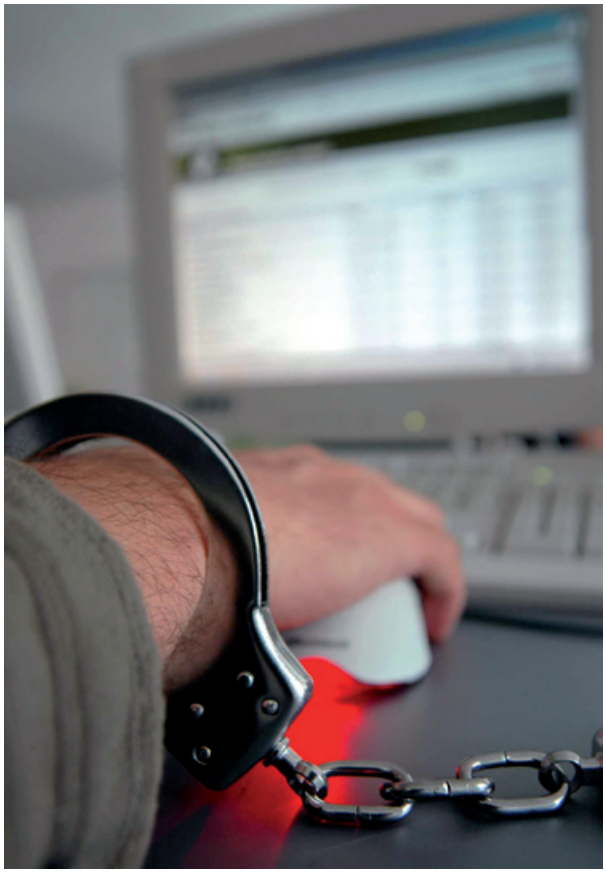
Kein Speichern unter dieser Nummer



Quelle: picture alliance / dpa Themendienst / Jens Schierenbeck

Informanten in Gefahr: Mittel und Wege gegen die Vorratsdatenspeicherung

Zusammenfassung

Kommt sie oder kommt sie nicht? Das ist gar nicht die Frage. Das Gesetz zur Einführung der Vorratsdatenspeicherung in Deutschland ist seit Januar 2008 in Kraft: Wer mit wem telefoniert hat, die Standorte der Handys und die Inhalte der SMS werden komplett gespeichert. Ab 2009 soll auch das gesamte Bewegungsprofil aller Bürger Deutschlands im Internet erfasst werden – wer wo wann wohin surft und wer mit wem E-Mails ausgetauscht hat. Für Journalisten heißt das: Jeder Informant muss damit rechnen, dass sein Kontakt zu den Medien bekannt wird. Da auch Geheimdienste auf die Daten zugreifen können, kann man davon ausgehen, dass kaum noch Verfassungsschutzskandale aufgedeckt und Whistleblower in Behörden verstummen werden. Die Inhalte unverschlüsselter E-Mails können ohnehin in Echtzeit mitgelesen werden, seitdem die rot-grüne Regierung die Telekommunikationsüberwachung (TKÜ) in Gesetzesform gegossen hat.

Die gute Nachricht: Gegen alle diese Maßnahmen kann man sich schützen. Wer will, kann seine elektronische Kommunikation unknackbar kodieren, mit einer virtuellen Tarnkappe im Internet surfen, ohne Spuren zu hinterlassen und sogar E-Mails anonym abschicken. Man muss dazu kein Computer-Experte sein. Wer einen Video-Recorder mit Hilfe des Handbuchs programmieren und wer die Handbremse eines Autos von der Kupplung unterscheiden kann, ist auch in der Lage, das Handwerkzeug zu konfigurieren, das Journalisten im Internet brauchen. Für alle Computer-Betriebssysteme – Windows, Mac OS und Linux – existieren sowohl einfache als auch sehr anspruchsvolle Lösungen, um die Kommunikation und das Surfen im World Wide Web „unsichtbar“ zu machen.

Alles zu Protokoll

Was ist „Anonymität“ im Internet? Jeder Rechner, der im Netz mit einem anderen verbunden ist, hat eine eindeutige Adresse. Wäre das nicht so, würde das Internet nicht funktionieren. Die Provider weisen den Surfern, die online gehen, jeweils wechselnde („dynamische“) IP-Adressen zu. Die Firma, die einen Internet-Zugang für ihre Kunden bereithält, kann daher immer nachvollziehen, wer mit welchem Rechner unterwegs war.

