Tages-Anzeiger

18. Juli 2009

# Geheime Pläne für Internet-Lauschangriffe gegen Verdächtige

Von Christian Bütikofer

Beim Surfen und Telefonieren im Web will der Bund dabei sein. Weitere Eingriffe sind geplant, obwohl alte Vorgaben für weniger aufwendige Massnahmen nur mangelhaft umgesetzt wurden.

Das Justiz- und Polizeidepartement (EJPD) plant die vollständige Überwachung der Internetnutzung von in Strafverfahren verdächtigten Leuten. Dies machte die «Wochenzeitung» am Donnerstag publik und veröffentlichte «vertrauliche» Dokumente. Ab diesem August müssen sich gemäss der neuen Richtlinie alle Internetprovider technisch aufrüsten und vom Bund zertifiziert werden – Zeit bleibt ihnen dafür bis Ende Juli 2010.

**«Abhörversuche sind sehr einfach zu umgehen»**

Für die kommende Echtzeitüberwachung des Internetverkehrs werden die Kosten hauptsächlich den Providern aufgebürdet. «Dazu sind kleine Unternehmen finanziell gar nicht in der Lage», sagt Fredy Künzler, Chef des Internetproviders Init7. Er kritisiert die kurze Anhörungsfrist von bloss drei Wochen, die Geheimnistuerei und meint zudem: «Abhörversuche sind durch Verschlüsselung der Daten sehr einfach zu umgehen.»

Guido Balmer, Sprecher des EJPD, begründet die Vertraulichkeit des Dokuments: «Der Inhalt war im Interesse der Strafverfolgungsbehörden nicht für die Öffentlichkeit bestimmt», denn es würden im Dokument auch prozessuale und technische Informationen erwähnt. Zudem habe die neue Richtlinie einen langen Vorlauf gehabt. Das sei nichts Spezielles. Die Anhörung der Provider stelle sozusagen den Zieleinlauf dar.

**Aufwändige Überwachung**

Was heisst «Echtzeitüberwachung» konkret? Dem TA ist ein Fall beim Provider Sunrise bekannt. Aufgrund eines richterlichen Beschlusses musste die Firma einem Kunden statt eines normalen DNS-Servers einen zuweisen, der direkt von Bundesbeamten überwacht wurde. Ohne DNS-Server ist niemand in der Lage, Webseiten aufzusuchen. Fortan konnten die Beamten die Aktivitäten des Verdächtigen mitverfolgen. Die Informationsperson aus dem Umfeld von Sunrise bezweifelt, dass neue Richtlinien solche Aktionen einfacher machten: «Für jeden Einzelfall ist das sehr aufwendig.»

Laut Guido Balmer sind Echtzeitüberwachungen heute sehr aufwendig, weil man mit jedem Provider einzeln eine Lösung finden müsse. Deshalb soll nun die Richtlinie hier eine bessere Handhabe schaffen.

**Überlastete Überwacher**

Ob eine neue Richtlinie strukturelle Probleme löst, ist fraglich. Denn bisher hat das EJPD noch immer Probleme, bereits seit Jahren bestehende Vorgaben zur Überwachung von Internetaktivitäten in die Tat umzusetzen. So berichtet ein Insider der Provider-Szene: «Bis heute sind einige Internetprovider noch nicht einmal in der Lage, die E-Mail-Header zu speichern, weil das EJPD die dazu notwendigen Implementationen und Tests noch gar nicht durchgeführt hat.» E-Mail-Header sind Angaben, aus denen man sieht, über welche PCs im Web die Mails verschickt werden. Seit 2003 müssten alle Provider solche Daten für eine gewisse Zeit sichern. Guido Balmer bestätigt, dass hier ein Problem bestehe. Die Leute vom EJPD seien aber bemüht, zusammen mit den Providern diese Prozesse zu «optimieren».

**Handys werden separat behandelt**

In der bekannt gewordenen neuen Richtlinie fehlt UMTS. Durch UMTS kommunizieren wir heute übers Handy, laden Programme aufs iPhone herunter. Immer mehr Leute benutzen Abos bei Swisscom, Orange und Sunrise, um damit mit ihren Laptops im Web zu surfen. Warum also fehlt diese Technologie? Balmer bestätigt, dass UMTS in der vorliegenden Richtlinie nicht erwähnt wird. Diese Richtlinie sei aber nicht die einzige und nicht die letzte. Näher wollte er darauf nicht eingehen. Die bekannt gewordenen «vertraulichen» Dokumente sind demnach nicht die einzigen geheimen Massnahmen zur Internet-Überwachung in der Schweiz.

## So einfach wird man abhörsicher

Die Tendenz des Staates, seine Bürger im Internet auszuhorchen, nimmt nicht nur in der Schweiz zu. Die Behörden versprechen sich von den Überwachungsmöglichkeiten viel, oft zu viel. Denn wer wirklich will, bewegt sich schon jetzt im Internet ohne Probleme anonym, indem er Daten nur verschlüsselt überträgt.

Surfen: Nutzt man das Tor-Netzwerk (www.torproject.org), werden alle Daten verschlüsselt.

E-Mail: E-Mails lassen sich bei jedem ernsthaften Anbieter per «https:» sicher übertragen. Per PGP verschlüsselt man die Texte.

Tauschbörsen: Über Netzwerke wie Bittorrent lädt man anonym, etwa durch den Gratisdienst Bit Blinder (www.bitblinder.com) oder zahlt für Anbieter wie Torrent Privacy (torrentprivacy.com).