

Druckversion

Url: http://www.focus.de/digital/internet/tid-7620/internetueberwachung_aid_135360.html

10.10.07, 11:27

Drucken

Internetüberwachung

Wie der Staat das Netz belauscht

E-Mail, Internettelefonie und Web: Während die Politik über Olinedurchsuchungen streitet, ist die virtuelle Überwachung längst Realität.

Von FOCUS-Online-Autor *Torsten Kleinz*

„Das Internet darf sich nicht zu einem rechtsfreien Raum entwickeln“, **erklärte jüngst der Chef des Bundeskriminalamts Jörg Zierke**. Doch ohne Recht und Gesetz ist das Internet nie gewesen. Gerade in den vergangenen Jahren haben Strafverfolger und Geheimdienste immer mehr Kompetenzen bekommen, um im Internet zu recherchieren. Ob E-Mail-Kommunikation oder Internettelefonie – Fahnder schauen Kriminellen auch online über die Schulter. FOCUS Online erklärt, was die Fahnder dürfen.



Bequem für Fahnder: E-Mail-Überwachung

Heute verschickt kaum noch jemand Briefe – viel schneller und unkomplizierter geht das per E-Mail. Auch für die Polizei ist das Verfahren viel bequemer: Seit 2005 sind die deutschen Mailprovider verpflichtet, den elektronischen Briefkasten ihrer Kunden für Fahnder zu öffnen.

Die E-Mail-Überwachung ist in Deutschland mittlerweile Alltag. Registrierte die amtliche Statistik im Jahr 2004 nur 78 Überwachungsanordnungen, griffen die Ermittler im vergangenen Jahr schon in 701 Fällen auf elektronische Postfächer zu.



E-Mail-Kommunikation

Mitlesen bei Mordermittlungen

Voraussetzung für die E-Mail-Überwachung ist ein Richterbeschluss, bei Gefahr in Verzug reicht auch die Anordnung eines Staatsanwalts. Mitlesen dürfen die Ermittler bei schweren Verbrechen wie Mord oder Bildung einer kriminellen Vereinigung. Aber auch bei Drogendelikten oder wegen der Verbreitung pornografischer Schriften werden Mails abgefangen.

Grundlage ist die Telekommunikations-Überwachungsverordnung (TKÜV), die vor fünf Jahren in Kraft getreten ist. Je nach Größe eines Providers sind die Vorschriften unterschiedlich streng – hat ein Provider weniger als 1000 Kunden, muss er keine Vorkehrungen treffen. Größere Provider müssen jedoch auf eigene Kosten Abhöranlagen installieren, die sie auf Anforderung den Behörden zur Verfügung stellen.

Jede Mail geht an die Fahnder

Kernstück der E-Mail-Überwachung ist die sogenannte SINA-Box – ein spezieller Computer, auf dem sich die Strafverfolger einloggen können. Liegt eine Überwachungsanordnung vor, leitet der Provider jede Mail des überwachten Kunden an die SINA-Box weiter – die Daten landen umgehend auf den Rechnern von Polizei und Staatsanwaltschaft. Der Kunde bekommt davon nichts mit, auch der Provider darf die weitergeleiteten E-Mails nicht mitlesen.

Nach Medienberichten wollten die im September im Sauerland verhafteten Terrorverdächtigen diese E-Mail-Überwachung umgehen, in dem sie Mails nicht verschickten – sondern Daten in einem gemeinsam genutzten Webmail-Account als „Entwürfe“ speicherten. Doch so einfach ist die Überwachung nicht zu umgehen – die Fahnder fingen die elektronische Post trotzdem ab.

Alles wird mitgehört: Internettelefonie

Immer beliebter werden Telefonate über das Internet. Doch der Staat hat vorgesorgt und verpflichtet die Anbieter über das Telekommunikationsgesetz zur Kontrolle. Auch hier ist ein Richterbeschluss erforderlich.



Telefoniert der überwachte Kunde per Internet zu einem Festnetzanschluss, verläuft die Überwachung ähnlich wie im analogen Telefonnetz. Am Übergabepunkt zwischen Internet und normalem Festnetz werden Computer installiert, die die Gespräche aufzeichnen und den Behörden übermitteln. „Die Telekommunikationsunternehmen müssen den Behörden eine 1:1-Kopie der Gespräche liefern“, erklärt der Düsseldorfer Anwalt Jens Eckhardt, der sich intensiv mit den Überwachungsmaßnahmen beschäftigt. Im vergangenen Jahr wurden laut Statistik der Bundesnetzagentur 54 Internettelefonie-Kunden abgehört.

