# 1998/50 Inland

https://ads.jungle.world/artikel/1998/50/zugriff-auf-gesamtverkehr

# »Zugriff auf Gesamtverkehr«

Von **christiane schulzki-haddouti**

**Europas Justizbehörden wollen kein Wort mehr überhören - im Internet, am Telefon oder am Handy**

Die europäische Union plant die umfassende Überwachung des Telekommunikationsverkehrs sowie des Internet. Dies geht aus jüngst durch das Internet-Magazin Telepolis ( **www.telepolis.de/tp/** deutsch/special/enfo/6333/1.html) publizierten geheimen Unterlagen unter der Bezeichnung "Enfopol 98" hervor.

Strafverfolgungsbehörden, Zollämter und Geheimdienste wollen den "Zugriff auf den gesamten Fernmeldeverkehr": Festnetz- und Mobiltelefonie, Internet und Fax, Pager und interaktives Kabel-TV. Die Abhörschnittstellen jedes einzelnen EU-Mitgliedstaates sollen künftig jedem anderen EU-Staat das Abhören über Fernzugriff ermöglichen.

Möglicherweise werden auch die USA, Kanada, Australien und Neuseeland an dem Abhörnetzwerk teilnehmen können. Auch das FBI und andere nicht-europäische Sicherheitsbehörden hätten dann jederzeit Zugriff auf die Kommunikation innerhalb Europas. Als "inakzeptabel, gefährlich und teuer" verurteilt der SPD-Bundestagsabgeordnete Jörg Tauss die Pläne der EU-Innenminister. Empört stellt der SPD-Politiker fest, daß Enfopol sogar "alle deutschen Bestimmungen zum Lauschangriff in den Schatten stellt".

Vor allem die mobile satellitengestützte Telefonie, wie sie durch das im Herbst an den Start gegangene Unternehmen Iridium ermöglicht wird, ist den Sicherheitsbehörden ein Dorn im Auge. Sie ermöglicht Telefongespräche von jedem beliebigen Ort der Welt aus. Mit einem Zugriff auf die Daten des Telekommunikationsbetreibers können nicht nur Gespräche abgehört werden, der Handybesitzer läßt sich darüber hinaus sogar orten. Das kommt den Strafverfolgungsbehörden entgegen, denn sie fordern auch Informationen über den "möglichst genauen geographischen Standort innerhalb des Netzes". Diese Forderung ist nach deutschem Recht schlicht illegal.

Im Fall von Iridium stellen sich die Behörden eine möglichst simple Lösung vor: In Europa gibt es bislang nur eine Bodenstation - in Italien. Das geforderte "sekundenschnelle" Abhören ist daher am einfachsten über "Remote Control" zu verwirklichen: Mit dem Zugriff auf die europäische Masterstation, die zu Abrechnungszwecken auch alle Iridium-Gateways in den anderen europäischen Ländern kontrolliert, können auch alle Verbindungsdaten zentral abgerufen werden. Zur Zeit ist dies jedoch nur eingeschränkt möglich.

Lücken in der Telekommunikationsüberwachung schließen - unter diesem Motto stehen die Enfopol-Papiere. Zu tief sitzt den Strafverfolgungsbehörden der Mobilfunkschock: Mittels Handy organisierten Häftlinge von ihrer Zelle aus unbeobachtet kriminelle Machenschaften. Mobilnetzbetreiber warben sogar mit der "abhörsicheren" verschlüsselten Kommunikation. Nun will sich die Polizei nicht mehr dem Vorwurf aussetzen, sehenden Auges Abhörlücken in Kauf zu nehmen. Auf der Wunschliste stehen daher neben Satellitenkommunikation auch "Internet, Kryptografie, Prepaid Cards udgl. sowie neue Technologien".

Ein Richterbeschluß im Land des Abhörers soll in Zukunft genügen, um im gesamten Enfopol-Vertragsgebiet abzuhören. Bilaterale Rechtsabhilfeabkommen ermöglichen dabei den automatisierten und sekundenschnellen Abruf im Ausland. Auch US-Kryptobotschafter David Aaron strebt solche bilateralen Rechtshilfeabkommen ausdrücklich an. Um diese jedoch nicht durch die umstrittene Kryptoregelung zu gefährden, setzen die USA im Falle verschlüsselter Kommunikation zunächst auf den Austausch von Klartext. Die angestrebte Vereinbarung über eine Zusammenarbeit US-amerikanischer und europäischer Sicherheitsbehörden impliziert allerdings auch eine Lösung der Kryptographie-Frage. Aaron gegenüber dem Computermagazin c't: "Hoffentlich können wir diese Art von Zusammenarbeit auch noch zu einer Zeit durchführen, in der Telefongespräche nur noch verschlüsselt übertragen werden - und wir sie dann doch entschlüsseln können."

Bereits seit 1993 wird die Zusammenarbeit zwischen den Polizeibehörden der EU-Mitgliedstaaten sowie dem US-amerikanischen FBI vorbereitet (www.privacy.org/pi/activities/tapping/statewatch_tap_297.html). Die "Ergänzenden Anforderungen", die einen großen Teil der Enfopol-Papiere ausmachen, sehen eine Menge Verpflichtungen von Netzwerkprovidern, Satellitenkommunikationsnetzwerken, Serviceprovidern, Firmen und einzelnen Personen vor. Ein Beschluß des EU-Rats aus dem Jahr 1993 sieht sogar "aus praktischen Gründen eine Erweiterung nach Hong Kong, Australien und Neuseeland" vor. Neben Großbritannien, Kanada und den USA befinden sich in diesen Ländern die Hauptpunkte des Abhörsystems - sie laufen unter dem Kodenamen "Echelon".

