Bund verstärkt Internetüberwachung

25. Mai 2010

Einschleusen von Programmen und Rasterfahndung

Der Bundesrat plant, das erst 10 Jahre alte Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs zu erweitern. Die Kernpunkte:

Internetprovider wie Swisscom oder Cablecom müssten gewisse Kundendaten doppelt so lange speichern - von heute sechs Monaten sollen die Daten ein Jahr lang zur Verfügung stehen. Zudem plant der Bund, die entsprechenden Kosten vollständig den Providern zu belasten.

Neu sollen die Überwachung des Post- und Fernmeldeverkehrs auch für die Suche nach einer Person in Anspruch genommen werden können, die rechtskräftig und vollstreckbar zu einer Freiheitsstrafe verurteilt wurde oder gegen die rechtskräftig und vollstreckbar eine freiheitsentziehende Massnahme verhängt worden ist.

Daten aus Überwachungen werden nicht mehr an die Auftraggeber übermittelt, sondern zentral beim Bund gespeichert und bis zu 30 Jahren aufbewahrt.

Ein spezieller Clou ist Art. 22 (Identifizierung von Internet-Benutzern): **Die Personen, die Überwachungen des Fernmeldeverkehrs nach diesem Gesetz durchführen, müssen die nötigen technischen Vorkehren treffen, um die Personen identifizieren zu können, die über ihre Vermittlung Zugang zum Internet erhalten.** Aus dem Bericht die Erläuterung: Artikel 22 verpflichtet Personen, die Überwachungen des Fernmeldeverkehrs gemäss dem BÜPF durchführen, die nötigen technischen Vorkehren zu treffen, um die Internet-Benutzer identifizieren zu können, welche über ihre Vermittlung Zugang zum Internet erhalten. Diese Pflicht gilt für alle Arten des Internetzugangs innerhalb der Grenzen, die sich aus Artikel 20 Absatz 2 VE ergeben. Diese Pflicht wird durch Artikel 20 Absatz 3 VE ergänzt. Artikel 22 verpflichtet insbesondere die Anbieter von Internetzugängen (Internetanbieter/Zugangsmittler) und hat eine besondere Bedeutung in Fällen, in denen die Benutzerinnen und Benutzer über ein drahtloses Netz auf das Internet zugreifen (Wireless LAN, WLAN, Wireless Local Area Network, Hotspot, Wi-Fi usw.). Diese Bestimmung bezieht sich insbesondere auf jene Fälle, bei denen ein solches Netzwerk beispielsweise in einem Internetcafé oder Cybercafé, in einer Schule, in einer Gemeinde, in einem Hotel, in einem Restaurant, in einem Spital oder bei einer Privatperson, der Verfügung einer Drittperson überlassen wird (z.B. einem Hotelgast), damit diese Zugang zum Internet erhält, wobei dies gegen Entrichtung einer Gebühr oder kostenlos sein kann. In diesem Fall muss der Anbieter des Internetzugangs (Internetanbieter/Zugangsmittler) der erwähnten Einrichtungen und Personen (z.B. das Hotel) in der Lage sein, diese Drittperson identifizieren zu können oder diejenigen Computer zu eruieren, die über das fragliche Netzwerk Zugang zum Internet haben...

Richtig deftig wird es in den Schlussbestimmungen:

Art. 270bis StPO **Abfangen und Entschlüsselung von Daten (neu)**

Sind bei einer Überwachung des Fernmeldeverkehrs die bisherigen Massnahmen erfolglos geblieben oder wären andere Überwachungsmassnahmen aussichtslos oder würden die Überwachung unverhältnismässig erschweren, so kann die Staatsanwaltschaft auch ohne Wissen der überwachten Person das Einführen von Informatikprogrammen in ein Datensystem anordnen, um die Daten abzufangen und zu lesen. Die Staatsanwaltschaft gibt in der Anordnung der Überwachung an, auf welche Art von Daten sie zugreifen will.

Art. 270ter StPO **Einsatz von Ortungsgeräten (neu)**

Die Staatsanwaltschaft kann den Einsatz von Geräten durch die Polizei anordnen, mit denen spezifische Kennzeichen von Mobiltelefongeräten und ihr Standort ermittelt werden können. Die Geräte müssen vorgängig von der zuständigen Behörde bewilligt worden sein.

Diese Ortungsgeräte simulieren eine UMTS-Basisstation, alle Mobiltelefone in der Nähe melden sich bei ihnen an. Es handelt sich also nicht um eine Überwachung einer bestimmten Person, sondern um eine Rasterfahndung.

Mitte August 2010 lief die Frist der Vernehmlassung ab. Ein breites Spektrum von Parteien und Verbänden lehnt die Neuerungen entschieden ab. Eine kleine Auswahl von Vernehmlassungsantworten ist unten bei den Links.

Im Switch Journal vom März 2011 wurde berichtet, dass versucht werde, die Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) zum geltenden BÜPF zu revidieren, und dass dabei Teile des Revisionsgegenstandes des BÜPF, u. a. die Erweiterung der Internetdienstleistern, ohne Konsultation des Parlaments in die Verordnung transferiert werden soll.

********* Indymedia.org beschrieb im Juni 2010 in einem Artikel, wie Trojaner von staatlichen Stellen unsichtbar gemacht werden können (Wie das BKA Trojaner FUD macht).

********** Die «Vorratsdatenspeicherung» ist in ganz Europa ein Thema:

Zivilgesellschaft fordert Stopp des europaweiten Zwangs zur Vorratsdatenspeicherung

In einem gemeinsamen Brief haben über 100 Organisationen aus 23 europäischen Ländern Ende Juni 2010 die EU-Kommission aufgefordert, «die Aufhebung der EU-Vorgaben zur Vorratsdatenspeicherung zugunsten eines Systems zur schnellen Sicherstellung und gezielten Aufzeichnung von Verkehrsdaten vorzuschlagen». Unter den Unterzeichnern befinden sich Bürgerrechts-, Datenschutz- und Menschenrechtsorganisationen ebenso wie Telefonseelsorge- und Notrufvereine, Berufsverbände etwa von Journalisten, Juristen und Ärzten, Gewerkschaften wie ver.di, Verbraucherzentralen und auch Wirtschaftsverbände wie der deutsche eco-Verband.

Entwurf BÜPF

Bericht BÜPF

Basler Zeitung vom 25. Mai 2010

WOZ vom 27. Mai 2010

Vernehmlassungsantwort grundrechte.ch

SDA - Meldung vom 18. August 2010

Vernehmlassungsantwort Swiss Privacy Foundation & Swiss Internet User Group (SIUG)

Vernehmlassungsantwort Stiftung für Konsumentenschutz

Wie das BKA Trojaner FUD macht

Demonstration «Freiheit statt Angst» 2010

«Switch Journal» vom März 2011