



[ENFOPOL: EU-Abhörstandards für die Telekommunikationsnetze](#)

Die ETSI Dossiers IV
Erich Moechel 11.02.2002

[Abhörstandards für digitale Netze vor der Verabschiedung](#)

Die ETSI-Dossiers
Erich Moechel 13.08.2001

[Enfopol gedeiht](#)

In einem neuen Papier fordern die europäischen Strafverfolger, dass sie unabhängig von der jeweiligen Technik jede denkbare Art der Telekommunikation in Echtzeit belauschen können
Florian Rötzer 26.06.2001

[Widerstand gegen die neuen Enfopol-Überwachungspläne](#)

Vertreter von Providern, Lobbyvereine und Datenschützer kritisieren die geplante Ausweitung der Speicherung sämtlicher Telekommunikationsdaten
Stefan Krempl 23.05.2001

[Europäische Strafverfolger fordern die totale Telekommunikations-Überwachung](#)

Nach der Verabschiedung zahlreicher Lauschgesetze sollen nun die Verkehrsdaten jahrelang gespeichert und anonyme Netzzugänge verboten werden
Stefan Krempl 19.05.2001

[Der Griff der Geheimdienste nach dem Internet](#)

Seit Anfang April gibt es nun einen Entwurf, der den Lauschangriff auf IP-Netze und die technische Überwachung im Internet europaweit vereinheitlichen soll.
Erich Moechel 23.04.2001

[Die ETSI-Dossiers](#)

Europäische Schnittstellen zur Überwachung sämtlicher digitaler Netze

Erich Moechel 26.03.2001

Europäische Kommission ruft zum Kampf gegen Cyberkriminalität

Europol soll Cyberkriminalität bekämpfen; 'Enfopol-Papiere' werden derzeit nicht weiter ausgearbeitet; Angleichung nationaler Gesetzgebung sei zur Bekämpfung von High-Tech-Kriminalität nötig

Jelle van Buuren 10.01.2001

Europäische Minister holen zum Schlag gegen Cyberkriminalität aus

Informelles Meeting der Justizminister setzt Cyberkriminalität ganz oben auf die Agenda

Jelle van Buuren 30.07.2000

Euro-Fälschungen und Geldwäsche als Tests für EU-

Polizeizusammenarbeit

Europol-Fahrplan bis 2004

Christiane Schulzki-Haddouti 13.07.2000

Telepolis erhält für Enfopol-Berichterstattung den Europäischen Preis für Online-Journalismus

Gewürdigt wird Telepolis in der Kategorie "Investigative Reporting"

Telepolis erhält für Enfopol-Berichterstattung den Europäischen Preis für Online-Journalismus 06.07.2000

Die Globalisierung der Überwachung

Schengen, Europol, Eurodac und die EU-FBI-Überwachungspläne.

Thomas Mathiesen 20.06.2000

Neue Zugriffsrechte auf private Kommunikation geplant?

Die Arbeitsgruppe "Lawful Interception" tagt wieder in London

Brigitte Zarzer 07.06.2000

Europäisches Rechtshilfeabkommen verabschiedet

Trotz Kritik des Europäischen Parlaments keine Änderungen mehr an der Fassung vom 15.Mai. Präventions- und Schutzmaßnahmen sollen Missbrauch bei der Fernmeldeüberwachung ausschließen.

Christiane Schulzki-Haddouti 30.05.2000

Europäisches Rechtshilfeabkommen kurz vor Verabschiedung

Bis zuletzt Geheimhaltung; deutscher Parlamentsvorbehalt aufgehoben

Christiane Schulzki-Haddouti 26.05.2000

[Digitale Detektive in Holland](#)

Sonderbefugnisse für den Lauschangriff im Internet; der geheime Einfluss von ILETS; Wanzen im Keyboard und Angriffe auf die Anonymität.

Jelle van Buuren 10.04.2000

[Feinschliff am Abhörstandard](#)

Europäische Kommission hält an Abhör-Artikel des Rechtshilfeübereinkommens fest; das europäische Standardisierungsinstitut ETSI hat den entsprechenden technischen Standard schon vorsorglich definiert.

Christiane Schulzki-Haddouti 04.04.2000

[Kein endgültiger Beschluss über europäisches Übereinkommen zur Rechtshilfe in Strafsachen](#)

Luxemburg blockiert die Vereinbarung wegen Bankgeheimnis; Kompromiss bei grenzüberschreitendem Abhören.

Jelle van Buuren 28.03.2000

[EU will Informationen über Terrorismus im Internet sammeln](#)

Die Geheimdienste scheinen mit Hacker-Slang ihre Probleme zu haben, wie zum Beispiel mit der Benutzung des Buchstabens "z" in "passwordz, gamez, crackz, softwarez".

Jelle van Buuren 16.03.2000

[Europäisches Rechtshilfeabkommen wird im März verabschiedet](#)

Datenschutzregeln sollen integriert werden, Kompromiss mit Echelon-Staat Großbritannien

Christiane Schulzki-Haddouti 29.02.2000

[»Grenzüberschreitendes Abhören führt in gesetzliches Minenfeld«](#)

Ausschussbericht des Europäischen Parlaments lehnt grenzüberschreitendes Abhören der Telekommunikation ab.

Jelle van Buuren 15.02.2000

[Erste offizielle Bestätigung für Echelon aus den USA](#)

Aufgrund des Freedom of Information Act wurde jetzt ein Dokument gefunden, das explizit auf Echelon hinweist

Florian Rötzer 26.01.2000

ENFOPOL bis Mai im Trockenen

Aber noch immer ist der Entwurf Verschlusssache
Christiane Schulzki-Haddouti 26.2.1999

Neues von Echelon

Dänische Journalisten über Beteiligung Dänemarks und anderer NATO-Staaten
Florian Rötzer 27.12.1999

ENFOPOL und das Recht auf »Eigentumsfreiheit«

Scheitert die Realisierung des Überwachungsstaates an einer "grundrechtswidrigen Kostenüberwälzung"?
Thomas Keul 30.11.1999

Bundesregierung arbeitet weiter an Enfopol-Plänen

"Nur eine sprachliche Anpassung der Anforderungen von 1995"
Christiane Schulzki-Haddouti 15.11.1999

Keine Einigung bei europäischem Rechtshilfeübereinkommen

Echelon-Staat Großbritannien blockiert Überwachungspläne der europäischen Strafverfolger.
Christiane Schulzki-Haddouti 12.11.1999

Enfopol-Pläne in Europäisches Rechtshilfeabkommen integriert

Genereller Fernzugriff?
Christiane Schulzki-Haddouti 08.11.1999

Enfopol-Vorhaben vorläufig ad acta gelegt?

Der Europäische Rat will nach der Kritik offenbar die Pläne für das EU-Lauschsystem zur Überwachung der Telekommunikation und des Internet vollständig überarbeiten
Florian Rötzer 14.10.1999

Europa: Die totale Überwachung?

ZDF berichtet über Enfopol
Europa: Die totale Überwachung? 02.06.1999

Ein Wort zur Überwachung

Ad Enfopol: Weder Paranoia schüren, noch Gefahren verharmlosen.
Armin Medosch 21.05.1999

[EU-Parlament verabschiedet Enfopol-Überwachungspläne](#)

Kritik ist "übertrieben"

Christiane Schulzki-Haddouti 10.05.1999

[Enfopol-Abstimmung im Europa-Parlament](#)

Europäische Datenschützer fordern Präzisierung

Christiane Schulzki-Haddouti 07.05.1999

[ILETS, die geheime Hand hinter ENFOPOL 98](#)

Die Geschichte von ENFOPOL aus dem Kontext von ILETs, eine US-dominierte, internationale Organisation hinter Europas umstrittenen Plänen zur Internetüberwachung.

Duncan Campbell 29.04.1999

[EU-Polizei will ENFOPOL-Ratsbeschluss durchdrücken](#)

Dokument umbenannt, Ziele gleich geblieben. Amerikas leitende Hand wird sichtbar.

Duncan Campbell 29.04.1999

ENFOPOL: EU-Abhörstandards für die Telekommunikationsnetze

Erich Moechel 11.02.2002

Die ETSI Dossiers IV

Noch fehlt dem in den Rang eines europäischen Standards erhobenen Definitionen zum Abhören von Telekommunikationsnetzen die politische Legitimation durch die EU. In der aktuellen Version sind aber bereits auf technischer Ebene alle notwendigen Schnittstellen zum Abhören durch Strafverfolgungsbehörden und Geheimdienste festgelegt. Den EU-Mitgliedsländern bleibt es immerhin überlassen, ob sie automatische elektronische Schnittstellen oder nur ein manuelles Interface gestatten.

Seit der Verabschiedung des Schnittstellen-Standards ES 201 671 Version 2.0 am 31. August, der sowohl der novellierten deutschen wie auch der österreichischen Überwachungsverordnung zu Grunde liegt, sei die Luft draußen, ist von einer Quelle aus der die Arbeitsgruppe "Lawful Interception" ETSI SEC LI [1]) des European Telecom Standards [2] (ETSI) zu hören. Beim Treffen in Warschau im September sei seitens der Netzbetreiber und Ausrüster sogar überlegt worden, SEC LI überhaupt aufzulösen. Wahrscheinlich werde die Arbeitsgruppe nur noch als beratendes Gremium weitergeführt, während die eigentliche Arbeit in den spezialisierten technischen Körperschaften (TIPHON, SPAN, TSG SA WG3) des ETSI geschieht, wohin bereits die technischen Lösungen für die UMTS-Überwachung und für die Überwachung von digitalen Breitbandzugängen - Telefonie und Internet über Kabel-TV-Netze - verlagert wurde.

Der seit längerem beobachtbare Trend, Kompetenzen aus der unter Behördenaufsicht stehenden Arbeitsgruppe SEC LI in zivil besetzte Techniker-Gremien verlagern [3], setzte sich auch in der ETSI-Generalversammlung fort. Das letzte Plenum im abgelaufenen Jahr stand unter dem Zeichen der Neustrukturierung aller Agenden für die "Next Generation Networks", die auf der Versammlung vorgestellte Studie aber hat die künftigen Aufgaben von SEC LI auf einen Bruchteil ihrer bisherigen Tätigkeit reduziert. Grund für diese Veränderung sei die "höhere Wahrscheinlichkeit", dass "die Anforderungen für Lawful Interception in allen technischen Körperschaften entsprechend verstanden würden", heißt es in der Studie.

Das skandalöse Wechselspiel: ETSI SEC LI und ENFOPOL

Bei der heterogenen und völlig aus dem Rahmen der übrigen Arbeitsgruppen des ETSI fallenden Zusammensetzung von SEC LI stellen je ein Drittel der Teilnehmer an den

Treffen Strafverfolger und Bürokratie, Lieferanten von Überwachungs-Equipment sowie die großen Telekom-Zulieferer und Netzbetreiber. Vornehmlich deren Beiträge finanzierten "Deliverables" mit, die "ausschließlich den Standpunkt der Strafverfolger" widerspiegeln, wie es in den entsprechenden Vorworten stereotyp heißt.

Im Fall von ES 201 671 aber lief der übliche Standardisierungsprozess - generelle Anforderungen der Behörden auf politischer Ebene, technische Spezifikation dieser Anforderungen, technischer Standard - genau umgekehrt. Nachdem die IT-Industrie sich in jahrelangem Ringen mehrheitlich auf einen umfangreichen Schnittstellen-Standard zur Überwachung der digitalen Netze in allen Details geeinigt und damit vollendete Tatsachen geschaffen hatte, wurde das Anforderungspapier der Strafverfolger erst nachgereicht.

Die mit August 2001 datierte "Technische Spezifikation" ETSI TS 101 331 (Version 1.1.1.) beschreibt die "Anforderungen bezüglich Handover Interfaces zur Überwachung für Strafverfolger und Staatssicherheitsagenturen" (1 Scope). Dieses verspätet eingereichte "Pflichtenheft" zum Standard ES 201 671 ist nichts anderes als die technische Umsetzung der unter ihrem Dokumenten-Namen ENFOPOL bekannt gewordenen International User Requirements (IUR) der Behörden.

TS 101 331 setzt fort [4], wo ETSI ETR 331 fast fünf Jahre zuvor aufgehört hat. Warum dieses technische "Pflichtenheft", auf dessen Vorgaben sämtliche Überwachungsstandards beruhen sollten, seit Dezember 1996 nicht bearbeitet worden war, hat gute Gründe. Seit Anfang 1997 sorgte noch jedes Auftauchen der International User Requirements für einen Skandal auf politischer Ebene. Erstmals bekannt wurden die IUR unter der Bezeichnung EU-FBI Surveillance Network [5] beziehungsweise unter dem Akronym ENFOPOL im Jahre 1997 (I LETS, die geheime Hand hinter ENFOPOL 98 [6]). Der Skandal begann mit einem EU Ratsbeschluss zur Überwachung des Fernmeldeverkehrs vom 17. Januar 1995 (ENFOPOL 1995 [7]).

Dieser auf einer Serie von ENFOPOL-Dokumenten der EU-Ratsarbeitsgruppe Polizeiliche Zusammenarbeit (Police Coordination Working Group PCWG) basierende Ratsbeschluss wurde als akkordierte Angelegenheit (fait accompli) ohne Anhörungen oder Diskussion am 17. Januar 1995 durch den Fischereiausschuss geschleust.

Die Abgeordneten des EU-Parlaments erlangten nicht einmal sofort davon Kenntnis, als der Ratsbeschluss 18 Monate später öffentlich wurde (Official Journal C 329 , 04/11/1996). Erst als die britische Bürgerrechtsorganisation Statewatch im Januar 1997 den Beschluss im Rahmen eines Berichts über ein geplantes "EU-FBI Surveillance System", veröffentlichte und wenig später ein Report des STOA-Komitees (Science and Technology Options Assesment der EU) ähnlichen Inhalts vorgelegt wurde, gab es empörte Anfragen an die EU-Kommission. Diese wurden ausweichend beantwortet, die dem Beschluss zu Grunde liegenden ENFOPOL-Dokumente wurden von der Kommission den Parlamentariern nicht ausgehändigt. Der Ratsbeschluss selbst war formalrechtlich

nicht angreifbar, da "akkordierte Angelegenheiten" ohne Anhörung jederzeit in jedem beliebigen Ausschuss verabschiedet werden können. Um diese Zeit lag das aus den ENFOPOL-Vorgaben erstellte technische "Pflichtenheft" ETR 331 im ETSI bereits vor.

Noch höhere Wellen schlug der zweite, groß angelegte Versuch, die in ETSI SEC LI längst laufende Standardisierungsarbeit politisch zu legitimieren. Als Telepolis ein Dokument mit dem Akronym ENFOPOL 98 (diese und andere Ratsdokumente werden jährlich von eins beginnend durchnummeriert) wenige Tage vor einer entsprechenden Sitzung des Rats der Innen- und Justizminister im Netz präsentierte [8], wurde zunächst seine Echtheit in Zweifel gezogen (Originaldokument 3: Revidierte Fassung von ENFOPOL 98 [9]).

Das unter der österreichischen EU-Präsidentschaft bereits in Form eines Ratsbeschlusses erstellte Dokument war insofern neuartig, als es sowohl in Umfang als auch im Inhalt über die "International User Requirements" von 1995 weit hinausging. Es war ein Versuch, technische Anforderungen zur Überwachung der neuen Telefonienetze sowie der Satelliten- und Internet-Kommunikation, die im Rahmen des ETSI (ETR 331) zum damaligen Zeitpunkt offenbar niemand anfassen wollte, auf der politischen Ebene zu verabschieden.

Nach Publikation von ENFOPOL 98 in Telepolis wurde der technische Teil, der den geplanten Vollzugriff auf alle digitalen Netze in aller Deutlichkeit zeigte, eiligst wieder ausgegliedert (Inside ENFOPOL [10]). Den versammelten Innen- und Justizministern wurde Anfang Dezember 1998 ein auf einen Bruchteil seines ursprünglichen Inhalts geschrumpftes Dokument präsentiert (EU-Minister billigen Abhörplan [11]).

Wie schon in der Fassung von 1995 wurde das Papier zweigeteilt. Die technischen Erläuterungen wurden aus dem Entwurf eliminiert und verschwanden in einem Annex, der nicht vorgelegt wurde. So blieb von 42 Seiten nur ein sehr abstrakter, vierseitiger Forderungskatalog (ENFOPOL 19/99), dessen Verabschiedung im EU-Parlament ebenso skandalträchtig war, wie der geheim gehaltene Ratsbeschluss von 1995 (Enfopol-Pläne: Streit im EU-Parlament [12]).

Nur etwas mehr als ein Viertel der EU-Parlamentarier war am Freitag, den 7. Mai 1999 anwesend, als die erneuerten IUR im Rahmen eines "Sicherheitspakets" durch das Parlament gingen. Als die "üblichen Verdächtigen" - Telepolis, ORF FutureZone [13], Statewatch - die Begleitumstände dieser Entscheidung verbreiteten, stand der Vorwurf der politischen Manipulation unübersehbar im Raum (EU-Parlament verabschiedet Enfopol-Überwachungspläne [14]). Das Paket war an zwei Sitzungstagen des EU-Parlaments vor dem Wochenende mehrmals auf die Tagesordnung gesetzt und wieder gestrichen worden, bis die Mehrzahl der Abgeordneten nicht mehr an eine Verabschiedung glaubte und Brüssel für das Wochenende verließ. Von 161 verbliebenen Parlamentariern (Vollbesetzung 626) stimmten 154 mit Ja, die Befürworter verteilten sich ziemlich

gleichmäßig auf Konservative und Sozialdemokraten.

Fehlende politische Legitimation

Der Rat der Innen- und Justizminister aber segnete den Beschluss des EU-Parlaments im Juni 1999 überraschenderweise nicht ab. Vielmehr wurde der Forderung europäischer Datenschutzorganisationen nach Zeit für Diskussion statt gegeben (Enfopol-Vorhaben vorläufig ad acta gelegt? [15]). Obwohl der Rat die Anforderungen von ENFOPOL 98 bzw. ENFOPOL 19 nicht beschlossen hatte, wurden sie aber dennoch in ETSI SEC LI technisch in weiten Teilen umgesetzt. Im November 1999 wurde der ETSI-Standard 201 671 (Version 1.1.1.) fertig gestellt und publiziert. Darauf folgte das "Pflichtenheft" TS 101 331, das weitgehend dem ursprünglichen Papier von 1996 (ETR 331) entspricht, aber um ADSL, GPRS, IP oder VoIP bereichert wurde und zwei neue als "normativ" ausgewiesene Annexe enthielt.

Als letztes Glied in der Kette fehlt nur noch die politische Legitimation, also ein EU-Ratsbeschluss der all das an neue Technologien abdeckt, was man zum Beschluss von 1995 noch nicht wissen konnte. Im Juni 2001 wurde von Statewatch und Cryptome ein internes Papier der EU-Arbeitsgruppe Polizeiliche Zusammenarbeit (PCWG) mit den Dokumentenkürzeln ENFOPOL 55, ECO 143 publiziert (Enfopol gedeiht [16]).

Dieses auf den 20. Juni 2001 datierte, bereits in Form eines Ratsbeschlusses abgefasste Dokument [17] ist das Missing Link von ES 201 671 2.0 zum "Pflichtenheft" TS 101 331. Erstaunlicher Weise fand es sich [18] danach in der Datenbank des Rats der Union, der ENFOPOL Papiere zum Überwachungskomplex in der Vergangenheit überhaupt nicht veröffentlicht hat. In der rechtsverbindlichen "Eur-Lex Datenbank" aller gültigen Ratsbeschlüsse aber war es bis Redaktionsschluss dieses Artikels nicht enthalten, auch die lange Reihe der als beschlossene Sache verabschiedeten "A-Items." Auch das mehr als einen Monat im ETSI publizierte "Pflichtenheft" TS 101 331 (August 2001) bezieht sich noch auf den Ratsbeschluss von 1995.

Allem Anschein nach ist ENFOPOL 55, obwohl es mit "ECO 143" das Kürzel eines Ratsdokuments trägt, bis heute nicht verabschiedet worden. Der in den Rang eines europäischen Standards erhobenen Neuauflage des ES 201 671 vom 31. August 2001 im ETSI fehlt damit jede politische Legitimation durch die EU.

Zwischenbilanz

Trotz der Verabschiedung von ES 201 671 2.0 kann eine Zwischenbilanz keineswegs nur negativ ausfallen. Eine bis dahin völlig ungeniert hinter den Kulissen agierende Gruppe von Geheimdienst-Verbindungsleuten und Fadenziehern kam erstmals an das Licht der Öffentlichkeit. Ihr Manövrieregebiet wurde durch die de facto Abschaffung von ETSI SEC

und die Kompetenzbescheidung von ETSI SEC LI erheblich eingeschränkt.

Dazu kommt, dass der Nachrichtendienstes liebste Kind, die vollelektronische Schnittstelle, in der zuletzt veröffentlichten Version von ES 201 671 nicht mehr obligatorisch ist. Nationalen Regulatoren steht es frei, den Handover Interface Port HI 1, über den Polizei und Dienste an sich direkt per Standleitung mit der Administrationsfunktion des Netzbetreibers, welche alle Vorgänge an der Schnittstelle kontrolliert, verbunden sind, als manuelles Interface zu gestalten. Der Netzbetreiber kann also darauf bestehen, dass Überwachungsbegehren nicht elektronisch ausgehandelt, sondern auch in Zukunft auf Papier oder persönlich vorgelegt werden.

Damit ist es in der Praxis vor allem für die Dienste nicht mehr ganz so einfach, die Kontrolle an der Schnittstelle zu übernehmen. Mit den beiden übrigen Ports HI2 und HI3, an denen Verkehrsdaten bzw. Kommunikationshalte aus dem Netzwerk an Polizei und Dienste fließen, werden sie erst verbunden, wenn die Verhandlungen an HI1 abgeschlossen sind. Es bleibt den nationalen Telekom-Behörden somit überlassen, ob sie ein sehr leicht überbrückbares elektronisches Interface HI1 vorschreiben, das den Diensten permanent Tür und Tor zum gesamten Netzwerk öffnen könnte, oder ob sie ein manuelles Interface gestatten. Dass auch in diesem Fall ein "Workaround" ganz einfach möglich ist, betont einer der SEC LI Regulars in einer Mail an den Autor. Es genüge, schreibt einer der Industrievertreter, den Administrationsrechner, mit dem der Netzbetreiber die Interfaces HI2 und HI3 frei schaltet, physisch neben dem Monitoring Center für Polizei und Dienste zu platzieren.

Eine ausführlichere Version dieses Artikels findet sich in der aktuellen c't 4/2002: "Lauschangriff: Die ETSI-Dossiers, Teil 4"

Das nächste Treffen [19] der Überwachungstruppe SEC LI ist für 19. bis 21. März am Sitz des ETSI in Sophia Antipolis nächst Nizza anberaumt.

Weitere Meetings in London und in Moskau wurden ohne Kommentar gestrichen: als Gastgeber hätten der Satellitenbetreiber Inmarsat oder das "Institut zur wissenschaftlichen Erforschung der Telekommunikation" (ZNIIS) im russischen Telekom-Ministerium fungiert.

Durch Eingabe des Stichworts "interception" erhält man bei der Suche [20] im offiziell öffentlichen Bereich mittlerweile 51 einschlägige Dokumente zum Komplex "lawful interception", einfache Registrierung per Mail genügt. Nicht offiziell erhältliche Papiere wie das detaillierte Abstimmungsprotokoll zu ES 201 671 und Namenslisten sind bei Cryptome [21] erhältlich.

Die umfangreichste Sammlung an ENFOPOL-Papieren hat die britische

Bürgerrechtsgruppe Statewatch [22]. Im Archiv des Newsletters q/depesche [23] findet sich die Chronologie der Berichterstattung zum Wechselspiel von ETSI SEC LI und Enfopol..

Erich Moechel ist Redakteur von Futurezone [24].

Links

- [1] http://portal.etsi.org/portal_common/home.asp?TbId=503
- [2] <http://www.etsi.org/>
- [3] <http://webapp.etsi.org/meetingcalendar/MeetingDetails.asp?mid=22279>
- [4] http://pda.etsi.org/pda/home.asp?wki_id=8886
- [5] <http://www.statewatch.org/EUFBISW.HTM>
- [6] <http://www.heise.de/tp/deutsch/special/enfo/6396/1.html>
- [7] <http://www.heise.de/tp/deutsch/special/enfo/6334/1.html>
- [8] <http://www.heise.de/tp/deutsch/special/enfo/6333/1.html>
- [9] <http://www.heise.de/tp/deutsch/special/enfo/6332/1.html>
- [10] <http://www.heise.de/tp/deutsch/special/enfo/6386/1.html>
- [11] <http://www.heise.de/tp/deutsch/special/enfo/6374/1.html>
- [12] <http://www.heise.de/tp/deutsch/special/enfo/6390/1.html>
- [13] <http://futurezone.orf.at/futurezone.orf?read=detail&id=962&tmp=88099>
- [14] <http://www.heise.de/tp/deutsch/special/enfo/6404/1.html>
- [15] <http://www.heise.de/tp/deutsch/special/enfo/6501/1.html>
- [16] <http://www.heise.de/tp/deutsch/special/enfo/7968/1.html>
- [17] <http://cryptome.org/eu-intercept.htm>
- [18] <http://register.consilium.eu.int/pdf/en/01/st09/09194en1.pdf>
- [19] http://webapp.etsi.org/meetingDocuments/ViewDocumentList.asp?MTG_Id=21635
- [20] <http://webapp.etsi.org/WorkProgram/Expert/QueryForm.asp>
- [21] <http://cryptome.org/e-spy-telecom.htm>
- [22] <http://www.statewatch.org>
- [23] <http://www.quintessenz.org>
- [24] <http://futurezone.orf.at>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/11818/1.html>

Abhörstandards für digitale Netze vor der Verabschiedung

Erich Moechel 13.08.2001

Die ETSI-Dossiers

Die Frist läuft noch bis 31. August: Dann haben die Mitglieder der Arbeitsgruppe "Lawful Interception" (SEC LI) des European Telecom Standards Institute (ETSI) über ES 201 671 abgestimmt. Die vollständig erneuerte Version 2.1.1 des universellen Schnittstellen-Standards, der Polizei und Nachrichtendiensten Zugang zu allen digitalen Netzen verschaffen soll, ist als "Final Draft" bereits in Umlauf. Als europäischer Standard festgeschrieben wird damit ab Ende dieses Monats ein System von Überwachungs-Schnittstellen für alle digitalen Telefonnetze (PSTN, ISDN, GSM, GPRS); die Zapfstelle für den Behörden- und Betriebsfunk TETRA wird nachgereicht - ironischerweise stellen gerade zahlreiche Polizeibehörden ihre eigene Kommunikation in ganz Europa auf TETRA um. Die publizierten Überwachungs-Standards stehen auf dem ETSI- Server [1] zur Verfügung, über die Suche im Dokumententitel, Eingabe "interception".

Die in der c't (7/2001 und 9/2001)¹ und in Auszügen in Telepolis erschienenen ETSI-Dossiers, in denen personelle und institutionelle Verflechtungen der ETSI- Arbeitsgruppe zu Geheimdiensten aus Holland, England, Russland und Israel aufgezeigt wurden, lösten bei der ETSI ziemliche Aufregung aus (Die ETSI-Dossiers [2], Der Griff der Geheimdienste nach dem Internet [3]). Rechtliche Schritte gegen die c't sowie die Online-Magazine Telepolis und ORF Futurezone [4] wurden gefordert, wobei die Publikation mehrerer geheimer Originaldokumente mit Namenslisten der Arbeitsgruppe ETSI SEC LI auf der US-Website Cryptome [5] weiteres Öl ins Feuer goss. Die Angelegenheit gelangte bis in die Geschäftsführung des ETSI, die ihre Anwälte einschaltete. Bis Redaktionsschluss dieser Ausgabe lag allerdings noch kein definitives Ergebnis vor, ob und weswegen gegen den Heise Verlag, den ORF sowie den Betreiber von Cryptome rechtliche Schritte eingeleitet werden sollen.

Die ETSI und ENFOPOL

Das enge Zusammenspiel von Polizei und Politik, von Technik und Geheimdiensten hat freilich nicht erst im Jahr 2001 begonnen, erste Indizien gehen bis auf das Jahr 1993 zurück. Für die Öffentlichkeit blieben die gemeinsam von FBI und internationalen Polizeibehörden in den ILETS (International Law Enforcement Telecom Seminars) ausgearbeiteten Masterpläne jahrelang unbekannt. Die britische Bürgerrechtsgruppe Statewatch brachte Teile der Pläne ("The EU-FBI Surveillance System") erstmals Anfang

1997 an die Öffentlichkeit (ILETS, die geheime Hand hinter ENFOPOL 98 [6]).

Die Veröffentlichung des Überwachungs-Dokuments ENFOPOL 98 der "Arbeitsgruppe polizeiliche Zusammenarbeit" durch Telepolis (Das Originaldokument, 1: ENFOPOL 98, vom 3. September 1998 [7]) und eine dadurch ausgelöste Welle des Protests konnte zwar nicht verhindern, dass die Beschlüsse das EU-Parlament passierten. Die Veröffentlichung der Umstände - gerade ein Viertel der Abgeordneten war anwesend, die Einwände des Datenschutzrats wurden nicht einmal angehört - ließen den Rat der Innen- und Justizminister aber im Juni 1999 von einer Verabschiedung Abstand nehmen. Im Herbst 2001 steht allerdings der nächste Termin an.

Ein neuer Anlauf, die Befugnisse der Polizei auszuweiten, läuft gerade unter dem Codenamen ENFOPOL 55 und wird im Herbst vor den Rat der Innen- und Justizminister gelangen (Enfopol gedeiht [8]). Nutznießer aber werden neben den Polizeibehörden die nationalen Geheimdienste sein, deren Agenden durch die EU bekanntlich nicht geregelt werden. Es steht jedem EU-Mitgliedsland dadurch frei, den eigenen Diensten im Namen der nationalen Sicherheit die einmal angezapften Netze vollständig zu öffnen. Deshalb wirken Verbindungsleute zu holländischen, britischen und deutschen Diensten denn auch in der Arbeitsgruppe SEC LI und mindestens einem Subkomitee nachweislich mit.

In bewährter Manier sind die Nachrichtendienste selbst aus der Beschreibung (Scope) des ETSI-Standards ES 201 671 eliminiert, das erste Dokument, auf das ES 201 671 2.1.1. in den "Literaturangaben" verweist (ETR 331), erwähnt sie freilich ausdrücklich. Ein weiteres Dokument namens TS 101 331, das SEC LI in Fortschreibung des veralteten "Pflichtenhefts" ETR 331 in Arbeit hat, formuliert bereits die Abhör-Anforderungen für die nächste Version von ES 201 671.

Die wichtigste Änderung gegenüber den Versionen von ES 201 671 betrifft die Aktivierung des Abhörvorganges. Schrieben alle bisherigen Standard-Entwürfe eine elektronische Verbindung von "Law Enforcement" mit dem Netzwerk-Betreiber über das so genannte Handover-Interface HI vor, so ist es nunmehr möglich, dass diese Kommunikation auch in Papierform erfolgen kann. Die Verbindung der Behörden via Sandleitung direkt in das Administrationszentrum des Netzbetreibers hatte Anlass zu Befürchtungen gegeben, dass hier die Netze für Flächen deckende Überwachungsmaßnahmen vollständig freigeschaltet werden könnten.

Nunmehr ist vorgesehen, dass die Aktivierung der jeweiligen Überwachungsmaßnahme auch über ein "manuelles Interface" vorgenommen werden kann. Im Regelfall ist das die Genehmigung des Zugriffs durch ein ordentliches Gericht, die entweder überbracht oder per Fax an den Netzbetreiber übermittelt wird, der daraufhin die elektronischen Interfaces HI2 (für Gesprächsdaten) und HI3 (Inhalt der Kommunikation) freischaltet.

Direkter Draht

In Deutschland beschlossen die Parlamentarier anlässlich der Novelle des G-10-Gesetzes, das die Befugnisse des Bundesnachrichtendienstes regelt, die Erweiterung der strategischen Überwachung auf den leitungsgebundenen digitalen Verkehr (Bundestag verabschiedet Lauschgesetz [9]). Dies ist technisch nur durch eine Schnittstelle wie ES 201 671 realisierbar. Im Gespräch mit Telepolis hatte der grüne Abgeordnete Hans- Christian Ströbele kritisiert, das "verfassungskräftige Trennungsgebot zwischen Polizei und Geheimdiensten werde damit weiter aufgeweicht". Die Dienste sollten offenbar "als polizeiliche Hilfssheriffs Verdachtsschöpfung betreiben". Dieses Szenario steht nun unmittelbar bevor, Wirklichkeit zu werden (Bundesrat will Ausweitung der Abhörbefugnisse für Geheimdienste [10]).

Eines der ersten Dokumente, die auf dem Treffen der Arbeitsgruppe "Lawful Interception" (ETSI SEC LI) am 17. Juli 2001 in Helsinki diskutiert wurden, trägt das Akronym TS 101 331. Hinter dieser technischen Spezifikation verbirgt sich das zweifellos brisanteste Dokument, das die ETSI Abhörtruppe momentan in Arbeit hat.

TS 101 331 ist das technische Gegenstück zum jüngst von der britischen Foundation for Information Policy Research [11] veröffentlichten Papier ENFOPOL 55 der EU-Arbeitsgruppe Polizeiliche Zusammenarbeit (PCWG). Es enthält die so genannten "International User Requirements" (IUR), die die operativen Bedürfnisse der "User" - nämlich Behörden und Geheimdienste - für die Überwachung des gesamten Telekom- und Internet-Verkehrs laufend neu fest schreibt (Enfopol gedeiht [12]).

Was das Pflichtenheft TS 101 331 technisch fordert, ist in der Neuversion des Standards ES 201 671 technisch zum großen Teil bereits erfüllt. ENFOPOL 55 formuliert gewissermaßen nachträglich die Anforderungen an TS 101 331 auf einer Ebene, die auch EU-Politikern verständlich ist. Wie das Vorgänger-Dokument ENFOPOL 98 ist ENFOPOL 55 bereits in Form eines EU-Ratsbeschlusses abgefasst. Das Dokument macht einen ziemlich fertig ausgearbeiteten Eindruck, das Zusatzakronym ECO 143 weist es bereits als Ratspapier aus.

In Paragraph 8 verlangt ENFOPOL 55 von allen Betreibern digitaler Netze, dass sie die Möglichkeit "für eine Anzahl simultaner Überwachungen schaffen". Dabei seien alle Vorkehrungen zu treffen, "um die Identität der überwachenden Behörden zu schützen und so die Vertraulichkeit der Ermittlungen zu Gewähr leisten". Das bedeutet nichts anderes, als dass die Identität der überwachenden Behörden voreinander strikt geheim gehalten werden muss. Der Paragraph ist somit ein reiner Geheimdienstparagraph, der jedem EU-Mitgliedstaat die Möglichkeit schafft, die ETSI-Schnittstellen seinen eigenen Geheimdiensten zu öffnen. Ein Grundsatz aller Nachrichtendienste weltweit ist es, weder den eigenen Polizeibehörden noch befreundeten Diensten ihre augenblicklichen Tätigkeit und vor allem die Herkunft ihrer Informationen preiszugeben. Paragraph 5.1 von ENFOPOL 55 verpflichtet die Netzbetreiber zusätzlich zur Geheimhaltung darüber, wie

viele Überwachungen stattfinden und wie diese ausgeführt werden.

In der Einleitung (Scope) zum "Technischen Report" Draft TR 101 331 [13] vom Januar 2001, aus dem die beim Treffen von SEC LI in Helsinki vorgelegte "Technische Spezifikation" TS 101 331 hervorgegangen ist, heißt es denn auch unmissverständlich: "It provides a set of requirements relating to handover interfaces for the interception by law enforcement and state security agencies." Weder Draft TR 101 331 noch TS 101 331 sind außerhalb der Arbeitsgruppe SEC LI erhältlich und sind mit einem Veröffentlichungsverbot belegt.

"On journalistic interest"

Dass nach mehreren Jahren ihrer öffentlich so gut wie nicht beachteten Tätigkeit nun steigendes Medien-Interesse an der europaweiten Standardisierung von "Lawful interception" besteht, scheint die Führung der Arbeitsgruppe SEC LI [14] beträchtlich zu irritieren. "Um alle Zweifel auszuschalten", sei betont, dass die Arbeitsgruppe LI nicht vorhabe, "die Diskussion über ihre Arbeit zu behindern oder einzuschränken", leitete SEC LI Vorsitzender Robin Gape seine Mitteilung "On journalistic interest" an alle Mitglieder der Arbeitsgruppe ein. Es sei auch nicht Sache des ETSI, Journalisten vorzuschreiben, wie sie ihre Arbeit zu tun oder wie sie vorliegende Informationen zu bewerten hätten.

Was allerdings die Erwähnung von Namen der an SEC LI Beteiligten betreffe, so der Vorsitzende von SEC LI weiter, sei dieser Umstand "ungeheuerlich" (iniquitous). Der Heise-Verlag und der ORF mögen sich in Zukunft in Publikationen gut überlegen, dass dies auch als persönliche Bedrohung der jeweiligen Personen aufgefasst werden könne. Zudem verwechsle der Autor dieses Artikels in seinen Publikationen für c't und ORF Futurezone "lawful interception" notorisch mit "jenen Aktivitäten nationaler Nachrichtendienste", die "strikt ausserhalb der Aktivitäten der Arbeitsgruppe LI angesiedelt" seien. Unter den Adressaten dieses Schreibens befanden sich unter anderem die SEC-LI-Mitglieder Koen Jaspers als Vertreter des holländischen Geheimdienstkomitees "Platform Interceptie, Decryptie en Signaalanalyse" (PIDS [15]) sowie Viacheslav Gusev und Evgeny Zharov vom russischen "Zentralinstitut zur wissenschaftlichen Erforschung von Telekommunikation" (ZNIIS [16]).

Als weitere Vorgehensweise schlug Robin Gape vor, über dessen Funktion bei British Telecom weder von ihm selbst noch von BT irgendeine Auskunft zu erhalten war, den Betreiber der US-Website Cryptome, wo einige nicht zur Publikation bestimmte Dokumente von SEC LI erhältlich sind, durch ETSI-Anwälte auffordern zu lassen, die Dokumente vom Netz zu nehmen. Zeitgleich sollten Schreiben an den Heise-Verlag und den ORF mit der Aufforderung ergehen, die Links zu Cryptome in Futurezone und Telepolis zu entfernen. Die zitierte Mitteilung ging nicht nur an die Mitglieder der Arbeitsgruppe SEC LI, sondern wurde auch an die deutsche Regulierungsbehörde RegTP und an das österreichische Ministerium für Transport, Innovation und Verkehr gerichtet.

In einem weniger formellen Schreiben, nämlich dem internen Report [17] des Chairman SEC LI zum 28. Treffen der Arbeitsgruppe SEC LI vom 15. bis 17. Mai in Hamburg, schlug Robin Gape freilich eine andere Tonart an. Wie könne man es überhaupt wagen, vertrauliche Dokumente der Arbeitsgruppe, die obendrein unter dem Copyright des ETSI stünden, zu zitieren oder womöglich auch zu publizieren? Die Einladung zu einer Podiumsdiskussion im Rahmen eines Symposions zum Thema Surveillance in Design [18] an der London School of Economics (LSE) lehnte der Vorsitzende der ETSI-Arbeitsgruppe "Lawful Interception" hingegen trotz garantierter Redezeit ab (Protokolle [19] des "International Forum on Surveillance by Design").