Ob Telefonanrufe, E-Mails, Faxe, oder Telex, Echelon hört den gesamten über Satelliten geleiteten Kommunikationsverkehr ab. Gefiltert werden die riesigen Informationsmengen mit Hilfe des intelligenten Rastersystems "Memex". Memex ist ein Analyseprogramm, das Daten auf Schlüsselwörter hin untersuchen kann. Involviert in das Echelon-System sind die US-amerikanische National Security Agency (NSA), das Government Communications Headquarters (GCHQ) in Großbritannien, das Communications Security Establishment (CSE) in Kanada, das Defence Signals Directorate (DSD) in Australien und das Government Communications Security Bureau in Neuseeland. Die Abhörzentren befinden sich in den USA in Sugar Grove/Virginia und in Yakima im Staate Washington, außerdem in Waihopai in Neuseeland, Geraldton/Australien und in Morwenstow/England.

Es ist unwahrscheinlich, daß für die fallweise Überwachung eine völlig neue technische Infrastruktur implementiert wird. Vermutlich plant die Enfopol-Arbeitsgruppe, den derzeit für Echelon genutzten Überwachungsapparat schrittweise auch der polizeilichen Nutzung zuzuführen. Standardisierte Schnittstellen und die Entwicklung von gemeinsamen Technologiestandards spielen bei der länderüber- greifenden Überwachung eine entscheidende Rolle.

Tony Bunyan, Direktor der europäischischen Bürgerrechtsorganisation Statetwatch sieht eine "große Bedrohung der bürgerlichen Grundrechte" vor allem darin, daß der EU-FBI-Plan zur Telekommunikationsüberwachung "völlig im Geheimen", "ohne jeden Bezug zum europäischen Parlament, den nationalen Parlamenten oder der bürgerlichen Gesellschaft" entwickelt wurde.

Schien die Debatte um die freie Nutzung von Verschlüsselungsprodukten im Sommer bereits befriedet, so rufen die Enfopol-Papiere die alten Gegner wieder auf den Plan: Sicherheitsbehörden gegen Wirtschaft, Datenschützer und Bürgerrechtler. Schließlich läßt sich das Abhören verschlüsselter Kommunikation nicht binnen Sekunden, Minuten oder Stunden umsetzen, wenn Kommunikationsinhalte mit starken Kryptomethoden - beispielsweise auch vor Wirtschaftsspionage - geschützt werden. Ohne gesetzliche Beschränkungen für Kryptographie ist es nicht möglich, verschlüsselte Inhalte zu verwerten.

Ute Bernhardt und Ingo Ruhmann, Vorstandsmitglieder des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) sehen in den Enfopol-Plänen zwar "keine Präjudizierung einer EU-weiten restriktiven Kryptopolitik", gleichwohl ermögliche sie jedoch die Nutzung nationaler Key-Recovery-Regelungen.

Der Entwurf könne daher für die Bundesregierung wieder "Anlaß sein, vorerst zurückgezogene Vorhaben wieder aus der Schublade zu holen", warnen die beiden Informatiker. Sie sehen in dem Entwurf eine ähnliche Vorgehensweise wie bereits beim europäischen Polizeicomputer-Verbund, dem Schengen Informationssystem: "Wiederum wird zuerst die technische Basis gelegt für eine polizeiliche Kooperation, deren rechtliche Basis erst in Ansätzen existiert."

Der schleswig-holsteinische Landesbeauftragte für den Datenschutz, Helmut Bäumler, vermißt in den Plänen die "notwendige Sensibilität". So fallen bei der rechtmäßigen Überwachung der Telekommunikation nicht nur Inhalte von Telefongesprächen an. Aus den Überwachungsdaten lasse sich auch ein "detailliertes Persönlichkeitsbild" zusammenstellen. Zudem stecke hinter der Aufzählung jeglicher Form technischer Adressenkennung ein unrealistischer "Datenhunger". So verlangten die EU-Experten ausführliche Daten selbst zu "Internet Domain Namen" - doch diese sind jederzeit für jeden im Internet abrufbar.

Zwar ist die angestrebte EU-Ratsentschließung Enfopol für die Mitgliedstaaten nicht rechtsverbindlich, da Überwachungsmaßnahmen auch weiterhin nationale Angelegenheit bleiben. Doch sie bestimmt die Ausgestaltung künftiger Rechtshilfeabkommen. So heißt es in einer vergangene Woche bekannt gewordenen Tischvorlage, daß die für die Telekommunikation zuständigen Minister die EU-Auffassung unterstützen und mit den Justiz- und Innenministern zusammenarbeiten sollen, um eine europäische Standardisierung zu erreichen.

Bereits letzte Woche trat der europäische Justiz- und Innenausschuß zusammen. Tagesordnungspunkt: Die "Konvention zur gegenseitigen Rechtsbeihilfe sowie das Protokoll für das Abhören von Telekommunikation". Anfang nächsten Jahres sollen letzte Details der Konvention im Europäischen Rat vereinbart werden. Bereits im Jahr 2000 könnten die Parlamente in den EU-Mitgliedstaaten die Konvention als Bestandteil der nationalen Gesetzgebung ratifizieren.

Der bündnisgrüne Bundestagsabgeordnete Christian Ströbele forderte jetzt das deutsche Innen- und Justizministerium auf, in Brüssel auf die "erforderliche Denkpause und Überprüfung dieses gefährlichen, teuren und fragwürdigen Vorhabens" zu dringen. Die geplante Reglung dürfe in der vorgesehenen Form nicht verabschiedet werden.