Diese so genannte IP-Adresse ist ein Zahlencode. Computer, die mit anderen kommunizieren sollen, müssen sich die Buchstaben einer Adresse im World Wide Web – wie zum Beispiel www.dfjv.de – aber erst „übersetzen“ lassen – hier in 195.30.230.79. Das macht ein Domain Name Server (DNS), ein Rechner, den der Provider als „Dolmetscher“ konfiguriert hat. Wer technisch versiert ist, kann sich sogar den DNS-Server selbst auswählen. Der Provider hat fast immer die Kontrolle über den „Dolmetscher“, also auch den Überblick darüber, welche Websites seine Kunden aufgerufen haben. Erst mit dieser IP-Adresse findet ein Computer andere Rechner und kann mit ihnen Daten austauschen. Das gilt nicht nur für das World Wide Web, sondern auch für E-Mail und andere Dienste. Wer im

Eingabefeld des Browsers 195.30.230.79 eingibt, kommt also auch ohne „Dolmetscher“ direkt zum Deutschen Fachjournalisten-Verband.

Nicht nur Websites haben eine IP-Adresse, sondern auch diejenigen Rechner, die E-Mails weiterleiten oder etwa für das Usenet, den ältesten Foren-Bereich des Internet, zuständig sind. Die Inhaber der Websites protokollieren ebenfalls, welche Rechner bzw. IP-Adressen bei ihnen vorbeigeschaut haben. Wenn der Provider Daten zu Abrechnungszwecken für eine kurze Zeit speichert, ist das unbedenklich. Aus juristischer Sicht und laut mehrerer aktueller Urteile sind IP-Adressen aber „personenbezogene Daten“, dürfen also nicht ohne weiteres gespeichert werden.

Die Rechneradresse allein ist nur ein Teil dessen, was man im Internet über sich verrät. Die Software, die man beim Surfen nutzt („Browser“), ist vor allem bei dem Betriebssystem Windows, „ab Werk“ so voreingestellt, dass zahlreiche Informationen über den Computer des Nutzers in fremde Hände gelangen können. Cookies – winzige Datenpakete – nisten sich auf Dauer als unsichtbare Nummer ein und verraten demjenigen, der sie erstellt hat, wann der Surfer wo wie unterwegs war. Die Cookies der Suchmaschine Google etwa haben eine „Haltbarkeitsdauer“ von rund 30 (!) Jahren, wenn man sie nicht per Hand löscht. Es gibt Software, die den Verlauf („history“) des Surfens protokolliert, die aus den Daten, die der Browser preisgibt, auf andere Komponenten des Rechners Schlüsse zieht, die den Zwischenspeicher („cache“) ausliest, in dem Grafiken und Websites temporär gespeichert werden. Legt man alle diese Informationen wie Klarsichtfolien übereinander, können auch kommerzielle Anbieter aussagekräftige Nutzerprofile erstellen und diese für viel Geld verkaufen.

Für E-Mails ist das noch dramatischer: Wenn, wie das Gesetz zur Vorratsdatenspeicherung beabsichtigt, lückenlos dokumentiert wird, wer mit wem kommuniziert, gibt es nur noch gläserne Nutzer. Vergleichbar wäre das mit dem Vorhaben, für jeden Deutschen zu protokollieren, wann man mit wem ein persönliches Gespräch geführt hat – und das für mindestens ein halbes Jahr, wann er oder sie wohin wie lange spazieren gegangen oder gereist ist oder eingekauft hat. Ein Traum für Marktforscher, Datenkraken wie Google und Befürworter eines totalitären Überwachungsstaates – ein Alptraum für diejenigen, die sich einen Rest von Privatsphäre behalten wollen.

http://www.ccc.de/censorship/dns-howto	Chaos Computer Club Anleitung zur Konfiguration der DNS-Einstellungen
http://www.daten-speicherung.de/?p=197#ag	IP-Adressen sind personenbezogene Daten

Wer also im Internet anonym bleiben und der geplanten Vorratsdatenspeicherung ein Schnippchen schlagen will, darf beim Surfen keine Daten über sich hinterlassen, muss seine IP-Adresse „tarnen“ und seine E-Mails nicht nur verschlüsselt, sondern auch anonym verschicken – und empfangen können. Das hört sich komplizierter und aufwendiger an als es ist.