Am 22. September 2000 [20], als die Recherche am Komplex ETSI SEC LI erste signifikante Schlussfolgerungen zuließ, erschien an der LSE vielmehr eine Delegation von vier ernst in die Welt blickenden Herren mittleren bis fortgeschrittenen Alters, die sich allesamt mit Hotmail-Adressen angemeldet hatten. Man nahm in der letzten Reihe Platz, notierte nach Kräften mit und nahm den Verlauf der Diskussion offenbar übel. Dies resultierte in einer von einem nachweislich echten, offiziellen Account gerichteten Mail des ETSI-SEC LI Regulars Rupert Thorogood an den Autor. Inhalt des Schreibens war, dass Letztgenannter sich wohl gehütet hätte, den Mund am Podium so voll zu nehmen, hätte er gewusst, dass drei Vertreter von ETSI SEC LI und ein Repräsentant der Arbeitsgruppe Polizeiliche Zusammenarbeit (PCWG) im Publikum alles notierten. Das eigentlich Spaßige dabei war, dass Bekannte von der holländischen Nettime-Mailinglist zufällig neben Mr. Thorogood zu sitzen kamen und aus Gründen räumlicher Beengtheit von den Notizen gleichsam Notiz nehmen mussten. Um Reputation und Privatsphäre der genannten Person zu wahren, fand keine der durch diesen Zufall gewonnenen Erkenntnisse Eingang in diesen Artikel.

Was den weiteren Fortgang der Arbeiten in der Arbeitsgruppe SEC LI betrifft, so widmet man sich neben der Neufassung der "International User Requirements" in TS 101 331 den Vorarbeiten [21] zur Überwachung von Breitband-Internet-Zugängen via Kabelmodem. Die nächste Sitzung [22] findet vom 11. bis 13. September auf Einladung von Lucent in Warschau statt.

Vollständiger Text "Lauschangriff: Die ETSI-Dossiers III" in: c't 17/2001, Seite 78

Erich Moechel ist leitender Redakteur von ORF Futurezone [23]

Literaturangaben

1) Erich Moechel, Die ETSI-Dossiers, Europäische Standards für das Abhören digitaler

Links

- [1] <http://pda.etsi.org/pda/queryform.asp>
- [2] <http://www.heise.de/tp/deutsch/special/enfo/7220/1.html>
- [3] <http://www.heise.de/tp/deutsch/special/enfo/7447/1.html>
- [4] <http://futurezone.orf.at/>
- [5] <http://cryptome.org/e-spy-telecom.htm>
- [6] <http://www.heise.de/tp/deutsch/special/enfo/6396/1.html>
- [7] <http://www.heise.de/tp/deutsch/special/enfo/6326/1.html>
- [8] <http://www.heise.de/tp/deutsch/special/enfo/7968/1.html>
- [9] <http://www.heise.de/tp/deutsch/inhalt/te/7630/1.html>
- [10] <http://www.heise.de/tp/deutsch/inhalt/te/7194/1.html>
- [11] <http://www.fipr.org>
- [12] <http://www.heise.de/tp/deutsch/special/enfo/7968/1.html>
- [13] <http://cryptome.org/esp/ETR331e01p.pdf>
- [14] http://webapp.etsi.org/tbhomepage/TBDetails.asp?TB_ID=503&TB_NAME=SEC+LI
- [15] <http://cryptome.org/esp/TIITv012.pdf>
- [16] <http://www.gl.ru/uch/page1.htm>
- [17] http://webapp.etsi.org/meetingDocuments/ViewDocumentList.asp?MTG_Id=21151
- [18] <http://www.cs.ucl.ac.uk/staff/I.Brown/ifsd.html>
- [19] http://www.notatla.demon.co.uk/MISC/interception_con.txt
- [20] http://www.notatla.demon.co.uk/MISC/interception_con.txt
- [21] <http://www.etsi.org/technicalactiv/IPcable/Ipcablecommunications.htm>
- [22] <http://webapp.etsi.org/meetingcalendar/MeetingDetails.asp?mid=21153>
- [23] <http://futurezone.orf.at>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/9306/1.html>

Enfopol gedeiht

Florian Rötzer 26.06.2001

In einem neuen Papier fordern die europäischen Strafverfolger, dass sie unabhängig von der jeweiligen Technik jede denkbare Art der Telekommunikation in Echtzeit belauschen können

Einer Veröffentlichung zugänglich gemacht wurde über Cryptome am Wochenende das neueste Papier der EU Arbeitsgruppe Polizeiliche Zusammenarbeit, das bereits als Entschließung des Europäischen Rats formuliert ist. Thema des Dokuments [1] mit der Bezeichnung ENFOPOL 55 vom 20. Juni 2001 sind Richtlinien für die Überwachung der öffentlichen Telekommunikationsnetzwerke und -dienste.

Seit Jahren werden von den europäischen Strafverfolgungsbehörden im Rahmen von Enfopol technische Leitlinien für Telekommunikations-Abhörmaßnahmen in Form der International User Requirements (IUR) propagiert. Telepolis hatte 1998 die ersten Papiere der Arbeitsgruppe veröffentlicht. Wegen der damals entstandenen öffentlichen Kritik wurden die Enfopol-Pläne erst einmal auf Eis gelegt und schließlich reduziert in das Europäische Rechtshilfeabkommen eingebaut (Enfopol-Pläne in Europäisches Rechtshilfeabkommen integriert [2]).

Für erneutes Aufsehen hatten kürzlich die von Statewatch vor den britischen Wahlen veröffentlichten neuen Papiere der Arbeitsgruppe gesorgt, die fordert, dass jede Kommunikation vom Telefon- oder Handygespräch bis hin zu Emails und allen Internetdaten mindestens sieben Jahre lang gespeichert werden soll (Europäische Strafverfolger fordern die totale Telekommunikations-Überwachung [3]). Provider, Lobbyvereine und Datenschützer haben diese Pläne scharf kritisiert (Widerstand gegen die neuen Enfopol-Überwachungspläne [4]).

Zu Beginn des neuen Dokuments mit der Bezeichnung Enfopol 55 wird zwar bekräftigt, dass bei der Einführung von Überwachungsmöglichkeiten das Recht des Einzelnen auf die Wahrung seiner Privatsphäre zu beachten sei, aber dann geht es nur noch darum, dass die Strafverfolger ungehinderten Zugriff auf "alle Arten der Telekommunikation" haben müssen, von ISDN über GPRS, UMTS, TETRA bis hin zu Email- oder Message-Diensten. Sinn des Entschlusses ist es offenbar, die Richtlinien so zu formulieren, dass die Anforderungen der Überwachungsmöglichkeiten unabhängig vom jeweiligen Stand der Technik formuliert werden, um nicht gleich wieder zu veralten.

So würden die Strafverfolgungsbehörden Zugang zu jeder *Telekommunikation* (1) und zu allen damit zusammenhängenden Anruflaten (*Call* (2)) benötigen, wozu die technischen

Identifikationsmöglichkeiten gehören, aber auch Wohnort oder Adresse des Arbeitsplatzes oder Kreditkartendaten. Im Fall von Internetkommunikation müssen so zur Identifizierung beispielsweise IP-Adresse, Account-Nummer, Passwort, PIN-Nummer und Emailadresse den Strafverfolgungsbehörden mitgeteilt werden. Die Strafverfolgungsbehörden brauchen auch dann den Zugang zur Telekommunikation, "wenn der Abgehörte zeitweise ein Netzwerk oder eine Telekommunikationseinrichtung benutzt". Das betrifft beispielsweise die Verwendung von Telefonkarten oder den Fernzugriff durch einen anderen Internetprovider.

Ganz entscheidend ist, dass die Strafverfolger Informationen "über den genauesten geographischen Ort" verlangen, die ein Netzwerk von einem Mobilteilnehmer besitzt. Das würde nicht nur geographische, sondern auch materielle und logische Informationen betreffen, wozu auch Einwählnetze für Internetprovider oder Rerouting gehören. Diese Informationen hätten die Strafverfolger gerne in einer "leicht verständlichen" Version.

Erforderlich sei natürlich die Möglichkeit zur ganztägigen Echtzeit-Überwachung, auch die mit einem Call verbundenen Daten sollten in Echtzeit den Strafverfolgern vorliegen. Dazu müssen die Netzbetreiber oder Internetprovider eine oder mehrere Schnittstellen einrichten, um die abgehörte Telekommunikation den Strafverfolgern zuzuleiten. Die Daten müssen in einem "allgemein erhältlichen Format" übermittelt werden, das einzeln festgelegt werden soll.

Sichergestellt werden müsse auch, dass die Belauschten nicht merken, dass sie abgehört werden. Keine Veränderung dürfe für sie bemerkbar sein. Die Netzbetreiber und Internetprovider sollen auch nicht mitteilen dürfen, ob, wie und wie oft bei ihnen abgehört wurde. Und wenn diese Telekommunikation komprimieren oder verschlüsseln, dann wollen die Strafverfolger einen Zugriff auf die unverschlüsselte Kommunikation.

Abgesehen vom ersten Satz, dass der Datenschutz beachtet werden müsse, spielt das Prinzip der Sparsamkeit bei der Erhebung ansonsten keine Rolle, die ja auch technisch berücksichtigt werden könnte. Wie immer - und offenbar ungetrübt durch Kritik - werden Maximalforderungen formuliert.

Links

- [1] <http://cryptome.org/eu-intercept.htm>
- [2] <http://www.heise.de/tp/deutsch/special/enfo/6515/1.html>
- [3] <http://www.heise.de/tp/deutsch/special/enfo/7684/1.html>
- [4] <http://www.heise.de/tp/deutsch/special/enfo/7709/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/7968/1.html>

Telekommunikation

"Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system."

Call

"Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system."

Copyright © 1996-2003. All Rights Reserved. Alle Rechte vorbehalten

Heise Zeitschriften Verlag, Hannover

Widerstand gegen die neuen Enfopol-Überwachungspläne

Stefan Krempf 23.05.2001

Vertreter von Providern, Lobbyvereine und Datenschützer kritisieren die geplante Ausweitung der Speicherung sämtlicher Telekommunikationsdaten

Die Ziele der europäischen Polizeistäbe sind technisch unausgegoren, erzeugen einen überzogenen Überwachungsdruck und stellen einen Angriff auf demokratische Werte dar, urteilen Experten. Den nationalen Regierungen geht die Verbrecherjagd dagegen über alles.

Der Verband der deutschen Internet-Wirtschaft eco [1] will gegen die Überlegungen der Arbeitsgruppe für polizeiliche Zusammenarbeit auf europäischer Ebene (Enfopol) zur Ausweitung der Speicherfristen sämtlicher Telekommunikationsdaten (Europäische Strafverfolger fordern die totale Telekommunikations-Überwachung [2]) von vornherein "anrennen". Das kündigte eco-Geschäftsführer Harald Summa gegenüber Telepolis an. Jede Minute fließen allein durch Deutschlands Internetleitungen rund 2,3 Gigabyte Daten. Um diese Kommunikationsmengen aufzuzeichnen, "müssen wir Lagerhäuser aufmachen", fürchtet der Providervertreter.

Anders als bei der geplanten Telekommunikations-Überwachungsverordnung (TKÜV) der Bundesregierung, deren Neufassung die Provider laut Summa regelrecht verschlafen haben (Doppeltes Spiel [3]), will eco dieses Mal die Strafverfolger und die Politiker schon im Vorfeld gesetzgeberischer Aktivitäten auf die "Unmöglichkeit" der Vorhaben aufmerksam machen. Die Ausarbeiter der neuen Enfopol-Papiere haben seiner Meinung nach "geträumt".

Die technische Ebene ist gerade bei kleinen Providern nicht einmal das größte Problem, so Lutz Donnerhacke, einer der Gründer des Jenaer Internet Service Providers (ISP) IKS [4]. Über "verteilte Backups" sei da einiges machbar – auch wenn es noch "keine aussagekräftigen Erfahrungen mit Langzeitspeichermedien gibt". Über welches Protokoll die "Bedarfsträger" an die Datenberge der Provider allerdings herankommen wollen, ist Donnerhacke ein Rätsel.

Angriff auf die freiheitlich-demokratische Grundordnung

Für besonders gefährlich hält der Mitbegründer des Fördervereins Informationstechnik

und Gesellschaft (Fitug [5]) allerdings den sich in den Enfopol-Plänen manifestierenden Trend, "Big Brother" in immer mehr Lebensbereich zu installieren. "Als nächstes verlangen die Strafverfolger", prognostiziert Donnerhacke, "dass in jedem Zimmer in jedem Haushalt Videokameras installiert werden". Jeder Bürger müsse dann selbst nachweisen, dass er an einem Verbrechen nicht beteiligt gewesen sein könnte, da er ja gleichzeitig im Blickfeld von Kamera XY gewesen wäre.

Hinter den diskutierten Backup-Pflichten sieht Donnerhacke daher den Versuch der Polizei, die Beweislage umzukehren. Das führe allerdings in eine "absurde Situation", die außerhalb jeder Rechtstaatlichkeit stünde. Was die Eurocops planen, ist für den Kryptoexperten daher ein klarer "Angriff auf die freiheitlich-demokratische Grundordnung".

Die auf der Ebene des Europäischen Rats angesiedelte Enfopol-Arbeitsgruppe will nach Informationen der Organisation Statewatch [6] alle Telekommunikationsanbieter dazu verpflichten, jedes Telefongespräch, jedes Fax und jede Email "für mindestens sieben Jahre" lang zu archivieren. Aus einem weiteren, Telepolis vorliegenden Enfopol-Papier geht hervor, dass der Kampf um die Verbindungsdaten sowie gegen die anonyme Netzbenutzung die wichtigsten Prioritäten der Strafverfolger sind (Europäische Strafverfolger fordern die totale Telekommunikations-Überwachung [7]).

Die Eurocops wollen mit ihren neuen Vorstößen verhindern, dass innerhalb der EU neue Datenschutzgesetze verabschiedet werden, die ihnen die Arbeit erschweren könnten. Der Chef der in Den Haag sitzenden Polizeibehörde Europol [8], Jürgen Storbeck, warnte ganz in diesem Sinne am Dienstag erneut davor, dass die "E-Kriminalität" einen uneinholbaren Vorsprung gegenüber den Strafverfolgern erringe. Es drohe die Gefahr einer "strafrechtslosen Zeit". In Rage gebracht hat die Eurocops daher vor allem eine Entschließung zur Regelung der Datenverarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in der Union, die der Rat innerhalb der Arbeitsgruppe "Informationssysteme und Datenschutz" Anfang März diskutiert hatte (Brüssel an Strafverfolger: Es gibt ein Recht auf Privatsphäre [9]).

Darin geht es um Grundsätze wie "Vertraulichkeit der Verarbeitung", Löschfristen sowie das "Auskunftsrecht und das Recht auf Berichtigung" von Daten. Obwohl die Formulierungen des Papiers äußerst vage blieben, alarmierten sie die Strafverfolger dennoch und ermutigten sie zu ihrer "Gegenoffensive". Die geht nun soweit, dass selbst bestehende Datenschutzvorkehrungen abgebaut werden sollen.

Unzumutbarer Überwachungsdruck

Demgegenüber hatte der Bundesdatenschutzbeauftragte Joachim Jacob bereits in seinem jüngsten Tätigkeitsbericht davor gewarnt, dass die vorsorgliche Speicherung aller personenbezogenen Daten aus allen Nutzungen des Internet offensichtlich

unverhältnismäßig wäre und für jeden Einzelnen einen unzumutbaren Überwachungsdruck erzeugen würde. Angesichts der Überlegungen der europäischen Polizeistäbe warnte seine Sprecherin, Helga Schumacher, aber auch vor überzogener Paranoia. Denn letztlich entscheidend sei, was davon mittelfristig in nationales Recht umgesetzt würde.

Als erste nationale Regierungsstelle hat sich inzwischen das Londoner Wirtschaftsministerium zu Enfopol geäußert. Einer Sprecherin zufolge unterstützt die britische Regierung eine Ausweitung der Befugnisse der Polizei. Überprüft würde ja nur die Email-Kommunikation Verdächtiger, versuchte sie die Nutzer zu beruhigen. Niemand habe die Zeit und das Geld, jede Email zu prüfen.

Bisher konnte die eng mit dem FBI und der NSA (National Security Agency) zusammenarbeitende Enfopol-Arbeitsgruppe ihre Wunschvorstellungen zur lückenlosen Überwachung der Telekommunikation weitgehend den Ministerialbeamten der nationalen Regierungen schmackhaft machen und – oft an den Parlamenten vorbei – in Gesetzen und Verordnungen unterbringen. Ihre Handschrift zeigt auch die TKÜV, die in Deutschland zwar noch diskutiert wird, vom Gesetzgeber aber jederzeit einfach erlassen werden kann.

Ob das Bundesinnen- oder das Bundesjustizministerium großen Widerstand gegen die jetzt aufgedeckten Ziele der Eurocops entwickeln werden, ist fraglich. Zumindest hat gerade das Justizministerium bei den "Fragen der unangemessenen Ausweitung der landesübergreifenden Eingriffsbefugnisse der Strafverfolgungsbehörden" im Rahmen der Cybercrime-Konvention des Europarats den Datenschutz bisher hinten angestellt, wie der Netzexperte der SPD, Jörg Tauss, kritisiert (Ein großer Schritt in Richtung europäischer Überwachungsstaat [10]).

Links

- [1] <http://www.eco.de/>
- [2] <http://www.heise.de/tp/deutsch/special/enfo/7684/1.html>
- [3] <http://www.heise.de/tp/deutsch/inhalt/te/7306/1.html>
- [4] <http://www.iks-jena.de/>
- [5] <http://www.fitug.de/>
- [6] <http://www.statewatch.org/>
- [7] <http://www.heise.de/tp/deutsch/special/enfo/7684/1.html>
- [8] <http://www.europol.eu.int/>
- [9] <http://www.heise.de/tp/deutsch/inhalt/te/7166/1.html>
- [10] <http://www.heise.de/tp/deutsch/inhalt/te/7472/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/7709/1.html>

Europäische Strafverfolger fordern die totale Telekommunikations-Überwachung

Stefan Krempf 19.05.2001

Nach der Verabschiedung zahlreicher Lauschgesetze sollen nun die Verkehrsdaten jahrelang gespeichert und anonyme Netzzugänge verboten werden

Polizeistellen und Geheimdiensten in Europa reicht der große Lauschangriff aufs Netz nicht mehr aus. Nun wollen sie mit einer verschärften Neuauflage der angestaubten Enfopol-Papiere auch noch erreichen, dass Telekommunikationsanbieter aller Couleur ihnen die gesamten anfallenden Verbindungsdaten über Jahre hinweg aufbewahren. Ihr Ziel ist es, umfangreiche Nutzerprofile zu erstellen. Selbst Verschlüsselung hilft da nur noch begrenzt weiter, da sich durch das softwaregestützte Schürfen in den Datenbergen Relationsorganigramme erstellen lassen. Einzig mit Anonymisierungsdiensten könnten die Nutzer ihre Privatsphäre noch schützen. Sie stehen daher auf der Abschussliste der Eurocops ganz oben.

Es liest sich wie eine Mischung aus dem Alptraum von Datenschützern, Bürgerrechtlern sowie der Telekommunikationswirtschaft und einem Märchen aus 1001 Nacht, was die britische Organisation Statewatch [1] Mitte der Woche auf den Webseiten ihrer Kampagne SOS Europa [2] veröffentlicht hat: Geht es nach den Wünschen der europäischen Strafverfolger sollen in Zukunft jedes Telefongespräch – aus dem Festnetz genauso wie vom Handy –, jedes Fax, jede Email, die Inhalte aller Webseiten sowie der gesamte Netztraffic aufgezeichnet und "für mindestens sieben Jahre" archiviert sowie für die "Bedarfsträger" zugänglich gemacht werden.

Hinter der exorbitanten Forderung steht mal wieder die europäische Arbeitsgruppe für polizeiliche Zusammenarbeit, besser bekannt unter dem Kürzel Enfopol. Telepolis hatte das Treiben der jahrelang außerhalb jeglicher Kontrolle agierenden Truppe 1998 aufgedeckt (Telepolis Special Echelon [3]). Schon damals hatte die Organisation, hinter der ein vom FBI [4] und der NSA [5] bestimmtes, euphemistisch "International Law Enforcement Telecommunications Seminar" (ILETS) getauftes Gremium steht (ILETS, die geheime Hand hinter ENFOPOL 98 [6]), umfangreiche technische Leitlinien für Telekommunikations-Abhörmaßnahmen in Form der so genannten International User Requirements (IUR) propagiert.

Der damit geplante "Lauschangriff hoch zehn" wurde nicht zuletzt aufgrund der von den Telepolis-Berichten ausgelösten Medienschelte zunächst auf Eis gelegt beziehungsweise

teilweise in das Europäische Rechtshilfeabkommen eingebaut (Enfopol-Pläne in Europäisches Rechtshilfeabkommen integriert [7]), das vor knapp einem Jahr verabschiedet wurde und nun von den Parlamenten der 15 Mitgliedsstaaten der Europäischen Union ratifiziert werden soll. Damit soll der grenzenlose Austausch abgehörter Telekommunikationsdaten möglich werden.

Ähnliche Bestimmungen sieht die Cybercrime-Konvention des Europarats vor, dem neben den EU-Staaten zahlreiche andere Nationen angehören oder assoziiert sind. Trotz heftiger Kritik von Datenschützern und Politikern hat das umstrittene Abkommen die Parlamentarische Versammlung des Gremiums bereits passiert (Ein großer Schritt in Richtung europäischer Überwachungsstaat [8]). Es soll im Spätsommer dem Ministerkomitee vorgelegt und verabschiedet werden.

Big Brother formiert sich

Die neuen Enfopol-Dokumente, die Statewatch teilweise bereits vom zuständigen – nicht mit dem Europarat zu verwechselnden – Rat der Europäischen Union ausgehändigt bekommen und auf der SOS-Europa-Seite veröffentlicht hat, knüpfen weitgehend an die alten Leitlinien und das in ihnen steckende Gedankengut an. Wie bisher stellen die Strafverfolger klar, dass es ihnen um die lückenlose Überwachung aller Formen von Telekommunikation geht, also neben dem "klassischen" Telefonverkehr auch um Email, Mobil- und Satellitenfunk sowie die Webnutzung geht. "Kennungen", zu den die Europolizisten Zugang haben wollen, umfassen Nutzeradressen, Gerätenummern, Passwörter oder Email-Accounts. Den "Diensten" und Behörden verlangt es außerdem nach dem "vollständigem Namen" einer zu überwachenden Person oder Unternehmung, ihrem Wohnsitz und Kreditkarten-Nummern mit Verfallsdatum.

Diesen Anforderungen haben mehrere Länder der EU bereits Rechnung getragen. In England etwa hat das britische Unterhaus bereits im Juli ein Gesetz mit dem unscheinbaren Titel "Regulation of Investigatory Powers" (RIP) verabschiedet, demzufolge Strafverfolger auf Verdacht hin seit Oktober den gesamten bei den Providern des Landes anfallenden Emailverkehr mitschneiden dürfen (UK-RIP-Gesetz über Ermittlungsbefugnisse verabschiedet [9]). Auch in Holland ist der Lauschangriff auf die Surfer bereits gesetzlich vorgeschrieben (Digitale Detektive in Holland [10]). In Deutschland zeigt sich der neue Entwurf der wieder aus den Schubladen der Überwachungsonkels im Bundeswirtschaftsministerium hervorgekramten Telekommunikations-Überwachungsverordnung (TKÜV) ebenfalls deutlich von Enfopol inspiriert (Rot-Grün will Telekommunikation lückenlos überwachen [11]).

Doch die mit den IUR und ihrer Umsetzung in nationales Recht einhergehende Installation von Big Brother geht den Strafverfolgern inzwischen nicht mehr weit genug. Das fehlende Mosaikstück in ihrem Überwachungsszenario ist die Fähigkeit, zeitlich möglichst unbegrenzt in einem gigantischen Archiv der gesammelten Telekommunikation stöbern

und dank Data-Mining nach (verborgenen) Beziehungen zwischen einzelnen Teilnehmern forschen zu können.

Der Kampf um die Verbindungsdaten

Im Papier Enfopol 38 vom 24. April, das Telepolis vorliegt, verdeutlicht die französische Delegation der beim Rat der EU angesiedelten Polizei-Arbeitsgruppe die Hintergründe der neuen Forderung: Verbindungsdaten werden darin als "eines der Fundamente der Verfolgung von Computerverbrechen" bezeichnet. Allein diese technischen Daten könnten Kriminalbeamte auf die Spur von Cybergangstern oder zur Quelle eines Verbrechens führen. Sie seien daher der "unverzichtbare Startpunkt jeder Ermittlung im Bereich der Informationstechnologie".

Die Erfassung dieser Daten ist für die Strafverfolger besonders wichtig, da sie den Kampf gegen die Verschlüsselungsfreiheit als verloren betrachten. Umso interessierter sind sie nun daran, wer mit wem kommuniziert. Ihre Hoffnung ist, dass sich aus den Bitanhäufungen die Relationen ablesen lassen, in denen Leute miteinander stehen. Momentan, so die Klage der Polizisten, würden die wertvollen Untersuchungsdaten aber aufgrund bestehender Datenschutzgesetze nach 30 Tagen oder wenigen Monaten gelöscht, was sich "klar als Schwachstelle beim Kampf gegen Cybercrime" herausgestellt habe.

Wie die Franzosen weiter ausführen, haben sich alle Regierungsvertreter beim Rat bereits dafür ausgesprochen, dass Zugangs- und Serviceprovider alle Verbindungsdaten für "mindestens 12 Monate" speichern sollen. Den Informationen von Statewatch zufolge schwebt den Strafverfolgern selbst eine Aufbewahrungsfrist von mindestens 7 Jahren vor – eine Zeitspanne, die den Ratsmitgliedern anscheinend noch zu heikel erschien.

Die Wünsche der Eurocops dürfte sich an den im Sommer vergangenen Jahres ausgearbeiteten Plänen des britischen National Criminal Intelligence Service (NCIS) orientieren, die im Dezember aufgefliegen waren (Britische Geheimdienste und Polizeibehörden wollen alle abhören [12]). Die dem Londoner Innenministerium untergeordnete Behörde plädierte bereits damals dafür, die gesamte Telekommunikation der Bürger mitsamt der Internetverbindungen zu erfassen und die ominösen sieben Jahre in einer Datenbank zu archivieren.

Doch auch die Totalerfassung der Telekommunikation ist den Enfopol-Predigern nicht genug. "Es ist ebenfalls erforderlich", heißt es im Ratspapier der französischen Delegation, "dass eine Lösung für die mit den verschiedenen Formen der Anonymität im World Wide Web verbundenen Probleme gefunden werden". Als Beispiel nennt das Papier Internetcafés, die bereits in vielen Fällen für Betrügereien genutzt worden seien. Das Beispiel Bombay könnte einen Weg zeigen, wie derartige Verbrechen verhindert werden können: In der indischen Großstadt soll das Surfen in öffentlichen Internetcafés bald nur noch mit Ausweis möglich sein (Ausweise für Internetcafes [13]).

Anhaltende Ignoranz

Es ist absehbar, dass der neue Vorstoß der Enfpopol-Truppe auf heftigen Widerstand stoßen wird. Datenschützer aus Bund und Ländern hatten bereits im vergangenen Jahr die Verlängerung der Speicherung von Verbindungsdaten in Deutschland auf ein halbes Jahr heftig kritisiert: "Die gewaltigen, bei den Anbietern vorgehaltenen Datenfriedhöfe," fürchteten die Experten schon damals, "sind im besten Fall unnützlich und teuer, in jedem Fall aber ein unnötiger Eingriff in das Fernmeldegeheimnis" (Telefonbenutzer und private Surfer unter pauschalem Kriminalitätsverdacht [14]). Auch Jörg Tausch, Beauftragter für Neue Medien der SPD-Bundestagsfraktion, bemängelt seit langem, dass eine Totalerfassung der Kommunikation die Nutzung der neuen Medien behindert und in Deutschland auch verfassungswidrig ist (Fette Bugs im Cybercrime-Abkommen [15]).

In einer ersten Reaktion zeigte sich Andy Müller-Maguhn, Sprecher des Chaos Computer Clubs [16] im Gespräch mit Telepolis "irritiert von der anhaltenden Ignoranz" des Enfpopol-Gremiums gegenüber Datenschutzaspekten. Harald Summa, Geschäftsführer des Verbands der deutschen Internet-Wirtschaft eco [17] hält die Planung angesichts der anfallenden Speichermengen für "vollkommen unmöglich".

David Banisar, stellvertretender Direktor der Organisation Privacy International [18], ist vor allem entsetzt darüber, wie die Polizisten die bestehenden Datenschutzrichtlinien der Europäischen Union auf den Kopf stellen und das Internet in ihr persönliches Spionagesystem umwandeln wollen. Europa dürfte nun die "bislang wichtigste Schlacht über bürgerliche Freiheitsrechte bevorstehen", prognostiziert Tony Bunyan, der unermüdliche Frontmann von Statewatch. Viel Zeit, ihre Kräfte zu mobilisieren, haben die Bürgerrechtler allerdings nicht: Geht es nach der Arbeitsgruppe des Rats der Union, sollen das Parlament und die Kommission ihre Träume schon im Sommer Wirklichkeit werden lassen.

Links

- [1] <http://www.statewatch.org/>
- [2] <http://www.statewatch.org/soseurope.htm>
- [3] <http://www.heise.de/tp/deutsch/special/enfo/default.html>
- [4] <http://www.fbi.gov/>
- [5] <http://www.nsa.gov/>
- [6] <http://www.heise.de/tp/deutsch/special/enfo/6396/1.html>
- [7] <http://www.heise.de/tp/deutsch/special/enfo/6515/1.html>
- [8] <http://www.heise.de/tp/deutsch/inhalt/te/7472/1.html>
- [9] <http://www.heise.de/tp/deutsch/inhalt/te/8452/1.html>
- [10] <http://www.heise.de/tp/deutsch/special/enfo/6726/1.html>

- [11] <http://www.heise.de/tp/deutsch/inhalt/te/4954/1.html>
- [12] <http://www.heise.de/tp/deutsch/inhalt/te/4393/1.html>
- [13] <http://www.heise.de/tp/deutsch/inhalt/te/7677/1.html>
- [14] <http://www.heise.de/tp/deutsch/inhalt/te/8825/1.html>
- [15] <http://www.heise.de/tp/deutsch/inhalt/te/7239/1.html>
- [16] <http://www.ccc.de/>
- [17] <http://www.eco.de/>
- [18] <http://www.privacy.org/pi/>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/7684/1.html>

Seit Anfang April gibt es nun einen Entwurf, der den Lauschangriff auf IP-Netze und die technische Überwachung im Internet europaweit vereinheitlichen soll.

Drei verschiedene Arbeitsgruppen in European Telecom Standards Institute (ETSI) entwickeln Modelle zum Anbohren aller digitalen Netzwerke laufend weiter und integrieren neue Technologien wie etwa GPRS oder das erst geplante UMTS (siehe dazu: Erich Moechel, Die ETSI-Dossiers, c'17/2001, S. 58 und [Europäische Schnittstellen zur Überwachung sämtlicher digitaler Netze](#) [1]). Techniker und Manager jener Firmen, die das gesamte Abhörerequipment für diese Standard-Schnittstellen liefern, wirken in diesen ETSI-Arbeitsgruppen ebenso mit, wie Behördenvertreter, die ganz offensichtlich über enges Verbindungsnetz vor allem zu deutschen, britischen und holländischen Nachrichtendiensten verfügen.

Die Welt der Diagramme und des dezentralen Paketerverkehrs kommuniziert jedoch auf andere und komplexere Weise als das vergleichsweise simple Telefonmodell, das im Grunde nur aus anrufernder und angerufener Partei und einem Übertragungskanal besteht. Trotzdem wurde Anfang April der Entwurf eines ersten Standards präsentiert, der die technische Überwachung des Internet europaweit normieren soll.

Zur weiteren Information bringt c'1 einen detaillierten Bericht zum Vorgehen und den Vorhaben der Geheimdienste in Ausgabe 9/2001: "Die ETSI-Dossiers II - Der Griff der Geheimdienste nach dem Internet".

Die Lauscher und das Internet

Die Welt größte [Abhörtafelgriff](#) [1] in Sachen neuer Abhörstandards in Europa fand vom 3. bis 5. April 2001 in Grimstad an der Südküste Norwegens statt. Zu den dreizehnteilig Teilnehmern der zentralen Arbeitsgruppe "Lawful Interception" (ETSI SEC LI) kamen noch etwa halb so viele aus der [Working Group 3.1.1](#) [3] des so genannten *Third Generation Partnership Projects* (3GPP TSG SA WG-1). Beim [3GPP](#) [4] handelt es sich um einen Zusammenschluss europäischer, amerikanischer (Standards Committee T1 der Alliance for Telecom Industry Solutions ATIS), japanischer (ARIB, TTC) und koreanischer (TTA) Normenanstalten. Auch China ist mit seiner Wireless Telecommunication Standard Group (CWTS) im 3GPP vertreten.

Zwei weitere ETSI-Arbeitsgruppen, die sich ebenfalls mit der Erstellung von Überwachungsstandards beschäftigen, machen den Abhörreigen in Grimstad komplett: *Services and Protocols for Advanced Networks* ([SPAN LI](#) [5]), in der eben ein Standard über die Verbindung von IP- und Telekommunikations-Netzwerken erstellt wurde, sowie die [TIPHON Security Working Group](#) [6]. Das Akronym TIPHON - Telecommunications and Internet Protocol Harmonization Over Networks - war gleichsam auch Programm des Treffens.

Gerade rechtzeitig zum großen, gemeinsamen Workshop in Grimstad wurde den Modellenwürfen zur "IP Interception" ein Update zum orientalischen "Technischen Report" verpasst. Eine "komplette IP-Lösung", heißt es in [ETSI TR 101 944 Version 0.0.8](#) [7], stelle eine "technische Herausforderung" dar und sei in hohem Maß von der Zusammenarbeit zwischen Zugangs- und Service-Providern abhängig. Aus Gründen von "Security und Privacy" sei ein solcher, umfassender Zugriff allerdings "sehr umstritten" und deshalb für Telekom-Regulatoren in vielen Ländern "höchstwahrscheinlich unakzeptabel".

Die nationalen Regulatorien seien davon zu überzeugen, heißt es im einzigen fett gedruckten Satz des in Grimstad vorgestellten TCP/IP-Papiers, das die Überwachungsanforderungen der gesetzlich ermächtigten Behörden sowohl Access-Provider wie auch Service-Provider jeweils separat betrifft. Von "allerhöchster Wichtigkeit" sei es, zwischen Netzwerk- und Serviceebene strikt zu unterscheiden und zu beachten, dass beide unterschiedlich zu behandeln seien. Dieses sei notwendig, um den "gesamten Inhalt der Kommunikation einer Ziel-Identität während der gesamten Dauer der Überwachung zu erfassen." So will es der "Technische Report" Draft TR 101 331 Version 0.1.2, das Pflichtenheft der Behörden, das parallel zu den Standards, die diesen Pflichten genügen sollen, laufend fortgeschrieben wird.

Lauschangriff in Stereo

In jedem Fall greifen die Behörden parallel auch beim Service-Provider zu. Nur so erschließen sich jene Daten der Zielperson, die eben nicht live an Switches oder ADSL-Routern abzugreifen sind: Logfiles für alle möglichen Dienste von WWW bis ICQ, Inhalte von Mailboxen oder auch Daten, die auf ftp-Servern geparkt worden sind.

Naturngemäß machen sich eben jene, deren Aufgabe es ist, die Strukturen für einen groß angelegten Angriff auf die Daten der Informationsgesellschaft zu schaffen, Gedanken über die Sicherheit des eigenen Materials: Eine IPSEC-Lösung Pflicht. Ein sicherer Tunnel soll die Daten dann über das unsichere Terrain von TCP/IP nicht beobachtbar und unversehrt bei den Behörden abliefern. Anderswo in Europa ist man jedoch schon deutlich weiter. Während auf europäischer Ebene noch über sichere Transportmethoden im Allgemeinen meditiert wird, ist in den Niederlanden ein Koalition von Geheimdiensten und Polizei bereits beim Besonderen angelangt. So wird die Standard-Schnittstelle [ES 201 671](#) [8], die auch der deutschen Überwachungsverordnung zu Grunde liegt, bereits seit Anfang 2000 in alle Netze implementiert und für den nationalen Abhörgebrauch adaptiert und verfeinert.

Die Spuren der Nachrichtendienste

Sämtliche in ETSI definierten Abhörstandards schreiben vor, dass die [Handover-Interfaces](#) [9] dazu fähig sein müssen, mehrere "User" separat zu bedienen, ohne dass sichtbar wird, wie viele Zielpersonen Gegenstand der jeweiligen Überwachung sind. Hersteller und Netzwerkbetreiber sind außerdem verpflichtet, über die verwendete Technik, deren Konfiguration und sämtliche Abhöraktivitäten Stillschweigen zu bewahren.

Sofern die Netzwerker über letztere überhaupt informiert sind, ist für das kommende UMTS doch eine Administrations-Funktion [ADME](#) [10] (PDF-Daten) definiert, die genau das verhindern soll. "Zusammen mit anderen Funktionen" diene sie dazu, vor dem Mobile Switching Center 3GMS - also dem Netzwerkbetreiber - "zu verborgen, dass es multiple Aktivierungen durch verschiedene Law Enforcement Agencies" auf dasselbe Ziel" gebe. Das ADMF sei dazu, eben diese Aktivitäten zuverlässig voneinander zu trennen.

Eine der treibenden Kräfte in der ETSI-Arbeitsgruppe "Lawful Interception" ist der Holländer Koen Jaspers. In älteren Protokollen der Working Group SEC LI wird Jaspers noch dem ITO ("Informatic en communicatie technologie organisatie") zugeschrieben, einer EDV-Abteilung der niederländischen Polizei. In der Teilnehmerliste des Treffens von Grimstad Anfang April firmiert Jaspers jedoch als Vertreter einer Organisation namens PIDS, was nichts anderes als "Platform Interceptie, Decryptie en Signaalanalyse" heißt ([Holländischer Geheimdienst wird der flächendeckenden Überwachung des Email-Verkehrs beschuldigt](#) [11]). So genannte Signals Intelligence (SIGINT) ist wie das Brechen von Verschlüsselungscodes sei jeder in allen Staaten in der Domäne der militärischen Geheimdienste angesiedelt ([Engge Polizei- und Geheimdienstkooperation in den Niederlanden bezüglich Überwachung und Kryptographie](#) [12]).

In Absenz von Bernd Adams (Deutsche Telekom), dem Vizevorsitzenden der Arbeitsgruppe "Lawful Interception", assistierte dem Vorsitzenden Robin Gape (British Telecom) bei dem Treffen Anfang April mit Rupert Thorogood, einer der [absoluten SEC LI Regulars](#) [13], als Schriftführer. Neben Thorogood, der im ETSI mindestens seit 1997 einmal als [Verbindungsoffizier zur Police Cooperation Working Group](#), dann als Vertreter des Handelsministeriums, meistens aber als Angehöriger des Innenministeriums aufgetreten ist, mischt noch ein zweiter Vertreter des britischen Home Office namens Ian Cooper regelmäßig mit.

