PIRATENMAGAZIN

DAS MAGAZIN FÜR POLITISCHE THEMEN DER INFORMATIONSGESELLSCHAFT

PIRATENMAGAZIN

SONDERAUSGABE

WWW.PIRATEN-MAGAZIN.DE/SONDERAUSGABE

Nr. 1 / 2008

Die Vorrats-datenspeicherung

...und was kommt dann? S. 4

Inhaltsverzeichnis

Ahoi, Landratten!

Im vergangenen Jahr ist so einiges passiert. Die Terrordatei wurde eingerichtet, Reisepässe enthalten nun Fingerabdrücke, die USA erhalten fast uneingeschränkten Zugriff auf Daten von Flugpassagieren und einige EU-Staaten haben ihre Biometriedatenbanken zusammengeschaltet. Als wären diese Verstöße gegen den Datenschutz nicht genug, ist am ersten Januar das Gesetz zur Vorratsdatenspeicherung in Kraft getreten. Ab sofort wird also für 6 Monate gespeichert, wer wann mit wem telefoniert, per SMS oder Email kommuniziert und im Falle von Mobiltelefonen auch der Standort zum Zeitpunkt der Kommunikation.

Dieser zweifellos schwerste Eingriff in unsere Grundrechte seit langem gefährdet nicht nur Tauschbörsennutzer, Anwälte, Ärzte, Journalisten und politische Aktivisten, sondern jeden Einzelnen. Aus diesem Grund ist diese Ausgabe des Piratenmagazins genau diesem Thema gewidmet. Wir lassen das Zustandekommen der Richtlinie noch einmal Revue passieren, beleuchten die sich daraus ergebenden Gefahren und zeigen Möglichkeiten zur Umgehung der Vorratsdatenspeicherung und zum Schutz der Privatsphäre auf.

Mit der Vorratsdatenspeicherung abfinden werden wir uns auf keinen Fall. Der Arbeitskreis Vorratsdatenspeicherung hat bereits eine sehr aussichtsreiche Verfassungsbeschwerde eingelegt und die neu gegründete German Privacy Foundation gibt weitere technische und rechtliche Unterstützung gegen den Überwachungsstaat.

Natürlich ist dem Piratenmagazin ebenfalls die Privatsphäre seiner Leser wichtig. Deswegen bieten wir neben der Emailadresse zusätzlich noch eine vorratsdatenspeicherungsfreie Mailbox für Feedback an. Ihr solltet bei Benutzung der Nachricht eine ebenfalls vorratsdatenspeicherungsfreie Kontaktmöglichkeit angeben, falls ihr eine Antwort wollt.

Eines sollte aber jedem klar sein: Wir befinden uns nun an einem entscheidenden Punkt im Kampf um die Grundrechte. Gelingt es uns jetzt, die Vorratsdatenspeicherung rückgängig zu machen und die Entwicklung in Richtung Überwachungsstaat aufzuhalten, besteht eine realistische Chance, zu einer freiheitlich demokratischen Grundordnung zurückzukehren. Andernfalls droht ein jahrzehntelanger Überwachungsstaat, der nicht so einfach zu überwinden sein wird.

Aufruf zur Demonstration gegen den Überwachungsstaat in Köln

Am 15. März 2008 findet in Köln unter dem Motto "Für ein Morgen in Freiheit"gegen den Überwachungswahn, für die Achtung der Bürgerrechte und für eine freiheitliche Gesellschaft ohne Panikmache eine Demonstration statt.

Nicht erst seit den Anschlägen vom 11. September 2001 wurden von den Bundesregierungen immer schärfere gesetzliche Vorschriften zur Überwachung der Zivilbevölkerung erlassen. Triebfeder der zunehmenden Bespitzelung der Bürger von Staats wegen ist nicht zuletzt der Bundesinnenminister Dr. Wolfgang Schäuble, der in der Vergangenheit zahlreiche Maßnahmen angekündigt hat, deren Konformität mit dem Grundgesetz deutlich in Frage gestellt werden kann. Allein die zum 01.01.2008 in Kraft getretene flächendeckende Zwangsspeicherung aller Kommunikationsdaten von Telefon, Handy, Internet und E-Mail unbescholtener Bürger schränkt die Freiheitsrechte aller Bürger in einer Weise ein, die in einem Staat mit freiheitlich-demokratischer Grundordnung kaum mehr zu vertreten ist.

Darüber hinaus sind sich Kriminalistikexperten weitgehend einig, dass die beschlossenen und geplanten Überwachungsmaßnahmen keinen nennenswerten Effekt bei der Terrorismus- und Kriminalitätsbekämpfung haben, sondern lediglich eine Vergeudung von Steuergeldern in Millionenhöhe darstellen, deren Verwendung bei der nachweislich wirksamen Kriminalitätsprävention weitaus positivere Effekte hätte.