Konfiguration des Rechners und der Software

Sicherheit

Wer zu bestimmten Zwecken anonym im Internet unterwegs sein will, muss sich schon vorher um die Sicherheit kümmern. Wer den Browser offen wie ein Scheunentor lässt und danach anonym surfen will, kann gleich das Schloss vor die eigene Wohnungstür nageln.

Die schon vorhandene und genutzte Software muss so konfiguriert werden, dass man möglichst wenig über sich verrät, aber dennoch nicht umständlich herumklicken muss, wenn eine seriöse Website den Einsatz von Cookies verlangt – etwa beim online-Einkauf. Wer in der Redaktion die „Internet-Einstellungen“ des Browsers nicht verändern darf, ist im Nachteil, aber auch nicht in der Verantwortung.

Für den Browser Firefox werden nützliche und sehr bequeme Erweiterungen („Plugins“ oder „Extensions“) angeboten, die man per Mausklick installieren kann. Für die Praxis sind CookieSafe und NoScript unbedingt zu empfehlen. Beide Programme arbeiten über einen Button im Browser und erlauben, für jede besuchte Website eine Regel

https://tor-proxy.net/de/node/5	Tor-Proxy.NET, Anonym surfen mit JonDos per Web-Interface – keine zusätzliche Software nötig!
http://www.awxcnx.de/tor-i2p-proxy.htm	Anonyme Webservices der German Privacy Foundation
http://www.all-nettools.com/toolbox,privacy	Anonym surfen und mailen:
http://anonymouse.org/anonwww_de.html	Anonym surfen
http://de.wikipedia.org/wiki/Proxy_%28Rechnernetz%29	Proxy (Wikipedia)
http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/	Alles über Proxies (für Fortgeschrittene)

aufzustellen, die sich das Programm merkt. Man kann alle Cookies verbieten und hat damit die lästige Datenspionage der Suchmaschine Google außer Kraft gesetzt, kann aber für andere Websites Cookies zulassen. NoScript arbeitet für das mitunter gefährliche und auf vielen Websites im Quellcode eingesetzte Javascript ähnlich: Man sollte zunächst „alle Scripte“ verbieten und kann dann, wenn eine Website nicht barrierefrei ist und etwa aktiviertes Javascript zur Navigation verlangt, punktuell das Verbot wieder aufheben.

Wer andere Browser bevorzugt, für die es keine bequemen Erweiterungen zugunsten der Sicherheit gibt, sollte sich bemühen, alle sogenannten „aktiven Inhalte“ zu verbieten. Leider bedeutet das manchmal, dass man in den Optionen/Voreinstellungen des Browser umständlich suchen muss, wo sich das Gewünschte verändern und einstellen lässt.

http://www.mozilla.org	Praktische Erweiterungen für den Browser Firefox (für alle Betriebssysteme, deutsch)
http://noscript.net	Firefox-Erweiterung NoScript, für jede einzelne Website lässt sich bestimmen, ob Scripte zugelassen werden.
https://addons.mozilla.org/de/firefox/addon/2497	Firefox-Erweiterung CookieSafe Konfiguration der Cookies für die jeweilige Website – empfehlenswert!

Anonymität

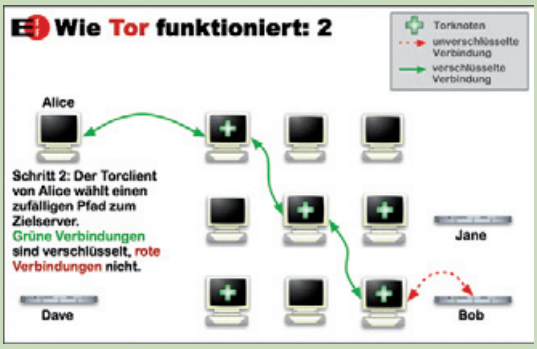
Ist der Browser „wasserdicht“ gemacht, kann man sich zwischen zwei Methoden entscheiden, um mit einer Tarnkappe zu surfen: Man benutzt Websites, die als Service zeitweilige Anonymität anbieten oder man installiert selbst Programme, die das garantieren. Die erste Methode setzt voraus, dass man dem Betreiber eines solchen Angebots vertraut, dass das, was versprochen wird, auch zutrifft. Der Vorteil: Man kann auch spurenarm surfen, wenn man nicht den eigenen Rechner benutzt. Die zweite Methode ist verlässlicher, funktioniert aber nur bei Computern, die die Installation neuer Programme gestatten, die man also selbst verwaltet.