John Horrocks vom Department of Trade and Industry empfahl der Arbeitsgruppe SEC LI mit einiger Dringlichkeit, ihre Arbeit stärker mit jener in anderen Standardisierungs-Gruppen abzugleichen. Wie bereits bei den letzten Meetings waren vier Vertreter des im russischen Telekom-Ministerium angesiedelten "Zentralen Telekommunikations-Instituts für wissenschaftliche Forschung" an dem Meeting teil, ohne in den Protokollen durch technische Beiträge oder andere Wortmeldungen aufzufallen.

Bernie McKibben von Motorola, Vorsitzender der Arbeitsgruppe 3GPP, gab einen Überblick über die Beziehungen zur US-Schwestergruppe T1P1, dem Standardisierungs-Gremium zur Überwachung von Mobiltelefonie der amerikanischen Telecom Industry Association (TIA). Im Zentrum des Vortrags stand das Abhörinterface für die mobilen Dienste der dritten Generation, dessen Handover-Ports gerade ein neues Design erhielten. Die Kernanfrage von McKibbens Vortrag aber war, dass die Architekt der Schnittstelle von ES 201 671 nicht den Anforderungen für Dienste der dritten Generation des Mobilfunks entspreche. Ebenso wenig würden die Anforderungen der Arbeitsgruppe-TIPHON zur Überwachung von Voice-over-IP durch das Interface abgedeckt.

Dies stieß nicht nur beim Vorsitzenden Arbeitsgruppe Acht von TIPHON Stephen Fischer (Aravox), sondern bei allen Teilnehmern des Workshops auf allgemeine Zustimmung und löste eine lange und "penetrierende" Debatte aus, in welcher ETSI-Arbeitsgruppe ein zukünftiges Interface entwickelt werden sollte.

Hightech für Bedarfsträger

Wädhlich bestechende finanzielle Aufwindungen für die Abhörschnittstellen fallen jetzt und in naher Zukunft bei Telecom-Anrüstern wie Alcatel und Siemens, Ericsson, Nokia, Nortel und anderen an. Wie Ericsson ein System namens LIS anbietet, dessen Produktmanager Stefan Björnson ein Regular der Arbeitsgruppe Lawful Interception ist, haben auch alle anderen in ihre Produkte - Wädhämter und Vermittlungsstellen - mehr oder weniger komplexe Überwachungslösungen integriert.

"Hightech speziell für Bedarfsträger" - so preist etwa Siemens seine "flexible und ausbaufähige Gesamtlösung an." Ähnliche Techniken haben auch die anderen Telecom-Anrüster wie Nortel im Angebot. Nach Angaben von Siemens ist diese Erfolgsprodukt mit über 240 Millionen Ports in 105 Ländern das am weitesten verbreitete System für Sprachtelefonie, jeder fünfte Anruf weltweit erfolgt über diese Hardware, die vollständig überwachungsgeeignet ist.

Statt "vermittlungstechnisches Sonderequipment" einzusetzen, das "schwierig zu tarren" sei, ließen sich Überwachungsaufträge nun mit zusätzlicher EWS-Standard-Hardware "unauffällig abwickeln". Die Software wiederum verfüge über "spezielle Filterfunktionen für die Materialauswertung", um "schnell an die wesentlichen Informationen" zu kommen.

Dass es den "Bedarfsträgern" dabei in erster Linie nicht um Gesprächsinhalte, sondern um andere Daten geht, erklärt der Siemens-Prospekt, der nur im Rahmen eines persönlichen Gesprächs an potenzielle Kunden weiter gegeben wird, mit bemerkenswerter Offenheit: "Ereignisdatenstätze liefern aufschlussreiche Informationen über das Kommunikationsverhalten des überwachten Netzteilnehmers."

Ein vollständig ausgebauten System kann "bis zu 10⁴ Teilnehmeranschlüsse pro Vermittlungsstelle gleichzeitig überwachen", dazu weitere 1000 fremde Teilnehmeranschlüsse, etwa an Roaming-Gateways. Die "aufschlussreichen Ereignisdatenstätze" können dann über die Schnittstelle ES 201 671 an Interface HI 2 an "bis zu fünf Überwachungsseinrichtungen" gleichzeitig via ftp abgelifert werden.

Was wo gesetzmäßig ist

Wie für alle Standards ist auch für ETSI ES 201 671 und Nachfolger eine international möglichst breite Akzeptanz-Voraussetzung. Zu diesem Zweck muss der Standard offen sein und so flexibel, dass er auch in jenen Ländern akzeptiert wird, in denen grundlegende Menschenrechte nicht beachtet, oder mit Füßen getreten werden. In diesen Ländern, die noch äußerst niedrige Penetrationsraten für gewöhnliche Telefonie aufweisen, aber lebt die überwältigende Mehrheit der Weltbevölkerung - ein einziger großer Hoffungsmarkt für die gesamte Telekomindustrie.

Der Schlüsseltext des "Pflichtenhefts" (TR 101 331, Scope) auf dem alle Überwachungsstandards basieren, ist, dass es die Anforderungen für Übergabe-Interfaces zum Abhören für Polizei und Staatssicherheitsagenturen enthalte ("It provides a set of requirements relating to handover interfaces for the interception by law enforcement and state security agencies.,") Darunter steht, das Dokument beschreibe die Anforderungen aus der Sicht von "Law Enforcement." ("The present document describes the requirements from a Law Enforcement Agency's (LEA's) point of view.")

Am nächsten Meeting der Arbeitsgruppe SEC LI vom 15. bis 17. Mai in Hamburg - Gastgeber: Deutsche Telekom - will man Vorschläge aus allen erwähnten Gruppen präsentieren, wie ES 201 671 adaptiert werden könne, auf dass der Standard "multimediatauglich" werde und künftig den Anforderungen paketermittelten Datenverkehrs entsprecht.

Erich Moechel ist leitender Redakteur von [OPREON FutureZone](#) [14]

Links

- [1] <http://www.heise.de/tp/deutsch/special/enfo/7220/1.html>
- [2] <http://cryptome.org/esp/200104/Meeting27GI.html>
- [3] http://webapp.etsi.org/MeetingCalendar/ViewMeetings.asp?smfTG_ID=&smfTG_REF=&TB=386&3B3GPP-SA-3&INCLUDE_SUB_TB=Tron&LOCAL_FLG=&LOCAL_CITY=&START_DAY=01&START_MONTH=1&START_YEAR=1998&END_DAY=&END_MONTH=&END_YEAR=&DISPLAY_TYPE=SHORT&TODAY_DAY=13&TODAY_MON=1&TODAY_YEAR=2001&START_DATE=&E
- [4] <http://www.etsi.org/3gpp/home.htm>
- [5] http://webapp.etsi.org/3bhomepage/TBDetails.asp?TB_ID=417&TB_NAME=SPAN
- [6] http://webapp.etsi.org/3bhomepage/TBDetails.asp?TB_ID=487&TB_NAME=TIPHON-18
- [7] <http://cryptome.org/esp/TR101-944r08.doc>
- [8] <http://futurezone.orf.at/futurezone.orf/?read=detail&id=39971>
- [9] <http://futurezone.orf.at/futurezone.orf/?read=detail&id=32924>
- [10] <http://cryptome.org/esp/TSI133-107.pdf>
- [11] <http://www.heise.de/tp/deutsch/special/enfo/3461/1.html>
- [12] <http://www.heise.de/tp/deutsch/special/enfo/3483/1.html>
- [13] <http://cryptome.org/esp/20010405Meeting27GI.html>
- [14] <http://futurezone.orf.at>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/7447/1.html>

Die ETSI-Dossiers

Erich Moechel 26.03.2001

Europäische Schnittstellen zur Überwachung sämtlicher digitaler Netze

Ein internationaler Verbund von Polizeibehörden und Geheimdiensten entwickelt einen weltweiten Standard zum Abhören digitaler Netze. Hand in Hand mit der Industrie legen die Gremien, die ihre Tätigkeit immer mit dem Etikett "lawful" schmücken, die Technik der Abhörschnittstellen fest - am EU-Parlament vorbei. Von Anfang an arbeiteten hier US-Behörden mit den EU-Ländern zusammen.

Der Masterplan der Nachrichtendienste

Das aus der Nachkriegszeit stammende ECHELON-Konzept, analoge Informationen während ihrer drahtlosen und unverschlüsselten Übertragung auf Richtfunkstrecken oder von Satelliten abzufangen, erwies sich angesichts des Aufkommens digitaler Protokolle in der Telefonie Anfang der Neunziger Jahre als wenig zukunftssicher ([Inside Echelon](#) [1]).

Für die anderen, weit weniger öffentlich bekannten Praktiken der Dienste, Telefonkabel durch einfache Induktion von außen anzuzapfen, galt im Wesentlichen dasselbe.

Die Dienste befürchteten, dass die Digitalisierung den Abhör-Zugriff auf Sprach-, Telex-, und Faxkommunikation entscheidend erschweren würde. Jeder Angriff von außen auf die Netze würde nicht zuletzt durch den möglichen Einsatz von Verschlüsselungsmethoden durch die Netzbetreiber mit hohem Aufwand verbunden oder überhaupt unmöglich sein. Innerhalb desselben Netzes stehen die Daten jedoch problemlos zur Verfügung - wenn man den Betreiber dazu bringt, standardisierte Schnittstellen für die Überwacher einzubauen.

Von Beginn waren das FBI und unterschiedliche europäische Polizeibehörden auf EU- und nationalen Ebenen daher in vorderster Linie involviert, um den Plänen einen rechtstaatlichen Anstrich zu geben. Die Exekutive musste dazu nicht lang gebeten werden, da ohnehin großes Interesse bestand, zum Abhören des Telekommunikationsverkehrs nicht mehr Beamte zum Netzbetreiber entsenden zu müssen, sondern per Fernsteuerung agieren zu können.

Dass ein derartiges Vorhaben angesichts der fortschreitenden Globalisierung der Telekommunikation nur weltweit funktionieren konnte, war ebenso klar, wie seine Finanzierung. Die Kosten für den Aufbau dieses Überwachungssystems würden weder aus

Polizei- noch aus Militärbudgets gedeckt werden können: als Zahlmeister hatten die Behörden die Telekomindustrie vorgesehen.

Die Arbeitsgruppe "Lawful Interception"

Die rund 30 Mann, die auf dem 26. Treffen der Arbeitsgruppe "Lawful Interception" (SEC LI) des European Telecom Standards Institute (ETSI [2]) Ende Februar teilnahmen, können sich über Arbeitsmangel nicht beklagen. Es ist ihre Aufgabe, Schnittstellen zur Überwachung sämtlicher digitaler Netze von ISDN über das Internet bis hin zu UMTS zu entwerfen. Zu diesem Zweck wird ein Meta-Standard namens ETSI ES 201 671 [3] (PDF-Datei) laufend erweitert und entlang der technologischen Entwicklung fortgeschrieben. Auf ES 201 671 basieren sowohl die deutsche [4] (PDF-Datei) als auch die österreichische [5] Verordnung zur Überwachung des Telekom-Verkehrs, die beide jüngst neu aufgelegt worden sind.

Die Arbeitsgruppe SEC LI traf [6] zuletzt am 21. und 22. Februar im südlich von Paris gelegenen Industriepark Courtaboeuf/Les Ulis auf Einladung der französischen Aqsacom zusammen. Dieses Unternehmen produziert nach eigenen Angaben "mediation solutions" auf den Gebieten "identification" und "geographical location" für digitale Telefonie. "Single Subscriber", eine dieser "Vermittlungslösungen", eröffnet den Behörden zum Beispiel schnellen Zugriff auf alle Verbindungsdaten eines Benutzers. "Foreigner Survey" dient der Überwachung von Roaming Gateways, über die Mobilfunk-Carrier zusammengeschaltet sind. Die Produktpalette [7] Aqsacoms aber krönt "Mobile Track", womit Handy-Benutzer diskret, schnell und ohne technische Vorkenntnisse geographisch genau lokalisiert werden können.

Daneben setzte die Arbeitsgruppe, der nicht nur Techniker, sondern auch Verbindungsleute vor allem zu britischen, deutschen und niederländischer Polizei und anderen Behörden angehören, ihre Arbeit am Gegenstück zu ES 201 671 fort. Dieser "technische Report" (TR 101 331), ein Pflichtenheft der Polizei und anderer Behörden für Netzwerk-Betreiber, wird gerade um das Abfangen von E-Mails und die Überwachung des IP Verkehrs erweitert. Es handelt sich um dabei um die Fortschreibung des Papiers "ENFOPOL 98", dessen Publikation durch Telepolis 1998/99 für einiges Aufsehen gesorgt hatte.

Symptomatisch für das Geschehen in und um die Arbeitsgruppe, die ihre Überwachungsstandards grundsätzlich mit dem Epithet "lawful" versieht, aber ist der Verweis im Vorwort, dass neben Polizeibehörden auch "Staatssicherheitsdienste" diese Überwachungs-Interfaces nützen werden: "It provides a set of requirements relating to handover interfaces for the interception by law enforcement and state security agencies." (Draft TR 101 331 V0.1.2, Scope [8] PDF-Datei).

Am Montag, den 26. Juni 2000, schickte Erich Möchel eine Email an Herrn Bum, Communications Director von Alcatel Austria, und bat um die Beantwortung der Fragen:

Welche Alcatel-Produkte entsprechen egal welcher Version des ETSI Standards ES 201 671 bzw. haben ihn implementiert?

Welche sind davon auf dem österreichischen Markt?

Anfang diesen Jahres haben nach mir vorliegenden Informationen zwei Herren namens Markus Lutz [Alcatel SEL AG] und Laurent Perrine [Alcatel] an einem Treffen der ETSI-Arbeitsgruppe SEC LI [Lawful Interception] in Oslo teil genommen, die genau diesen Standard entwickelt. Alcatel ist offenbar in dieser Angelegenheit sehr engagiert, das nächste Treffen von ETSI SEC LI fand vom 7-9 März 2000 in Stuttgart statt.
Gastgeber: Alcatel SEL

Am 10.07.2000 erhielt Erich Möchel über Anton Bum die Beantwortung der Fragen durch einen anderen Alcatel-Mitarbeiter, Markus Lutz:

"Folgende Alcatel Produkte sind ES 201 671 konform (nur SRD)

A1000 S12:

Fixed Networks:

Alle Projekte basierend auf World Release 1A (WR1A)

z.B. Call Server Phase 2 (CLS2)

Mobile Networks: (geplant)

alle GPRS Projekte

alle UMTS Projekte

- für bestehende GSM Projekte gibt es bis jetzt noch keine Kundenforderung ETSI konform zu werden. Zur Zeit ist in GSM (z.B. ALM7) etwas vergleichbares implementiert.

Meines Wissens ist z.Z. von SRD nichts auf dem österreichischen Markt, was 100% ES 201 671 konform ist."

(SRD ist Alcatel intern die Abkürzung für "Switching & Routing Division)

Das Design der Überwachung

Dieses Szenario ist dabei, in ganz Europa und darüber hinaus Wirklichkeit zu werden. Alle Vermittlungszentralen (Circuit Switched Networks) für digitale Telefonie und Daten (ISDN, GSM und andere) werden mit derartigen so genannten "Handover Interfaces" ausgestattet.

Die auf die polizeiliche Komponente reduzierte Funktionsbeschreibung verschweigt freilich, was sich an diesen Schnittstellen tatsächlich abspielen wird. Der Abschnitt 4.3 der "General Requirements" zum Standard ES 201 671 vermittelt eine Ahnung davon: "Eine Person kann das Ziel der Überwachung mehrerer LEAs [gleichzeitig] sein. Es soll ermöglicht werden, diese Abhörmaßnahmen strikt zu trennen." Obwohl das gesamte Setup wie auch die Beteiligten von SEC LI aus der Telefoniewelt stammen, soll am Interface 2 mit FTP ein Protokoll aus der TCP/IP-Welt zum Einsatz kommen. Dass für diese Schnittstelle, an der während der Überwachung nur eine Handvoll Daten anfallen, ein Protokoll eingesetzt wird, das im Allgemeinen für die Übertragung großer Datenmengen dient, macht klar, dass diese Schnittstelle prädestiniert ist, Zugriff auf die Logfiles der Netzbetreiber eröffnen.

Auf mehr als hundert Seiten enthält ES 201 671 daneben alle Befehlssätze, die für die Kontrolle der gesamten Kommunikation rund um das Interface notwendig sind. Natürlich fehlt der Hinweis nicht, dass diese Befehle grundsätzlich nur vom Netzbetreiber und nicht etwa von den Behörden zur Anwendung zu bringen sind. Da keinerlei Kontrolle vorgesehen ist, wird an diesen Schnittstellen alles bis hin zur flächendeckenden Überwachung möglich sein.

Zu technischen Einzelheiten und für weitere Informationen siehe den Artikel von Erich Möchel "Lauschangriff: Abhörstandard für Europa" in der c't 7/2001.

"International User Requirements" reichen bis in das Jahr 1993 zurück

Wie Duncan Campbell in einem grundlegenden Artikel über die Tätigkeit der ILETS in Telepolis dargelegt hat ([ILETS, die geheime Hand hinter ENFOPOL 98](#) [9]), reichen die so genannten "International User Requirements" bis in das Jahr 1993 zurück. Im ersten einer Reihe der so genannten "Law Enforcement Telecom Seminars" einigten sich die Nachrichtendienste und die Polizei der ECHELON-Betreiber USA, England, Kanada und Australien mit den wichtigsten EU-Staaten bereits 1993 auf ein gemeinsames Vorgehen. Auf der FBI-Akademie in Quantico, Virginia wurde ein Papier erstellt, das die so genannten "Internationalen Abhörerforderungen" (International Requirements for Interception) der Nachrichtendienste formulierte. Zentrale Aussage: Die gesetzlich

ermächtigten Behörden benötigen Zugriff auf den gesamten Telekommunikationsverkehr in Echtzeit rund um die Uhr. Dies würde nur durch permanente Verbindung der Dienste an standardisierte Andockstellen in den Netzen möglich sein.

Bei weiteren, ebenso geheimen ILETS-Treffen (Bonn 1994, Canberra 1995) wurde das Vorgehen bereits mit Vertretern aller EU-Staaten abgesprochen, die "Abhöranforderungen" aber wurden in "Benutzeranforderungen" (International User Requirements, IUR) umbenannt. In den USA gingen die IUR unter dem Titel CALEA (Communications Assistance Law Enforcement Act) nach teilweise heftigen Diskussionen leicht modifiziert im Jahr 1994 durch den US-Kongress. Zum EU-Ratsbeschluss wurden sie wenig später, nämlich am 17. Januar 1995 erhoben. In einer Nacht- und Nebelaktion gingen die IUR fast unverändert und als "beschlossene Sache" am EU-Parlament vorbei – durch den Fischerei-Ausschuss.

Ein mit Dezember 1996 datierter "Technischer Report" ([ETSI ETR 331 \[10\] PDF-Datei](#)), der von einer nicht näher spezifizierten "Beratergruppe für Sicherheitstechniken" (Security Techniques Advisory Group) verfasst wurde, beschreibt im Vorwort "die Anforderungen bezüglich von Schnittstellen für die Überwachung" durch "law enforcement and state security agencies."

Am 29. Juni 2000 schickte Erich Möchel eine Email an Herrn Michael Kochwaller von der Siemens AG Österreich folgende Fragen:

Welche Siemens-Produkte, namentlich Switches, entsprechen egal welcher Version des ETSI Standards ES 201 671 [European Telecommunications Standards Institute] bzw. haben ihn implementiert?

Welche sind davon auf dem österreichischen Markt?

ES 201 671 definiert die Standards für Abhörschnittstellen [lawful interception] in den verschiedensten Kommunikationsnetzen

Nach mir vorliegenden Informationen nehmen zwei Herren namens Herbert Pxxxx und Bernhard Sxxx an den Treffen der ETSI-Arbeitsgruppe SEC LI [Lawful Interception] teil, die genau diesen Standard entwickelt.

Am 1. August 2000 erhielt von Frau Sylvia Schwarz, Öffentlichkeitsarbeit bei Siemens AG Österreich, die Antwort:

"Vorab möchte ich mich für die lange Bearbeitungsdauer Ihrer Anfrage entschuldigen. Nachfolgend finden Sie das für Siemens gültige Statement zur ETSI-Thematik:

Siemens arbeitet in allen Fragen des ETSI Standards eng und vertrauensvoll im Rahmen

der Gesetze mit den jeweils verantwortlichen Behörden zusammen. Wir möchten Sie daher bitten, sich für Fragen im Zusammenhang mit dem ETSI Standard an die zuständigen Behörden zu wenden."

Am EU-Parlament vorbei

Im Januar 1997 veröffentlichte die britischen Bürgerrechtsgruppe Statewatch eine Untersuchung unter dem Titel "Das EU-FBI Überwachungssystem", der eine Neufassung der IUR (ENFOPOL 90) der "Police Cooperation Working Group" (PCWG) zu Grunde lag. Dies und die Aufdeckung der Umstände, wie die IUR am EU-Parlament vorbei zum Ratsbeschluss erhoben wurden, sorgten 1997 ebendort für einen Eklat. War es in diesem Fall noch gelungen, das Parlament der Union zu übergehen, so scheiterte der zweite Anlauf, die "Benutzeranforderungen" um das Internet-Protokoll und GSM zu erweitern und dies auch parlamentarisch absegnen zu lassen, in letzter Minute am Druck der Öffentlichkeit.

Nachdem Telepolis mit den so genannten ENFOPOL-Papieren [11] im November 1998 eine ganze Serie von Dokumenten der Ratsgruppe Polizeiliche Zusammenarbeit (PCWG) im Volltext publiziert hatte, herrschten erst Zweifel an der Echtheit des Dokuments. Nach einem Bericht des britischen Channel 4 griffen dann die Medien des westlichen Europa das Thema auf, ENFOPOL wurde zum Synonym für die drohende Überwachungsunion. In Polizei- und Geheimdienstkreisen wurden die österreichischen Beamten, die das Papier während der EU-Präsidentschaft Österreichs verfasst hatten, herb kritisiert.

Im Frühjahr 1999 exerzierten die Kollegen den Österreichern vor, wie man mit Papieren vom Kaliber der IUR umzugehen hat. Wie schon in den dar Fassung von 1995 wurde das Papier zweigeteilt. Alle brisanten Punkte wurden aus dem Entwurf eines Ratsbeschlusses eliminiert und verschwanden in einem Annex mit technischen Erläuterungen, der nicht vorgelegt wurde. So blieb von 42 Seiten nur ein sehr abstrakter, vierseitiger Forderungskatalog (ENFOPOL 19/99) übrig.

Die runderneuerte IUR wurde schließlich statt in der Form eines Ratsbeschlusses der EU wieder am Parlament vorbei als europäischer Telekommunikations-Standard eingeführt. Während das EU-Parlament einen Ausschuss für das Überwachungssystem ECHELON einberufen hat, ist der Aufbau eines völlig anders strukturierten Überwachungssystems quer durch Europa schon sehr weit fortgeschritten, das den Diensten Zugriff auf die gesamte digitale Sprach- und Datenkommunikation der europäischen Zivilgesellschaft eröffnen wird (Europäisches Rechtshilfeabkommen verabschiedet [12]).

Am 3. August 2000 schickte Erich Möchel an Herrn Harald Dörr, Leiter Presse und Öffentlichkeitsarbeit bei der Regulierungsbehörde für Telekommunikation und Post (Reg TP), folgende Fragen:

Ist es richtig, dass nur noch Telekommunikationsequipment [Switches etc] dem ETSI Standard ES 201 671 entsprechen muss? Wie viel derartig spezifiziertes Gerät ist Ihrer Meinung nach bereits in Gebrauch?

Nach mir vorliegenden Informationen agiert ein Herr Theo Metzger als stellvertretender Vorsitzender des Technischen Komitees SEC im ETSI, dessen Unterabteilung SEC LI diesen Abhörstandard entwickelt. Herr Metzger wird in mehreren Dokumenten als Angehöriger der deutschen RegTP bezeichnet, auch im öffentlich zugänglichen Teil der Website und er benutzt offenbar auch eine regtp.de Emailadresse.

Am 8.8. 2000 erhielt Erich Möchel von Herrn Rudolf Boll, Pressesprecher der Reg TP, folgende Antwort:

"Antwort zu Frage 1: Zukünftige Einrichtungen müssen auf ES 201 671 basieren.

Antwort zu Frage 2: Dazu kann die Regulierungsbehörde für Telekommunikation und Post keine Auskunft geben, da dies außerhalb unseres Zuständigkeitsbereiches liegt.

Antwort zu Frage 3: Unser Kollege ist uns wohl bekannt. Da aber Auskünfte an Medienvertreter nur von dem Präsidenten der Regulierungsbehörde oder der Pressestelle gegeben werden, sind Sie zur Pressestelle vermittelt worden.

Antwort zu Frage 4: Ja.

Antwort zu Frage 5: Ja.

Für technische Fragen zum ETSI Standard ES 201 671 möchten wie Sie bitten, sich direkt an ETSI oder an den Vorsitzenden ETSI SEC LI Gruppe, Herrn Robin Gape, BT zu wenden."

Propaganda-Offensive 2000

In einem internen Protokoll des Treffens der Ratsgruppe Polizeiliche Zusammenarbeit (PCWG) vom 13. und 14. Oktober 1999 (Dok DGJHA B/1/TB D99) werden die Kommissionsvertreter in der PCWG zum Punkt "Interception of Telecommunications" mit folgender Empfehlung an die anwesenden Behörden-Vertreter zitiert: Um das durch die "negative Presse" zur Affäre ENFOPOL 98 ausgelöste Patt auf politischer Ebene zu durchbrechen, empfehlen die Vertreter der Kommission den versammelten Behörden und

Diensten "eine ähnliche Strategie wie jene bezüglich der Kinderpornographie im Internet zu verfolgen", die auch "eine Abhördimension" habe.

Der am 27. April 2000 vorgelegte Entwurf einer "Konvention zur Cyber-Kriminalität" wurde nicht ganz überraschend mit den Schlagworten "Kinderpornographie" und "Cyberterroristen" eröffnet und kam schnell auf den eigentlichen Punkt: "Zur Diskussion stehen Computer-spezifische investigative Methoden", genauer gesagt, "die Überwachung von Daten, die über Netzwerke" aller Art übertragen werden. Dazu sorgte eine unüberschaubare Zahl von Regierungsvertretern und nationalen Behörden, Gremien und Initiativen für ein mediales Flächenbombardement, das über zehn Monate ging (Codename "organisierte Kriminalität" [13], Kampf gegen das transnationale organisierte Verbrechen und die Computerkriminalität [14]).

Die Botschaft war immer gleich: Die Polizei muss hilflos zusehen, wie digital hochgerüstete Drogenhändler und organisierte Kriminelle, Hacker und Kinderpornographen die Informationstechnologien für ihre Zwecke nutzen. Ein wesentlicher Teil der aus ENFOPOL 98 bekannten IUR ging genau um diese Zeit in ein EU-weites Vertragswerk ein - gegen den Willen einer Mehrheit im Parlament der Europäischen Union.

EU-Rechtshilfe-Übereinkommen

Am 29. Mai 2000 unterzeichneten die Justizminister der EU-Mitgliedsländer während der Ratstagung in Brüssel ein Rechtshilfeübereinkommen, das "den Informationsaustausch und die Vernetzung bei Ermittlungen vereinfachen" sollte. Das EU-Parlament hatte im Frühjahr zwar mehrheitlich verlangt, die entsprechenden Paragraphen 18 (in der damals vorliegenden Fassung 21) zum grenzüberschreitenden Abhören aus dem Übereinkommen zu eliminieren (Europäisches Parlament stimmt gegen unkontrolliertes grenzüberschreitendes Abhören [15]). Damit wurde dem Parlament sein Anhörungsrecht zugestanden, aber mehr nicht. Die Endfassung entsprach der vom 15. Mai (Fassung 32), wurde dem Parlament nicht mehr vorgelegt und auch sonst bis zuletzt geheim gehalten (Europäisches Rechtshilfeabkommen verabschiedet [16]).

In der Praxis werden im Rechtshilfe-Übereinkommen den ermächtigten Behörden Freiheiten eingeräumt, die in der Geschichte der modernen Kommunikation einmalig sind. Mit der Unterzeichnung ist es für alle Polizeibehörden legal möglich geworden, eine Zielperson (und alle ihre Telefonate) auf fremdem Hoheitsgebiet bis zu 12 Tage lang legal abzuhören, ohne dass ein ordentliches Gericht im Ziel-Land dies genehmigt hätte.

Damit wurde ein bestehendes Rechtsproblem einer EU-weiten Regelung zugeführt. Wenn es die beteiligten Behörden allerdings darauf anlegen, die jeweiligen Fristen im Rechtshilfe-Übereinkommen gemeinsam auszunützen, öffnen sie nicht nur den eigenen Ermittlern dauernden Zugang zu den wichtigsten Knotenpunkten der zivilen

Kommunikation in Europa. Sollte nach Ablauf aller Fristen ein ordentliches Gericht im Ziel-Land entschieden haben, dass die Überwachung nicht der nationalen Rechtslage entspricht, dürfen die abgefangenen Informationen von den gesetzlich ermächtigten Behörden nicht verwendet werden. Ob dieses Verbot auch jene Behörden tangiert, die -- für Netzbetreiber und sonstige Parteien unsichtbar -- an den Schnittstellen Daten zapfen, muss wohl bezweifelt werden.

Rein technisch lässt das Design von ES 201 671 und der dazu gehörigen Standards alle Möglichkeiten offen, solange es keine gesellschaftliche Kontrolle über die Schnittstellen und "Handover Interfaces" gibt, an denen es den Diensten erstmals möglich sein wird, praktisch alle Datenflüsse der Informationsgesellschaft nahezu in Echtzeit zu kontrollieren.

Die Arbeitsgruppe "Lawful Interception" wird als nächstes [17] auf Einladung der Telenor im norwegischen Grimstad wieder zusammen treffen. Mit von der Partie sind die Abhörtruppe des Third Generation Partnerships Projects [18] (3GPP SA3 LI) und die Gruppe TIPHON, die ebenfalls mit Überwachungsfragen beschäftigt ist. Vom 15. bis 17. Mai trifft man sich auf Einladung der Deutschen Telekom in Hamburg, ein weiteres Meetings erfolgt auf Einladung von Siemens, ebenfalls drei Tage lang, vom 27. bis 29. November in Wien.

Erich Möchel ist Redakteur bei der Futurezone [19] und betreibt die q/depesche [20].

Links

- [1] <http://www.heise.de/tp/deutsch/special/ech/6928/1.html>
- [2] <http://www.etsi.org>
- [3] <http://cryptome.org/esp/ES201-671.pdf>
- [4] http://www.regtp.de/imperia/md/content/tech_reg_t/ueberwachu/5.pdf
- [5] <http://www.vibe.at/misc/uevo.htm>
- [6] http://webapp.etsi.org/MeetingDocuments/ViewDocumentList.asp?MTG_Id=10314
- [7] <http://www.aqsacom.com/english/about/index.htm>
- [8] <http://cryptome.org/esp/ETR331e01p.pdf>
- [9] <http://www.heise.de/tp/deutsch/special/enfo/6396/1.html>
- [10] <http://cryptome.org/esp/ETR331e01p.pdf>
- [11] <http://www.heise.de/tp/deutsch/special/enfo/default.html>
- [12] <http://www.heise.de/tp/deutsch/special/enfo/8204/1.html>
- [13] <http://futurezone.orf.at/futurezone.orf?read=detail&id=25328>
- [14] <http://www.heise.de/tp/deutsch/inhalt/te/5988/1.html>
- [15] <http://www.heise.de/tp/deutsch/inhalt/te/5810/1.html>
- [16] <http://www.heise.de/tp/deutsch/special/enfo/8204/1.html>

[17] http://webapp.etsi.org/MeetingDocuments/ViewDocumentList.asp?MTG_Id=21150

[18]

http://webapp.etsi.org/tbhomepage/TBDetails.asp?TB_ID=375&TB_NAME=3GPP+SA

[19] <http://futurezone.orf.at/>

[20] <http://www.quintessenz.at/>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/7220/1.html>

Copyright © 1996-2003. All Rights Reserved. Alle Rechte vorbehalten

Heise Zeitschriften Verlag, Hannover

Europäische Kommission ruft zum Kampf gegen Cyberkriminalität

Jelle van Buuren 10.01.2001

Europol soll Cyberkriminalität bekämpfen; 'Enfopol-Papiere' werden derzeit nicht weiter ausgearbeitet; Angleichung nationaler Gesetzgebung sei zur Bekämpfung von High-Tech-Kriminalität nötig

Die Europäische Kommission veröffentlichte letzte Woche einen neuen Vorschlag zur Bekämpfung Computer-bezogener Verbrechen. Das Dokument enthält keine konkreten gesetzgeberischen Vorschläge, skizziert aber in groben Zügen, wie sich die Kommission die Bekämpfung von Cyberkriminalität vorstellt. Ein Europäisches Forum, bestehend aus Strafverfolgungsbehörden, Telekommunikations-Service-Providern, Konsumentengruppen und Datenschützern soll die Kooperation auf europäischer Ebene verstärken.

Der Vorschlag der Europäischen Kommission mit dem Titel "Creating a Safer Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime" [1] (PDF-Datei), stellt fest, dass effektives Handeln zur Bekämpfung von High-tech-Kriminalität auf nationaler und internationaler Ebene nötig seien, da solche Verbrechen im grenzenlosen Cyberspace sich nicht an die Staatsgrenzen halten würden. Nationale Gesetze haben deutliche Unterschiede, zum Beispiel bezüglich der Strafgesetze über Hacking, den Schutz von Handelsgeheimnissen und illegale Inhalte. Große Unterschiede würden auch bezüglich der Verfügungsgewalt von Untersuchungsbehörden bei verschlüsselten Daten und Ermittlungen in internationalen Netzwerken bestehen. Obwohl die Kommission zugibt, dass sie über keine verlässlichen Statistiken über Cyberkriminalität verfügt, stellt sie fest, dass "es kaum Zweifel daran gibt, dass diese Straftaten eine Bedrohung für Investitionen und Anlagen der Industrie darstellen, ebenso wie gegenüber der Sicherheit und dem Vertrauen in die Informationsgesellschaft".

Die Kommission sagt, dass es notwendig ist, dass grundlegende Gesetze auf dem Gebiet der High-Tech-Kriminalität angeglichen werden. Während des EU-Treffens zu Sicherheitsfragen in Tampere (1999) forderten führende Politiker gemeinsame Definitionen, Anklagepunkte und Sanktionen. Im Entwurf für den Vertrag über Cyberkriminalität [2] des Europarats werden solche Angleichungen der Gesetze in vier Bereichen gefordert: Verbrechen gegen die Vertraulichkeit und Integrität von Computerdaten und -Systemen; mittels Computer begangene Verbrechen; illegale Inhalte; Verbrechen in Zusammenhang mit dem Schutz geistigen Eigentums und verwandter Rechte.

Die Europäische Kommission möchte aber, dass die EU noch weiter geht. In diesem Jahr wird die Kommission neue Vorschläge zur Bekämpfung von Kinderpornographie als ein erster Schritt zur Harmonisierung nationaler Gesetze unterbreiten. Auf längere Sicht will die Kommission auch Gesetze über das Hacken und Denial-of-Service-Attacks ausarbeiten. "Es soll sichergestellt werden, dass ersnthaft Fäkle von hacking und Denial-of-Service-Attacks in allen Ländern mit einer Mindeststrafe geahndet werden können", kündigt die Kommission an. Darüberhinaus will die Kommission auch gegen Fremdenfeindlichkeit und Rassismus im Internet vorgehen. Nicht zuletzt will die Kommission auch überlegen, wie die Bemühungen im Kampf gegen illegalen Drogenhandel über das Internet [3] verbessert werden können.

Hinsichtlich der Prozessverordnungen möchte die Kommission sicherstellen, dass schnelle internationale Zusammenarbeit bei Ermittlungen möglich ist. Die Kommission unterstützt die Schaffung neuer Abhörmöglichkeiten bei neuen Technologien und kommt zu der Feststellung, dass internationale Koordination nötig sei, um an die Service Provider und Telekommunikationsunternehmen neue technische Abhörerforderungen [4] stellen zu können. In diesem Kontext gibt die Kommission einen Hinweis auf die sogenannten Enfpol-Papiere, die von Telepolis 1998 veröffentlicht worden waren. Laut der Kommission sei der "Entwurf des Ratsbeschlusses vom Rat und seinen Arbeitsgruppen in den letzten Monaten nicht aktiv weiter behandelt worden".

Das mag der Wahrheit entsprechen, doch Teile des Plans werden trotzdem weiter ausgearbeitet. Die Arbeitsgruppe über Polizeizusammenarbeit zum Beispiel stellt gerade eine Liste mit den Netznummern der Mobiltelephongesellschaften und ihren Roaming-Vereinbarungen auf. Ermittlende Behörden beobachten häufig Verdächtige, indem sie das Identifikationssignal ihres Mobiltelefons verfolgen. "Diese einfache Ermittlungsmethode kann unterbrochen werden, wenn ein Verdächtiger die Grenze überquert. Deshalb ist es nötig, die Roaming-Vereinbarungen der Mobiltelephonfirmen zu kennen", schrieb die Arbeitsgruppe in einem Dokument vom 15. September 2000. "Wenn eine Liste der Netznummern von Mobiltelephongesellschaften zusammengestellt wird, auf der Basis von Telephonnummern, IMSI-Nummern und Roaming-Verträgen, dann kann eine Polizeibehörde die Behörde eines anderen Landes direkt auffordern, einen Nutzer zu lokalisieren, ohne die nationale Mobiltelephonfirma um Kooperation bitten zu müssen. Auf die selbe Weise kann eine Polizeibehörde die ausländische GSM-Nummer beobachten, die von einem Inländer benutzt wird."

Unter der gerade beendeten französischen EU-Präsidentschaft wurden auch neue Maßnahmen vorgeschlagen, versteckt in Vorschlägen zu verstärkter Bekämpfung von Drogenhandel. Die französische EU-Präsidentschaft ersuchte die Arbeitsgruppe über gegenseitige Unterstützung in Strafsachen die Möglichkeit zu untersuchen, "Telefonnummern zu identifizieren, ohne sich an den formellen prozeduralen Rahmen zu

halten". Die Franzosen wandten sich, wie aus einem Dokument vom 16. Oktober 2000 hervorgeht, auch an die informelle Arbeitsgruppe ILETS, sich die "technischen Probleme des Abhörens von Mobiltelefonen und von Mobiltelefonen mit vorausbezahlten Karten" anzusehen. (siehe dazu ILETS, die geheime Hand hinter ENFOPOL 98 [5])

Die Europäische Kommission hat noch keine feste Meinung zu ausgesprochen kontroversiellen Angelegenheiten wie anonymer Zugang und Nutzung des Internet, grenzüberschreitende Durchsuchungen und Beschlagnahmungen und die Speicherung von Verbindungsdaten. Es wird nur festgehalten, dass diese schwierigen Fragen zunächst von Strafverfolgungsbehörden und der Industrie zu diskutieren seien, um akzeptable Lösungen zu finden, bei denen sich Rechte und Pflichten die Waage halten. Die Kommission möchte ein Europäisches Forum zur Besprechung dieser und anderer Themen schaffen. "Effektive Zusammenarbeit zwischen Regierung und Industrie innerhalb des gesetzlichen Rahmens wird als ein wichtiges Element jeder Politik betrachtet, mit der Computer-bezogene Verbrechen bekämpft werden sollen", sagt die Kommission. Bürgerrechtsgruppen, Konsumentenverbände und Datenschutzbehörden sollen ebenfalls eingeladen werden, an diesem Forum teilzunehmen.