Gesamter Datenverkehr wird mitgeschnitten

Schwieriger ist es, wenn beide Gesprächsteilnehmer über das Internet telefonieren. Denn die Gespräche werden nicht unbedingt direkt über die Leitungen des Telefonie-Anbieters geführt. Er vermittelt nur die beiden Gesprächspartner, die anschließend über das Internet miteinander sprechen. Theoretisch kann das Gespräch dabei um die ganze Welt laufen, ohne dass die Ermittler etwas davon mitbekommen.

Aber auch hier haben die Behörden eine Möglichkeit zum Mitschneiden gefunden: Sie können kurzerhand den gesamten Datenverkehr abfangen, der bei einem Verdächtigen ankommt. Jedes einzelne Bit, das über den DSL-Anschluss des Überwachten läuft, wird parallel auch an die Polizei geliefert – im vergangenen Jahr geschah das 477-mal.

Skype-Nutzer sind außen vor

Die Polizei muss die für sie nutzbaren Informationen allerdings selbst aus dem Datenstrom herausfischen. Bei klassischen Telefoniediensten ist das kein Problem. Beim beliebten Dienst Skype hingegen funktioniert es nicht: Gespräche zwischen Skype-Teilnehmern werden verschlüsselt und können deshalb nicht einfach mitgeschnitten werden. So beschwerten sich Schweizer Ermittler, dass Kriminelle immer öfter auf diesen Dienst ausweichen würden, was ihnen die Ermittlungen erschwere. Ein sicherer Hafen für Kriminelle ist aber auch Skype nicht: Das Luxemburger Unternehmen verspricht, mit den Ermittlungsbehörden zusammenzuarbeiten.

Umstritten ist, ob die Polizei auch den Rechner eines Verdächtigen manipulieren darf, um die Internettelefonate abzuhören. Nach der derzeitigen Rechtslage ist dies zumindest nicht ausdrücklich vorgesehen. „Nach der geplanten Neufassung der Vorschriften der Strafprozessordnung könnten die Strafverfolgungsbehörden hier aber direkt eingreifen“, erklärt Eckhardt.

Ohne Richterbeschluss: Surfer-Überwachung

Während bei E-Mail-Kommunikation und Internettelefonie der Verdächtige bekannt sein muss, bevor er überwacht werden kann, können Fahnder im Internet auch auf vergangene Aktivitäten zugreifen. So speichert fast jeder Server im Internet ab, von wo aus auf ihn zugegriffen wird. Anhand der IP-Adressen kann die Polizei dann oft bei dem Provider in Erfahrung bringen, wer auf eine bestimmte Internetseite zugegriffen oder wer eine bestimmte Datei ins Netz gestellt hat. Ermittlungen nach IP-Adressen sind Alltag: Zu Tausenden fragen Polizeibehörden und Staatsanwaltschaften die Besitzer von IP-Adressen bei den Providern ab, ein Richterbeschluss ist dazu nicht erforderlich.



Surfen im Internet

Um an IP-Adressen von Verdächtigen zu gelangen, sind die Fahnder durchaus erfinderisch. So hat das Bundeskriminalamt nach Medienberichten im Frühjahr genau analysiert, wer den **Online-Steckbrief der „Militanten Gruppe“** abgerufen hat. Offenbar hofften die Beamten, dass die Linksextremisten neugierig waren, welche Informationen das BKA über sie verbreitet.

Musikindustrie ist auf der Jagd

Aber auch bei geringfügigeren Delikten werden die IP-Adressen von Verdächtigen gespeichert: So manipulierten im vergangenen Jahr Ermittler der Musikindustrie in

Zusammenarbeit mit der Staatsanwaltschaft Köln einen Server, über den Musikdateien getauscht wurden. Jede einzelne Aktion der Nutzer wurde abgespeichert, über 14 Gigabyte Informationen wurden über mehrere Wochen mitgeschnitten. Ergebnis der Aktion: 130 Hausdurchsuchungen im gesamten Bundesgebiet, gegen 3500 Internetnutzer wurde ermittelt. Mit dem geplanten Gesetz zur Vorratsdatenspeicherung dürfen noch mehr Daten auf längere Zeit gesichert werden.



Fotos: ddp (2), Symantec, Photodisc
Copyright © 2008 by FOCUS Online GmbH