Die Hochsicherheits-Version der Anonymität bedeutete: Auf dem Rechner, von dem aus gearbeitet wird, bleiben keine Spuren der Recherche zurück; zu keinem Rechner, über deren Inhalte recherchiert wurde, sind eigene Daten geflossen, und der gesamte Weg der Kommunikation bleibt im Verborgenen.

Unsichtbar per Website

Tor-Proxy.NET bietet gleich zwei verschiedene Wege an, anonym surfen zu können, ohne dass man sich mit der Technik beschäftigen müsste. Man gibt einfach die Adresse ein, etwa www.islamic-world.net, und niemand kann etwas darüber erfahren, welcher Rechner in Wahrheit die Website angesteuert hat.

Anonymisierungsdienste wie Anonymouse arbeiten mit sogenannten anonymen Proxies: Das ist eine Art „Zwischenrechner“, der sich zwischen dem Surfer und sein Ziel postiert und dem Rechner, auf den man gelangen will, eine andere IP-Adresse übergibt als die des Nutzers. Diese Methode kann man auch mit „Bordmitteln“ nutzen: Man sucht nach Listen anonymer Proxies und befiehlt dem eigenen Browser (in den Netzwerk-Einstellungen), nicht direkt zu surfen, sondern



Quelle: https://www.torproject.org

einen Zwischenrechner zu benutzen, dessen IP-Adresse man selbst einträgt. Mit dieser Methode sollte jeder Journalist vertraut sein, da so auch die Zensur bestimmter Websites und Internet-Filter umgangen werden können.

Zwiebeln mit Zwischenrechnern

Zwei kostenlose Programme bzw. Dienste eignen sich in der Praxis zum anonymen Surfen: TOR („The Onion Router“) und der Java Anon Proxy (JAP). Andere Anonymisierungsdienste wie das „Invisible Internet Projekt“ (I2P) werden noch entwickelt oder sind nur etwas für Nutzer mit fortgeschrittenen technischen Kenntnissen. Der Java Anon Proxy garaniert fast vollständige Anonymität im World Wide Web; das Tor-Netzwerk anonymisiert auch andere Dienste im Internet – wie Filesharing, E-Mail oder bei Bedarf Postings im Usenet.

Sowohl JAP als auch TOR funktionieren nach dem Prinzip, eine Kette vernetzter Rechner im Internet als Proxy zu benutzen. Der „Zwischenrechner“ besteht hier aus einer Software, die auf dem eigenen Computer installiert wird und die dann mit einer Reihe anderer kommuniziert, die Anonymität garantieren. Die eigene unverwechselbare IP-Adresse, die man beim Surfen vom Provider zugewiesen bekommt, wird geschreddert und durch eine andere ersetzt. Beim Java Anon Proxy surft man unter dem Deckmantel einer der Rechner, der der „Mixkaskade“ angeschlossen ist. Im Tor-Netz wechseln die internen Adressen alle paar Minuten – selbst die Logfiles des Administrators eines Tor-Servers haben nicht den geringsten Wert, sobald einer der beteiligten Computer im „sicheren“ Ausland steht.

Java Anon Proxy bietet den Vorteil, leicht installiert werden zu können. Falls man kein exotisches oder uraltes Betriebssystem benutzt, kann das jeder Computer-Laie. Auch die Bedienung ist einfach – für Installation und einen ersten Versuch, anonym zu surfen, benötigt man in der Regel nicht mehr als zehn Minuten. JAP hat auch Nachteile: Anonymität wird nur im World Wide Web geboten, die Software hat zu wenige Nutzer, um höchstmögliche Sicherheit zu garantieren, und Zukunft des Projekts ist ungewiss, auch die der kommerziellen Version JonDonym.