Schließlich unterstützt die Kommission auch die Erweiterung der Zuständigkeit von Europol für Cyberkriminalität. Als Frankreich die alle sechs Monate rotierende Präsidentschaft der Europäischen Union inne hatte, schlug es Erweiterungen von Europol's Mandat [6] in dieser Hinsicht vor. Die Möglichkeit, dass Europol für Cybercrime zuständig sein solle, war bereits im Europol-Vertrag erwähnt worden.

Laut Frankreich soll die neue Rolle von Europol "vor allem" pragmatisch sein und darin bestehen, eine Basis "für die operationale Begegnung der Probleme im Kampf gegen Cyberkriminalität" zur Verfügung zu stellen. Angriffe auf automatisierte Datenverarbeitungsvorgänge - das Schreiben und die Verbreitung von Viren, Einbrüche in, Veränderungen von oder Manipulationen an fremden Betriebssystemen, Veränderungen von Datenbeständen - sind bislang außerhalb der Reichweite von Europol's Mandat. Frankreich möchte daher, dass auch diese Art von Vergehen unter das Mandat von Europol fallen.

Die offizielle Definition von Computerkriminalität in diesem Zusammenhang werde lauten, "alle Arten von Angriffen auf automatische Datenverarbeitungssysteme". Laut Frankreich habe diese Erweiterung den Vorteil "unzweideutig" bezüglich der Definition dessen zu sein, welche Vergehen davon tatsächlich erfasst würden. Als ein "Ergebnis dieser klar definierten Vorgaben" sei es Europol möglich, "ihre Bemühungen zu optimieren und den Einsatz ihrer Ressourcen zu rationalisieren".

Der Vorstand von Europol soll nun weitere Ratschläge bezüglich dieser französischen Vorschläge ausarbeiten und feststellen, welche Implikationen dies für Europol's

Mitarbeiter und Budget hätte, bevor der Europäische Rat für Justiz und Inneres eine formelle Vereinbarung über diese neue Aufgabe für Europol schließen kann.

Europol wird dann das Mandat haben, Informationen über Computerangriffe zwischen den Mitgliedsstaaten auszutauschen. Darüberhinaus wird Europol dann sowohl analytische Arbeits-Daten über Computerangriffe sammeln, die für strategische Zwecke gedacht sind, als auch operationale Arbeits-Daten, die grenzüberschreitenden Ermittlungen dienen. Frankreich stellt fest, dass dieses neue Mandat für Europol nötig sei, um "das Aufblühen neuer Informations- und Kommunikationstechnologien zu ermöglichen, ohne dass dadurch gleichzeitig Sicherheitsdefizite erwachsen".

Die Europäische Kommission lädt interessierte Parteien ein, die neuen Vorschläge zu kommentieren. Kommentare können noch bis zum 15. Februar an die folgende Email-Adresse gesandt werden:

info-jai-cybercrime-comments@cec.eu.int <mailto:info-jai-cybercrime-comments@cec.eu.int>

Die Kommentare sollen dann auf der folgenden Website publiziert werden:
europa.eu.int/ISPO/eif/InternetPoliciesSite?Crime/crime1.html [7]

Die Kommission wird auch eine öffentliche Anhörung zu den Vorschlägen veranstalten, die in dieser Kommunikation gemacht wurden. Die Anhörung soll am 27. Februar 2001 stattfinden. Anträge für eine Einladung zur Abgabe einer Stellungnahme bei dieser Anhörung können noch bis zum 31. Januar ebenfalls via Email erfolgen:

info-jai-cybercrime-hearing@cec.eu.int <mailto:info-jai-cybercrime-hearing@cec.eu.int>

Links

- [1] <http://www.privacyinternational.org/issues/cybercrime/EUCrimeCommEN.PDF>
- [2] <http://www.heise.de/tp/deutsch/inhalt/te/4550/1.html>
- [3] <http://www.heise.de/tp/deutsch/inhalt/te/8858/1.html>
- [4] <http://www.heise.de/tp/deutsch/special/enfo/6334/1.html>
- [5] <http://www.heise.de/tp/deutsch/special/enfo/6396/1.html>
- [6] <http://www.xs4all.nl/~respub/europol/cyberpol.html>
- [7] <http://europa.eu.int/ISPO/eif/InternetPoliciesSite?Crime/crime1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/4657/1.html>

Europäische Minister holen zum Schlag gegen Cyberkriminalität aus

Jelle van Buuren 30.07.2000

Informelles Meeting der Justizminister setzt Cyberkriminalität ganz oben auf die Agenda

Die Justizminister der EU-Staaten erklärten nach ihrem informellen Treffen am letzten Freitag und Samstag in Marseille, dass sie neue Gesetze zur Bekämpfung von Cyberkriminalität im Sinn haben. Frankreich, das in den nächsten 6 Monaten die EU-Präsidentschaft inne hat, hat Cyberkriminalität zu einem der Hauptthemen gemacht, das bezüglich der Zusammenarbeit in Justizangelegenheiten angegangen werden müssten.

Die französische Justizministerin Elisabeth Guigou erklärte, das Internet sei im Begriff, eine "gesetzesfreie Zone" zu werden. Laut Guigo sei die EU langsam in der Bekämpfung der schnell ansteigenden Kriminalität im Internet gewesen. Guigo kündigte an, die EU würde die Zusammenarbeit mit den G8 und der UNO nun zu verbessern versuchen. Die EU möchte auch die Verhandlungen über einen Vertrag des Rats der Europäischen Union über Cyberkriminalität vorantreiben.

Der EU-Kommissar für Justiz und Inneres, Antonio Vitorino, stellte auch neue Vorschläge vor, wonach gemeinsame Regeln zur Bekämpfung von Cyberkriminalität geschaffen werden sollen. Diese Regeln würde man benötigen, um z.B. der Polizei die Befugnis zu erteilen, Computerdaten in anderen Ländern zu beschlagnahmen. Auch sollten Internetverbrechen in allen EU-Ländern zu Straftaten erklärt werden.

Vitorino gab an, dass existierende Formen der wechselseitigen Zusammenarbeit ungeeignet für schnelle und komplexe Ermittlungen im Internet wären. Deshalb schlug er letzten Mittwoch den sogenannten "Mechanismus zur wechselseitigen Anerkennung von strafrechtlichen Entscheidungen" bei Internetermittlungen vor. Dieser Mechanismus bedeutet, dass ein Gerichtsentscheid oder eine Anordnung EU-weite Gültigkeit erhält. Das würde die Mitgliedsstaaten zwingen, auf Verfügungen zu reagieren, die bereits im Ermittlungsstadium und noch vor einem Gerichtsverfahren getroffen wurden (wie z.B. Haftbefehle, Zeugenvorladungen und Sicherstellung von Beweismitteln). Das würde die europäische Polizei-Zusammenarbeit vereinfachen und beschleunigen.

Vitorino kündigte auch an, dass die Kommission neue Gesetze gegen Kinderpornografie, Drogenschmuggel, Rassismus und Hacking plant.

Links

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6940/1.html>

Copyright © 1996-2003. All Rights Reserved. Alle Rechte vorbehalten
Heise Zeitschriften Verlag, Hannover

Euro-Fälschungen und Geldwäsche als Tests für EU-Polizeizusammenarbeit

Christiane Schulzki-Haddouti 13.07.2000

Europol-Fahrplan bis 2004

Sowohl die Schlussfolgerungen von Tampere, als auch der Amsterdamer Vertrag (Artikel 30, Paragraph 2) zeichnen die nächsten Schritte der europäischen Strafverfolgung vor. Für Europol [1] bedeutet dies zum einen die Einbindung in die EU-Strukturen, zum anderen die Entwicklung neuer Methoden, um die Kooperation der Strafverfolger auf europäischer Ebene zu verbessern.

Ermittlungen gegen Euro-Betrug?

Eines der ersten Einsatzgebiete für Europol wird die Bekämpfung von Betrügereien bei der europäischen Währung sein. Dabei handelt es sich nämlich nicht mehr um eine Aufgabe, die ausschließlich in die Zuständigkeit einzelner Mitgliedstaaten fällt.

Im Artikel 30 des Europäischen Vertrages steht, dass das Sammeln, Speichern, Verarbeiten, Analysieren und Austauschen von Informationen der Strafverfolger hinsichtlich verdächtiger Finanztransaktionen ein Bereich für die europäische Polizeizusammenarbeit sein soll. Der Europäische Rat forderte in Tampere [2] dazu auf, die Kompetenz von Europol allgemein auf Geldwäsche zu erweitern (Tampere-Schlussfolgerung 51 und 56). Zur Aufgabe würde es dann gehören, entsprechende Hinweise aufzuspüren, einzufrieren, zu beschlagnahmen und zu konfiszieren.

Die deutsche Delegation machte bereits klar, dass sie eine Ausdehnung des Mandats auf Geldwäsche "im Zusammenhang mit allen denkbaren Straftaten [...] nicht befürwortet". Generell sei für die Ausdehnung des Mandats auf eine "allgemeine Zuständigkeit" für Geldwäsche "in jedem Fall eine Änderung der Europol-Konvention mit allen erforderlichen Konsequenzen" notwendig.

Die G-7-Staaten und die Geldwäsche

Steuerhinterziehung ist die eine Quelle schwarzer Kassen im Ausland, organisierte Kriminalität die andere. Die illegale Kapitalflucht droht Staaten handlungsunfähig zu machen - Stichwort "leere Kassen". Der Kampf gegen Geldwäsche steht daher auf der Agenda der Financial-Action-Task-Force (FATF) der OECD. Auch auf dem nächsten G-8-Gipfel in Okinawa steht die Geldwäsche auf der Tagesordnung [3] - wobei die G-7-Staaten unter anderem den G-8-Staat Russland an die Kandare nehmen wollen.

Am 8. Juli veröffentlichte das US-amerikanische Finanzministerium eine Liste von 15 Ländern [4], deren Geldwäschegesetze zu wünschen lassen. Von der FATF [5] wurden die selben 15 Länder im letzten Monat [6] (PDF-Dokument) als "unkooperativ im internationalen Kampf gegen die Geldwäsche" identifiziert. Dabei handelt es sich (in alphabetischer Folge) um die Bahamas, Cayman-Inseln, Cook-Inseln, Dominikanische Republik, Israel, Libanon, Liechtenstein [7], Marshall-Inseln,

Praktische Probleme

Aus Sicht der Praktiker von Europol gibt es einige Probleme bei der europäischen Zusammenarbeit. So ist es beispielsweise in gemeinsamen Ermittlungsteams nicht immer klar, welche Rolle und welche Befugnisse die einzelnen Mitglieder haben. Unklar ist auch die Rolle von Staatsanwälten und Richter im Laufe einer gemeinsamen Entwicklung. So könnte eine Teilnahme von Mitgliedern aus Justizbehörden "den Austausch von Beweismaterial auf unkompliziertem Wege" ermöglichen, meinen die Europol-Beamten. Ebenfalls nicht vollständig geklärt sind wohl auch die Rechten und Pflichten der Mitglieder sowie die Frage, wie solche Teams bezahlt werden.

In der Vergangenheit wurde das Mandat von Europol mit neuen Aufgabengebieten und Funktionen wie den so genannten "Centres of Excellence" erweitert. Bereits im Mai 1998 beschloss der Rat der Europäischen Union 50 neue Stellen für Europol pro Jahr. Da Polizeibehörden europaweit mit knappen Budgets zu kämpfen haben, wollen die Europol-Beamten ähnlichen Diskussionen a la "mehr Aufgaben, gleiches Geld" vorbeugen. In einem Arbeitspapier der Europol-Ratsarbeitsgruppe heißt es deshalb:

"Um seine Aufgaben zu erfüllen kann Europol nicht die Prioritäten ändern und Ressourcen von anderen wichtigen Aufgaben abziehen. Für die Erweiterung seines Mandates und seiner Funktionen braucht Europol künftig eine bessere Ausstattung, also Personal, aber auch technische und finanzielle Ausstattung."

Dies gilt jedoch nicht nur für die Ausstattung von Europol, sondern auch für die so genannten Europol National Units, die Europol-Einheiten auf nationaler Ebene. Sie versorgen Europol mit Informationen und Aufklärungsmaterial und reagieren auf entsprechende Anforderungen von Europol.

Telepolis veröffentlicht an dieser Stelle eine Übersicht, die anstehende Aufgaben von Europol im Zeithorizont beschreibt:

Aufgabe	Termin	Quellen
Datenbank zu laufenden Ermittlungen	31. Dez. 2000 31. Jul. 2001	JAI 41 para. 43 (a)(I) CRIMORG 80, rec. 30
Netzwerk zur illegalen Immigration - Kooperation bei Ermittlungen	31. Dez. 2000 31. Dez. 2001	JAI 41 para. 43 (a)(iii) CRIMORG 80, rec. 26
Verstärkter Austausch von Informationen zur Bekämpfung von Terrorismus	31. Dez. 2000 31. Jul. 2001	JAI 41 para. 43 (a)(iv) CRIMORG 80, rec. 33
Erweiterung der Kompetenzen von Europol	31. Dez. 2000 31. Jul. 2001	JAI 41 para. 43 (a)(v) CRIMORG 80, rec. 34

Zugang zu SIS	31. Dez. 2000 31. Dez. 2001 31. Dez. 2003 (Überprüfung)	JAI 41 para. 43 (c) CRIMORG 80, rec. 36
Entwicklung einer Rolle von Europol Betreffs des Informationsaustausches mit PAPEG-Staaten	31. Dez. 2000 31. Jul. 2001	JAI 41 para. 43 (d) CRIMORG 80, rec. 65
Überlegung, unter welchen juristischen Voraussetzungen Strafverfolgungsbehörden im Territorium eines anderen Mitgliedstaates operieren können	31. Dez. 2000	JAI 41 para. 44 (b) Art. 32 TEU
Operative und technische Kooperation; Europol dient als Back-Up für künftige Initiativen; Standards für Ermittlungen	31. Dez. 2000 31. Dez. 2002	JAI 41 para. 44 (c) CRIMORG 80, rec. 27
Situationsbericht zu organisiertem Verbrechen; Harmonisieren von Analyseparametern; Identifizierung entstehender Trends	31. Dez. 2000 laufend	JAI 41 para. 44 (d) CRIMORG 80, rec. 1
Implementation von ZIS und Neapel II	31. Dez. 2000	JAI 41 para. 44 (e)
Fördern von Verbindungsvereinbarungen zwischen Staatsanwälten und Ermittlern	01. Okt. 2003 31. Dez. 2002	JAI 41 para. 48 (a)(I) CRIMORG 80, rec. 50 Art. 30(2)(c)TEU
Entwickeln eines Forschungs- und Dokumentationsnetzwerkes	01. Okt. 2003 31. Dez. 2003	JAI 41 para. 48 (a)(ii) CRIMORG 80, rec. 32 Art. 30(2)(d)TEU
Verbesserung der Statistik "grenzüberschreitende Verbrechen"	01. Okt. 2003 31. Dez. 2000	JAI 41 para. 48 (a)(iii) CRIMORG 80, rec. 2 Art. 30(2)(d)TEU
Aufsetzen eines Informations- und Analysesystems zur Geldwäsche	01. Okt. 2003 31. Dez. 2001	JAI 41 para. 48 (a)(iv) CRIMORG 80, rec. 41
CIS-Zugang	1. Okt. 2003	JAI 41 para. 48 (a)(v)

Medieninformationsstrategie	01. Okt. 2003 31. Dez. 2003	JAI 41 para. 48 (a)(vi) CRIMORG 80, rec. 37
Austausch von elektronischen Fingerabdrücken	01. Okt. 2003 31. Dez. 2003	JAI 41 para. 48 (a)(vii) CRIMORG 80, rec. 38
Training von Strafverfolgungspersonal	31. Dez. 2003	JAI 41 para. 48 (b)(iii) CRIMORG 80, rec. 29
Studie zur möglichen Rolle von Europol bei der Koordination internationaler Ermittlungen und Task-Forces zur Bekämpfung krimineller Organisationen	31. Jul. 2001	CRIMORG 80, rec. 31
Rolle und Ort von Justizbehörden im Rahmen der Entwicklung von Europol	31. Jul. 2001	JAI 41 para. 45 (g) CRIMORG 80, rec. 63
Integration antragstellender Länder im jährlichen Situationsbericht über organisiertes Verbrechen	laufend	CRIMORG 80, rec. 66
Engere Kooperation mit Drittstaaten und internationalen Organisationen und Organen	laufend	CRIMORG 80, rec. 71

Links

[1] <http://www.europol.eu.int/>

[2]

http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=DOC/99/14|0|AGED&lg=DE

[3] <http://usinfo.state.gov/topical/econ/g8okin/presumfi.htm>

[4] <http://usinfo.state.gov/topical/econ/g8okin/trmoney.htm>

[5] <http://www.oecd.org/fatf/>

[6] <http://www.oecd.org/fatf/pdf/NCCT2000-en.pdf>

[7] <http://de.news.yahoo.com/000623/11/y1b9.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/8374/1.html>

Telepolis erhält für Enfopol-Berichterstattung den Europäischen Preis für Online-Journalismus

06.07.2000

Gewürdigt wird Telepolis in der Kategorie "Investigative Reporting"

Telepolis erhält für seine Enfopol-Berichterstattung den Europäischen Preis für Online-Journalismus der Medien-Konferenz Net-Media 2000 [1] in der Kategorie "Investigative Reporting".

Der Preis wird in verschiedenen Kategorien von einer Jury verliehen, deren Mitglieder aus 15 europäischen Ländern kommen. Gesponsort wird der Preis unter anderem von Reuters, News Network, AOL Europe und Chello. Verliehen wird der Preis am Donnerstag in London, um 19.00 Uhr im Oliver Thompson Lecture Theatre, City University, Northampton Square, London EC1.

Armin Medosch wird den Preis für die Redaktion entgegen nehmen. Medosch: "Wir konnten nur deshalb so gut über Enfopol berichten, da verschiedene europäische Journalisten und Gruppen wie die britische Bürgerrechtsorganisation Statewatch und der österreichische Bürgerrechtsverein Quintessenz zusammen an dem Thema arbeiteten."

Die freien Telepolis-Autorinnen und -Autoren Christiane Schulzki-Haddouti in Deutschland, Erich Möchel in Österreich, Duncan Campbell in Großbritannien, Jelle van Buren in den Niederlanden sowie die Telepolisredakteure Armin Medosch in London und Florian Rötzer in München berichten seit 1998 über die geplante europaweite Überwachung für Internet und andere neue Technologien.

Telepolis veröffentlichte erstmals im November 1998 diverse unter Verschluss gehaltene Arbeitspapiere der Ratsarbeitsgruppe "Polizeiliche Zusammenarbeit", die ihre Dokumente unter dem Kürzel Enfopol ("Enforcement Police") publiziert. Die im Internet veröffentlichten Enfopol-Papiere sorgten bei europäischen Datenschützern und Politikern, aber auch Bürgerrechtsorganisationen für Aufsehen:

Der deutsche SPD-Bundestagsabgeordnete Jörg Tauss warf Vertretern der Bundesregierung vor, Dokumente zurückzuhalten und eine öffentliche Diskussion des Vorhabens zu verhindern. "Mit bewussten Falschinformationen sogar gegenüber Parlamentariern" würden die Eingriffsbefugnisse der Sicherheitsbehörden unzumutbar ausgeweitet.

Im Mai 1999 vertagten die Innen- und Justizminister der Europäischen Union die

Entscheidung über eine entsprechende Ratsentschließung. Sie erklärten, dass die Verschiebung nicht wegen sachlicher Vorbehalte erfolge, wolle man doch erst eine öffentliche Diskussion in den Mitgliedsländern eröffnen. Das Thema sollte dann erneut im Herbst auf die Agenda gesetzt werden.

Im Frühjahr diesen Jahres wurde ein internes Arbeitspapier der Arbeitsgruppe vom 18. Oktober 1999 bekannt, aus dem hervorging, dass überlegt wurde, ob aufgrund der negativen Presse die Mitgliedstaaten in Form einer Pressemitteilung reagieren sollten: "Mehrere Delegationen mahnten hinsichtlich der Vorbereitung einer Pressemitteilung zur Vorsicht und merkten an, dass dies eine Kettenreaktion und weitere negative Presse in den Medien provozieren könne". Telepolis-Redakteur Florian Rötzer bezeichnete dies "als Kompliment für unsere Arbeit."

Bis heute sind keine weiteren Veröffentlichungen der Enfpopol-Arbeitsgruppe bekannt geworden, ebenfalls wurde keine Ratsentschließung verabschiedet. Dennoch wurden im europäischen Rechtshilfeabkommen, über das Telepolis ebenfalls laufend berichtete, die rechtlichen Voraussetzungen für das grenzüberschreitende Abhören von Telekommunikation geschaffen, darunter auch Satellitentelefonie.

Links

[1] <http://www.net-media.co.uk/eolja/>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6892/1.html>

Die Globalisierung der Überwachung

Thomas Mathiesen 20.06.2000

Schengen, Europol, Eurodac und die EU-FBI-Überwachungspläne.

Verwaltungsregister wurden in der europäischen Geschichte nicht nur benutzt, um Einzelne, sondern auch ganze Bevölkerungsgruppen zu erfassen. Das Schicksal der Juden und anderer Bevölkerungsgruppen in den 30er und 40er Jahren ist nur ein Beispiel unter vielen.

So sollen deutsche Besatzungstruppen in Norwegen während des Zweiten Weltkriegs verschiedene Bevölkerungsregister benutzt haben, die zu unterschiedlichen Zwecken eingerichtet wurden, um norwegische Juden zu verfolgen. Über 50 Prozent der 1400 Juden in Norwegen waren 1942 ausgelöscht, in Dänemark waren es hingegen nur 1 Prozent von 5600.

Warum war der Prozentsatz in Norwegen so viel höher? Dafür gibt es mehrere Gründe: Unter anderem hatte Norwegen Register, die sich ganz speziell auf Juden bezogen. Die norwegische Verfassung von 1814 untersagte den Zuzug von Juden nach Norwegen. 1851 wurde das Verbot aufgehoben, dafür wurde jedoch ein eigenes Register eingerichtet: Ab 1866 registrierte das norwegische Büro für Volkszählung die Juden als eigene Bevölkerungsgruppe.

Für die deutsche Besatzungsmacht war die Volkszählung nützlich, auch für die norwegischen Nazis. Auch das Register des norwegischen Radioamtes erwies sich als nützlich: Gleich nach der deutschen Invasion 1940 ordneten die deutschen Behörden an, alle Radios, die Juden in der Hauptstadt gehörten, zu beschlagnahmen. Für diesen Zweck konnte das Register des Radioamtes genutzt werden. Folglich konnten auch die Juden selbst so ermittelt werden.

Verwaltungsregister können von unkontrollierten Polizeikräften missbraucht werden, aber auch von der politischen Obrigkeit, wenn der politische Wind aus der richtigen Richtung weht und die Zeit reif ist - wie es im Fall von Norwegen während des Zweiten Weltkriegs der Fall war. Die neuen, technisch extrem innovativen, kombinierbaren, versteckten, grenzüberschreitenden, unkontrollierbaren datenbasierten Registriersysteme, die sich derzeit entwickeln, stellen eine enorme Gefahr dar, die von niemandem ignoriert werden kann, der sich mit der Kontrolle von Polizei und Politik beschäftigt.

Ich werden mit dem Schengen-System beginnen, da es bereits recht gut funktioniert. Andere Systeme hingegen sind noch im Planungs-, Entwurfs- oder Ratifizierungsstadium.

Die zentrale Bedeutung von Schengen wird sich verringern, wenn diese anderen Systeme an den Start gehen. Besonders Europol, mit seinem Europol-Computersystem wird vermutlich eine Führungsrolle einnehmen.

Schengen

1985 trafen Deutschland, Frankreich und die Benelux-Staaten eine Vereinbarung in der kleinen Stadt Schengen in Luxemburg. Die Vereinbarung zielte auf die gegenseitige Anerkennung von Visa und eine verstärkte polizeiliche Zusammenarbeit. Der Hauptpunkt der Vereinbarung bestand darin, die nationalen Grenzkontrollen zwischen den Ländern abzubauen, während gleichzeitig entlang der Außengrenzen die Kontrollen verstärkt werden sollten.

1990 trafen dieselben Länder ein neues Abkommen, wieder in Schengen. Dieses Abkommen ist als Schengen-Konvention bekannt und es erfüllt die Vereinbarungen von 1985. Es regelt eine Reihe kritischer Fragen zu Grenzkontrollen und grenzüberschreitenden Fahndungen sowie zum grenzüberschreitenden Datenaustausch einschließlich der Erfassung von Personen und Objekten. Das Abkommen ermöglicht eine weitreichende Erfassung und Überwachung großer Bevölkerungsgruppen in den betroffenen Ländern. Italien, Spanien, Portugal, Griechenland und Österreich schlossen sich der Vereinbarung an. Großbritannien und Irland hielten sich zunächst zurück, da sie ihre nationalen Grenzkontrollen beibehalten wollen. Am 20. Mai 1999 bat Großbritannien formel darum, am SIS teilnehmen zu können, Irland folgte kurze Zeit später.

1999 ergab sich eine wichtige Veränderung. Am 1. Mai trat der Amsterdamer Vertrag in Kraft, der von den EU-Außenministern am 2. Oktober 1997 unterzeichnet worden war. Mit ihm wurde das Schengen-System in die EU-Strukturen, teilweise in den ersten Pfeiler, teilweise in den dritten Pfeiler integriert. Der Schengen-Exekutivausschuss wurde durch den Rat für Justiz und Inneres ersetzt.

Diese Integration erweitert den Einfluss verschiedener Schengen-Vereinbarungen wie die datenbasierte Erfassung und das Überwachungssystem. Hinzu kommt, dass sich nun die ganze Schengen-Organisation auf Hunderte von EU-Einrichtungen und Arbeitsgruppen verteilt und sich in Zehntausenden von EU-Dokumenten niederschlägt. Damit werden die Schengen-Aktivitäten, die bereits vorher nur sehr schwer zu verfolgen waren, künftig noch schwieriger zu untersuchen und zu kritisieren sein - zumindest für Außenstehende. Die nordischen EU-Mitgliedsstaaten - Finnland, Schweden und Dänemark - haben ebenfalls Schengen ratifiziert, die nordischen Nicht-EU-Mitgliedsstaaten - Norwegen und Island - haben eine so genannte Kooperationsvereinbarung mit der EU abgeschlossen.

Aufgrund von Schengen entsteht ein weitreichendes System und Netzwerk polizeilicher

Zusammenarbeit, Datenerfassung und Überwachung - von Island im Norden bis zum Mittelmeer im Süden, von der Spitze von Portugal im Westen bis zur deutsch-polnischen Grenze im Osten. Das ist zu Beginn des Jahres 2000 eine Realität. Da das Schengen-Abkommen die Grenzkontrollen an den gemeinsamen Außengrenzen verstärkt, ermöglicht es verschiedene Arten verdeckter Polizeiaktionen, dazu gehört auch die grenzüberschreitende Kooperation. So autorisiert Artikel 40 die Observation über nationale Grenzen hinweg bei Personen "die unter dem Verdacht stehen eine Straftat begangen zu haben".

Das Schengen-Informationssystem (SIS)

Mit dem Schengen-Informationssystem (SIS) verfügen europäische Strafverfolger bereits über ein einheitliches und erfolgreiches polizeiliches Fahndungsinstrument. Das SIS hat ein Gesamtvolumen von rund 9,5 Millionen Fahndungsdatensätzen, Tendenz steigend. Dabei handelt es sich überwiegend um Sachfahndungsausschreibungen. In der Personenfahndung sind derzeit 10.000 Straftäter zur Festnahme zwecks Auslieferung und circa 750.000 zur Einreiseverweigerung ausgeschrieben.

Nach Auskunft von Klaus-Henning Schapper, Staatssekretär im Bundesinnenministerium, konnten 1998 "rund 8.500 Fahndungstreffer aufgrund deutscher Ausschreibungen in anderen SIS-Teilnehmerstaaten registriert werden". Umgekehrt führten die Fahndungsnotierungen anderer Schengen-Staaten zu "über 4.600 Treffern in Deutschland". Nach Ansicht von Schapper müssen sich künftig "Schengen und Interpol im Bereich der Fahndung ergänzen". Für ihn ist es "wichtig, dass der geplante Zusammenarbeitsvertrag zwischen Europol und Interpol zügig vorangebracht wird". Europol, die G-8-Staaten und die Financial-Action-Task-Force (FATF) planen, künftig Informationen über verdächtige Geldwäschetransaktionen aufeinander abzustimmen.

Das Schengen-Informationssystem hat eine zentrale Datenbank in Straßburg, sowie nationale SIS-Datenbanken in allen Schengen-Staaten. In allen Datenbanken sind dieselben Daten gespeichert. 1995 hatten 30.000 Computer in den sieben Schengen-Staaten Online-Zugang über ihre nationalen SIS-Datenbanken zum Schengen-Informationssystem. 1997 gab es nach Angaben des Statewatch European Monitor¹ in den neuen Schengen-Staaten bereits 48.700 Zugangsknoten. Am 26. März 1996 wurden nahezu 3,9 Millionen Datensätze gespeichert. Deutschland und Frankreich waren die Hauptnutzer. Informationen über Hunderttausende von Personen wurden gespeichert, damals wurde die Kapazität des Systems auf neun Millionen Einträge geschätzt. Für jedes folgende Jahr stiegen die Zahlen: Von 5,6 Millionen 1997 bis zu 8,8 Millionen 1998.²

Erweiterungen wie die Integration der nordischen Länder in das System sind geplant. In einem Bericht des deutschen Innenministeriums von 1997 wird folgendes über die

Integration der nordischen Staaten gesagt:

"Es wurde beschlossen, das SIS komplett einem Redesign zu unterwerfen, um die fünf nordischen Staaten zu integrieren. Der Integration der nordischen Staaten wird eine zweite technische Generation des SIS folgen. Dieses neue SIS II wird so ausgelegt, dass die Integration künftiger Mitgliedstaaten jederzeit technisch möglich sein wird."

Sirene

Das SIS ist nur ein System für den Informationsaustausch in Schengen, das andere System heißt Sirene, eine Abkürzung für *Supplément d'Information Requis a l'Entrée Nationale*. Sirene soll den bilateralen und multilateralen Austausch erleichtern sowie ergänzende Informationen über Personen und Objekte, die im SIS registriert sind, liefern. Über das Sirene-System können Polizeibehörden in einem Land über eine Person, die im SIS eines anderen Landes registriert ist, zusätzliche Ergänzungsinformationen anfordern. Das SIS speichert ziemlich begrenzte und standardisierte Informationen. Die nationalen Sirene-Einheiten können hingegen mit weitreichenden, nicht-standardisierten Informationen oder "weichen" Daten umgehen. Auch von den Leuten, die in den Sirene-Büros arbeiten, wird explizit betont, dass solche Informationen sehr unpräzise sein können und nahezu alles beinhalten können. Der Direktor des portugiesischen Sirene-Büros sagte im norwegischen Fernsehen über das Sirene-System im März 1997 folgendes:

"Die Konvention bestimmt, wer Zugang zu dem System hat. Generell hat die Polizei Zugang. Sie sind natürlich auf Flughäfen und in Seehäfen und können Mobiltelefonate abhören. Jederzeit haben sie zu den Informationen Zugang. (...) Es ist ein schnelles System. Es ist auf dem neuesten Stand. Es gibt Massen von Informationen. Und natürlich ist das System effizienter als das traditionelle Interpol-System."

Informationen über Sirene werden in der Arbeitssprache Englisch ausgetauscht. Da es nicht die Sprache des Schengen-Landes ist, wird es "Schenglisch" genannt. Das Sirene-System formalisiert und legitimiert den Informationsaustausch zwischen den Polizeibehörden in den verschiedenen Staaten. Es gibt ein umfassendes Handbuch das, wie bereits zuvor erwähnt, geheim gehalten wird. Teile des Handbuches wie auch Zusammenfassungen sickerten an die Öffentlichkeit heraus und wurden bereits veröffentlicht.³ Laut Handbuch kann die Kommunikation zwischen den Sirene-Büros mündlich oder schriftlich erfolgen, aber auch über Bilder (Fotos, Fingerabdrücke). Der Text- und Bilderaustausch erfolgt über das Sirene-eigene Email-System, für die mündliche Kommunikation wird das Telefon benutzt. Die Sirene-Büros sollen Anfragen "so schnell wie möglich" beantworten: "Die Zeit sollte zwölf Stunden nicht

überschreiten".⁴

Zu den übermittelten Informationen gehören laut Artikel 46 des Schengen-Abkommens alle Informationen "von Interesse, um *künftige* Verbrechen zu verhindern und Straftaten gegen oder *Bedrohungen* der öffentlichen Ordnung und Sicherheit zu verhindern" (kursiv durch Autor). Dies bedeutet, dass kein konkreter Verdacht vorliegen muss. Der Artikel ermöglicht den bilateralen und multilateralen Austausch von Informationen bei sehr diffusen Angelegenheiten, die sicherlich auch politische Aktivitäten beinhalten, wenn sie als Bedrohung definiert werden. Wie auch das SIS wird das Sirene-System ständig erweitert. Das Arbeitsprogramm des deutschen Schengen-Vorsitzes im Herbst 1998 sah vor, "den Informationsaustausch auf der Basis der endgültigen Implementierung des Sirene-Netzwerkes, Phase II, zu modernisieren und zu beschleunigen".

Präventive Verbrechensbekämpfung?

Die norwegischen Behörden haben mehrmals behauptet, dass der Zweck von Schengen die Bekämpfung herkömmlicher, schwerer, internationaler Verbrechen ist. Auch die Schengen-Behörden selbst haben beispielsweise im Arbeitsprogramm des österreichischen Schengen-Vorsitzes im Herbst 1997 die Bekämpfung des internationalen Verbrechens hervorgehoben. Die Fakten sehen jedoch anders aus. Statistische Informationen aus Deutschland sowie statistische Informationen und Berichte von Schengen zeigen, dass das Schengen-System zu einem großen Ausmaß sich mit Identitätsausweisen und unerwünschten Ausländern beschäftigt, wie beispielsweise Asylsuchenden, denen die Einreise verweigert wurde und die in den Untergrund gegangen sind.

Die Zahlen zeigen, dass die Schengen-Grenzkontrolle hinsichtlich des organisierten Schleusertums komplett versagt. Von 563.423 Kontrollmaßnahmen an den Außengrenzen bezogen sich 41 Prozent auf die Einreiseverweigerung von Drittstaaten, 28,5 Prozent auf Bürger von Drittstaaten ohne Aufenthaltsgenehmigung nahe der Grenze, 24,5 Prozent auf die Rückkehr von Drittstaaten-Bürger in Drittländer, 3 Prozent auf Drittstaaten-Bürgern mit Besitz gefälschter Dokumente und lediglich 0,5 Prozent auf festgenommene Schleuser. Obwohl auch Inländer vom Schengen-System betroffen sind, werden Ausländer vermutlich in der Zukunft die Hauptbedrohung für die öffentliche Ordnung und die Staatssicherheit darstellen: Die muslimische "Bedrohung" beispielsweise stellt "einen neuen Feind" nach dem Untergang der Sowjetunion und dem Verschwinden "der kommunistischen Bedrohung" dar. Aus diesem Grund wurde Schengen auch als "Festung Europa" bezeichnet.

Der "Entwurf des Schengen-Handbuchs zur polizeilichen Zusammenarbeit zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit" lässt auf eine stärkere Kooperation in der Zukunft schließen. So können Polizeibehörden "gemeinsame Kommando- und Koordinationszentren" einrichten.

In der Erklärung des Exekutiv-Komitees vom 16. September 1998 wird dasselbe angedeutet: So wird die Schengen-Zentralgruppe angewiesen "zu untersuchen, ob die Beratung und Unterstützung durch die Beamten eines Vertragsstaates im Rahmen der Kontrollen der Außengrenzen durch einen anderen Vertragsstaat die Sicherheit der äußeren Schengen-Grenzen verbessern würde" und "falls notwendig schnell einen Plan zu entwerfen für eine entsprechende Entsendung von Verbindungsoffizieren an die Außengrenzen". Im Klartext bedeutet dies, dass beispielsweise ein deutscher Verbindungsoffizier entlang der italienischen Küste stationiert werden kann. Offensichtlich besteht der nächste logische Schritt darin, eine gemeinsame Polizeieinheit an den Schengen-Grenzen zu installieren, die mit der Umsetzung des Amsterdamer Vertrages möglicherweise in das entstehende Polizeikorps von Europol integriert werden kann.

Zwar gibt es das Schengen-System erst seit einigen Jahren, aber es gibt bereits konkrete Beispiele dafür, dass das System direkt für politische Zwecke eingesetzt wurde. So wurde im September 1998 einer Greenpeace-Aktivistin, die gegen die französischen Atombombentests 1995 protestiert hatte und von Frankreich als unerwünscht deklariert wurde, die Einreise in die Niederlande verweigert. Sie wurde im Amsterdamer Flughafen Schiphol festgehalten. Grund: Sie war zu einer "unerwünschten Ausländerin" laut Artikel 96 des Schengen-Abkommens erklärt worden.⁵

Ein weiteres Beispiel: Während des EU-Gipfels in Amsterdam im Juni 1997 gab es politische Demonstrationen. Nach Angaben der Polizei wurden 609 Personen verhaftet. Tatsächlich wurden mehr Leute in Haft genommen, darunter auch eine Gruppe von Italienern, die verhaftet und abgeschoben wurde. 29 Dänen wurden verhaftet und nach Dänemark mit Hilfe eines Militär-Flugzeuges abgeschoben, das von einem Kampfflugzeug eskortiert wurde. Die dänische Konsulin in Amsterdam protestierte, da es ihr nicht erlaubt war, die in Gewahrsam genommenen Dänen zu besuchen. Mehrere schwedische Bürger wurden ebenfalls abgeschoben. Später wurde Opfern von Polizeibrutalität Schadensersatz gewährt. Für dieses Beispiel können wir nicht ohne Zweifel dokumentieren, ob das Schengen-Informationssystem oder das Sirene-System benutzt wurden oder ob Demonstranten in diesen Systemen für spätere Zwecke registriert wurden.

Es ist höchstwahrscheinlich, dass eine Registrierung stattfand, da die Demonstrationen direkt gegen zentrale Einrichtungen der EU gerichtet waren. Beobachter sahen diese Polizeiaktionen, die auch unter Einsatz von Helikoptern und gepanzerten Fahrzeugen durchgeführt wurden, als groß angelegtes Trainingsmanöver zum Schutz der mächtigen EU-Institutionen.

