DuD
Datenschutz und Datensicherheit

IMSI-Catcher

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

1 Hintergrund

Die Bundesregierung hat am 23. Mai 1997 dem Bundesrat einen Gesetzentwurf für ein Begleitgesetz zum Telekommunikationsgesetz (BegleitG) zugeleitet,[1] der im wesentlichen die für die Arbeit der Regulierungsbehörde im Bereich der Telekommunikation (BAPT) erforderlichen personalrechtlichen Bestimmungen enthält, aber auch Regelungen zur Überwachung des Fernmeldeverkehrs. Der Bundesrat hat nun auf seiner Sitzung am 4. Juli 1997 die Bundesregierung aufgefordert, die Überwachungsbestimmungen des G 10 Gesetzes um folgenden Passus zu ergänzen:

„Eine [Abhör-] Anordnung berechtigt auch zur Identifikation der von einer Person benutzen Anschlußnummer durch technische Maßnahmen, auch soweit dabei das Fernmeldegeheimnis unbeteiligter Dritter technisch bedingt unvermeidbar beeinträchtigt wird."[2]

Mit dieser Einfügung soll nach der Begründung den Nachrichtendiensten die Ermittlung „unbekannter Rufnummern Verdächtiger auf technischem Wege" im Mobilfunk durch sogenannte „IMSI-Catcher" ermöglicht werden.[3] Hintergrund ist, daß in GSM-Mobilfunknetzen ein direktes Abhören von Handys durch die verschlüsselte Übertragung auf der Luftschnittstelle, d.h. zwischen Gerät und Basisstation, verhindert wird. Eine Identifikation des Mobilfunkteilnehmers ist wegen der Verwendung temporärer, wechselnder Teilnehmerkennungen, die damit wie eine Art technisches „Pseudonym"[4] wirken, für Netzfremde unmöglich.[5]

[1] BR-Drs. 369/1/97 = BT-Drs. 13/8016.
[2] Neuer Satz 3 Art. 1, § 2 Abs. 2 G 10.
[3] BR-Drs. 369/1/97, S. 4.
[4] Zum Begriff des Pseudonyms siehe Bizer/Bleumer, Gateway, DuD 1/1997, S. 46.
[5] Darstellung in Pütz, DuD 6/1997, S. 321 ff.

2 Funktionsweise

Unter „IMSI-Catchern" werden Geräte verstanden, die als „mobile Basisstation" arbeiten. Sie verhalten sich wie eine feste Basisstation des Mobilfunknetzes und beheimaten ein Visitor Location Register (VLR) für alle Teilnehmer, die sich in ihrer Funkzelle aufhalten. Jedes eingeschaltete Handy im Empfangsbereich registriert und authentisiert sich daher unbemerkt gegenüber diesem „IMSI-Catcher". Den Teilnehmern fällt ein solches als Basisstation „maskiertes" Gerät nicht auf, da die Authentikation nur einseitig, d.h. seitens des Handys gegenüber der Basisstation (VLR) erfolgt. Dies ließe sich durch ein gegenseitiges Authentikationsprotokoll vermeiden; in der GSM-Spezifikation wurde aber darauf verzichtet.

Das Gerät kann nun durch Vortäuschung eines Fehlers von jedem Handy die Übersendung seiner weltweit eindeutigen Identitätsnummer (International Mobile Subscriber Identity – IMSI) erzwingen. Zu dieser IMSI kann es beim Home Location Register (HLR) des Netzbetreibers die passende Rufnummer anfordern.[6] Auf diese Weise können auch Handy-Rufnummern in Erfahrung gebracht werden, die z.B. unter falschem Namen oder im Auftrag beantragt wurden. Diese Geräte „können für Strafverfolgungsbehörden, aber auch für das Zollkriminalamt und die Verfassungsschutzbehörden von großer Bedeutung sein".[7]

Zugleich kann das Gerät alle eingehenden und ausgehenden Telefonate, die mit einem der bei ihm registierten Handys geführt werden, unverschlüsselt mitprotokollieren, denn es kennt für alle diese Verbindungen die im Authentication Center (AUC) erzeugten Schlüssel, damit es die Daten einer Verbindung vor Einspeisung in das Festnetz ent- und in umgekehrter Richtung für die Funkübertragung zum Handy verschlüsseln kann. Rufnummernermittlung und Gesprächsaufzeichnung könnten direkt vor Ort durchgeführt werden.

Von einem Einsatz eines solchen „IMSI-Catchers" bei Überwachungsmaßnahmen im realen Netzbetrieb ist jedoch nicht nur der Teilnehmer betroffen, auf dessen Anschluß die Maßnahme zielt. Vielmehr werden alle Teilnehmer, die sich mit eingeschaltetem Handy in der Funkzelle des Gerätes aufhalten, identifiziert, bis der gewünschte gefunden ist. Eine Abhörmaßnahme beträfe zudem jede Verbindung eines Mobiltelefons im Einflußbereich des „IMSI-Catchers" und könnte je nach Funkzelle leicht die Gespräche einiger hundert Teilnehmer einschließen.

[6] Siehe Pütz, DuD 6/1997, S. 321 ff. und Beheim, DuD 6/1994, S. 327 ff.
[7] BR-Drs. 369/1/97, S. 4.

3 Verfügbarkeit

Die Firma Rohde & Schwarz (München) hat einen „IMSI-Catcher" mit der Typbezeichnung „GA 900" entwickelt, der – in verschiedenen Ausführungen – das Ermitteln von Rufnummern und das automatische Aufzeichnen von Gesprächen ermöglicht. Eine Variante soll lediglich ausgewählte Verbindungen entschlüsseln und aufzeichnen können; Verbindungen mit allen anderen Mobiltelefonen im Einflußbereich des Gerätes werden abgebrochen bzw. abgewiesen. Die Exportversion des Geräts soll alle Funktionen umfassen.

Die Netzbetreiber T-Mobil, Mannesmann Mobilfunk und E-Plus gehen davon aus, daß der Einsatz eines solchen Gerätes zu Störungen und einer Beeinträchtigung der Verbindungsqualität führen wird, da die vom „IMSI-Catcher" benutzten Frequenzen nicht mit der jeweiligen Netz-Frequenzplanung abgestimmt sind. Bisher hat das Bundesamt für Post und Telekommunikation (BAPT) für keine Variante dieses Geräts eine Betriebsgenehmigung für Deutschland erteilt.