The Onion Router hat sich zum Standard für Anonymität im Internet entwickelt. Das Netz besteht aus weltweit rund 1000 vernetzen Rechnern, die wie digitale Waschmaschinen die eingehenden IP-Adressen im Minutentakt immer wieder verändern, so dass der Input dem Output nicht zugeordnet werden kann. Daten gehen dabei nicht verloren. Das Tor-Netz funktioniert wie ein intelligentes Labyrinth von Briefkästen, die sich nach einem ständig ändernden System die Post zuschieben, ohne dass der Absender und der Weg im nachhinein rekonstruiert werden könnten.

Anonym surfen

http://anon.inf.tu-dresden.de	Projekt: AN.ON – Anonymität online
http://www.torproject.org	Tor: Anonymität online (Anleitung „Running the Tor client on MS Windows“: https://www.torproject.org/docs/tor-doc-windows.html)
http://www.berliner-journalisten.com/09/free/1984.html	Schröder, B./Ude, A. (2007): Verfolgungswahn (Berliner Journalisten 9/1-2007), in: Auch für Laien verständliche Anleitung zu Tor und Java Anon Proxy für alle Betriebssysteme, Linksammlung
http://flenda.gratis-server.de	Anonym Surfen in sieben Minuten – Anleitung für Nicht-Techniker
https://addons.mozilla.org/de/firefox/addon/2275	Torbutton: Ermöglicht auf Knopfdruck das Surfen normal und mit Tarnkappe, für alle Betriebssysteme
https://www.foebud.org/datenschutz-buergerrechte/vorratsdatenspeicherung/privacydongle	PrivacyDongle – Anonym im Internet surfen (nur für Windows) Tor auf einem USB-Stick, auch zum Download
http://foxyproxy.mozdev.org/	Firefox-Erweiterung FoxyProxy
https://addons.mozilla.org/de/firefox/addon/2464	Man kann zwischen mehreren Profilen wählen, ermöglicht den Wechsel etwa von Java Anon Proxy zu Tor im laufenden Betrieb

Auch beim „Zwiebel-Routen“ sind Nutzer des Browsers Firefox klar im Vorteil. Dessen Erweiterung Tor-Button ermöglicht Ein- und Ausschalten der Anonymität per einfachem Mausklick. Wer andere Browser benutzt, kann sich die Gratis-Software für alle Betriebssysteme herunterladen und installieren – auch das ist nicht übermäßig kompliziert.

Der Nachteil von TOR ist die Performance: Trotz schneller Internet-Verbindung verlangsamt der Einsatz manchmal das Surfen, vor allem bei Grafiken und Multimedia-Dateien. Je mehr Tor-Server in Betrieb sind, umso schneller wird das Netz insgesamt.

Das geplante Gesetz zur Vorratsdatenspeicherung wird mit TOR komplett ad absurdum geführt. Alle diese Methoden sind legal und werden es auch bleiben.

E-Mails im Zeitalter der Datenkraken

Seit es E-Mail gibt, war es möglich, diese anonym zu verschicken. Das geschieht durch sogenannte „anonyme Remailer“, kostenlose Software, die alle relevanten Informationen aus dem elektronischen Briefkopf einer E-Mail entfernt. Nur aus dem Text der Nachricht könnte der Empfänger eventuell schließen, vom wem sie stammt. Für Laien ist das jedoch kompliziert und technisch aufwendig. Daher bieten einige Websites diesen Service als Formular an. Falls man dem Betreiber vertraut, gibt man einfach die E-Mail-Adresse des Empfängers und den Text ein – das gilt für Klartext, aber auch für verschlüsselte E-Mails. Der Verein German Privacy Foundation offeriert zum Beispiel seinen Mitgliedern eine „vorratsdatenfreie Nachrichtenbox“, die technisch so umgesetzt worden ist, dass im Rahmen der Vorratsdatenspeicherung nichts protokolliert oder gespeichert werden müsste. Dieses Angebot wird bald kostenlos und auch öffentlich zugänglich sein.

http://www.awxcnx.de/anon-email.htm	Web-Formular, um anonym E-Mails zu verschicken
http://www.anon.gildemax.de/	Anonyme E-Mails über Remailer (FAQ)

Für Computer-Fachleute wird es immer möglich sein, sich dem Zugriff von Datenspionen oder der Überwachung zu entziehen. Eine noch höhere Anonymität als Java Anon Proxy oder TOR bieten abgeschottete Datennetze wie das Invisible Internet Project (I2P) oder das Freenet Projekt. Eine dezentrale und vollständig verschlüsselte Infrastruktur verbirgt nicht nur die Inhalte der Kommunikation, sondern auch, wer welchen Dienst nutzt und genutzt hat.