Datenschutz?

Die Sirene-Büros in den verschiedenen Ländern verwalten auch die nationalen SIS-Datenbanken. Soweit es Sirene betrifft, gibt es keine allgemein gültigen Datenschutzregelungen, da Sirene ja nicht einmal im Schengen-Abkommen erwähnt wird. Dies wurde auch als ernster Fehler von der "gemeinsamen Supervisionsbehörde" (Joint Supervisory Authority - JSA) bezeichnet. Für SIS gibt es allerdings spezielle Datenschutzregelungen im Abkommen.

Bei der JSA handelt es sich um eine Behörde zur Kontrolle des SIS. Tatsächlich verfügt sie praktisch über keine Kontrollmöglichkeiten und kann keine Sanktionen verhängen. In einer Anhörung des norwegischen Parlaments sagte Georg Apenes, Direktor der norwegischen Überwachungsbehörde, dass das JSA nicht einmal über ein Telefon verfüge. In ihrem ersten Bericht von 1997, der den Zeitraum von März 1995 bis März 1997 behandelte, sprach die JSA auch das Problem des sogenannten "SIS-Super-User" an: Dabei handelt es sich um Nutzer, die nicht nur Zugang zu jeder Datei im System haben, sondern die auch ohne Spuren zu hinterlassen Dateien verändern können. Die verschiedenen Datenschutzregelungen bezeichnete die JSA als "rechtliches Labyrinth". In ihrem zweiten Bericht von 1998 stellt die JSA fest, dass es "größere Schwierigkeiten hinsichtlich der Integrität" der Daten gäbe. Im November und Dezember 1997 zeigte ein Fall die fehlende Kontrolle der JSA über das SIS-System auf: Geheime Dokumente mit sensiblen persönlichen Daten wurden in einem belgischen Bahnhof gefunden. Die Dokumente waren jedem Passanten zugänglich. Auch wurde sensibles Material in einer Wohnung eines verhafteten Belgiers beschlagnahmt. Der dänische Justizminister Frank Jensen bezeichnete dies als "ernste Sicherheitslücke im SIS". Im Dezember 1997 kündigte die belgische Schengen-Präsidentschaft schließlich an, "den Datenschutz zu einer Priorität" zu machen.

Weitere Systeme

Schengen ist nicht das einzige europäische Informationssystem. In den 90er Jahren gab es eine ganze Reihe weiterer Vorschläge, Entwürfe und tatsächlicher Einrichtungen von Registrierungs- und Überwachungssystemen in Europa. Der Überwachungsstaat wird bald zur Realität. Schengen scheint ein Kernsystem zu sein, auf das sich andere Systeme beziehen. Dazu gehören das Eurodac-System, EIS sowie die Europol-Datenbank.

Das Dublin-Abkommen, das sich auf Asylfragen beschränkt, führt zur Einrichtung des so genannten Eurodac-Registers. Eurodac speichert die Fingerabdrücke von Asylsuchenden, aber auch andere persönliche Daten. Es soll zu einem "europäischen Zentralregister" werden. Geplant ist eine Registrierung aller Asylsuchenden über 14 Jahren in allen EU-Mitgliedsstaaten. Die Fingerabdrücke sollen bis zu zehn Jahre gespeichert werden können. Falls eine Person Bürger eines Mitgliedstaates wird, sollen die Dateien gelöscht werden.

Auch die Dateien von Flüchtlingen, denen ein Flüchtlingsstatus nach dem UN-Flüchtlingsabkommen gewährt ist, sollen vom allgemeinen Gebrauch ausgeschlossen werden und nur für statistische Zwecke verwandt werden dürfen.

Bei seiner Sitzung am 3. und 4. Dezember 1998 kam der Rat für Justiz und Inneres zu der Übereinkunft, dass Schengen, ungeachtet der Integration von Schengen in die EU-Strukturen über den Amsterdamer Vertrag, durch Eurodac unterstützt werden wird. Dies bedeutet, dass das Dublin-Abkommen die Asylregeln von Schengen bereits ersetzt hat. Es gibt einige weitere klare Hinweise auf eine klare Integration: Kürzlich wurde vorgeschlagen, dass Eurodac auch die Fingerabdrücke von so genannten illegalen Immigranten und nicht nur von Asylsuchenden speichern darf. Möglich ist der elektronische Austausch von Fingerabdrücken über das Sirene-Netzwerk.

Parallel zu Eurodac entwickelte eine Arbeitsgruppe in der EU ein europäisches zentrales Computersystem innerhalb des Generalsekretariats des Rats für Justiz und Inneres, um Bilder zu speichern und auszutauschen. Das System heißt FADU (falsche und authentische Dokumente). Laut einem Memo aus dem dänischen Innenministerium vom Dezember 1998 "wird das System auf Internet-Technologie basieren und über eine zentrale Datenbank in jedem Mitgliedstaat über eine sichere Internetverbindung benutzt werden. In Dänemark wird die Nationalpolizei darüber verfügen". Bis heute ist Eurodac als "Europäisches Zentralregister" in der europäischen Geschichte beispiellos. Es beinhaltet die langfristige beziehungsweise ständige Registrierung und Überwachung von großen Bevölkerungsgruppen in Europa.

Seit dem 1. Juli 1999 ist Europol eine gemeinsame Polizeieinheit innerhalb der EU (siehe auch "Computer - Daten - Macht" [1]). Im Gegensatz zu Schengen zielt Europol auf das internationale organisierte Verbrechen. Die Europol-Computersysteme bestehen aus drei Untersystemen: Erstens ist es das zentrale Informationssystem, in das Daten über verdächtige Personen, sowie Personen, die möglicherweise künftig Verbrechen begehen könnten, eingegeben werden. Zweitens gibt es Arbeitsdateien zum Zwecke der Analyse. Diese Dateien können nicht nur ausführliche persönliche Daten, sondern auch mögliche Zeugen, Opfer und mögliche Opfer, Kontaktpersonen und Verbündete sowie Informanten beinhalten. Drittens gibt es ein Indexsystem, das darüber Auskunft gibt, ob eine Information gespeichert ist. Selbst diejenigen, die innerhalb des Europol-Systems heute arbeiten, geben Probleme offen zu. So sagte der assistierende Koordinator der Europol Drogeneinheit (EDU - Einheit, die vor Europol eingerichtet wurde) W. Bruggemann folgendes:

"Die Vorkehrungen zum Datenschutz sind in der Theorie umfangreich, sie werden aber fatalerweise durch die Schwierigkeit, sie in die Praxis umzusetzen, unterminiert. Innerhalb der Union hängt das System erheblich davon ab, in welchem Grade Datenschutz und Bürgerrechte von jedem einzelnen Polizeibeamten respektiert werden. Das erfordert nicht nur rigoroses Training, aber auch in vielen Fällen einen radikalen Kulturwandel bei den nationalen Polizeikräften. [...] Wenn hier der Eindruck hinzu kommt, dass manche Polizeibeamte der Ansicht sind, dass bei der Verbrecherjagd die Resultate die Mittel rechtfertigen, ist die potenzielle Gefahr offensichtlich."⁶

Verschärft ist die jüngste Entwicklung: Der Rat für Justiz und Inneres autorisierte auf seiner Sitzung am 27. März 2000 Europol-Verhandlungen für den Datenaustausch mit nicht-europäischen Ländern und Behörden aufzunehmen. An erster Stelle stehen hier die Verhandlungen mit Interpol, an zweiter die Verhandlungen mit Ländern wie Kanada, Island, Norwegen, Russland, der Schweiz, der Türkei und den USA sowie Bolivien, Kolumbien, Marokko und Peru. (siehe auch: Europol will mit Kolumbien und Russland Daten austauschen [2])

Globale Überwachungssysteme

Schließlich gibt es eine internationale Kooperation bei der Überwachung von Telekommunikation. Zum einen gibt es das Echelon-System, das der "Militär-Geheimdienst-Gemeinde" dient und ein neues System, das für die Strafverfolger-Gemeinde geplant ist. Das System, das Telefonanrufe, E-Mails und Faxe überwachen soll, wurde bislang mit unterschiedlichen Namen wie Enfpopol, Quantico-Gruppe oder ILETS bezeichnet. Ich werde es nach Tony Bunyan von Statewatch [3] als EU-FBI-Telekommunikationsüberwachungssystem, beziehungsweise EU-FBI-System bezeichnen.

Im November 1995 unterzeichneten die EU-Staaten ein "Memorandum of Understanding" [4]. Darin heißt es, dass Strafverfolgungsbehörden Telekommunikationsüberwachungsmaßnahmen in Realzeit rund um die Uhr durchführen können müssen. Auch Verkehrsdaten müssen in Realzeit zur Verfügung gestellt werden.

Wie bereits erwähnt, handelt es sich bei dem Memorandum um ein EU-Dokument. Das Schengen-Abkommen berücksichtigt das Abhören von Telekommunikation nicht. Sirene speichert jedoch bereits Informationen, die beim Abhören von Handys gewonnen wurden. Mit der Integration von Schengen in die EU-Strukturen wird das grenzüberschreitende Abhören auf der rechtlichen Basis eines Memorandums ermöglicht. Es wird keine Trennung mehr zwischen EU-Vereinbarungen und Schengen-Vereinbarungen geben.

1993 veranstaltete das amerikanische FBI eine internationale Konferenz in der FBI-Akademie in Quantico. Elf Länder innerhalb und außerhalb der Europäischen Union

nahmen an der Konferenz teil. Seither arbeiten diese Staaten daran, die Anforderungen für das Abhören seitens der Strafverfolgungsbehörden zu standardisieren. Das Treffen in Quantico führte zur Gründung des so genannten International Law Enforcement Seminar, ILETS [5]. Diese Ilets-Gruppe, wurde nach und nach vergrößert und zählte 1995 20 Länder: Die 15 EU-Staaten sowie die USA, Kanada, Hongkong, Australien und Neuseeland. Das Quantico-Treffen, das auf die Initiative des FBI zurückgeht, und später die ILETS-Treffen der EU ebneten den Weg für ein globales Überwachungssystem der Telekommunikation: Das EU-FBI-System. Das neue europäische Rechtshilfeabkommen [6] legitimiert die grenzüberschreitende Überwachung, aber auch die Überwachung der Schengen-Staaten.

1998 veröffentlichte Telepolis, dass das EU-FBI-System auf das Internet erweitert werden sollte. Die Pläne zeigen ganz klar, in welche Richtung die Polizei-Kooperation gehen wird. Fraglich ist, ob diese Pläne technisch machbar sind. Das so genannte Echelon-System, das bereits Realität ist, zeigt, dass sie es sind.

Die Echelon-Technologie zielt auf das Abhören von Telekommunikation per Satellit. Sowohl das EU-FBI-System, als auch Echelon können leicht teilweise oder ganz integriert werden: Die fortgeschrittene Echelon-Technologie verbreitet sich und wird bald auch seitens des EU-FBI-Systems angewandt werden können. Die technologischen Ähnlichkeiten überlappen und der Austausch von Personal lädt zur Integration ein. Seinerseits werden die Quantico-Entwicklungen einen ähnlich wichtigen Unterstützungspfeiler für die Anstrengungen innerhalb von Schengen mit SIS und Sirene sowie Europol darstellen.

Auf dem Weg zu einem integrierten System

Es gibt eine Tendenz hin zur Konvergenz und Integration zwischen den verschiedenen Registrier- und Überwachungssystemen in Europa. Der Amsterdamer Vertrag, der Schengen in die EU-Strukturen integriert, wird diese Entwicklung beschleunigen. Ein in die EU-Strukturen verschwundenes Schengen wird nicht weiter über eigene Entscheidungsstrukturen verfügen, sodass die Verschmelzung mit Europol, Eurodac und anderen Systemen näherliegt. Am Horizont können wir die Konturen eines weitreichenden, zunehmend integrierten, multinationalen Registrier- und Überwachungssystems ausmachen, dessen Informationen sich mehr oder weniger frei zwischen den Subsystemen bewegen und große Bevölkerungsgruppen abdecken.

Natürlich würde auch eine volle technische Integration in dem Sinne, dass jeder Polizeibeamte Zugang zu jedem Informationsbit haben würde, die Geheimhaltung unterminieren. Von der Geheimpolizei beispielsweise in Norwegen wird dies als Problem erkannt. Dies wird dazu führen, dass spezielle Abteilungen sich mit speziellen Themen beschäftigen, aber mit wichtigen Personen zwischen den verschiedenen Abteilungen auf

verschiedenen Wegen kooperieren.

Ausgehend von den heutigen SIS-Zahlen müssen wir damit rechnen, dass Millionen Personen in einem mehr oder weniger integrierten System gespeichert werden. Eine Minderheit wird aufgrund vergangener Verbrechen registriert sein. Eine andere Minderheit aufgrund konkreter Verdachtsmomente. Eine große Mehrheit wird aus Leuten bestehen, die sich in extrem großen Kreisen um solche Personen bewegen, sowie Personen, die in einem difusen Sinne als Bedrohung der öffentlichen Ordnung und Staatssicherheit betrachtet werden sowie unerwünschte Ausländer.

Das Schengen-System sowie das geplante Europol-Computersystem werden in dem integrierten System eine zentrale Rolle spielen. Zu den Anfangsproblemen wird gehören, dass die gespeicherten Informationen zu umfangreich sind, sodass verschiedene Polizei- und andere Behörden mit einem "Information-Overload" zu kämpfen haben werden.

Die Notwendigkeit einer "alternativen Öffentlichkeit"

Doch das werden nur die Anfangsprobleme sein. Die Situation erfordert Widerstand. Das Schlüsselwort ist hier die "alternative Öffentlichkeit". Es geht darum einen alternativen öffentlichen Ort zu schaffen, wo gut begründete Kritik und ein von Prinzipien geleitetes Denken wichtige Werte repräsentieren. Dabei ist die Befreiung von der absorbierenden Kraft der Massenmedien nötig. Ebenso wichtig ist, dass Graswurzelbewegungen ihre Selbstachtung und den Glauben an sich erneuern. Schließlich müssen Intellektuelle wieder zu einem Verantwortlichkeitsgefühl finden.

Im Bereich der Strafrechtspolitik haben wir in Norwegen mit der Organisation KROM, dem norwegischen Verband für Strafrechtsreform, so etwas versucht. Über jährliche Konferenzen unter einer breiten Teilnahme verschiedener Berufsvertreter und Behörden sowie Seminare und andere Aktivitäten konnten wir ein Informations- und Meinungsnetzwerk in den relevanten Verwaltungs- und politischen Systemen aufbauen. Dasselbe könnte auch im Bereich der Überwachung getan werden: Kriminologen, Juristen und Sozialwissenschaftler sowie Lehrer, Journalisten, Musiker und Schauspieler könnten einen öffentlichen Raum für Kritik und Diskussion entwickeln. Sobald die Leute auch den Hintergrund der komplizierten Technologien erfahren, bekommen sie ein Gefühl, was vor sich geht und werden besorgt und engagieren sich.

Dies ist nur eine Möglichkeit, auf das Problem der Überwachung hinzuweisen. Es gibt natürlich auch andere Wege. Aber keiner dieser Wege ist breit und bequem. Schließlich möchte ich sagen, dass der entstehende Überwachungsstaat, der die demokratischen Strukturen unserer Gesellschaft, wie wir sie kennen, bedroht, eine ständige Herausforderung an uns, die wir uns politisch oder wissenschaftlich damit beschäftigen,

darstellt.⁷

Thomas Mathiesen, geboren 1933, ist seit 1972 Professor für Rechtssoziologie und lehrt an der Universität von Oslo, Norwegen. Er hat über 25 Bücher über Rechtssoziologie, Kriminologie, Mediensoziologie und politische Soziologie geschrieben, von denen auch einige ins Deutsche übersetzt wurden.

Literaturangaben

- 1) Statewatch European Monitor, Band 1, Nummer 1, 1998, Seite 30
- 2) Aus verschiedenen Ausgaben des Statewatch-Journals.
- 3) Fortress Europe?, Dezember 1996/Januar 1997
- 4) Seite 26 des Sirene-Handbuchs in der dänischen Übersetzung
- 5) Dagbladet, 7. September 1998
- 6) Bruggemann, W.: "Data Protection Issues in Interinstitutional Information Exchange: The Case of Criminal and Administrative Intelligence". Vortrag wurde auf dem 6. Schengen-Kolloquium des European Institute of Public Administration in Maastricht 1998 gehalten
- 7) Dieser Beitrag beruht auf dem von Statewatch im November 1999 veröffentlichten, im Juni 2000 aktualisierten Pamphlet von Thomas Mathiesen "On Globalisation of Control: Towards an Integrated Surveillance System in Europe"

Links

- [1] <http://www.heise.de/tp/deutsch/inhalt/te/1955/1.html>
- [2] <http://www.heise.de/tp/deutsch/inhalt/te/8213/1.html>
- [3] <http://www.statewatch.org>
- [4] <http://www.heise.de/tp/deutsch/special/enfo/6334/1.html>
- [5] <http://www.heise.de/tp/deutsch/special/enfo/6396/1.html>
- [6] <http://www.heise.de/tp/deutsch/special/enfo/8204/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6861/1.html>

Neue Zugriffsrechte auf private Kommunikation geplant?

Brigitte Zarzer 07.06.2000

Die Arbeitsgruppe "Lawful Interception" tagt wieder in London

In London trat gestern die Arbeitsgruppe "Lawful Interception" (SEC-LI) des European Telecom Standards Institute (ETSI [1]) erneut zusammen. Einem Bericht von Futurezone [2] zufolge dürfte dabei erneut das umstrittene IUR-Papier (International User Requirements) auf der Tagesordnung stehen.

Das Arbeitsgebiet der Experten umfasst im wesentlichen die Entwicklung von Standards für Abhörschnittstellen in digitalen Netzen. Brisant ist dabei die Diskussion um die Möglichkeiten des Zugriffs auf digitale Kommunikation durch verschiedene "gesetzlich ermächtigte Behörden", wie Polizei und Geheimdienste der EU-Staaten.

Das IUR-Papier wurde ohne Wissen des EU-Parlaments verhandelt. Als 1997 der Skandal aufflog, wurde das Konzept vorübergehend fallen gelassen. Der technische Report, ETR 331, verschwand aus der Öffentlichkeit. Erst 1998 tauchte das umstrittene Vorhaben wieder in den Medien auf, wozu Telepolis wesentlich beigetragen hat. Diesmal trug es den Namen ENFOPOL. Bürgerrechtsorganisationen initiierten im Internet Gegenkampagnen. Der öffentliche Druck wurde so stark, dass ENFOPOL vom EU-Parlament zu Fall gebracht wurde. Trotz Protest konnte allerdings das grenzüberschreitende Rechtshilfeabkommen Ende Mai verabschiedet werden (Europäisches Rechtshilfeabkommen verabschiedet [3]).

Offensichtlich wird aber an den Überwachungsplänen fleißig weiter gearbeitet. Die ETSI-Arbeitsgruppe SEC-LI, die primär den technischen Teil übernimmt, hat dieses Jahr noch einen dichten Terminplan.

Links

[1] http://www.etsi.org/sec/sec_li.htm

[2] <http://futurezone.orf.at/>

[3] <http://www.heise.de/tp/deutsch/special/enfo/8204/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6836/1.html>

Europäisches Rechtshilfeabkommen verabschiedet

Christiane Schulzki-Haddouti 30.05.2000

Trotz Kritik des Europäischen Parlaments keine Änderungen mehr an der Fassung vom 15. Mai. Präventions- und Schutzmaßnahmen sollen Missbrauch bei der Fernmeldeüberwachung ausschließen.

Wie Charles Elsen, Generaldirektor des Rates für Justiz und Inneres der Europäischen Union, gegenüber Telepolis bestätigte, wurde das Europäische Rechtshilfeabkommen am 29. Mai nachmittags unterzeichnet. An der Fassung vom 15. Mai [1] (Copen 32) wurde nichts mehr verändert. Bis zuletzt unterlag das Dokument der Geheimhaltung. Mit dem jetzt verabschiedeten Rechtshilfeabkommen sollen die bisherigen Rechtshilfeverfahren beschleunigt werden. Bisher waren sie auf bilaterale Kooperation ausgerichtet und in Fällen von Computerkriminalität zu langsam. Verabschiedet werden sollte das Übereinkommen bereits vor drei Jahren. Die Telefonvernehmung, das Fernabhören und die Bestimmungen über die gemeinsamen Ermittlungsgruppen wurden später noch eingebracht.

In einer Pressemitteilung gab der Rat nicht die Verabschiedung sondern seine "Schlussfolgerungen" bezüglich der Überwachung des Fernmeldeverkehrs bekannt: So habe der Rat "Gedanken" über die Erörterungen des Europäischen Parlaments [2] "ausgetauscht". Das Parlament hatte die Streichung des Paragraphen 18, der die "Überwachung von Personen im Hoheitsgebiet anderer Mitgliedstaaten ohne deren technische Hilfe" regelt, gefordert. Der Rat wies in diesem Zusammenhang darauf hin, dass die Menschenrechte und Grundfreiheiten, wie sie im Vertrag über die Europäische Union anerkannt wurden, gewahrt werden würden.

Keine Wirtschaftsspionage per Überwachungsschnittstelle?

Auch distanzierte er sich von dem Vorwurf, über einheitliche Überwachungsschnittstellen Wirtschaftsspionage zu ermöglichen. So stellte er fest, dass die TK-Überwachung "zwar ein wichtiges Instrument bei der Bekämpfung der Kriminalität oder bei der Verteidigung der nationalen Sicherheit darstellt", doch "auf keinen Fall für die Erlangung kommerzieller Vorteile genutzt" werden dürfe.

Der Rat verwies deshalb auf die Ankündigung der Europäischen Kommission "innerhalb eines Jahres nach Unterzeichnung ... ein sicheres System zur Übertragung der Abhörfragen sowie für die Übermittlung der abgehörten Kommunikation" auszuarbeiten (siehe auch Feinschliff am Abhörstandard [3]). Der Rat will deshalb darauf achten, dass die zuständigen Arbeitsgruppen nicht nur die Menschenrechte im Auge

haben, sondern auch "mit Blick auf die missbräuchliche Verwendung der neuen Technologien insbesondere alle Präventions- und Schutzmaßnahmen fördern".

Tele-Vernehmung

Das Europäische Rechtshilfeabkommen regelt nicht nur die grenzüberschreitende Telekommunikationsüberwachung, sondern auch die Vernehmung per Videokonferenz, wenn ein Zeuge oder Sachverständiger in einem anderen Mitgliedsstaat vernommen werden soll. Auch können Zeugen und Sachverständige per Telefonkonferenz vernommen werden.

Europäische Ermittlungsgruppen

Ebenso regelt das Abkommen den Einsatz gemeinsamer Gruppen für strafrechtliche Ermittlungen. Sie können bei schwierigen und aufwendigen Ermittlungen mit Bezug zu anderen Mitgliedstaaten gebildet werden, oder wenn ein koordiniertes und abgestimmtes Vorgehen erforderlich ist. Geleitet wird eine solche Gruppe von einem Vertreter der Polizeibehörde in dem Mitgliedstaat, in dem der Einsatz der Gruppe erfolgt. Dabei handelt der Gruppenleiter "im Rahmen der ihm nach innerstaatlichem Recht zustehenden Befugnisse". Auch muss sich die Gruppe nach den Rechtsvorschriften des jeweiligen Mitgliedstaat richten, in dem sie ihren Einsatz durchführt.

Dies gilt nicht für Ermittlungen in Uniform, sondern auch für verdeckte Ermittlungen. Diese Vereinbarung war allerdings nicht unumstritten. Deshalb wurde ein Passus eingefügt, nachdem jeder Mitgliedstaat jederzeit erklären kann, dass er dieser Vereinbarung nicht zustimmt. Falls die Beamten in dem anderen Mitgliedstaat Straftaten begehen oder falls Straftaten gegen sie begangen werden, werden sie "dem Beamten des Einsatz-Mitgliedstaates gleichgestellt". Dabei haftet der Mitgliedstaat, der den Beamten entsandt hat, für den durch die Beamten bei ihrem Einsatz verursachten Schaden.

Zugriff auf Internet noch auf Wunschliste

Das Übereinkommen bietet jetzt die rechtliche Grundlage, grenzüberschreitend Kommunikationsdaten abzugreifen und Kommunikationsinhalte abzuhören. Dabei geht es ausschließlich um den Telekommunikationsverkehr, nicht jedoch um das Internet. Unter dem Dokumententitel Enfopol 19 stehen derzeit noch die Forderungen der Polizei im Raum, auch bei den neuen Telekommunikationstechniken den grenzüberschreitenden Zugriff zu ermöglichen. Deutsche Politiker konnten in der Kürze der Zeit noch keinen Kommentar abgeben. In einer Pressemitteilung des Bundesinnenministeriums zur Ratssitzung fand sich kein Wort zum verabschiedeten Abkommen, Justizministerin Däubler-Gmelin kommentierte die Sitzung gar nicht.

Der Europäische Rat für Justiz und Inneres diskutierte gestern während eines Mittagssessens auch Echelon, das anglo-amerikanische Spionagenetzwerk und wie sich die Mitgliedsstaaten vor dessen missbräuchlicher Verwendung schützen [4] können.

Links

[1] <http://www.heise.de/tp/deutsch/special/enfo/6807/1.html>

[2] <http://www.heise.de/tp/deutsch/special/enfo/5795/1.html>

[3] <http://www.heise.de/tp/deutsch/special/enfo/6711/1.html>

[4] <http://www.heise.de/tp/deutsch/special/ech/6815/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/8204/1.html>

Copyright © 1996-2003. All Rights Reserved. Alle Rechte vorbehalten

Heise Zeitschriften Verlag, Hannover

Europäisches Rechtshilfeabkommen kurz vor Verabschiedung

Christiane Schulzki-Haddouti 26.05.2000

Bis zuletzt Geheimhaltung; deutscher Parlamentsvorbehalt aufgehoben

Voraussichtlich wird der Justiz- und Innenrat auf seiner nächsten Sitzung am 29. und 30. Mai in Brüssel das Europäische Rechtshilfeabkommen mit dem Entwurfsstand vom 15. Mai verabschieden. Nach Information des grünen Bundestagsabgeordneten Christian Ströbele will die Bundesregierung das Abkommen unterzeichnen. Am 19. Mai hatte der Bundestags-Rechtsausschuss in einer Sondersitzung auf Drängen des Bundesjustizministeriums sowie der SPD den bestehenden Parlamentsvorbehalt aufgehoben. Der Vorbehalt bezog sich auf die Überwachungsbestimmungen zum Telekommunikationsverkehr.

Das Rechtsabkommen in der Fassung vom 15. Mai (COPEN 32), das Telepolis nun vorliegt, sieht in Artikel 17 bis 22 Regelungen zur grenzüberschreitenden Kommunikationsüberwachung vor. Demnach können laut Artikel 18 die Mitgliedsstaaten einen anderen Staat ersuchen, in seinem eigenen Interesse die Überwachung durchzuführen. Irritierend ist, dass auch diese Fassung wie alle vorangegangenen als Geheimmaterial mit "Limite" klassifiziert worden ist.

In dem Ersuchen muss die Behörde angegeben sein, die das Ersuchen erstellt. Hinzu kommt eine Bestätigung, "dass eine rechtmäßige Überwachungsanordnung im Zusammenhang mit einer strafrechtlichen Ermittlung erlassen wurde". Schließlich muss das Ersuchen "Angaben zum Zwecke der Identifizierung der Zielperson", des "strafbaren Verhaltens", der "gewünschten Dauer der Überwachung" sowie nach Möglichkeit "ausreichende technische Daten, insbesondere Netzanschlussnummer "enthalten", um sicher zu stellen, dass dem Ersuchen entsprochen werden kann". Der ersuchte Mitgliedsstaat kann zusätzliche Information verlangen, um festzustellen, ob die Überwachungsmaßnahme unter diesen Voraussetzungen auch im eigenen Land legal wäre.

In Artikel 19 regelt das Rechtshilfeabkommen den Fall von Telekommunikationsdienstleistungen, die nur über ein bestimmtes Land möglich wären, wie beispielsweise Satellitentelefonie. Dabei dürfen die ermittelnden Staaten die Überwachung "ohne Einschaltung desjenigen Mitgliedsstaats, in dessen Hoheitsgebiet sich die Bodenstation befindet" durchführen.

In Artikel 20 wird die Überwachung per Fernzugriff geregelt. Dabei handelt es sich um die umstrittenste Regelung, die lange von vielen Staaten boykottiert (Keine Einigung bei europäischem Rechtshilfeübereinkommen [1]) wurde. Hier ging es vor allem darum, wann und wie der überwachende Mitgliedsstaat den anderen Mitgliedsstaat von der Überwachung unterrichtet.

Die Lösung sieht nun vor, dass nach Benachrichtigung der unterrichtete Mitgliedsstaat "unverzüglich und spätestens innerhalb von 96 Stunden dem überwachenden Mitgliedsstaat" die Überwachung genehmigen oder versagen muss. Falls bereits Überwachungsmaterial gesammelt wurde, kann der Staat festlegen, unter welchen Bedingungen es verwendet werden darf. Er kann die Verwendung auch ganz versagen. Die 96-Stunden-Frist kann auf höchstens acht Tage verlängert werden, "damit die nach ihrem innerstaatlichen Recht erforderlichen Verfahren durchgeführt werden können".

So lange keine Entscheidung vorliegt, darf die Überwachung zwar fortgesetzt werden, aber das bereits gesammelte Material nicht verwendet werden. Dies gilt nicht, wenn die Staaten etwas anderes vereinbart haben oder wenn es sich um die Abwehr "einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit" handelt.

Generell kann der überwachte Staat eine kurze Darstellung des Sachverhalts und jede weitere Information verlangen, damit er beurteilen kann, ob in einem vergleichbaren innerstaatlichen Fall eine Überwachung genehmigt werden würde.

Aufgrund dieser Regelungsmechanismen wollen die Staaten ausschließen, dass ein Befugnis-Hopping einreißt. Auch die Kostenfrage wurde geregelt: So trägt der ersuchende Mitgliedsstaat die Kosten, die Betreibern einer Telekommunikationsanlage oder Diensteanbietern durch die grenzüberschreitende Überwachung entstehen.

Auf Wunsch Deutschlands wurde ein Artikel zum Schutz personenbezogener Daten eingefügt. Demnach dürfen die personenbezogenen Daten ohne besondere Zustimmung nur für gerichtliche und administrative Verfahren verwendet werden, die mit dem Verfahren unmittelbar zusammenhängen. Ebenso dürfen sie dann verwendet werden, wenn es darum geht eine "unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit" abzuwehren.

Zuletzt hatte das Veto Luxemburgs die geplante Verabschiedung am 27. März verhindert. Auch hatten die Abgeordneten des Europäischen Parlaments die Streichung des Paragraphen 18 zum Thema "Überwachung von Personen im Hoheitsgebiet anderer Mitgliedsstaaten oder deren technische Hilfe" gefordert. Jedoch vergebens.

Nach wie vor umstritten bleibt jedoch die technische Schnittstelle, die das Fernabhören ermöglichen soll. So erstellte das Europäische Standardisierungs-Institut ETSI bereits im vergangenen Jahr dafür eine erste Richtlinie (Feinschliff am Abhörstandard [2]). Sie

ermöglicht den Zugriff auf alle nutzbaren Daten in Telekommunikationsnetzen: Telefonanrufe, SMS-Messages, Handy-Gespräche und sogar Internet-Telefonie. Der SPD-Bundestagsabgeordnete Jörg Tauss befürchtet, dass die gemeinsame Schnittstelle das Abhören nicht nur Strafverfolgern, sondern auch Geheimdiensten und Wirtschaftskriminellen erleichtert.

Das Rechtshilfeabkommen ist ein wesentlicher Baustein für eine künftige gemeinsame europäische Strafverfolgung und damit auch für ein politisch vereintes Europa. Diskutiert wurde es allerdings in der Öffentlichkeit kaum, vom Europäischen Parlament wurde der zentrale Abhörparagraph gar abgelehnt. Vermutlich werden wie in Deutschland auch andere Parlamentsvorbehalte schnell überwunden. Die geplante Konvention zur Cyberkriminalität wird mit ihren Maßnahmen auf dem Abkommen aufsetzen. Bisher fand jedoch zur Konvention, die ebenfalls von Fachleuten ausgearbeitet wird, kaum eine öffentliche Aussprache statt.

Links

[1] <http://www.heise.de/tp/deutsch/special/enfo/5476/1.html>

[2] <http://www.heise.de/tp/deutsch/special/enfo/6711/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6807/1.html>

Digitale Detektive in Holland

Jelle van Buuren 10.04.2000

Sonderbefugnisse für den Lauschangriff im Internet; der geheime Einfluss von ILETS; Wanzen im Keyboard und Angriffe auf die Anonymität.

Seit einiger Zeit nun schon ist der Kampf gegen Cyberkriminalität ein heißes Thema auf politischen Tagesordnungen überall auf der Welt. Auch in den Niederlanden haben die Strafverfolgungsbehörden die virtuelle Welt zu ihrem Jagdgrund gemacht. Neue Gesetze ermöglichen es den Behörden, das Internet abzuhören und Ermittlungen im Internet auszuführen. Um Probleme mit verschlüsselter Kommunikation zu vermeiden, ist es der Polizei erlaubt, Wanzen in den Keyboards von Verdächtigen einzubauen. Ein Bericht aus den *Low Lands*.

Ab August 2000 sind niederländische Internetprovider gesetzlich verpflichtet, ihre Systeme für die Strafverfolgungsbehörden abhörfähig zu machen. Diese gesetzliche Verpflichtung ist Teil des neuen Telekommunikationsgesetzes, das 1998 in Kraft trat. Doch für die Internetprovider wurde diese Verpflichtung um zwei Jahre verschoben, um ihnen Zeit zur Vorbereitung auf die Aufgabe des Abhörens zu geben. Die technischen, finanziellen und legalen Konsequenzen des Abhörens waren noch ungeklärt. Die Abhörstandards, welche die Provider einzubauen hatten, waren eine genaue Kopie der technischen Anforderungen [1] (IUR), welche die Europäische Union 1995 formuliert hatte.

Interne Dokumente des Justizministeriums und des für Telekommunikation zuständigen Ministeriums bestätigen, dass diese Anforderungen in der Tat vom sogenannten "International Law Enforcement Telecommunication Seminar" (ILETS), eine Gruppe amerikanischer und europäischer Experten, verfasst worden waren.

Ein Beamter des für Telekommunikation zuständigen Ministeriums sagte laut Sitzungsprotokollen der Arbeitsgruppe für Überwachung - eine beratende Versammlung der Behörden und der Telekommunikationsindustrie -, die unter dem niederländischen "Freedom of Information Act" erlangt worden waren, "der Inhalt des Ratsbeschlusses von 1995 wurde zwischen globalen Marktteilnehmern und Vertretern der USA, Kanadas und Australiens im Rahmen der ILETS-Konferenz abgestimmt." Laut Unterlagen des Justizministeriums haben "viele der Themen, die in der europäischen Arbeitsgruppe für polizeiliche Zusammenarbeit diskutiert werden, ihren Ursprung in den sogenannten ILETS-Beratungen". (siehe auch ILETS, die geheime Hand hinter ENFOPOL [2])

Wie diese Anforderungen auf einer praktischen Ebene umzusetzen waren, war weder den Providern noch den Behörden klar. Die Protokolle der Arbeitsgruppe für Abhörmaßnahmen zeigen einige der Probleme auf. So sagte zum Beispiel der Vertreter des Verbandes der niederländischen Internetprovider (NLIP) 1999: "Es gibt nur zwei oder drei amerikanische Unternehmen, die Abhör-Equipment für das Internet herstellen. Es wird noch zwei Jahre oder länger dauern, bevor es Abhörgeräte für das Internet gibt." Der sogenannte *Justice Interception Standard* (JIS), welcher derzeit in den Niederlanden benutzt wird, ist für das Abhören von Hochgeschwindigkeitsdatenübertragung wie zum Beispiel mittels xDSL oder ATM nicht geeignet. Abgesehen davon gab es auch Meinungsverschiedenheiten darüber, welches Abhörprotokoll einzuhalten sei.

Das Protokoll, das vom "European Telecommunication Standardisation Institute" (ETSI) entwickelt wurde und das als Protokoll für alle europäischen Telekommunikationsunternehmen dienen wird, erfüllt derzeit noch nicht alle Anforderungen der niederländischen Regierung. Dieses gesamteuropäische Abhörprotokoll ist noch Gegenstand von Verhandlungen mit europäischen Regierungen. Die niederländischen Provider waren dagegen, Veränderungen an ihrem Gerätepark vorzunehmen, um das niederländische JIS zu erfüllen, mit dem Risiko, neue Veränderungen und Investitionen vornehmen zu müssen, wenn dann das europäische Protokoll vereinbart werden wird.

Marktmechanismen

Die großen niederländischen Provider haben inzwischen ihre technischen und organisatorischen Vorbereitungen abgeschlossen, um ihre Systeme abhörfähig zu machen. Sie haben sogenannte "Black boxes" an zentraler Stelle in ihren Anlagen installiert. Damit sind sie in der Lage 95% des Traffics auf ihren Servern abzufangen. Für die verbleibenden 5%, zum Beispiel direkte Kommunikation von Client zu Client, wird noch nach Lösungen gesucht. Die Provider sträuben sich noch, weil dies teuer werden könnte. Für die kleineren Provider ist die Abhörverpflichtung insgesamt eine große Belastung.

Die Provider und die Behörden verhandeln noch über die Anzahl der Verbindungsstellen, die gleichzeitig abhörbar sein sollen. Es gibt einen Vorschlag, demzufolge kein gesetzliches Minimum eingeführt werden sollte und wobei diese Entscheidung den Providern überlassen wird. Die Provider sind aber gezwungen, Anweisungen der Behörden zum Abhören zu befolgen, was bei Nichterfüllen mit einer hohen Geldstrafe geahndet werden kann. Das bedeutet also, so etwas wie einen Marktmechanismus auf dem Gebiet des Abhörens einzuführen. Für die Behörden ist diese Lösung ideal, denn die Regierung muss keine genauen Normen setzen, welche Gefahr liefern, in der Zukunft die Anforderungen zu unterschreiten. Es ist eine flexible Lösung, die Platz lässt für eine große

Anzahl von Abhörbefehlen.

Die Black box wird von den Service-Providern verwaltet. Sie sind die einzigen, die den Knopf drücken können, wenn ein Abhörbefehl kommt. Zufallsfischereien der Behörden sind nicht möglich - noch nicht. Doch die Gefahr liegt in der Stück-für-Stück-Taktik. Wenn alle Provider permanente Abhörssysteme in ihre Anlagen integriert haben, dann gibt es keine technischen Hindernisse für eine Erweiterung der Abhörbefugnisse.

Für Kabelprovider und Hochgeschwindigkeits-Internettraffic müssen immer noch Lösungen gefunden werden. Insbesondere die große Menge an Daten, die ein einzelner User in solchen Systemen erzeugen kann, ist ein Problem.

