgelehnt.

[11] „Der Spiegel“, Heft 33/2001, S. 54 f.

[12] Zu den Sicherheitsmechanismen von UMTS siehe ausführlich Pütz/Schmitz/Martin, DuD 6/2001 [PüSM_01].