Manchmal gibt es jedoch ganz einfache Methoden, dem Großen Bruder zu entkommen. Ein technisch versierter Informant, der einem Journalisten etwas geheim mitzuteilen hat, wird diesem vermutlich Internet Relay Chat empfehlen. Dort konnte man, wenn man sich der Identität des Kommunikationspartners gewiss war, schon immer ungestört und unbelauscht plaudern und Daten transferieren. Und wer seine Nachrichten per Instant Messaging in Echtzeit austauscht, wird auch im Jahr 2009 und danach nicht gespeichert – diese Form der Kommunikation hat man im Gesetz zur Vorratsdatenspeicherung schlicht vergessen.

Der Autor
Burkhard Schröder arbeitet seit zwei Jahrzehnten als freier Journalist in Berlin-Kreuzberg für Print- und Online-Medien mit den Schwerpunkten Internet, Netzkultur und Sicherheit. Er ist ständiger Mitarbeiter beim Online-Magazin Telepolis und war von 2004 bis 2007 Chefredakteur des unabhängigen Medienmagazins „Berliner Journalisten“. Neben zahlreichen Büchern zum Thema Rechtsextremismus hat er auch Science-Fiction-Stories und einen historischen Roman geschrieben. Schröder ist Honorardozent an der Berliner Journalisten-Schule für Internet-Recherche und Vorsitzender des Vereins German Privacy Foundation. Im Mai erscheint sein neues Buch „Die Online-Durchsuchung“.
www.burks.de
www.privacyfoundation.de

Mehr Informationen

Holger Bleich: Selbstverdunkelung. Anonymes Mailen in der Praxis (c‘t 16/2000, S. 156):
http://www.heise.de/ct/00/16/156/
Detailreicher Artikel mit zahlreichen Links über Geschichte und Technik des anonymen Mailens in den letzten zehn Jahren, eine gute Übersicht, aber nicht immer aktuell und in der Praxis nur für technische Versierte umsetzbar.

Jens Lechtenbörger: Informationelle Selbstbestimmung im Internet mit Firefox, NoScript, JAP/JonDo, Tor, GPG/PGP und Mixminion:
http://www.informationelle-selbstbestimmung-im-internet.de/
sehr ausführlich, aber fast immer auch für Laien verständlich

German Privacy Foundation/Linksammlung zur Anonymität und zum Schutz der Privatsphäre:
http://www.privacyfoundation.de/links_partner/

Kai Raven: Anonym im Internet mit Anon-Plattformen:
http://hp.kairaven.de/bigb/asurf.html
Hier gibt es für alle Themen rund um die Anonymität im Internet eine umfassende und anschauliche Antwort. Der Laie verliert bei der Fülle der Informationen aber leicht den Überblick.

Privacy Handbuch der German Privacy Foundation:
https://www.awxcnx.de/handbuch.htm
Anleitungen zum spurenarmen und anonymen Surfen, zur E-Mail Verschlüsselung, zur anonymen Nutzung von E-Mails, zur Datenverschlüsselung und zum Betreiben von Anon-Servern – für jemanden, der sich gründlich mit dem Thema beschäftigen will.

Albrecht Ude: Anonymisierung - Kommunikationssicherheit im Internet (nur für Windows)
http://www.ude.de/seminar/anonymisierung-script.pdf

Das deutsche I2P-Handbuch:
http://www.planetpeer.de/wiki/index.php/Das_deutsche_I2P-Handbuch
widmet sich der technisch sehr anspruchsvollen Methode des anonymisierten Kommunikationsnetzwerks Invisible Internet Project. Für Laien nicht zu empfehlen.

Invisible Internet Project I2P:
http://de.wikipedia.org/wiki/I2P