Aufklärungseinheiten

Die Überwachung des Internet-Traffic ist nicht die einzige Waffe, welche niederländische Behörden in der Bekämpfung von Cyberkriminalität nun zur Verfügung haben. Im Entwurf des Gesetzes über Computerkriminalität II, das nun vor dem niederländischen Parlament ist, werden der Polizei Befugnisse zu Ermittlungen im Cyberspace verliehen. Polizeibeamte können sich nun, ganz wie normale Bürger, frei im Internet bewegen, ohne sich als Polizisten ausweisen zu müssen. Sie können auch Informationen herunterladen und auf Polizei-Rechnern speichern. Das "Gesetz über besondere Ermittlungsbefugnisse", das seit Februar 2000 in Kraft ist, gibt der Polizei die Erlaubnis zum Einsatz besonderer Ermittlungstechniken. Beamten ist es erlaubt, Newsgroups zu infiltrieren, auf systematische Art und Weise Informationen über Verdächtige zu sammeln, Fassadenshops im WWW aufzuziehen und vorzugeben, an illegalen Geschäften interessiert zu sein.

Die Polizei ist nun auch ermächtigt, sogenannte "Aufklärungspatrouillen" durchzuführen - der "proaktive" Zugang. Laut einem erklärendem Zusatz zu dem Gesetz ist das eine Ermittlung über "eine Gruppe von Verdächtigen um herauszufinden, auf welche Art sie Computerverbrechen begehen oder vorbereiten". Der erklärende Zusatz des Gesetzes sagt auch, dass es "denkbar" sei, dass "bestimmte Teile der Internet-Community Gegenstand solcher proaktiver Ermittlungen sein werden".

Wanzen im Keyboard

Das Gesetz über besondere Ermittlungsbefugnisse enthält auch Artikel über die Verwendung von Kryptographie. Nach gescheiterten Bemühungen, den Gebrauch von Kryptographie zu regulieren oder zu verbieten, sagte die niederländische Regierung 1998, dass die Benutzung von Kryptographie frei ist. Doch es wurden andere Mittel eingeführt um zu bekämpfen, was von der Regierung als das "Krypto-Problem" betrachtet wird.

Verdächtige können zwar nicht gezwungen werden ihre Schlüssel zu übergeben, doch "Dritte", bei denen eine "berechtigte Annahme" besteht, dass sie im Besitz der Schlüssel sind, können zum Entschlüsseln von Kommunikation gezwungen werden. Diese Verpflichtung findet zum Beispiel bei sogenannten "Trusted Third Parties" Anwendung oder auch bei Telekommunikationsunternehmen, welche die Kommunikation ihrer Kunden verschlüsseln oder auch bei Empfängern verschlüsselter Nachrichten.

Die Polizei ist nun auch ermächtigt, Wohnungen und Büros von Verdächtigen abzuhören. Die Regierung sagte explizit, dass es auch hierbei um das "Krypto-Problem" geht. "Aufzeichnungen geheimer Kommunikation machen zu können, ist besonders da wichtig, wo verschlüsselte Email eingesetzt wird. Die Erlaubnis zum Abhören heißt in diesem Zusammenhang, dass ein Abhörgerät in der Tastatur eines Verdächtigen eingebaut wird, so dass vertrauliche Kommunikation abgefangen werden kann noch bevor Verschlüsselung stattfindet", heißt es in den Erläuterungen zu dem Gesetz.

Zusammenarbeit mit den Geheimdiensten

Die niederländische Polizei hat nun sieben interregionale "digitale Expertenzentren" eingerichtet, die bei Ermittlungen helfen sollen, bei denen Informationstechnologie eine Rolle spielt. Der *Centrale Recherche Informatie dienst* (CRI), eine nationale Einheit zur Koordination von Ermittlungen, hat eine Sondereinheit von "Cybercops" eingerichtet, die im Internet aktiv Verbrechensaufklärung betreiben. "Als Team ermitteln wir in bestimmten Fällen, bei Kinderpornographie, Drogenschmuggel, Menschenhandel, Dokumentenfälschung, Betrug und Handel mit gestohlenen Kunstwerken", sagte der Leiter der Einheit, Richard Vriesde, der holländischen Wochenzeitung *Vrij Nederland*.

Die Polizei sucht nun auch Unterstützung von der Wissenschaft und der Wirtschaft zur Entwicklung von Tools, welche Internetermittlungen verbessern und Kryptographie cracken können. "Zu Forschungszwecken müssen die Strafverfolgungsbehörden auch Partner in der wissenschaftlichen und akademischen Welt und in der Wirtschaft finden. Auf diese Art kann das nötige Wissen angesammelt werden, um Ermittlungen und Strafverfolgung zu verbessern", schrieb das CRI in einem Bericht.

Ein wichtiger Partner des CRI ist das Justizlabor, eine auf Kryptographie spezialisierte Einrichtung. Dieses Labor hat beispielsweise ein Programm entwickelt, das den Code elektronischer Tagebücher knacken kann. Die Software gehört nicht nur zur Ausrüstung der Computerspezialisten der niederländischen Polizei sondern ist auch ihr Exportschlager. Das Labor ist auch in der Lage die Schutzmechanismen weit verbreiteter Programme wie Microsoft Word oder Excel zu durchbrechen.

Das Justizlabor arbeitet eng mit dem Nachrichtendienst der niederländischen Marine und

dem Inlandsgeheimdienst zusammen. Das CRI möchte ebenfalls an dieser Zusammenarbeit beteiligt sein. "Neben Gesetzen und Vorschriften sind Initiativen nötig, die auf die technischen Möglichkeiten zur Aushebelung kryptografischer Techniken zielen. Zusammenarbeit zwischen der Polizei und Nachrichtendiensten in diesem sensiblen Bereich sollte auch ein Diskussionsthema sein", heißt es in dem oben erwähnten Bericht.

Anonymität im Internet

In ihrer Haltung bezüglich Cyberkriminalität folgen die Niederlande internationalen Entwicklungen. Die Abhörerfordernisse sind eine Kopie der europäischen Anforderungen, die von den Experten der ILTES-Gruppe erarbeitet wurden. Auch bezüglich Kryptographie befindet man sich in internationalem Fahrwasser. Mehr und mehr Regierungen betrachten ein Verbot von Kryptographie als verlorenen Fall. Mit dem Anzapfen von Keyboards hat man eine Ausweichmöglichkeit geschaffen.

Das nächste Ziel der Behörden wird mit größter Wahrscheinlichkeit die Anonymität im Internet sein. Die Behörden haben bereits erste Fühler ausgestreckt. Einer ihrer ersten Vorschläge ist, dass die Benutzung einer Anrufer-Identifikation verpflichtend wird. Derzeit ist es möglich, die Identifikationsnummer abzuschalten, die es ermöglicht, den Telefonanschluss herauszufinden, über den der Zugang ins Internet erfolgt. Ein anderer Vorschlag ist, "Nummernschilder" für Internetbenutzer einzuführen. Jede/r Nutzer/in muss eine feste und registrierte IP-Nummer haben, die in einer nationalen Datenbank gespeichert ist. Die Polizei sollte "gesetzlich erlaubten Zugang" zu diesem Verzeichnis haben.

Eine Sache scheint allerdings immer noch sehr unklar zu sein: wie real ist die Gefahr durch Cyberkriminalität und Kryptographie? Viele wüste Geschichten zirkulieren, doch es gibt wenig Beweise. Eine kürzlich erschienene Studie einer Polizei-Beratungsfirma zeigt, dass es derzeit noch wenig Probleme mit Kryptographie gibt.

"Digitale Detektive begegnen selten Fälle, bei denen kryptographische oder andere technische Methoden zur Verschleierung von Informationen benutzt werden. Laut diesen Beamten ist Verschlüsselung kein echtes Problem, zumindest noch nicht im Augenblick, es werde aber wahrscheinlich in der Zukunft Fuss fassen. Die Beamten erklärten uns, dass es relativ leicht sei, Zugang zu verschlüsselten Daten zu erhalten, da viele Verdächtige ihr Passwort irgendwo aufgeschrieben haben, zum Beispiel auf einem Zettel in der Nähe des Computers, oder sie verraten das Passwort, wenn sie danach gefragt werden."

Soweit also zu den gefährlichen holländischen Cyberkriminellen. Man kann sich des Eindrucks nicht erwehren, dass die Behörden die Bedrohung eines gefährlichen und unkontrollierten Cyberspace beschwören, um mehr Macht und Befugnisse zur Überwachung, zum Abhören und bei Ermittlungen zu erhalten.

Übersetzung: Armin Medosch

Links

[1] <http://www.heise.de/tp/deutsch/special/enfo/6334/1.html>

[2] <http://www.heise.de/tp/deutsch/special/enfo/6396/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6726/1.html>

Copyright © 1996-2003. All Rights Reserved. Alle Rechte vorbehalten

Heise Zeitschriften Verlag, Hannover

Feinschliff am Abhörstandard

Christiane Schulzki-Haddouti 04.04.2000

Europäische Kommission hält an Abhör-Artikel des Rechtshilfeübereinkommens fest; das europäische Standardisierungsinstitut ETSI hat den entsprechenden technischen Standard schon vorsorglich definiert.

Bereits letzte Woche wurde klar, dass der Rat der Innen- und Justizminister sich in Sachen grenzüberschreitende Überwachung über den Willen des Europäischen Parlaments hinweg zu setzen plant. Nur am Festhalten Luxemburgs am Bankgeheimnis scheiterte [1] die endgültige Beschlussfassung über das Europäische Rechtshilfeabkommen vorläufig. Das österreichische Online-Magazin FutureZone [2] veröffentlichte diese Woche Details aus einem internen EU-Papier namens COPEN 21 über die Vorstellungen des Rats bezüglich grenzüberschreitender Überwachung.

Auch Telepolis liegt nun ein internes EU-Papier namens COPEN 18 vom 10. März 2000 vor. Demnach schlug die Europäische Kommission für Artikel 17 folgendes vor:

"Innerhalb eines Jahres nach Unterzeichnung des Übereinkommens, aber spätestens zum in Kraft treten des Übereinkommens, wollen die Mitgliedsstaaten und die betroffenen Telekommunikations-Service-Provider ein sicheres System zur Übertragung der Abhörerfragen sowie für die Übermittlung der abgehörten Kommunikation zum Zwecke der Implementierung der Vorgaben des Artikels 17 des Übereinkommens ausarbeiten. Sie sollen Vorgehensweisen und technische Modalitäten entwickeln und vereinbaren, die ein Abhören durch direkten Zugang ermöglichen, um einen hohen Sicherheitsstandard bei den Übertragungen zwischen allen berechtigten Behörden und Service-Providern zu gewährleisten."

Hinzu kommt, dass dieses Abhörssystem ebenso die Datenschutzbestimmungen laut Richtlinie 97/66/EC gewährleisten muss.

Vorausblickend erarbeitete bereits im letzten Jahr das europäische Standardisierungsinstitut ETSI (European Telecommunications Standards Institute [3]) einen europäischen Abhörstandard. Die Richtlinie ES 201-671 definiert eine europaweit einheitliche Telekommunikationsnetztechnik. Sie sieht darin auch den nutzbaren Zugriff auf alle Daten vor. Handy- und Festnetztelefonate, SMS-Nachrichten und sogar Internet-Telefonie.

Hintergrund: Gelten europaweit die selben technischen Regeln, so lassen sich auch Abhörmaßnahmen im Ausland leicht bewerkstelligen. Offensichtlich hatte sich das Standardisierungsinstitut der europäischen Wirtschaft bereits frühzeitig auf die künftige Abhörharmonisierung in Europa vorbereitet.

Der SPD-Bundestagsabgeordnete Jörg Tauss hat sich die öffentliche Debatte, die er im Zusammenhang mit den Enfpol-Abhörplänen ankündigte, "so nicht vorgestellt". Ihm sind die technischen Vorschriften der ETSI-Norm nicht bekannt. Für problematisch hält er, dass diese technischen Schnittstellen auch von Wirtschaftskriminellen oder Geheimdiensten gebraucht werden können.

Die Forderungen der Europäischen Kommission machen eins jetzt schon klar: Auf die Überlegungen des Europäischen Parlaments wird die Kommission, aber auch der Rat keine Rücksicht nehmen. Der Abhörartikel wird bestehen bleiben. Hinzu kommt eine technische Harmonisierung des Abhörens. Erst sie ermöglicht problemlos den schnellen grenzüberschreitenden Zugriff auf die Kommunikation.

Links

- [1] <http://www.heise.de/tp/deutsch/special/enfo/6692/1.html>
- [2] <http://futurezone.orf.at/futurezone.orf?read=detail&id=23922&tmp=65557>
- [3] <http://www.etsi.org>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6711/1.html>

Kein endgültiger Beschluss über europäisches Übereinkommen zur Rechtshilfe in Strafsachen

Jelle van Buuren 28.03.2000

Luxemburg blockiert die Vereinbarung wegen Bankgeheimnis; Kompromiss bei grenzüberschreitendem Abhören.

Der Europäische Rat für Justiz und Inneres konnte gestern keine endgültige Übereinstimmung bezüglich der umstrittenen Rechtshilfe in Strafsachen erzielen. Es wurde allerdings eine Kompromissformel über den Artikel gefunden, der das grenzüberschreitende Abhören in einem anderen Mitgliedsstaat ohne dessen technische Unterstützung betrifft. Die Verabschiedung des gesamten Rechtsakts wurde von Luxemburg blockiert, weil es sein Bankgeheimnis aus dem Vertrag heraushalten will.

Mher als drei Jahre lang haben die Mitgliedsstaaten der EU am Entwurf der Vereinbarung gefeilt. Die meisten Auseinandersetzungen gab es bezüglich der Artikel, die das Abhören betreffen. Zunächst gab es Probleme mit dem Abhören der neuesten Generation von satellitengestützten Mobiltelefonen. Italien plädierte dafür, dass die Länder, auf deren Territorium sich Bodenstationen für Satellitentelefone befinden, jedes Mal dann konsultiert werden sollen, wenn ein anderes Land Satellitentelefonate abhören will, auch wenn das ohne die technische Unterstützung des betroffenen Landes möglich wäre - der sogenannte "Fernzugang". Dabei können nationale Telekommunikations-Dienstleister Anrufe direkt abhören, die über die italienische Bodenstation laufen.

Iridium, der einzige satellitengestützte Mobiltelefondienst in Europa, hatte seine Bodenstation in Italien, doch Iridium ist ja inzwischen bankrott gegangen [1]. Italien betrachtete es als Bruch seiner Souveränität, wenn es bei Abhörmaßnahmen nicht konsultiert werden würde. Auch sah Italien verfassungsmäßige Probleme aufgeworfen. Es verlangte Garantien, dass andere Mitgliedsstaaten, die Iridium-Kommunikation abhören, keine italienischen Gesetze brechen, die es zum Beispiel verbieten, dass Parlamentsmitglieder abgehört werden. Daher forderte Italien, dass jede Abhörmaßnahme durch eine schriftliche Anfrage genehmigt werden müsse.

Die übrigen Mitgliedsstaaten waren hier anderer Ansicht. Ihrer Meinung nach würde der Fernzugang die Rechte Italiens nicht beeinträchtigen. Italien sei nur Gastland der Bodenstation und hätte keine gesetzliche Verantwortung für das Abhören von Telekommunikation über diese Bodenstation. Italien solle eine einzige, allgemeingültige Anordnung an die Bodenstation geben, wonach diese ihre technische Struktur so

einzurichten habe, dass nationale Dienstleister Abhörmaßnahmen selbständig einleiten könnten ebenso wie die automatische Übertragung der abgehörten Gespräche. Die Lösung, die nun gefunden wurde, ist die, dass es keine Verpflichtung für Länder gibt, auf deren Territorium sich Bodenstationen befinden, die Betreiber dazu zu zwingen, einen Fernzugang zu ermöglichen, dass dies aber als prinzipielle Möglichkeit besteht.

Ein weiteres Problem betraf den Artikel über grenzüberschreitendes Abhören von Personen auf dem Hoheitsgebiet eines anderen Mitgliedsstaats ohne dessen offizielle Zustimmung. Einige Mitgliedsstaaten wollen sicherstellen, dass solche Abhörmaßnahmen einer vorherigen Zustimmung bedürfen, um über sie im Bilde sein zu können. Andere Mitgliedsstaaten, insbesondere Großbritannien, stellten sich wiederum gegen die Notwendigkeit des Einholens einer Zustimmung. Auf Grund seiner Teilnahme am weltweiten Abhörsystem Echelon ist Großbritannien ohnehin in der Lage, Telekommunikation in anderen Mitgliedsstaaten abzuhören. Vor allem möchte Großbritannien keine Einmischung anderer Mitgliedsstaaten in die Angelegenheiten seiner Geheimdienste. Diese haben allerdings auch Aufgaben bei der Bekämpfung des "organisierten Verbrechens". Die Grenze zwischen diesen Aufgabenbereichen ist wesentlich verwischter als in den meisten anderen EU-Staaten.

Großbritannien hat nun zugestimmt, andere Mitgliedsstaaten zu informieren, wenn grenzüberschreitendes Abhören im "Zuge einer Ermittlung in Strafsachen" ausgeführt wird. "Ermittlung in Strafsachen" heißt nach der neuesten Version des Vereinbarungsentwurfs, "eine Ermittlung in Folge einer spezifischen strafbaren Handlung einschließlich versuchter Handlungen, insofern sie nach nationalem Gesetz als kriminell gelten, um die Verantwortlichen zu identifizieren, zu verhaften, anzuklagen, zu verfolgen oder zu verurteilen". Mit dieser Definition braucht Großbritannien nun nicht mehr um eine Einmischung in seine Geheimdienstangelegenheiten zu fürchten, da geheimdienstliches Abhören meist viel breitere Zielsetzungen verfolgt, die nicht auf direkte strafrechtliche Verfolgung ausgerichtet sind.

Ein anderes ungelöstes Problem war, was es bedeuten würde, wenn ein über eine Abhörmaßnahme in Kenntnis gesetzter Staat nicht darauf reagiert. Einige Mitgliedsstaaten unterstützten die Interpretation, dass Schweigen Zustimmung signalisiere, andere waren genau der gegenteiligen Ansicht. Ein Kompromiss sieht nun vor, dass Mitgliedsstaaten innerhalb von 96 Stunden reagieren müssen. Innerhalb dieses Zeitraums können sie das Abhören und die Benutzung abgehörter Informationen verbieten. Erfolgt nach vier Tagen, in manchen Fällen 8 Tagen, immer noch keine Antwort, so bedeutet das stillschweigende Zustimmung.

Wenn ein Land eine Abhörmaßnahme verbietet, muss diese sofort gestoppt werden. Das dabei angefallene Material kann allerdings immer noch vor Gericht verwendet werden,

"wenn die öffentliche Ordnung oder die nationale Sicherheit" gefährdet sind. Was das nun genau bedeutet, ist nicht klar. Sicher ist nur, dass Drogendelikte unter diese Regelung fallen. Es gibt keine Regelung bezüglich der Vernichtung von Materialien, die durch unerwünschtes Abhören gewonnen wurden. Diese könnten also für spätere Ermittlungen benutzt werden.

Mit dieser Regelung haben die Justiz- und Innenminister die Meinung des Europaparlaments [2] übergangen. Das Parlament sprach sich im Februar für die Streichung der Abhörartikels aus. Laut einem Bericht des Europaparlamentarier Di Pietro "führt dieser Artikel in ein gesetzliches Minenfeld [3], wobei einige Mitgliedsstaaten im Interesse ihrer nationalen Sicherheit (und mittels des Einsatzes von Geheimagenten?) völlig unabhängige Ermittlungen in anderen Mitgliedsstaaten ausführen und sich dabei der zeitaufwendigen Aufgabe entledigen möchten, dafür die Zustimmung der gesetzlichen Autoritäten des anderen Landes einzuholen." Dies könnte, so Di Pietro, "zur Legalisierung der in einer Grauzone stattfindenden Aktivitäten der Geheimdienste" führen.

Wenn Luxemburg seine Bedenken zurücknimmt, dann steht der endgültigen Beschlussfassung über den Rechtsakt bei der nächsten Sitzung des Rats für Justiz und Inneres im Mai nichts mehr entgegen. Wirksam würde ein solches Übereinkommen aber erst werden, nachdem die nationalen Parlamente es ratifiziert haben.

Übersetzung: Armin Medosch

Links

- [1] <http://www.heise.de/tp/deutsch/inhalt/te/5898/1.html>
- [2] <http://www.heise.de/tp/deutsch/inhalt/te/5810/1.html>
- [3] <http://www.heise.de/tp/deutsch/special/enfo/5795/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6692/1.html>

EU will Informationen über Terrorismus im Internet sammeln

Jelle van Buuren 16.03.2000

Die Geheimdienste scheinen mit Hacker-Slang ihre Probleme zu haben, wie zum Beispiel mit der Benutzung des Buchstabens "z" in "passwordz, gamez, crackz, softwarez".

Die Nachrichtendienste der Europäischen Union entwickeln ein System für den Austausch von Informationen über Terrorismus im Internet. "Namentlich durch das Internet haben sich Gruppen gebildet, die sich seiner ungebührlichen Ausbeutung und zweckentfremdeten Nutzung verschrieben haben", sagte Portugal, das derzeit die Präsidentschaft der Europäischen Union inne hat.

Die portugiesische Präsidentschaft präsentierte ihre Sichtweise bei der Arbeitsgruppe über Terrorismus, eine europäische Gruppe hochrangiger Mitarbeiter von Nachrichtendiensten, die Teil des Europäischen Rates für Justiz und Inneres ist. In dem Dokument (5724/00 ENFOPOL 6, Brüssel, 4. Februar 2000) sagt die portugiesische Präsidentschaft:

"Solche Arten von Aktivitäten erlauben diesen Gruppen, die verschiedene Formen illegaler Aktivitäten betreiben, namentlich Terrorismus, Sekten, Neonazismus, Cyberterrorismus, Rassismus, etc., die Verbreitung und propagandistische Förderung ihrer Ideale. Die Leichtigkeit und Schnelligkeit im Aufbau von Kontakten ermöglicht ihnen desweiteren die Internationalisierung solcher Phänomene und ermöglicht zugleich größeren Zusammenhalt und bessere Rekrutierungsmöglichkeiten für ihre Anliegen."

Portugal schlägt die Schaffung eines Systems zum "Austausch offener, im Internet gesammelter Informationen" vor, mit dem Ziel, "bessere Informationen ebenso wie effizientere Nutzung der Ressourcen" verfügbar zu machen. Das System sollte es allen Mitgliedern möglich machen, über "bessere Werkzeuge zum Aufspüren von Informationen im Kontext des Kampfes gegen Terrorismus" zu verfügen.

Portugal möchte ein gemeinsames Lexikon schaffen, das aus einer Anzahl von Schlüsselbegriffen in verschiedenen europäischen Sprachen besteht. Besondere Probleme scheint man mit Hacker-Slang zu haben, "wie zum Beispiel mit der Benutzung des Buchstabens "z" am Ende von Worten in der Hacker-Community (passwordz, gamez, crackz, softwarez)." Unwissenheit über solche Mechanismen macht es, laut dem Dokument "extrem schwierig bei Nachforschungen gute Resultate zu erzielen".

Nach erfolgten Internet-Nachforschungen sollen die Resultate analysiert und mittels verschlüsselter Email an die jeweiligen nationalen Nachrichtendienste verschickt werden, je nachdem, was für welches Land relevant ist. Als Endprodukt wird von jedem Land ein Bericht über die entdeckten Fakten als Periodikum erstellt

Die Delegationen begrüßten den Vorschlag der portugiesischen Präsidentschaft beim Treffen der Arbeitsgruppe über Terrorismus. Der Vertreter von Europol, die ebenfalls Anti-Terrorismus-Aufgaben haben, erklärte, dass Europol die Vorschläge weiter prüfen und Vorschläge für die Implementierung machen könnte.

Doch die Nachrichtendienste sind nicht die einzigen europäischen Strafverfolgungsbehörden, die das Internet als große Bedrohung der öffentlichen Ordnung und inneren Sicherheit sehen. Auch die Zollbehörden der Mitgliedsstaaten der Europäischen Union bereiten einen "Aktionsplan für den Kampf gegen Internet-Betrug" vor (Dokument 5254/00 CRIMORG 6 ENFOCUSTOM 4, Brüssel 17. Januar 2000). Laut diesem Aktionsplan ist das Internet ein Hort des Steuerbetrugs und des Handels in gefälschten Produkten, Tabak und Drogen. Der Aktionsplan schlägt die Schaffung nationaler "zentraler Internet-Kontroll-Einheiten" vor, die als nationale Kontaktstellen für informelle Arten der Zusammenarbeit dienen sollen. Dieses informelle Netzwerk solle das Internet so "strikt wie möglich" überwachen, heißt es im Aktionsplan.

Die Zollbehörden sollen Zugang zu Dokumenten haben, welche Transaktionen betreffen, die Gegenstand von Ermittlungen sind. Deshalb ist es laut dem Aktionsplan "wünschenswert, dass Provider verpflichtet sind, digitale Dokumente zu speichern" (Diese Formulierung bezieht sich wahrscheinlich auf das Speichern von Verbindungsdaten. Die aktuelle EU-Position dazu siehe [hier](#) [1]). Der Zoll solle auch Zugang zu finanziellen Informationen bei Banken haben, um die Herkunft von Gütern nachvollziehen zu können.

Übersetzung aus dem EU-Englischem von Armin Medosch

Links

[1]

http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp25en.htm

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6673/1.html>

Europäisches Rechtshilfeabkommen wird im März verabschiedet

Christiane Schulzki-Haddouti 29.02.2000

Datenschutzregeln sollen integriert werden, Kompromiss mit Echelon-Staat Großbritannien

Bereits am 27. März soll das Europäische Rechtshilfeabkommen in einer Sitzung des Rates für Justiz und Inneres verabschiedet werden. Der aktuelle Entwurf vom 3. Dezember 1999 zielt auf eine engere Zusammenarbeit der europäischen Strafverfolgungsbehörden. Der Einsatz modernster technischer Kommunikationsmittel spielt hierbei eine wesentliche Rolle.

Im Rechtshilfeabkommen wird unter anderem eine Rechtsgrundlage geschaffen, um eine gemeinsame Ermittlungsgruppe verschiedener Mitgliedsstaaten zu errichten und einzusetzen. Sie kann aus Mitgliedern nationaler Polizeibehörden, aber auch im Einzelfall aus Mitgliedern von Europol bestehen. Auch sollen Ermittler auf dem Hoheitsgebiet eines anderen Mitgliedsstaates künftig verdeckt ermitteln können (Artikel 14).

Wesentlich sind die neuen Bestimmungen zur Überwachung von Telekommunikationsverkehr zum Zwecke strafrechtlicher Ermittlungen. Geregelt ist die "Überwachung von Personen im Hoheitsgebiet anderer Mitgliedsstaaten ohne deren technische Hilfe" im Artikel 18. Dieser wurde Mitte Februar vom Europäischen Parlament jedoch abgelehnt (Europäisches Parlament stimmt gegen unkontrolliertes grenzüberschreitendes Abhören [1]) Die endgültige Entscheidung trifft jedoch der Rat für Justiz und Inneres.

Kompromiss mit Echelon-Staat Großbritannien

Dieser fand nach langen Verhandlungen am 2. Dezember zu einer Kompromissformel. So war vor allem umstritten, wie weit die Informationspflichten bei der Telefonüberwachung durch die Nachrichtendienste Großbritanniens reichen. Hintergrund ist, dass dort die Geheimdienste aufgrund einer besonderen Kompetenzzuweisung Abhörmaßnahmen im Rahmen strafrechtlicher Ermittlungen durchführen können. Eine klare Trennung zwischen Abhörmaßnahmen von Strafverfolgungsbehörden einerseits und britischen Diensten andererseits findet nicht statt.

Um das Problem zu lösen, wurden präventive und repressive Abhörmaßnahmen voneinander abgegrenzt. Präventive Abhörmaßnahmen werden grundsätzlich von Geheimdiensten durchgeführt, repressive durch die Strafverfolgungsbehörden. Zudem

wurde in der endgültigen Fassung bestimmt, dass Artikel 18 für ministerielle Überwachungsanordnungen gilt, die in Großbritannien an den Polizeidienst oder die Zoll- und Steuerbehörden gerichtet sind. Er gilt aber auch für den Geheimdienst, wenn dieser die Strafverfolgungsbehörden bei einer Ermittlung unterstützen.

Kein Grundrechts-Dumping

Führen andere Mitgliedsstaaten eine Überwachungsmaßnahme durch, die nicht nur im Widerspruch zu Grundsätzen der Rechtsordnung des abgehörten Mitgliedsstaates steht, sondern auch nach nationalem Recht unzulässig wäre, kann widersprochen werden. Auf diese Weise kann nicht ein höheres Rechtsniveau durch ein niedrigeres im anderen Mitgliedsstaat unterlaufen werden.

Kein Überwachungsautomatismus

Wird ein Mitgliedsstaat von einer Überwachungsmaßnahme unterrichtet, schweigt jedoch, muss nach Ablauf von 96 Stunden die Überwachung und die Verwendung des Materials untersagt werden. Dagegen protestierten die italienische, belgische, niederländische und dänische Delegation sowie die Kommission, da sie befürchten, dass eine effiziente Strafverfolgung dadurch behindert werden würde. Aufgrund der "mutmaßlich verschwindend geringen Anzahl auftretender Fälle" hielt die deutsche Delegation jedoch eine solche Regelung für vertretbar. Dennoch wurde hierzu keine endgültige Einigung gefunden.

Datenschutz

Auf der Sitzung am 2. Dezember sprach sich der Rat auf Druck Deutschlands erstmals verbindlich und einvernehmlich für die Aufnahme einer Datenschutzbestimmung in das Übereinkommen aus. Nach Auffassung der Deutschen werden sensitive Daten verarbeitet und übermittelt. Aus diesem Grund seien Datenschutzbestimmungen "unverzichtbar". Bis zum 27. März soll sie erarbeitet sein.

Fernsteuerung

Noch keine endgültige Lösung konnte der Rat bei der sogenannten "Fernsteuerung" erzielen. Dabei geht es darum, dass Telekommunikationsanschlüsse auf eigenem Hoheitsgebiet unter Einschaltung nationaler Diensteanbieter per Fernsteuerung der in einem anderen Mitgliedsstaat liegenden Bodenstation überwacht werden sollen. Hierbei geht es um die Überwachungsmöglichkeiten von Satellitentelefonie.

Um einen solchen Fernzugriff durchführen zu können, müssen die nationalen Telekommunikationsbetreiber generell zur Durchführung nationaler

Überwachungsanordnungen verpflichtet werden. Sie müssen eine Schnittstelle vorhalten, die den direkten Zugriff der Strafverfolger ermöglicht. Bei einem Fernzugriff auf die Bodenstation in einem anderen Staat ist jedoch nicht nur eine technische Schnittstelle, sondern auch die Zustimmung des Staates nötig.

Zur Zeit befindet sich die einzige Bodenstation des Satellitensystems Iridium in Italien. Der italienische Staat wollte jedoch den Fernzugriff nur dann zulassen, wenn die Grundsätze der italienischen Verfassung durch den Zugriff anderer Staaten nicht verletzt werden würden. Dies lehnten jedoch die anderen Mitgliedsstaaten ab.

In einem Kompromiss vom November 1999 wird Italien dazu verpflichtet, alle innerstaatlichen gesetzlichen Vorschriften zu beseitigen, die einen Fernzugriff behindern würden. Nicht damit verbunden ist jedoch ein garantierter Fernzugriff.

Keine Kostenfrage?

Generell werden die Telekommunikationsbetreiber nur durch nationales Recht dazu verpflichtet, Überwachungen zu ermöglichen. So regelt das Rechtshilfeabkommen allein die Beziehungen der Mitgliedsstaaten untereinander, nicht jedoch deren Beziehungen zu Betreibern von Telekommunikationsanlagen. Daher wird auch hier nicht geregelt, wer die Kosten für die Überwachungen tragen soll, da dies eine nationale Angelegenheit ist.

Generell erwarten die Beamten Einsparungen aufgrund der vereinfachten Geschäftswege - trotz einem quantitativ erhöhten Rechtshilfeverkehr. Entstehen Kosten durch die Überwachung von Telekommunikation oder die Vernehmung von Videokonferenzen, trägt dies der ersuchende Mitgliedsstaat. Bislang galt der Grundsatz, dass für die Kosten der ersuchte Staat aufkommen müsse.

Am 27. März soll im Rat das Rechtshilfeabkommen verabschiedet werden. Noch besteht jedoch ein parlamentarischer Vorbehalt der Bundesregierung zur Frage der Telekommunikationsüberwachungen. Hierzu trifft sich der Bundestags-Rechtsausschuss am 23. März. Eine Stellungnahme des Bundesrates ist bislang noch nicht erfolgt.

Links

[1] <http://www.heise.de/tp/deutsch/inhalt/te/5810/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6632/1.html>

»Grenzüberschreitendes Abhören führt in gesetzliches Minenfeld«

Jelle van Buuren 15.02.2000

Ausschussbericht des Europäischen Parlaments lehnt grenzüberschreitendes Abhören der Telekommunikation ab.

Ein Ausschuss des Europäischen Parlaments äußerte schwerwiegende Kritik am Entwurf eines Rechtsakts über die Rechtshilfe in Strafsachen zwischen den Mitgliedsstaaten der Europäischen Union. Der Hauptpunkt der Kritik bezieht sich auf den umstrittenen Artikel 18. Dieser ermöglicht Mitgliedsstaaten das Abhören einer Person auf dem Territorium eines anderen Mitgliedsstaates ohne die Unterstützung des letzteren anzufordern. Wenn es nach Antonio Di Pietro vom Ausschuss für die Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten geht, soll Artikel 18 ersatzlos gestrichen werden.

Der Vorschlag Artikel 18 zu streichen, ist Bestandteil eines *Berichts* über den vorgeschlagenen Rechtsakt über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, über den das Europäische Parlament am kommenden Donnerstag abstimmen wird. Laut dem Berichterstatter Antonio Di Pietro (Italien, Gruppe der Europäischen Liberalen, Demokraten und Reformpartei) würde der umstrittene Artikel die EU in ein gesetzliches Minenfeld führen. Er ermöglicht das Abhören über Staatsgrenzen hinweg, ohne dass Behörden in dem Land, in dem abgehört wird, informiert werden müssen - also direkte länderübergreifende Überwachung.

Die Mitgliedsstaaten sind über diesen Punkt geteilter Ansicht. Einige Mitglieder wollen die Möglichkeit haben, solche Ermittlungen mit zu verfolgen, so dass zuvor das Einholen einer offiziellen Erlaubnis nötig wäre. Andere Länder, insbesondere Großbritannien, sind gegen eine solche Erlaubnis. Großbritannien hat durch seine Teilnahme am weltweiten Abhörsystem Echelon bereits die Möglichkeit grenzübergreifenden Abhörens. Es möchte keine Einflussnahme anderer Mitgliedsstaaten, insbesondere da sich die Zuständigkeit der Geheimdienste in Großbritannien für nachrichtendienstliche Zwecke und Strafverfolgungsmaßnahmen überschneidet. (siehe TP-Bericht Europäisches Rechtshilfeübereinkommen vor baldigem Abschluss [1])

Großbritannien hat zugestimmt, andere Mitgliedsstaaten dann über Abhörmaßnahmen zu unterrichten, wenn sie im Zuge einer strafrechtlichen Ermittlung erfolgen. Die genaue Definition einer solchen Ermittlung ist jedoch umstritten und Anlass für weitere Änderungsanträge, neben der Streichung von Artikel 18. In einer früheren Version des Berichts wurde dieser Umstand bereits bemängelt:

"Es besteht ein Definitions­mangel in Bezug auf die Straftaten, die durch dieses Übereinkommen abgedeckt werden. Das Ziel des Übereinkommens muss auf schwere organisierte Kriminalität beschränkt bleiben."

Ein weiterer Streitpunkt ist die Frage, was passiert, wenn ein Staat nicht reagiert, wenn er von einem anderen Staat über eine Ermittlung informiert wird. Einige Mitgliedsstaaten folgen dem Prinzip, dass Schweigen stillschweigende Zustimmung signalisiert. Andere sind genau der gegenteiligen Ansicht. Antonio Di Pietro möchte Artikel 18 am liebsten einfach gestrichen sehen.

"Es wird vorgeschlagen, dass dieser höchst umstrittene Artikel gestrichen wird, erstens weil er die der nationalen Sicherheit und Integrität dienenden geheimdienstlichen Aktivitäten behindern könnte, und zweitens weil er den Ermittlungsbehörden eines Mitgliedsstaates erlauben würde, Abhörmaßnahmen auf dem Boden eines anderen Mitgliedsstaates ohne dessen Zustimmung und Unterstützung durchzuführen".

An einer anderen Stelle im Bericht sagt Di Pietro: "Dieser Artikel führt uns in ein gesetzliches Minenfeld, wobei einige Mitgliedsstaaten völlig unabhängige Ermittlungen in anderen Mitgliedsstaaten ausführen möchten, im Interesse ihrer nationalen Sicherheit (und mittels des Einsatzes von Geheimagenten?), und sich dabei der zeitaufwendigen Aufgabe entledigen möchten, dafür die Zustimmung der gesetzlichen Autoritäten des anderen Landes einzuholen." Laut Di Pietro könnte das "zur Legalisierung der in einer Grauzone stattfindenden Aktivitäten der Geheimdienste" führen.

Andererseits würde Artikel 18 von den Mitgliedsstaaten verlangen, ihre Aktivitäten auf dem Gebiet der "vorbeugenden Sicherheit" den gesetzlichen Behörden anderer Mitgliedsstaaten bekannt zu machen - doch Strafverfolgungsbehörden und Gerichte sind per Definition nur zuständig, nachdem eine Straftat begangen wurde.

Aus all diesen Gründen ist Di Pietro der Ansicht, dass "die Zeit noch nicht reif ist, dieses Problemfeld zum Bestandteil der Gesetzgebung der Union zu machen". "Es handelt sich um eine sehr heikle Angelegenheit, die weiterer Überlegungen bedarf. Sorgfältige Abwägung aller möglichen Maßnahmen führt zu der Schlußfolgerung, dass die Verabschiedung von Gesetzen auf europäischer Ebene zu diesem Zeitpunkt kein weiser Schritt wäre", sagte Di Pietro. Die Meinung des Ausschusses des Europäischen Parlaments, dem Antonio di Pietro angehört, ist in dieser Angelegenheit allerdings nicht bindend.

Links

[1] <http://www.heise.de/tp/deutsch/inhalt/te/5696/1.html>

Glossar

Berichts

ENTWURF EINES BERICHTS von Antonio Di Pietro (PE 232.057) über den Entwurf eines Rechtsakts des Rates über die Erstellung des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union.

Copyright © 1996-2003. All Rights Reserved. Alle Rechte vorbehalten

Heise Zeitschriften Verlag, Hannover

Erste offizielle Bestätigung für Echelon aus den USA

Florian Rötzer 26.01.2000

Aufgrund des Freedom of Information Act wurde jetzt ein Dokument gefunden, das explizit auf Echelon hinweist

Obgleich es bislang so erschienen sein mag, als sei Echelon, das globale Lauschsystem des amerikanischen Geheimdienstes NSA und der Geheimdienste von Australien, Großbritannien und Neuseeland, möglicherweise nur ein Produkt von paranoiden Verschwörungstheorien, so wurde jetzt erstmals ein Dokument gefunden, in dem dieser Name explizit auftaucht.

Jeffrey Richelson von den National Security Archives, ein Forschungsinstitut an der George Washington University und trotz des ähnlichen Namens nicht mit der NSA verbunden, hat das Dokument unter vielen weiteren über die Geheimdienste gefunden, die er aufgrund des Freedom of Information Act angefordert und erhalten hat.

Auf seiner Website hat er die Dokumente veröffentlicht und in einem [1] findet sich die namentliche Nennung: "Perform the following specific functions and tasks: 1) Maintain and operate an Echelon-Site, 2) ... process and report intelligence information ..., 3) Ensure the privacy of US citizens are properly safeguarded." Das Dokument stammt vom Naval Security Group Command in Sugar Grove, West Virginia, und stammt aus dem Jahr 1992.

Für Richelson ist das eine offizielle Bestätigung des Echelonsystems, doch möglicherweise habe es nicht das Ausmaß, das von Bürgerrechtsgruppen unterstellt wurde: "In reality, ECHELON is a more limited program, allowing the UKUSA allies to specify intelligence requirements and automatically receive relevant intercepts obtained by the UKUSA facilities which intercept satellite communications (but not the U.S. facilities that receive data from SIGINT satellites). It is also limited by both technological barriers (the inability to develop word-spotting software so as to allow for the automatic processing of intercepted conversations) and the limitations imposed on collection activities by the UKUSA allies-at least as regards the citizens of those countries.". Er glaubt auch nicht, dass amerikanische Bürger belauscht worden seien, was natürlich nicht heißt, dass die Vermutungen, Echelon habe weltweit die Satellitenkommunikation abgehört und auch der amerikanischen Wirtschaftsspionage gedient, nicht zutreffen müssen.

Richelson ist überdies der Meinung, dass das Echelonsystem nicht so viele Lauschposten

habe, wie man das angenommen hat. Aus einem weiteren Dokument [2] aus dem Jahr 1995 gehe hervor, dass dazu Lauschposten der AIA's 544th Intelligence Group in Puerto Rico, Sugar Grove, Yakima (Washington), Guam und Japan gehören, aber auch die Abhörstationen in Menwith Hill, Grossbritannien, Bad Aibling und Rosman, North Carolina.

Links

[1] <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/09-03.htm>

[2] <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/12-01.htm>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/5721/1.html>

Copyright © 1996-2003. All Rights Reserved. Alle Rechte vorbehalten

Heise Zeitschriften Verlag, Hannover

ENFOPOL bis Mai im Trockenen

Christiane Schulzki-Haddouti 26.2.1999

Aber noch immer ist der Entwurf Verschlusssache

Der europäische Justiz- und Innenausschuß verhandelte am 3. Dezember über den ENFOPOL-Ratsentwurf. Bis Mai sollen die letzten Details geklärt werden. Dies geht aus dem unzensierten ENFOPOL-Papier 10951/2/98 Rev 2 hervor, das jetzt der Redaktion vorliegt.

Druck kommt seitens der „Arbeitsgruppe für polizeiliche Zusammenarbeit“ und den sogenannten ILETS und IUR/ST-Experten - IUR steht für „International User Requirements“ -, die die Anpassungen der juristischen und technischen Abhörmöglichkeiten auf die neuen Technologien wie Satellitenkommunikation und Internet für „dringend notwendig“ erachten. Der vorliegende Entwurf basiert auf dem Ratsentschluß vom 17. Januar 1995.

Nun herrscht erstmals auch Klarheit über die Entstehungsgeschichte der verschiedenen ENFOPOL-Papiere: Bei einem Treffen vom 20. bis 22. Oktober in Wien sowie einem abschließenden Treffen vom 27./28. Oktober in Madrid überprüften die IUR-Experten, inwieweit die neuen Anforderungen bereits im vorhandenen Anforderungstext enthalten waren. Die Resultate flossen in die revidierte Version Rev 1 [1] ein, die am 5. November der Arbeitsgruppe für polizeiliche Zusammenarbeit“ übergeben wurde. Das vorliegende Dokument „Rev 2“ wird nun unter der deutschen Ratspräsidentschaft weiterhin überarbeitet. Noch immer ist das Dokument „limite“ - „Verschlusssache“.

Die Minister hatten im Dezembertreffen unter dem Tagesordnungspunkt „Konvention zur gegenseitigen Rechtsbeihilfe“ über das weitere Schicksal des Entwurfs positiv entschieden. Das nächste Arbeitstreffen der EU-Minister findet am 12. März in Brüssel statt. Bis dahin muß noch eine knifflige juristische Hürde überwunden werden. Denn noch besteht keine Einigung darüber, über welche der Rechte der Staat mit der Iridium-Bodenstation [2], sprich Italien, verfügen darf. Die Maximalforderung besteht darin, daß andere Länder via Remote-Control ohne richterlichen Beschluß italienischer Behörden auf den Telekommunikationsverkehr zugreifen können. Eine politische Richtungsentscheidung soll bis zum 12. März getroffen werden. Beobachter gehen davon aus, daß der Ratsentwurf bereits bis zum 27. Mai verabschiedet wird.

Damit könnten noch im laufenden Jahr die nötigen juristischen Anpassungen auf nationaler Ebene erfolgen. Je nach Land könnte dies in einer Verordnung geschehen, die von den Behörden erlassen wird, oder per Gesetz, das vom Parlament erlassen wird. Unterschied: Die Debatte in den Parlamenten ist öffentlich, die Diskussionen in den

Ministerien sind es nicht.

Links

[1] <http://www.heise.de/tp/deutsch/special/enfo/6332/1.html>

[2] <http://www.heise.de/tp/deutsch/special/enfo/6325/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6375/1.html>

Copyright © 1996-2003. All Rights Reserved. Alle Rechte vorbehalten

Heise Zeitschriften Verlag, Hannover

Neues von Echelon

Florian Rötzer 27.12.1999

Dänische Journalisten über Beteiligung Dänemarks und anderer NATO-Staaten

Journalisten der dänischen Zeitung Ekstra Bladets [1] spüren seit einiger Zeit den Tätigkeiten der Geheimdienste und der von ihnen praktizierten Überwachung der Kommunikation nach. Im Mittelpunkt der fast 50 Recherchen und Interviews, die Bo Elkjaer und Kenan Seeberg inzwischen veröffentlicht haben, steht Echelon, das von der NSA geleitete weltweite Lauschsystem, an dem offenbar nicht nur im Rahmen des UKUSA-Abkommens die USA, Neuseeland, Kanada, Australien und Großbritannien, sondern nach ihren Informationen nahezu alle NATO-Mitglieder als dritte Partner beteiligt sind.

Einige der Artikel sind inzwischen bei Cryptome.org [2] ins Englische übersetzt worden. Thema ist auch die Beteiligung des dänischen Geheimdienstes. So hat der dänische Verteidigungsminister Hans Haækkerup bereits im September dieses Jahres bestätigt, dass Dänemark an "einem globalen Überwachungssystem beteiligt" ist. Zwar könne er die Frage nicht beantworten, dass dies in Kooperation mit der NSA geschehe, aber der dänische militärische Geheimdienst FE höre Signale seit dem Ende des Zweiten Weltkriegs ab. Die Anlagen seien kontinuierlich aufgerüstet worden, abgehört und verarbeitet werden Informationen von Satelliten.

Bis zu dieser Bestätigung hatten das Justiz-, das Verteidigungs- und das Forschungsministerium jede Kenntnis eines globalen Überwachungssystem abgestritten. Der Verteidigungsminister räumte dann zwar ein, dass es ein derartiges globales Überwachungssystem gebe, Dänemark daran beteiligt sei und Informationen mit anderen Geheimdiensten austausche, aber dass es nicht den Namen Echelon trage. Garantieren wollte er nicht, dass dänische Bürger nicht illegal abgehört werden könnten.

Laut den beiden Journalisten habe Dänemark sich an dem globalen Überwachungssystem ab 1997 in Zusammenhang mit der Reorganisation des NATO-Hauptquartiers BALTHAP (Baltic Approach) in Karup, Jütland, stärker beteiligt. Angeblich wurde damals den Amerikanern im Zusammenhang mit der Erlaubnis, dass die US-amerikanische 650th Military Intelligence Group Maßnahmen zur Gegenspionage durchführen kann, auch das Recht eingeräumt, die dänische Bevölkerung zu belauschen. Die Aufgabe dieser Gruppe sei es, die Kooperation der Geheimdienste der NATO-Staaten zu koordinieren.

In einem Gespräch mit den Journalisten, das Ende November veröffentlicht wurde, versicherte ein ehemaliger Mitarbeiter der NSA, Wayne Madsen, dass man mit Echelon

neben der Kommunikation von Privatpersonen, Unternehmen und Interessengruppen die von dänischen Politikern und Ministern abgehört habe. Gefragt nach der Rolle der NSA nach dem Ende des Kalten Krieges antwortete er: "Zunächst haben sie ein globales Computernetzwerk, das Echelon genannt wird. Die Computer sind mit ihren Aufklärungssatelliten und Lauschposten überall auf der Welt verbunden. Und sie führen noch militärische Aufgaben aus. Der Unterschied aber ist, dass sie heute jeden und alles überwachen. Politiker, Organisationen, Unternehmen, Privatpersonen und sogar Freunde in verbündeten Ländern. 1985 war das langfristige Ziel "total hearability", also die Möglichkeit, jede Kommunikation in der ganzen Welt abhören zu können."

Dänemark sei zwar ein Partner der Überwachungsabkommen, aber dänische Minister und Politiker müssten davon ausgehen, ebenfalls belauscht zu werden: "Dänemark hat nicht viel davon, als eine dritte Partei beteiligt zu sein, denn die NSA hat die führende Rolle inne und entscheidet darüber, welche Informationen die anderen Länder erhalten. Wenn sie bestimmte Politiker oder Unternehmen in einem bestimmten Land überwachen, dann teilen sie natürlich dessen Regierung dies nicht mit. Die Informationen, die sie Dänemark geben, sollen entweder ihren eigenen Interessen dienlich sein oder stellen etwas dar, das sie als Bedrohung ansehen. Beispielsweise über die Zamilen oder die PKK. Wenn es um Informationen geht, die den eigenen finanziellen Interessen dienen, dann nutzen sie diese natürlich zu ihrem eigenen Vorteil ... Das Problem ist, dass die NSA ihre Aufgabe aus dem Blick verloren hat. Es ist nicht richtig, dass Steuergelder dazu verwendet werden, großen Shareholders in großen Unternehmen dabei zu helfen, riesige Profite zu erzielen, oder dass die NSA normale Menschen, legale Organisationen und Politiker unter permanentem Verdacht."

Die Journalisten haben auch ein Gespräch mit Margaret Newsham geführt, einer ehemaligen Angestellten der NSA, die bei Lockheed gearbeitet hat und im britischen Menwith Hill stationiert war. Sie sagt, sie an der Entstehung von Echelon beteiligt gewesen und dass das Computernetzwerk von der NSA Echelon genannt wurde: "Die Programme heißen SILKWORTH und SIRE, und einer der wichtigsten Satelliten ist VORTEX. Er belauscht unter anderem Telefongespräche." Sie sagt, die dänischen Minister können glauben, was sie wollen: "Ich weiß, dass es Echelon gibt, weil ich beim Aufbau des Systems mitgeholfen habe." Die Überwachung sei schon zu ihrer Zeit sehr stark zielorientiert gewesen: "Wir konnten eine Einzelperson oder eine einzelne Organisation herausgreifen und in Echtzeit jede Kommunikation zu jeder Zeit abhören. Die Person wurde überwacht, ohne jemals eine Chance zu haben, dies zu entdecken, und die meisten Informationen wurden mit Lichtgeschwindigkeit an eine andere Station gesendet, an der es eine gewaltige digitale Verarbeitungskapazität gab. Alles fand ohne richterliche Genehmigung statt." Funktioniert habe das System wie eine Suchmaschine: "Indem wir unsere Suche auf bestimmte Nummern, Personen oder Begriffe beschränkt haben, bekamen wir Resultate, die alle mit dem zu tun hatten, was wir eingegeben hatten." Echelon war eines der sogenannten "Black Programs", über die auch die amerikanische Regierung nicht informiert wurde. "Wir spionieren unsere eigenen Bürger und den Rest

der Welt aus, selbst unsere europäischen Verbündeten. Wenn ich 'Amnesty' oder 'Margaret' sage, dann wird dies abgehört, analysiert, koordiniert, weitergeleitet und registriert, falls dies im Interesse der Geheimdienste ist. Ich sprach kürzlich mit einem Radiologen, der dasselbe wie ich, nur 10 Jahre später, 1991 während der 'Operation Desert Storm', machte. Wenn ich Ihnen alles erzählen könnte, dann würden Sie verstehen, dass Echelon so groß ist, dass sein Ausmaß fast die Vorstellungskraft übersteigt."

Der republikanische Kongressabgeordnete Bob Barr [3], der früher bei der CIA gearbeitet hat und im Rahmen seiner Beteiligung am House Judiciary and Government Reform Committee mit durchgesetzt hat, dass NSA, CIA und das Justizministerium einen Bericht über den gesetzlichen Rahmen beim Abhören der Kommunikation von amerikanischen Bürgern mit dem Echelon-System leisten müssen, äußerte in einem am 10.12. veröffentlichten Gespräch mit den beiden Journalisten erneut den Verdacht, dass die am Echelon-System beteiligten Staaten Informationen über andere Länder sammeln und dann diese austauschen. So könnte etwa der britische Geheimdienst Informationen über amerikanische Bürger sammeln. Für Barr ist das eine Aushebelung des Rechts: "Die Bevölkerung hat ein Recht zu wissen, was vor sich geht, besonders wenn wir den starken Verdacht haben, dass nicht nur bestimmte Ziele überwacht werden, sondern auch gewöhnliche Bürger, Unternehmen und so weiter." Barr betonte, er sei ganz überrascht, "dass die Länder, die das System zusammen mit der NSA betreiben, bislang nicht verlangt haben, mehr darüber informiert zu werden, d.h. die sogenannten UKUSA-Partner Kanada, Australien, England und Neuseeland. Überdies ist, soweit ich Informationen habe, anscheinend fast jedes westeuropäische Land daran beteiligt." Bis zum letzten Jahr habe man nicht erkannt, was da vor sich geht: "Je mehr wir davon erfahren, desto mehr erkenne ich, dass wir hier ein ernsthaftes Problem haben." Die Arbeit der Geheimdienste habe sich in den letzten Jahren enorm verändert: "Unser Kongress hat in den letzten 20 Jahren die Arbeit der Geheimdienste nicht mehr überprüft. Während dieser Zeit haben sie völlig neue Möglichkeiten erworben, Informationen zu sammeln und auszuwerten. Deswegen habe ich Anhörungen im Kongress gefordert, die im nächsten Jahr beginnen werden."

Mal schauen, wann die Parlamentarier in Deutschland aufwachen.

Links

- [1] <http://www1.ekstrabladet.dk/>
- [2] <http://jya.com/crypto.htm>
- [3] <http://www.house.gov/barr/>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6572/1.html>

ENFOPOL und das Recht auf »Eigentumsfreiheit«

Thomas Keul 30.11.1999

Scheitert die Realisierung des Überwachungsstaates an einer "grundrechtswidrigen Kostenüberwälzung"?

Ein heute Vormittag in Wien präsentiertes Rechtsgutachten attestiert dem ENFOPOL 98 Papier [1], dass es "das Ausmaß der technisch möglichen und rechtlich (mit geringen Ausnahmen) bereits zulässigen Datenerfassung im Zuge der Überwachung des Fernmeldeverkehrs in erschreckender Deutlichkeit" festhalte.

Das "Unbehagen" gegenüber den ENFOPOL-Beschlüssen geht, laut Gutachten [2] (RTF-Dokument, veröffentlicht von quintessenz.at [3]), vor allem auf zwei Entwicklungen zurück: Einerseits sei die Datenbasis, die von den Behörden genutzt werden kann, durch neue technische Möglichkeiten größer denn je, andererseits sei der von der Überwachung potentiell betroffene Personenkreis - ebenfalls technologiebedingt - stark gewachsen.

Das Gutachten, dessen Präsentation unter dem Titel "ENFOPOL-Vorstufe zum totalen Überwachungsstaat?" stand, beschäftigt sich in der Hauptsache mit der Frage, wie die ENFOPOL-Bestimmungen zur Überwachung des Fernmeldeverkehrs mit der österreichischen Verfassung vereinbar sind.

Die beiden Autoren, der Verfassungsrechtler Heinz Mayer und der auf Telekomfragen spezialisierte Anwalt Michael Pilz, kommen in ihrem Gutachten zu dem Schluss, dass die Umsetzung der ENFOPOL-Bestimmungen zumindest in zweierlei Hinsicht bedenklich wäre:

- Erstens würde das Fernmeldegeheimnis ausgehöhlt und dadurch vor allem die Nutzer von Mobilfunktelefonen über weite Strecken ihres grundrechtlichen Schutzes beraubt.
- Zweitens stelle es einen Eingriff in das "Recht auf Eigentumsfreiheit" dar, wenn den Betreibern die Pflicht auferlegt werde, Überwachungseinrichtungen auf eigene Kosten zu installieren. Die Passage im Wortlaut: "Die Verpflichtung zur Bereitstellung der notwendigen Infrastruktur ohne Kostenersatz und die damit verbundene Überwälzung der Kosten der Überwachungseinrichtungen auf die Kommunikationsgebühren ist grundrechtswidrig und daher abzuändern."

An dieser letzten Einsicht erkennt man, aus welcher Ecke der Wind diesmal weht: Das Gutachten wurde von den österreichischen Mobilfunkbetreibern finanziert. Deren Vertreter bemühte sich in der Diskussion, auch darauf hinzuweisen, dass die Kosten für die Überwachung doch, bitte schön, der "Bedarfsträger" zu zahlen habe - in diesem Fall das

Innen- und das Justizministerium. Wer die Daten anfordere, der solle auch berappen. Die Kosten mit denen zu rechnen sei, bewegen sich nach Angaben den Mobilfunkanbieter in "dreistelliger Millionenhöhe". [Anm.: Österreichische Schilling]

Feigenblatt User-Vertretung

Ein wenig fadenscheinig nimmt es sich allerdings aus, wenn Unternehmen, die wegen ihres saloppen Umganges mit Kundendaten kürzlich noch für den Big Brother Award [4] nominiert waren, plötzlich die Liebe zu den Grundrecht entdecken. Die sowohl von den Mobilfunkbetreibern, wie auch von den Internet Service Providern im Zusammenhang mit ENFOPOL heftig geforderte Öffentlichkeit scheint ein Ende zu haben, wenn sie nicht so berechenbar ist, wie ein paar Journalisten, denen man Brötchen reicht.

So ist wohl auch der Eiertanz um die Beteiligung der User-Vertretung VIBE!AT [5] an der Pressekonferenz zu interpretieren. Diese hätte zuerst mit am Podium sitzen sollen, wurde dann auf die Teilnahme als Zuhörer zurückgestuft und schließlich im letzten Moment ohne Angabe von Gründen ganz ausgeladen. Am Ende durften die User-Vertreter ihre Erklärung immerhin der offiziellen Pressemappe beilegen. "Als Feigenblatt", meint Peter Kuhm von VIBE!AT, "damit es nicht so aussieht, als würde es nur um die Kohle gehen."

Links

[1] <http://www.heise.de/tp/deutsch/special/enfo/6332/1.html>

[2] http://www.quintessenz.at/ftp/enfopol_gutachten.rtf

[3] <http://www.quintessenz.at/>

[4] <http://www.heise.de/tp/deutsch/inhalt/te/5425/1.html>

[5] <http://www.vibe.at>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6538/1.html>

Bundesregierung arbeitet weiter an Enfopol-Plänen

Christiane Schulzki-Haddouti 15.11.1999

"Nur eine sprachliche Anpassung der Anforderungen von 1995"

Die in dem Dokument Enfopol 19 beschriebenen grenzüberschreitenden Überwachungsmaßnahmen für Satellitenkommunikation und Internet sind eigentlich nur "eine sprachliche Anpassung der Anforderungen von 1995", teilte die Bundesregierung in einer Antwort auf die große Anfrage der CDU/CSU-Fraktion (Drucksache 14/1031) mit.

Die CDU/CSU-Fraktion hatte sich danach erkundigt, "welche Ziele für den Bereich Information und Kommunikation (...) die Bundesregierung in internationalen Arbeitsgruppen wie Enfopol, die dem Schutz der Inneren Sicherheit dienen, verfolgt." Brav antworteten die Beamten, dass sich "die Ratsarbeitsgruppe polizeiliche Zusammenarbeit (AGPZ) deren Dokumente die Kennung "Enfopol" tragen," mit der Frage befasst, "welchen Anforderungen die Netzbetreiber beziehungsweise Diensteanbieter genügen müssen, damit die legale (...) Telekommunikationsüberwachung technisch durchführbar ist".

Damit nicht der Verdacht entsteht, dass es sich bei dem neuen Enfopol-Papier um eine wesentliche Erweiterung der Eingriffsbefugnisse handelt, wiesen sie darauf hin, dass die Ratsentschließung von 1995 bereits einen Katalog von "nicht auf spezielle Kommunikationsmedien und -techniken bezogene Anforderungen enthalte". Das stimmt so nicht, da sich das Papier auf Sprachtelefonie bezog. Andernfalls wäre die Beratung und Verfassung eines neuen Papiers nicht nötig gewesen.

Sowohl die bündnisgrüne, als auch die sozialdemokratische Bundestagsfraktion halten sich in der umstrittenen Überwachungsfrage deutlich aus der Diskussion heraus. Zwar hatte auf Anregung des SPD-Bundestagsabgeordneten Jörg Tausch im Sommer noch eine Veranstaltung des Industrie- und Handelstags in Bonn stattgefunden, seither arbeiten alle Protagonisten jedoch still in ihren Kämmerchen weiter.

Links

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/5486/1.html>

Keine Einigung bei europäischem Rechtshilfeübereinkommen

Christiane Schulzki-Haddouti 12.11.1999

Echelon-Staat Großbritannien blockiert Überwachungspläne der europäischen Strafverfolger.

Die Verhandlungen zu dem europäischen Rechtshilfeübereinkommen stagnieren. Bei einem Treffen des Justiz- und Innen-Rats am 29. Oktober in Luxemburg konnten die Minister erneut keine Einigung erzielen. In der Frage der Telekommunikations-Überwachung fährt die britische Regierung einen eigenen Kurs.

Referenten hatten zuvor einen neuen Vorschlag erarbeitet, um endlich eine Entscheidung herbei zu führen. In Großbritannien gibt es keine klare Trennung zwischen den Abhörmaßnahmen, die von den Polizei- und Zollbehörden einerseits und den Geheimdiensten andererseits durchgeführt werden. Deshalb will Großbritannien, das in das UKUSA-Abkommen zur Signalüberwachung eingebunden ist, unbedingt verhindern, dass Aufklärungsmaterial des Geheimdienstes anderen Mitgliedsstaaten zur Verfügung steht.

In ihrem Abschlusskommunikee einigten sich die europäischen Regierungschefs in Tampere darauf, dass Finnland einen Krompromissvorschlag erarbeiten wird: So soll definiert werden, wer mit welcher Kompetenz in Abhörmaßnahmen involviert sein darf, und welche strafrechtlichen Ermittlungen davon erfaßt sind. Ungelöst scheint das Problem der Mitteilungspflicht: Die britische Delegation hatte vorgeschlagen, dass dem überwachenden Mitgliedsstaat die Möglichkeit eingeräumt werden sollte, von der Unterrichtung des anderen Mitgliedsstaats aus Gründen der "nationalen Sicherheit" abzusehen.

Der Vorschlag hat einen pikanten Hintergrund: Als Mitglied des Echelon-Abhörverbundes hört Großbritannien laut zweier STOA-Berichte, die vom europäischen Parlament in Auftrag gegeben wurden, gemeinsam mit den USA, Kanada, Australien und Neuseeland weltweit die Satellitenkommunikation ab. Die von der britischen Delegation vorgeschlagene Regelung hätte die weitere Geheimhaltung von Aufklärungsergebnissen, die über das Echelonsystem gewonnen werden, garantiert. Wäre Großbritannien jedoch rechtlich dazu gezwungen, den anderen Mitgliedsstaaten Ergebnisse aus diesen Überwachungsmaßnahmen zukommen zu lassen, bekämen diese einen Einblick in das Überwachungssystem.

Unakzeptabel bleibt für Großbritannien daher der alternative Vorschlag der anderen Mitgliedsstaaten, wonach vereinbart werden kann, dass die mitzuteilenden Informationen "über besondere Kanäle weitergeleitet werden, wenn sie geheimhaltungsbedürftig sind". Für Großbritannien steht fest, dass unabhängig davon, ob die Überwachung zum Zwecke einer strafrechtlichen Ermittlung erfolgt oder nicht, geheimgehalten werden muß, wenn sie von den Sicherheits- und Nachrichtendiensten durchgeführt wird.

Überprüft wird daher jetzt im Rat, ob Großbritannien in punkto Telekommunikationsüberwachung nicht an dem Rechtshilfeübereinkommen teilnehmen wird. Interessanterweise gelangte der Präsident des Ausschusses der Ständigen Vertreter in Brüssel zu der Schlußfolgerung, dass eine "Nichtbeteiligung nicht als Ermächtigung angesehen werden könnte, in anderen Mitgliedsstaaten befindliche Personen zu überwachen." Eine entsprechende Klausel sollte dann aufgenommen werden, wenn die Verhandlungen mit Großbritannien scheitern.

Die Telekommunikationsüberwachung soll nach dem Luxemburger Treffen erneut im Ausschuss der Ständigen Vertreter und im Artikel-36-Ausschuss beraten werden.

Links

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/5476/1.html>

Enfopol-Pläne in Europäisches Rechtshilfeabkommen integriert

Christiane Schulzki-Haddouti 08.11.1999

Genereller Fernzugriff?

Monatelang war es um die Enfopol-Pläne still. Der europäische Lobbyverband der Provider EuroISPA wählte sich sogar schon auf der Siegerseite: Er nahm an, die Pläne für das grenzüberschreitende Abhören würden nicht mehr verfolgt. Wie der vorliegende Entwurf eines umfassenden Europäischen Rechtshilfeübereinkommens vom 28. Juni zeigt, bleibt allerdings die Abhörbarkeit von Satellitenkommunikation trotz des Pleitegeiers über Iridium ein Thema. Umstritten war bis zuletzt über welche Rechte der Staat mit der Iridium-Bodenstation - das ist in Europa Italien - verfügen soll.

Beim im Artikel 11 b des Rechtshilfeübereinkommens geregelten "Remote approach" können nationale Überwachungsmaßnahmen "in Bezug auf Telekommunikationsanschlüsse auf eigenem Hoheitsgebiet unter Einschaltung nationaler Diensteanbieter mittels Fernsteuerung der in einem anderen Mitgliedsstaat gelegenen Bodenstation" durchgeführt werden. Dafür ist kein eigenes Rechtshilfeersuchen an den Mitgliedsstaates mit der Bodenstation nötig. Voraussetzung dafür ist natürlich, dass alle Telekommunikationsdiensteanbieter "die Durchführung nationaler Überwachungsanordnungen ermöglichen". Genau das hatten die Enfopolpläne gefordert. Jetzt sind sie in das EU-Rechtshilfeübereinkommen integriert.

Italien wollte den Fernzugang nur unter der Voraussetzung zulassen, dass die nationalen Überwachungsmaßnahmen anderer Mitgliedstaaten die Grundsätze der italienischen Verfassung nicht verletzen. Nach intensiven Beratungen lehnten dies die meisten anderen Mitgliedstaaten jedoch ab. Darauf hin gab Italien am 10. Juni dem Druck nach. Es ging in die Gegenoffensive, indem es einen neuen Vorschlag unterbreitete: Er sieht vor, dass die Telekommunikationsbetreiber verpflichtet sein sollen, anderen europäischen Diensteanbietern "Einrichtungen zur Überwachung von Telekommunikationsverkehr direkt zugänglich zu machen". Damit wäre ein genereller Fernzugriff gestattet - unabhängig von der zugrundeliegenden Technologie.

Der italienische Vorschlag wurde jedoch dann allerdings in einer weiteren Verhandlungsrunde entschärft, da die Mitgliedstaaten befürchteten, ein garantierter "Remote Approach" könnte "Folgeprobleme bei der Durchsetzung auslösen. Von daher wurde die "Verpflichtung" durch eine "Berechtigung" im Dokument COPEN 6 ersetzt. Unter der finnischen Präsidentschaft will die EU darüber noch weiter beraten.

Grenzüberschreitende Zusammenarbeit

Im Artikel 12 des Rechtshilfeübereinkommens wird geregelt, dass ein anderer Mitgliedsstaat dazu verpflichtet werden kann, eine technische Überwachung des Telekommunikationsverkehrs "in Echtzeit" vorzunehmen oder bereits bestehende Überwachungsaufzeichnungen auszuliefern. Wurden die Logfiles eines Internet-Providers gespeichert, können sie laut Artikel 12 ausgeliefert werden. Benötigt ein Staat für die Überwachung in einem anderen Staat nicht die technische Unterstützung von diesem, so soll auch das unter bestimmten Voraussetzungen möglich sein.

Dieser kann das Ersuchen jedoch ablehnen, wenn die Maßnahmen "im Widerspruch zu Grundsätzen seiner Rechtsordnung steht" und "wenn die Überwachung nach seinem nationalen Recht unzulässig gewesen wäre. Wurde bis zum Widerspruch bereits Beweismaterial erlangt, darf dieses nicht in Strafverfahren verwendet werden. Schweden ist mit dieser Regelung noch nicht einverstanden - da dies dem Grundsatz der freien richterlichen Beweiswürdigung nach schwedischem Strafprozessrecht widerspricht. Frankreich hat zusammen mit Schweden einen neuen Vorschlag vorgelegt, der vorsieht, dass die Überwachungsmaßnahme dann nicht weiter durchgeführt werden darf, wenn der Aufenthaltsstaat nach am vierten Tage seiner Unterrichtung schweigt. Eine Klärung steht jetzt an.

Auf Kosten der Provider

In Artikel 14 schließlich wird die Frage der Kosten erklärt. So trägt der ersuchende Mitgliedsstaat die Überwachungskosten des Betreibers, nicht jedoch die Investitionskosten, die der Betreiber aufwenden muss, um die Überwachung technisch möglich zu machen. Ganz geklärt ist diese Frage allerdings noch nicht. Nach "Ansicht des Vertreters der Kommission" soll diese Frage in "einem geeigneten Gremium" behandelt werden.

Sonderrolle Großbritannien

Unklar ist, ob mit Großbritannien eine Einigung erzielt werden kann. Dort erlässt nämlich der Secretary of State im Home Office die Überwachungsanordnung - im Interesse der nationalen Sicherheit oder der präventiven beziehungsweise repressiven Strafverfolgung. Er wird dann tätig, wenn die britischen Geheimdienste oder Polizei- und Zollbehörden einen entsprechenden Antrag eingebracht haben. Eine klare Trennung zwischen Abhörmaßnahmen von Strafverfolgungsbehörden einerseits und Geheimdiensten andererseits gibt es daher in Großbritannien nicht. Zudem unterstützen seit 1996 die Geheimdienste die Polizeibehörden bei der Aufklärung schwerer Straftaten. Allerdings darf das Abhörmaterial nicht als Beweismittel in Strafverfahren verwendet werden, sondern immer nur zu Aufklärungszwecken.

Großbritannien wollte daher die auf Antrag der Geheimdienste ergangenen Abhörenordnungen komplett aus der Vereinbarung ausschließen, ebenso die Maßnahmen von Strafverfolgungsbehörden, die im Interesse der nationalen Sicherheit tätig werden. Das war jedoch für die anderen Staaten "nicht akzeptabel". Nach intensiven bilateralen Beratungen im Ausschuss der Ständigen Vertreter, auf der EU-Rat-Tagung am 27. und 28. Mai sowie auf einer Sondersitzung des Artikel 36-Ausschusses am 10. Juni kam jedoch etwas Bewegung in die harte britische Position, berichtet das Bundesjustizministerium. Am 10. Juni erarbeiteten die Beamten einen Kompromiss, der eine Einbeziehung der Abhörmaßnahmen erlaubt, die allein aufgrund von strafrechtlichen Ermittlungen vorgenommen wurden.

Zeitplan

In den Enfpopol-Plänen ging es im Prinzip immer um das grenzüberschreitende Abhören von Kommunikation - egal, mit welchen technischen Geräten sie übermittelt wird. Während die Arbeitsgruppe "Polizeiliche Zusammenarbeit (Enfpopol)" versuchte, sich auf eine dafür notwendige einheitliche Abhörterminologie zu verständigen, erarbeiteten die Juristen in der Arbeitsgruppe "Justpen" die rechtlichen Voraussetzungen. Das unter anderem von ihnen erarbeitete Rechtshilfeabkommen zeigt deutlich, dass sich an der Zielsetzung nichts geändert hat. Gleichwohl wurden Sicherungsmechanismen eingebaut, um ein Befugnis-Hopping zu verhindern. Abgehört werden kann nur auf Grundlage der jeweils nationalen Befugnisse - ausgenommen davon ist allerdings nach aktuellem Stand der Fernzugriff auf die Bodenstationen von Satellitenkommunikationssystemen wie Iridium.

Wann das Übereinkommen verabschiedet werden soll, ist noch ungewiss. Aufgrund eines niederländischen Änderungsvorschlags von 1998 hatte die Bundesregierung einen bis heute nicht aufgehobenen parlamentarischen Vorbehalt zu den Überwachungsbestimmungen eingelegt. Die politische Bedeutung wurde jedoch vom Bundesjustizministerium als "dringlich" eingestuft. Bis jetzt wurden diese im Bundestag noch nicht behandelt. Auch eine Stellungnahme des Bundesrates steht noch aus. Vor der Annahme des Übereinkommens durch den Rat muss das Europäische Parlament angehört werden.

Im Rat wird allerdings noch über die datenschutzrechtlichen Regelungen diskutiert. Deutschland und Belgien bestehen auf einer Vereinbarung datenschutzrechtlicher Regelungen. Doch das stößt bei den anderen Mitgliedstaaten auf Widerstand. Sie sind der Auffassung, dass die Regelungen auf nationaler Ebene auch für die Übermittlung personenbezogener Daten im Rahmen des Rechtshilfeabkommens ausreichen.

Links

Enfopol-Vorhaben vorläufig ad acta gelegt?

Florian Rötzer 14.10.1999

Der Europäische Rat will nach der Kritik offenbar die Pläne für das EU-Lauschsystem zur Überwachung der Telekommunikation und des Internet vollständig überarbeiten

Nach einem Bericht des britischen Online-Magazins The Register [1] scheint das Vorhaben der EU, ein umfassendes Lauschsystem für das Internet einzuführen, das auch unter der Bezeichnung Enfopol formuliert wurde, erst einmal ad acta gelegt, wenn nicht deswegen auch schon ganz begraben worden zu sein.

Wie The Register von Informanten aus dem Umkreis der finnischen EU-Präsidentschaft erfahren haben will, soll diese Entscheidung des Europäischen Rats in den nächsten Tagen bekannt gegeben werden. Das gesamte Vorhaben soll dann neu überarbeitet werden. Kritik am umfassenden Lauschsystem entstand auch deswegen, weil die Ausführungen und Anforderungen von Enfopol zu ungenau gewesen seien. Jean Christophe Le Toquin, Präsident der EuroISPA [2], der europäischen Vereinigung der Internetprovider, begrüßte die Entscheidung: "Der größte Mangel beim Enfopol-Vorhaben war, dass viele der Punkte nicht klar definiert worden sind. Der aktuelle Text verlangt nach einem ganzzeitigen Zugang in Echtzeit' auf die 'neuen' Kommunikationsmittel, ohne jemals genau darzulegen, welche genau davon betroffen sind und wer das bezahlen soll." Er hofft überdies, dass die europäischen Politiker, wenn sie das neue Enfopol-Papier formulieren, auch Experten aus der Wirtschaft hören und einbeziehen werden.

Links

[1] <http://www.theregister.co.uk/>

[2] <http://euroispa.org/>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6501/1.html>

Europa: Die totale Überwachung?

02.06.1999

ZDF berichtet über Enfopol

Die Ankündigung von ZDF:

Offene Grenzen und Freizügigkeit für die EU-Bürger versprach das Schengener Abkommen. Gleichzeitig ist die Europäische Union jedoch auf dem Weg zum Überwachungsstaat. Das ZDF-auslandsjournal berichtet am Donnerstag, 3. Juni 1999, 23.00 Uhr, über den europaweiten Lauschangriff, den Brüssel jetzt plant.

Auf Initiative des amerikanischen FBI bereitet die Europäische Union eine vollständige polizeiliche Überwachung des Datenverkehrs in der Gemeinschaft vor. Der Ratsentwurf "Enfopol" sieht die "permanente Überwachung des Fernmeldeverkehrs in Echtzeit" vor und zwingt alle Betreiber von Funktelefon- und Computernetzen, "Einbruchstellen" für den polizeilichen Lauschangriff in ihren Systemen bereitzustellen. Nach dem EU-Entwurf ist auch das Verschlüsseln zum Beispiel von geheimen Firmendaten nicht erlaubt. Nach Ansicht der nordrhein-westfälischen Datenschutzbeauftragten Bettina Sokol ist dieser EU-Plan verfassungswidrig.

Auch die Befugnisse der europäischen Polizeibehörde "Europol" gehen weit über die Möglichkeiten des nationalen Polizeirechts hinaus. Ab 1. Juli 1999 darf Europol umfassend Intimdaten von Bürgern speichern, zum Beispiel zum Sexualverhalten und zur Gesundheit. Vor Gericht können EU-Bürger die Löschung ihrer bei Europol gespeicherten Daten nicht durchsetzen. Auch Datenmißbrauch durch die Europol-Beamten ist nicht strafbar. Die Beamten genießen Immunität.

Links

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6414/1.html>

Ein Wort zur Überwachung

Armin Medosch 21.05.1999

Ad Enfopol: Weder Paranoia schüren, noch Gefahren verharmlosen.

Die Verschiebung des EU-Ratsbeschlusses über die Enfopol-Überwachungspläne markiert einen wichtigen Etappensieg. Nicht dass wir diesen für uns allein beanspruchen wollen. Doch ohne falsche Bescheidenheit läßt sich sagen, daß Telepolis mit den ersten Artikeln im November 1998 und der Veröffentlichung des Enfopol 98 Papiers den Stein ins Rollen gebracht hat. Sie, liebe Leserinnen und Leser, haben zur Verbreitung dieser alarmierenden Nachrichten beigetragen und wir möchten Ihnen an dieser Stelle für Ihre Aufmerksamkeit und Interesse danken. Doch es besteht kein Grund für verfrühten Jubel, aufgeschoben ist nicht aufgehoben. Während der EU-Bürokratietiger vorübergehend beschwichtigt erscheint, bleibt der Druck auf Individuen bestehen und droht die Aushöhlung demokratischer Freiheiten nicht nur von Seiten einer unkontrollierbaren Techno-Bürokratie.

Es scheint leider der Fall zu sein, daß Themen wie Überwachung des Telekommunikationsverkehrs nicht die Aufmerksamkeit erhalten, die es benötigen würde, um Fehlentwicklungen wirkungsvoll entgegenzuarbeiten. Die deutsche Presse hat Enfopol weitgehend verschlafen. Man kann nur Spekulationen darüber anstellen, warum dem so ist. Möglicherweise fehlt in den Redaktionen das Verständnis für Sachzusammenhänge und es wird die fatale Fehlannahme getroffen, das betreffe "nur" Computernerds. Es ist allerdings schon eher journalistische Fahrlässigkeit, wenn die Recherche von Journalisten, durch Telepolis oder die Freedom For Links Kampagne aufmerksam geworden, sich darauf beschränkt, einmal beim Bundesinnenministerium anzurufen und sich von der dort erhaltenen Auskunft, das sei ja "nur" ein Update eines bereits 1995 gefassten Ratsbeschlusses, ruhig stellen zu lassen.

Dann scheint es auch, nicht nur bei der Presse, diese Haltung zu geben, was denn eigentlich so schlimm an Überwachungsmöglichkeiten der "gesetzlich ermächtigten Behörden" sei, die schliesslich nichts anderes tun, als ihrer Arbeit nachzugehen, die in unser aller Interesse ist und sich gegen organisiertes Verbrechen, Kinderpornographie, etc., richtet. Wer dagegen etwas hat, müsse für Verbrechen und Kinderpornographie sein. Nicht nur ist das moralische Erpressung, sondern es geht, im Falle der Enfopol Affäre, schlicht an einigen wichtigen Tatsachen vorbei. Ohne die ganzen Fakten und Argumente wieder aufrollen zu wollen, die in der Berichterstattung von Christiane Schulzki-Haddouti, Erich Möchel und Duncan Campbell vorgebracht wurden, läßt sich zusammenfassend sagen, daß es eine Vielzahl von Gründen gibt, warum die Sache zum Himmel stinkt: die geheimniskrämerische Art und Weise, wie bereits der erste Ratsbeschluss 1995 unter FBI-

Einfluss zustande kam; die Vermischung von Geheimdienst- und Polizeiinteressen; der ökonomische Aspekt einer indirekten "Überwachungssteuer", die letztlich von den Nutzern bezahlt wird; der Mangel an Kontrollmöglichkeiten über Ergebnisse von Überwachungsmaßnahmen; die potentiellen Sicherheitsrisiken durch Überwachungsschnittstellen; der Export von Überwachungsgesetzgebung und -Technologien in totalitär regierte Länder; potentielle Schäden durch Wirtschaftsspionage usw.. Dies alles sind handfeste Gründe, um gegen die vorgeschlagenen Massnahmen zu sein, dazu muss man sich nicht erst auf den moralischen Hochsitz der Diskussion allgemeiner Bürgerrechte und Grundfreiheiten begeben.

Ich muss persönlich zugeben, daß ich in manchen Phasen der Berichterstattung, obwohl grundsätzlich überzeugt, richtig zu handeln und weder Sensationsjournalismus zu betreiben, noch Überwachungsparanoia zu schüren, Gefahr lief, die Relevanz der Angelegenheit zu unterschätzen. Bei soviel Berichterstattung über Überwachungsthemen und verwandte Bereiche, nicht nur bezüglich Enfpol sondern auch Datenschutz, Telekommunikationsüberwachungsverordnung, Kryptoregulierung, kann sich so etwas wie Überwachungs müdigkeit einstellen. Was ist schliesslich so ein EU-Ratsbeschluss wert, er muss ja ohnehin erst in nationales Recht umgesetzt werden, um reale Auswirkungen zu haben. Ein Schlüsselmoment, der diese Anfälle des Schwächelns zu überwinden half, war, als ungefähr zeitgleich Duncan Campbells Bericht über ILETS - die geheime Hand hinter Enfpol [1], und Christiane Schulzki-Haddoutis Bericht über die Revision der deutschen Telekommunikationsüberwachungsverordnung [2] erschien. Da wurde einerseits erläutert, wie die International User Requirements (IUR) unter FBI-Einfluss und in einer klandestinen Polizeiarbeitsgruppe zustande kamen, und wie diese IUR nun tatsächlich Einfluss auf deutsche Gesetzgebung haben, indem sich ein für die TKÜV zuständiger Beamter darauf berief, daß unter anderem wegen dieser IUR nur geringer Spielraum für eine liberalere und bürgerfreundlichere TKÜV bestehe. Zieht man dann noch in Betracht, daß die selben IUR nun bereits am Weg durch die Standardisierungsinstanzen für Telekommunikationsgeräte sind und Überwachungsschnittstellen bald zum Bestandteil aller serienmässigen Telekommunikationsanlagen werden könnten, da wurde klar, daß Enfpol, auch wenn es nur Codename für bestimmte EU-Papiere ist, alles andere als ein Papiertiger ist. Wie sich daraus ableiten ließ, ist die Arbeitsgruppe für polizeiliche Zusammenarbeit schon viel weiter, als in den schlimmsten Befürchtungen angenommen.

Es gibt aber auch das andere Extrem: die übertriebene Furcht vor dem totalen Überwachungsstaat, die schliesslich in die Resignation führt; die von manchen Leserstimmen im Forum zum Ausdruck gebrachte Angst, daß der totale Überwachungsstaat bereits Realität ist und der einzelne Bürger dem völlig hilflos ausgesetzt ist. Wie unter anderem die Verschiebung der Enfpol-Resolution nun zeigt, ist ein wenig mehr Vertrauen in die Demokratie und Optimismus bezüglich der Möglichkeiten des Einzelnen angebracht. Resignation führt nur in die Isolation, Handlungsmöglichkeiten sind durchaus gegeben und das Internet ist ein sehr geeignetes Instrument, um

Sammelbecken für Bürgerprotest herzustellen. Selbst wenn es manchmal so aussieht, als wäre "Widerstand zwecklos", so kann auch ein noch so kleines Sandkorn die Mühlen der mächtigen EU-Bürokratie zumindest vorübergehend blockieren und eine wichtige Denkpause erzwingen. Genau das ist geschehen. Es gibt keinen Grund, die Sektkorken knallen zu lassen, aber man kann zumindest ein wenig still in sich hineinlächeln, der ganze Aufwand war nicht nur für den Papierkorb am Desktop.

Zugleich bedeutet "aufgeschoben ja nicht aufgehoben". Die Indifferenz der Mainstream-Presse wird uns erhalten bleiben und geschickte Technokraten werden weiterhin versuchen, alle juristisch-technischen Möglichkeiten auszuschöpfen, während die Protestfront wenig organisiert und sehr fragmentiert erscheint. Es geht hier nicht um Politik alten Stils. Kein Info-Proletariat wird sich weltweit organisieren, um der Info-Elite die Macht zu entreissen. Die Konfliktlinien ziehen sich quer durch Gesellschafts- und Einkommensschichten, verschiedene Niveaus technischen Wissens und Awareness-Levels bezüglich der Bedeutung elektronischer Bürgerrechte. Bei manchen Enfpopol- und Überwachungsgegnern besteht die Gefahr, sich der politischen Blauäugigkeit im Stile der amerikanischen Electronic Frontier Foundation anzuschliessen. Diese erscheint manchmal wie das Cyber-Äquivalent der National Rifle Association. Propagieren die einen das Recht auf den Besitz von Feuerwaffen um jeden Preise und gegen jede Erfahrung und Vernunft, so ist es bei den anderen ein amerikanisch-fundamentalistisches Verständnis von "free speech", das letztlich dazu führt, die "Rechte" texanischer Porno-site-Betreiber und kanadischer Neonazis zu wahren. Bei den Waffenbrüdern ebenso wie den Free-Speech-Fanatikern paart sich dies mit einem tiefen Misstrauen gegenüber dem Staat und finanzielle Lobby-Interessen von Industrien. Durch den Import der Internet-Diskussion nach Europa verbreiten sich auch hier diese Anti-Staats-Ideen. Der oft wie taub und blind agierende Superstaat EU scheint alle Bedenken gegen staatlichen und bürokratischen Machtmissbrauch noch zu unterstützen. Doch die Anti-Staatlichkeit könnte letztlich zum Eigtor werden. Wer schließlich, als der Staat, kann uns vor der Macht multinationaler Konzerne beschützen? Gemessen am Umsatz, bzw. Bruttonationalprodukt, sind die Hälfte der weltweit größten Wirtschaften bereits nicht mehr Staaten, sondern Konzerne. Anders als die Staaten, deren politische Führer ihren Bürgern Rechenschaft schuldig sind, sind diese Unternehmen allein dem Shareholder-Value verpflichtet. Bei aller Wachsamkeit gegenüber politischen Fehlentwicklungen ist die selbe Wachsamkeit gegenüber antidemokratischen Tendenzen geboten, die von solchen Mega-Unternehmen ausgehen.

Faktum ist, daß das Individuum zunehmendem Druck von verschiedenen Seiten ausgesetzt ist, dem Überwachungsstaat, dem Big Brother am Arbeitsplatz. Trotz dieser Tendenzen wird die Welt nicht von Multinationals regiert und auch nicht von totalitären Staaten oder NATO-Bombern. Ob als Bürger oder Mitarbeiter haben wir die Möglichkeit, immer wieder, trotzig, fest und auch optimistisch zu behaupten: "Der Staat sind wir, die Firma sind wir." Unter diesem Ausgangspunkt können Interessen auch gegenüber übermächtig erscheinenden Instanzen vertreten werden. Das ist nicht einfach, dazu sind

komplexe soziale Verhandlungen nötig. Aber es ist "möglich", und das genügt, um in diesem Sinne weiterzumachen.

Links

[1] <http://www.heise.de/tp/deutsch/special/enfo/6396/1.html>

[2] <http://www.heise.de/tp/deutsch/inhalt/te/2793/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6410/1.html>

Copyright © 1996-2003. All Rights Reserved. Alle Rechte vorbehalten

Heise Zeitschriften Verlag, Hannover

EU-Parlament verabschiedet Enfpol-Überwachungspläne

Christiane Schulzki-Haddouti 10.05.1999

Kritik ist "übertrieben"

Am Freitag nahm das Europäische Parlament (EP) den Entwurf der Ratsentschließung zur Überwachung des Telekommunikations- und Internetkommunikationsverkehrs an. Der Gegenantrag des "Ausschusses für Recht und Bürgerrechte" sowie die vier Änderungsanträge der Grünen [1] wurden abgelehnt.

Intensives Lobbying war der Abstimmung vorausgegangen, ohne jedoch bei den Abgeordneten zu einer klaren Meinungsbildung zu führen. Vor allem innerhalb der SPD-Fraktion wurden unterschiedliche Positionen vertreten. Während Erika Mann eine Entschärfung forderte, setzte sich ihr Parteigenosse Gerhard Schmid [2] vehement für die Abhörpläne ein. Gegenüber der New York Times hatte er die Einwände der Kritiker als "übertrieben" bezeichnet. Der Rat der Innen- und Justizminister wird den Ratsbeschluss nun voraussichtlich bei einem Treffen Ende Mai endgültig verabschieden.

Links

[1] <http://www.heise.de/tp/deutsch/special/enfo/6403/1.html>

[2] <http://www.euroschmid.de>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6404/1.html>

Enfopol-Abstimmung im Europa-Parlament

Christiane Schulzki-Haddouti 07.05.1999

Europäische Datenschützer fordern Präzisierung

Am heutigen Freitag findet im Europa-Parlament eine kurzfristig angesetzte Abstimmung über die Enfopol-Überwachungspläne statt. Die Pläne sehen vor, die grenzüberschreitende Überwachung von Telefonanrufen im Fest- und Mobilnetz, Faxe, Telex und E-Mails sowie Datenflüsse im Internet zu überwachen. Dabei geht es nicht nur um die Erfassung der Inhalte, sondern auch um die Erfassung jeglicher Kommunikationssignale, die in Bezug zur überwachten Person stehen.

Die Ratsentschließung "ist nicht nur ein technisches Update", kritisiert der grüne Europabgeordnete Johannes Voggenhuber. "Jeder Telekommunikationsbetreiber wird dazu verpflichtet, für die Polizei eine wasserdichte Hintertür einzubauen."

Mit der parlamentarischen Abstimmung wird erstmals offiziell die Existenz der EU-Überwachungspläne anerkannt. Allerdings wurde der Termin so angesetzt, daß die SPD-Abgeordneten keine Zeit mehr hatten, untereinander eine gemeinsame Linie festzulegen. Allein die Grünen konnten vier Änderungsanträge vorbereiten: Sie fordern eine Überprüfung bis zum 1. Juli 2000, inwieweit die Mitgliedstaaten die Ratsentschließung vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs in nationales Recht umgesetzt haben. Diese Entschließung bezog sich allein auf den traditionellen Kommunikationsverkehr und soll jetzt auf das Internet, Satellitenkommunikation, Prepaid-Cards und "andere Technologien erweitert werden.

Zudem soll folgender Passus eingefügt werden, der die Übernahme der Überwachungskosten durch die privaten Betreiber verhindern soll:

"Es besteht nicht die Absicht, einen Rechtsrahmen zu schaffen, der die Internet-Diensteanbieter zwingen würde, sich aufgrund der finanziellen, die Wettbewerbsfähigkeit beeinträchtigenden Belastungen außerhalb der Union niederzulassen."

Damit griffen die Grünen einen Kritikpunkt des "Ausschusses für Recht und Bürgerrechte" auf. Der Abgeordnete Luigi Florio hatte auf die finanziellen Belastungen aufmerksam gemacht [1]: Systembetreiber müssen ihre Anlagen erheblich nachrüsten, um beispielsweise das Telefonieren mit Pre-Paid-Cards nachverfolgen zu können. Florio hatte die Zurückweisung und die Erarbeitung eines neuen Vorschlags verlangt. Soweit wollen jedoch selbst die Grünen nicht gehen.

Kein flächendeckendes Abhören von Telekommunikation

Schließlich fordern sie in den Erwägungen zum einen einen Hinweis auf das Übereinkommen des Europarats vom 28. Januar 1981 über den Schutz personenbezogener Daten sowie auf die europäische Datenschutzrichtlinie aufzunehmen. Die Arbeitsgruppe der europäischen Datenschützer hatte in der vergangenen Woche einen Empfehlungsentwurf erarbeitet, der sich mit dem "Datenschutz im Kontext des Abhörens von Telekommunikation" beschäftigt. Darin äußerten sie sich "besorgt über den Umfang der geplanten Maßnahmen". Falls die EntschlieÙung in nationales Recht umgesetzt werden würde, sollte unter anderem "strikt spezifiziert werden", daß eine proaktive oder allgemeine Überwachung der Telekommunikation in großem Umfang verboten ist. Ebenso sollte genau festgelegt werden, welche Behörden Überwachungsmaßnahmen durchführen dürfen. Die abhörenden Behörden sollten zudem unabhängig kontrolliert werden können und die Öffentlichkeit beispielsweise in regelmäßigen statistischen Berichten über ihre Überwachungs politik informieren. Schließlich sollte ein Datentransfer an Dritte unter bilateralen oder multilateralen Übereinkommen nur unter bestimmten Bedingungen möglich sein.

Es ist unwahrscheinlich, daß die SPD sich den Anträgen der Grünen anschließen wird. Schließlich ist einer ihrer Parteigänger, der Abgeordnete Gerhard Schmid [2], im "Ausschuß für Grundfreiheiten und innere Angelegenheiten" der Kontaktmann der Enfpopol-Arbeitsgruppe. Seine Parteifreunde in Deutschland und Europa bezeichnen ihn als "nicht kommunikativ". Auf Anfragen ihrerseits habe er entweder nicht reagiert oder Unverständnis signalisiert. In einem eigenen Bericht hatte Schmid sogar verschärfende Nachbesserungen verlangt.

Links

[1] <http://www.heise.de/tp/deutsch/special/enfo/6390/1.html>

[2] <http://www.euroschmid.de>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6403/1.html>

ILETS, die geheime Hand hinter ENFOPOL 98

Duncan Campbell 29.04.1999

Die Geschichte von ENFOPOL aus dem Kontext von ILETS, eine US-dominierte, internationale Organisation hinter Europas umstrittenen Plänen zur Internetüberwachung.

Europas Überwachungspläne für das 21. Jahrhundert wurden an einer sehr unwahrscheinlichen Örtlichkeit entwickelt. Fünfzig Kilometer südlich von Washington DC, an den sumpfigen westlichen Ufern des Potomac Flusses liegt Quantico, in Virginia. Hier, auf einer großen Militärbasis, befindet sich die Ausbildungs-Akademie und das Forschungs- und Entwicklungszentrum des FBI. Die Öffentlichkeit hat keinen Zutritt zu dieser Hochsicherheitszone.

Zwischen 1990 und 1992 hat der FBI wiederholt versucht, den US-Kongress dazu zu bewegen, neue Gesetze zur Telefonüberwachung zu beschliessen. Die Behörde befürchtete, daß die neuen, digitalen Telefonsysteme es wesentlich schwieriger machen würde, Zielpersonen aufzuspüren und ihre Kommunikation abzufangen. Ihr Ziel war, alle Arten an modernen Kommunikationssystemen in ein nationales und globales Netzwerk zur Überwachung zu verwandeln, das ihnen Zugang "in Echtzeit und zu jeder Zeit" zu jenen geben sollte, die sie beobachten wollten.

Die Experten des FBI ignorierten die Kosten, die durch ihre Anforderungen entstehen würden. Sie wollten, daß die Hersteller und die Netzbetreiber die entsprechenden Systeme auf eigene Kosten bereitstellen sollten. Sie waren auch nicht an einem gesetzlichem Sicherungssystem interessiert, das ihre Überwachungsaktivitäten kontrollieren und die Privatsphäre schützen würde. Rechtsanwälte wurden nicht zu den Gesprächen eingeladen. Auch die Zivilgesellschaft würde ihre eigenen Kosten tragen müssen.

Da sich das FBI mit Blockaden im Kongress konfrontiert sah, versuchte man anfangs 1993 einen neuen Zugang. Man lud befreundete Staaten nach Quantico ein. Vertreter von Strafverfolgungsbehörden und Nachrichtendiensten trafen sich dort und gaben sich selbst den Namen "International Law Enforcement Telecommunications Seminar" (ILETS). Retrospektiv betrachtet kann die Bezeichnung "Seminar" nur als schwarzer Humor betrachtet werden. Sie agierten geheim, ohne das Wissen von Parlamenten und die Steuerung durch Regierungen. So konnte das FBI mittels ILETS seit 1993 die Politik von Regierungen und der Kommunikationsindustrie weltweit steuern. Im Schatten hinter dem FBI stand die NSA (National Security Agency), deren globale Überwachungsoperationen nur davon profitieren konnten, wenn Nutzern weltweit der Schutz der Privatsphäre

systematisch genommen werden würde.

Die Länder die 1993 nach Quantico kamen, waren traditionelle Alliierte der US-Nachrichtendienste wie Kanada, Vereinigtes Königreich und Australien. Es gab auch eine Kerngruppe an europäischen Teilnehmern, die an der Entwicklung flächendeckender Überwachungssysteme interessiert waren - Deutschland, Frankreich, die Niederlande, Schweden. Weitere Teilnehmer kamen aus Norwegen, Dänemark, Spanien und sogar Hong Kong. Das FBI präsentierte eine Tischvorlage mit dem Titel "Law Enforcement Requirements for the Surveillance of Electronic Communications", geschrieben im Juli 1992.

Im Juni 1993 einigten sich EU-Minister bei einem Treffen in Kopenhagen darauf, die Mitgliedsstaaten zu den Themen abstimmen zu lassen, die von FBI und durch ILETS aufgeworfen worden waren. Nach weiteren Diskussionen in Europa in der zweiten Jahreshälfte 93 traf ILETS Anfang 94 in Bonn erneut zusammen. Zu diesem Zeitpunkt zählten Österreich, Belgien, Portugal und Spanien zu den Mitgliedern der Gruppe von nun 19 Staaten.

Die Geburt der "International User Requirements"

Bei dem Treffen in Bonn einigten sich die Mitglieder von ILETS auf eine gemeinsame Politik, die in einem Dokument namens "International Requirements for Interception" festgehalten wurde. Darin stand, daß "Vertreter von Strafverfolgungsbehörden und Telekommunikationsexperten von Regierungen verschiedener Länder bei einem internationalem Workshop über Abhörmaßnahmen und fortgeschrittene Telekommunikations-Technologien die Notwendigkeit zur Verfassung dieses Dokuments festgestellt haben." Es enthielt ihre "gemeinsamen Anforderungen". Im Anhang an das zweiseitige ILETS-Dokument mit politischen Leitlinien befand sich ein vierseitiges Stichwortverzeichnis mit Erklärungen. Diese Liste von "International User Requirements" wurde als "IUR 1.0" oder "IUR95" betitelt.

Das ILETS-Treffen in Bonn führte auch zur Entstehung von zwei neuen politischen Leitgedanken. ILETS wollte, dass internationale Standardisierungs-Körperschaften wie ITU (International Telecommunications Union) und ISO (International Standards Organisation) Anforderungen zum Abhören in ihre neuen Systemspezifikationen aufnehmen. ILETS wollte ebenso, dass sich die Regierungen darauf einigen, dass das Abhören über Staatsgrenzen hinweg möglich ist, so dass eine Behörde Kommunikation in einem anderen Land abhören kann.

Im März 1994 schlug die Regierung der Niederlande vor, daß die EU die IUR 1.0 annehmen soll. Doch den Ministern wurde nicht gesagt, daß das Dokument von ILETS verfasst worden war. Stattdessen wurde es als ein ENFOPOL-Dokument präsentiert und

schließlich ENFOPOL 90 betitelt. (ENFOPOL ist eine Standard-Klassifizierung der Europäischen Kommission für Strafverfolgungs- und Polizeiangelegenheiten).

Europäische Minister haben ENFOPOL 90 nie diskutiert. Die Übereinkunft wurde mittels eines "schriftlichen Verfahrens" erzielt, durch den Austausch von Dokumenten per Telex. Für beinahe zwei Jahre blieb das Dokument völlig geheim und wurde erst im November 1996 im offiziellen Journal für Europapolitik publiziert. In der Zwischenzeit wurde den europäischen Betreibern von Telekommunikationssystemen klar gemacht, daß sie sich nach den Anforderungen zu richten hätten. Nach Aussagen des britischen Home Office (Innenministerium) beispielsweise, diene der Beschluss "als Grundlage für Verhandlungen mit Telekommunikations-Unternehmen in Übereinstimmung mit [britischer Gesetzgebung über Abhörmaßnahmen]."

ILETS hat auch das Problem der satellitengestützten Mobiltelefonsysteme (wie z.B. Iridium) zum Thema gemacht. Diese Systeme verbinden Nutzer über Satelliten, die nicht von Regierungen kontrolliert werden. Das führte zu einem britischem Vorschlag an die Europäische Kommission: "Regierungen ... werden neue Regelungen für internationale Zusammenarbeit einführen müssen, so dass die notwendige Überwachung operationsfähig werden kann".

In leicht modifizierter Fassung wurde IUR 1.0 im Oktober 1994 in den USA zum Gesetz. Europäische Nationen und Australien brachten es später in ihre inländische Gesetzgebung ein. Innerhalb von zwei Jahren, seit dem ersten ILETs-Treffen, waren die IUR, unangefochten und Wort für Wort, zur geheimen offiziellen Politik der EU geworden und Bestandteil von Gesetzen rund um den gesamten Globus.

Abhörschnittstellen als ITU und ISO Standards

Sechzehn Staaten von ILETs trafen 1995 in Canberra wiederum zusammen und einigten sich darauf, daß sie versuchen würden, Standardisierungs-Organisationen zu überzeugen, die IUR-Anforderungen anzunehmen. Das würde bedeuten, daß die Hersteller neuer Schaltzentralen und Kommunikationssysteme Abhörschnittstellen einbauen müssten, um die internationalen Standards einzuhalten, auf eigene Kosten selbstverständlich. Wenn dieses Komplott erfolgreich sein würde, dann würden die Sicherheits- und Strafverfolgungsbehörden Geld sparen und das Abhören würde wesentlich einfacher werden, weil die Netzwerke bereits mit eingebauten Überwachungsmöglichkeiten geliefert werden würden.

Bei ihrem Treffen in Canberra "schritten die teilnehmenden Länder dazu, sich schriftlich an "die relevanten Standardisierungs-Organisationen und-Komitees zu wenden und ihnen mitzuteilen, daß ihr Land gemeinsam mit anderen Ländern die IUR als Grundlage für ihre nationalen und systemspezifischen Anforderungen angenommen haben ...".

Einmal mehr war ILETS erfolgreich. Im Juni 1997 überzeugte die australische Regierung die International Telecommunications Union (ITU), die IUR-Anforderungen als "Priorität" anzunehmen. ITU wurde mitgeteilt, daß "einige Länder dringend Resultate auf diesem Gebiet benötigen".

Im Zeitraum von 1995 bis 1996 gelang es ILETS auch, die IUR über die Europäische Kommission auf die Ebene eines internationalen Vertrags zu bringen. Die EU lud Länder, die an ILETS-Treffen teilgenommen hatten, dazu ein, die immer noch geheime Abhörpolitik von 1995, also IUR 1.0, zu unterstützen.

Mitglieder von ILETS, die nicht zur EU gehören, wurden davon unterrichtet, daß "der Rat die gesetzliche Überwachung von Telekommunikationssystemen als wichtiges Werkzeug zur Verhinderung und zur Aufspürung von ernsthaften Verbrechen betrachtet, ebenso wie zur Aufrechterhaltung der nationalen Sicherheit ... Die Mitgliedsstaaten der Europäischen Union wurden aufgefordert, die Anforderungen bei Telekommunikationsunternehmen und Netzwerkdienstleistern in Anwendung zu bringen ..." Kanada, Australien, Norwegen und die Vereinigten Staaten antworteten der EU-Präsidentschaft und bestätigten ihre Übereinstimmung.

Die Entstehung von ENFOPOL 98

Zu diesem Zeitpunkt hatte ILETS zwei Arbeitsgruppen eingesetzt, eine zur Überarbeitung der IUR, eine andere (STC genannt, das "Standards Technical Committee"), die an den technischen Standards arbeitete. Die ILETS-Experten trafen 1997 in Dublin erneut zusammen. 1998 gab es Treffen in Rom, Vienna und Madrid. 1997 gab es keine Änderungen bei den IUR. Doch ILETS und seine Arbeitsgruppen waren damit beschäftigt, neue Anforderungen zur Abdeckung von Internet- und satellitengestützter Kommunikation zu entwickeln. Sie wollten auch strikte neue Sicherheitsanforderungen, die den neuen, privaten Telekommunikationsfirmen auferlegt werden sollten.

Die Expertengruppen schufen neue "Anforderungen" zum Abhören des Internet. Während des Treffens in Rom im Juli 1998 einigten sich die Experten auf neue IUR inklusive eines neuen "Glossars", ein Anhang zum Dokument mit Begriffsdefinitionen. Das Ergebnis war ENFOPOL 98 [1]. Am 3. September 1998 wurden die überarbeiteten IUR der Arbeitsgruppe für polizeiliche Zusammenarbeit vorgestellt. Die österreichische EU-Präsidentschaft schlug vor, daß, so wie bereits 1994 geschehen, die neuen IUR wortgetreu als Ratsbeschluss für Abhörmaßnahmen "in Hinsicht auf neue Technologien" angenommen werden sollten. Den Delegierten wurde gesagt, daß der Zweck von ENFOPOL 98 darin bestand, "das zugrundeliegende Dokument (IUR 1.0) in dem Sinn klarzustellen, wie es von den gesetzlich ermächtigten Behörden als Ausdruck ihrer gemeinsamen Anforderungen beschlossen worden war".

ENFOPOL 98 wird Internet-News

Doch ILETS und seine Experten waren allzu siegessicher geworden. IUR 1.0 hatte noch vier Seiten umfasst. Die neuen IUR, ENFOPOL 98, umfassten 36 Seiten. Den österreichischen Vertretern wurde gesagt, daß dies politisch nicht ratsam war - möglicherweise würde es durch seine Ausdrücklichkeit Politiker abschrecken. Oder, wie den ILETS-Experten später mitgeteilt wurde, "der große Umfang der behandelten Themen von ENFOPOL 98 war der allgemeinen Verständlichkeit nicht förderlich".

Im Oktober 1998 traf die IUR-Expertengruppe von ILETS nochmals in Wien und in Madrid zusammen und einigte sich auf ein kürzeres, 14 Seiten langes Dokument. Einige seiner umstritteneren Massnahmen wurden in anderen Dokumenten untergebracht. Europäische Polizeidelegierte trafen sich im November 98, um die revidierte Fassung, ENFOPOL 98 (rev 1) zu erörtern und einen Beschluss darüber zu fassen.

Doch plötzlich gab es einen neuen Faktor, den die ILETS-Experten in Betracht ziehen mussten. Am 20. November veröffentlichte Telepolis den ersten Artikel über ENFOPOL 98, 9 Tage später das ENFOPOL 98 Dokument in voller Länge. Die Geschichte fand rasch Verbreitung als Internet-Nachricht in aller Welt. Danach, und dank zweier weiterer Überarbeitungen unter der deutschen Präsidentschaft, schrumpfte ENFOPOL 98 (nun umbenannt in ENFOPOL 19, siehe anderer Bericht) auf nur mehr sechs Seiten. Die wirklich schwerwiegenden Massnahmen wurden an anderer Stelle untergebracht.

Der erschreckendste Aspekt der ILETS- und ENFOPOL-Geschichte mag gar nicht unbedingt der sein, wie diese US-gesteuerte Organisation sechs Jahre lang in der Dunkelheit operieren konnte, um Hintertüren für Spione in jedes neue Telekommunikationssystem einzubauen. Ihre feste Absicht im Dunklen zu agieren, ohne Beteiligung der Industrie oder juristischen Ratschlag, ohne parlamentarische Überprüfung und öffentliche Diskussion, hat sie für den Umstand blind gemacht, daß nicht jede Form von "Strafverfolgung" eine Wohltat für die Öffentlichkeit ist.

Während der gesamten Zeitspanne der Existenz von ILETS war auch Hong Kong, nun Bestandteil der Volksrepublik China, ein Mitglied. Und indem sie ihre Anforderungen Körperschaften wie ITU und ISO eingepflanzt haben, haben die beteiligten Polizei- und Sicherheitseinrichtungen de facto wie eine internationale Vertragsorganisation agiert.

Dabei waren sie blind gegenüber allen anderen Interessen als ihrer eigenen, engen Weltsicht. "Im Namen von Recht und Gesetz versuchen die USA nun ein internationales Abkommen zu erzielen, das Nationen mit einer abschreckenden Menschenrechtssituation stärkere Überwachungsmöglichkeiten nahelegt", sagt Susan Landau, Ko-Autorin von "Privacy on the Line".

Indem sie Hong Kong in ihren Club aufgenommen haben, haben sie ihre hochentwickeltsten Ideen zur Überwachung mit den Schlächtern vom Tiananmen-Platz geteilt. Indem sie versuchten, das Gütesiegel der ITU für gültige Standards bei der Einrichtung von Überwachungsschnittstellen in neuen Kommunikationssystemen zu erhalten, haben sie den widerlichen Schlächtern von Kosovo-Albanern und Kurden das zukünftige Werkzeug in die Hand gegeben, um ihre Gegner zunächst aufzuspüren und dann zu ermorden. Die neuen IUR werden in Thailand und Singapur und überall anders, wo die Feinde der Freiheit hoch im Kurs stehen, als willkommene Nachricht aufgenommen werden.

Selbst für konservative Politiker in Europa und den USA kann das nur eine Quelle der Schande sein. ILETS hat die lebenswichtigen Prinzipien des Europäischen Vertrags und der US-Verfassung in den Mülleimer geworfen. Aus diesem Grund, neben allen anderen Gründen, sollten die geheimen Verfahren von ENFOPOL 19, 98 und dem ganzen Rest zu einem Ende gebracht werden. Demokratische Gesellschaften verlangen nichts weniger als eine ausführliche und überlegte öffentliche Diskussion von Themen von derartiger Wichtigkeit.

Links

[1] <http://www.heise.de/tp/deutsch/special/enfo/6326/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6396/1.html>

EU-Polizei will ENFOPOL-Ratsbeschluss durchdrücken

Duncan Campbell 29.04.1999

Dokument umbenannt, Ziele gleich geblieben. Amerikas leitende Hand wird sichtbar.

Die letzte Version der ENFOPOL 98 Abhör- und Überwachungspläne wurde diese Woche in London publik. Dabei stellte sich heraus, daß zwar der Name des Schlüsseldokuments inzwischen geändert wurde, die Europäische Kommission aber die Überwachung des Internets immer noch bis Ende Mai zur offiziellen europäischen Politik machen möchte. Trotz starker Opposition in Deutschland und Österreich und harscher Kritik im Europa-Parlament wird das Vorhaben durchgedrückt.

Das neue Dokument wurde ENFOPOL 19 genannt. Caspar Bowden von der Foundation for Information Policy Research (FIPR) hat das Dokument in seinen Besitz gebracht und auf der IFPR-Website veröffentlicht [1].

ENFOPOL 19 wurde bei einem Treffen von Polizeibeamten in Brüssel am 11. März verfasst und von der deutschen EU-Präsidentschaft am 15. März herausgegeben. Laut der britischen Regierung hat "die deutsche EU-Präsidentschaft angedeutet, daß man hofft über den Entwurf des Ratsbeschlusses beim Treffen der Justiz- und Innenminister im Mai Übereinstimmung zu erzielen". Das Treffen findet am 27. und 28. Mai statt.

ENFOPOL 19 handelt immer noch von "Abhörmaßnahmen von Telekommunikation in Bezug auf neue Technologien". Doch anstatt einer detaillierten Aufstellung von Anforderungen für das Anzapfen des Internets und anderer neuer Kommunikationssysteme (wie im ursprünglichen Dokument ENFOPOL 98 [2]), gibt die Polizeigruppe nun vor, es gehe dabei nicht um eine neue politische Ausrichtung. Mit Verweis auf den ersten europäischen Überwachungsplan von 1995 [3] sagt ENFOPOL 19, "die Anforderungen der gesetzlich ermächtigten Behörden sind auf existierende ebenso wie neue Kommunikationstechnologien anwendbar, wie zum Beispiel satellitengestützte Telekommunikation und Internet-Kommunikation". So behauptet das Papier, die "technischen Richtlinien" des Plans von 1995 "sind so zu interpretieren, daß sie ... im Falle des Internets auch für statische und dynamische IP-Adressen, Kreditkartennummern und E-mail-Adressen zutreffen". Tatsächlich sagt die Übereinkunft von 1995 überhaupt nichts betreffend der Verwendung von Kreditkartennummern bei der Überwachung von Telekommunikation.

Das neue Dokument erläutert, daß es für ein Anzapfen des Internets nicht notwendig sei, Detailinformationen über Sender und Empfänger zu erfragen, da diese im "datagram" oder IP-Packet jeder Nachricht enthalten sind. Deshalb würden neue Regeln für das Internet gar nicht benötigt.

Doch das ist ein Ablenkungsmanöver. Wie den hintereinander erschienenen revidierten Fassungen von ENFOPOL 98 zu entnehmen ist, wurde das kontroversielle Vorhaben inzwischen in mindestens fünf Hauptbestandteile aufgebrochen, die getrennt behandelt werden:

- Die Pläne für das Abhören von Iridium und anderen persönlichen, satellitengestützten Kommunikationsmedien wurden herausgenommen und werden auf einer sehr hohen Ebene innerhalb der Kommission diskutiert;
- Teile von ENFOPOL 98, die neue Anforderungen bezüglich persönlicher Daten von Usern enthalten, sollen Bestandteil von "anderen, noch zu fassenden Ratsbeschlüssen sein".
- Ein anderer Ratsbeschluss wird von Internet-Service-Providern verlangen, Hochsicherheits-Abhörschnittstellen in ihren Geschäftsräumen einzurichten. Diese Schnittstellen sollen in einer Hochsicherheitszone eingerichtet werden, zu der nur Personal Zutritt haben wird, das bezüglich Sicherheit überprüft und vertrauenswürdig befunden wurde. Das ist nicht in ENFOPOL 19 enthalten.
- ENFOPOL 19 schlägt auch vor, daß einige Überwachungssysteme über "virtuelle Schnittstellen" laufen könnten. Das wäre spezielle bei Internetknoten zu installierende Software, ferngesteuert von Sicherheitskräften der Regierung.
- Eine vierte neue Richtlinie betreffend Kryptographie wird getrennt behandelt.

Die Arbeitsgruppe der Polizei hat nun vor, dass die alten und neuen Pläne in einem "Handbuch" für Abhörmaßnahmen zusammengefasst werden, einschliesslich detaillierter Anweisungen zur Überwachung von Internetkommunikation. Dabei handelt es sich um "technische Beschreibungen", die aus ENFOPOL 98 herausgenommen wurden. Wenn dieses Manöver Erfolg hat, wird sich ENFOPOL 98 der Überprüfung durch die Öffentlichkeit entziehen, indem es in Teilen durchgeschmuggelt wird, während das Europäische Parlament wegen der Europawahlen im Juni aufgelöst ist.

Doch das größte Geheimnis bezüglich ENFOPOL 98 wurde bisher noch nicht zur Sprache gebracht. Das umstrittene Dokument wurde gar nicht von europäischen Regierungen oder der Europäischen Kommission verfasst. ENFOPOL 98 ebenso wie der Ratsbeschluss von 1995 wurden von einer US-dominierten Expertengruppe aus dem Sicherheits- und Strafverfolgungsbereich verfasst, die sich ILETS nennt. In dieser Gruppe gibt es weder Vertreter der Industrie, noch Berater von Bürgerrechts- und Datenschutzanwälten. (siehe dazu Inside ENFOPOL [4])

Während der letzten sechs Jahre hat ILETS im Alleingang Regierungen und

Standardisierungs-Organisationen gezwungen, ihre "Anforderungen" zum Bestandteil von Gesetzen, Netzwerken und Kommunikationssystemen zu machen. Die Aktivitäten dieser Gruppe wurden bisher noch in keinem Parlament vorgetragen, weder einem nationalem Parlament, noch dem Europa-Parlament, und auch nicht dem US-Kongress.

Nicht bevor Telepolis die ENFOPOL 98 Affäre enthüllte, wurde die geheime Organisation ILETS öffentlich diskutiert und herausgefordert.

ILETS, die geheime Hand hinter ENFOPOL. [5]

Anmerkung der Redaktion: Die Telekommunikations-Überwachungsverordnung [6] für Deutschland zeigt deutlich die Spuren von ENFOPOL 98, bzw. der IUR (International User Requirements), ebenso wie der Ratsbeschluss zur Bekämpfung von Kinderpornographie [7]

Links

[1] <http://www.fipr.org/polarch/index.html>

[2] <http://www.heise.de/tp/deutsch/special/enfo/6326/1.html>

[3] <http://www.heise.de/tp/deutsch/special/enfo/6334/1.html>

[4] <http://www.heise.de/tp/deutsch/special/enfo/6386/1.html>

[5] <http://www.heise.de/tp/deutsch/special/enfo/6396/1.html>

[6] <http://www.heise.de/tp/deutsch/inhalt/te/2793/1.html>

[7] <http://www.heise.de/tp/deutsch/inhalt/te/2722/1.html>

Telepolis Artikel-URL: <http://www.telepolis.de/deutsch/special/enfo/6395/1.html>