Aktivisten verschiedener Organisationen tragen auf einer vergangenen Demonstration in Hamburg symbolisch die Privatsphäre zu Grabe

Diesem unsinnigen, bürgerrechtsfeindlichen und teuer bezahlten Überwachungsdrang der Bundesregierung wollen Parteien und Organisationen aus Köln und dem ganzen Bundesgebiet nicht länger tatenlos zusehen. Daher haben sie sich zu einem Bündnis gegen den Überwachungswahn der Bundesregierung und für die Stärkung der Bürgerrechte zusammengeschlossen. Dazu Jens Seipenbusch, Vorsitzender der Piratenpartei: „Die große Koalition ist sich offenbar nur bei einem einig: beim Abbau von Bürgerrechten. Insbesondere die CDU befindet sich in voller Fahrt Richtung gläsernem Bürger und Überwachungsstaat. Es wird höchste Zeit, dass wir den Regierenden hier unmißverständlich Einhalt gebieten."

Alle Menschen sind aufgerufen, an der Demonstration am 15.03.2008 teilzunehmen und so der Regierung zu zeigen, dass die Einwohner Deutschlands für ihre Freiheits- und Bürgerrechte auf die Straße gehen. Die Forderungen sind:

- Stopp der Totalprotokollierung von Telefon, Handy, Email und Internet (Vorratsdatenspeicherung)
- Stopp der Planungen zur geheimen Durchsuchung von Computern (Onlinedurchsuchung)
- Stopp der Videoüberwachung öffentlicher Räume
- Stopp der biometrischen Erfassung unbescholtener Bürger
- Keine Einrichtung zentraler Datenbanken über die Bevölkerung (z.B. elektronische Gesundheitskarte, zentrales Melderegister)
- Keine Speicherung von Flugpassagierdaten und keine Weitergabe solcher Daten an Drittstaaten
- Kein automatischer Kfz-Kennzeichenabgleich auf öffentlichen Straßen
- Stopp aller neuen Gesetzesvorhaben auf dem Gebiet der inneren Sicherheit, wenn sie mit weiteren Grundrechtseingriffen verbunden sind.
- Überprüfung aller seit 1968 beschlossenen Überwachungsgesetze auf ihre Wirksamkeit und schädlichen Nebenwirkungen

Mitglieder dieses Bündnisses sind:

- die Kölner Bürgerrechtsinitiative "Freiheit ist Sicherheit"

- der Arbeitskreis Vorratsdatenspeicherung
- der Chaos Computer Club Köln
- die Grünen Köln
- die Linke.Köln
- der Bezirksverband Köln der Piratenpartei
- der Landesverband NRW der Piratenpartei
- der Verband der freien Lektorinnen und Lektoren

deren Aufruf zur Demonstration mitgetragen wird von:

- Bündnis 90/Die Grünen Landesverband NRW
- Die Linke Landesverband NRW
- Die Linke Ortsverband Bergisch-Gladbach
- FoeBuD e.V.
- Piratenpartei Landesverband Hamburg
- Kein Mensch ist illegal
- Reflect

Datum: 15. März 2008
Ort: Köln
Treffpunkt: 14.00 Uhr auf dem Roncalli-Platz ("Domplatte")

Informationen:

Autor: Piratenpartei Köln
Bilder: AK Vorratsdatenspeicherung

Die Vorratsdatenspeicherung: Zustandekommen und Auswirkungen

Technische, historische und rechtliche Hintergründe

Die EU-Richtlinie zur Vorratsdatenspeicherung (Data Retention) schreibt allen Mitgliedsstaaten die zeitlich befristete Speicherung sämtlicher Verkehrsdaten elektronischer Kommunikation vor und hebt damit auch direkt und ausdrücklich bisherige Gesetze, die so auch in Deutschland mindestens bis Ende 2007 galten, teilweise auf. Zum Beispiel war die Speicherung von solchen Daten bei Internet-Flatrates bisher ausdrücklich verboten (ganz im Sinne des Gebots der Datensparsamkeit: wenn solche Daten nicht zur Abrechnung oder anderen zwingend erforderlichen Zwecken zu erheben nötig sind, dürfen sie nicht gespeichert werden).

Bei der elektronischen Kommunikation fallen zwei Arten von Daten an: Verkehrsdaten wie IP-Adressen, Handy-Standorte und Telefonnummern und Inhaltsdaten, wie der Text einer Email. Die Vorratsdatenspeicherung (VDS) bezieht sich ausschließlich auf Verkehrsdaten. Die Speicherung von Inhaltsdaten wird in der EU-Richtlinie ausdrücklich verboten.

Doch auch so ist der Eingriff schon schwer genug. Anhand der für 6 Monate gespeicherten Daten lassen sich nun umfassende Kommunikationsprofile einzelner Personen oder Personengruppen erstellen. Diese können in Deutschland nicht nur wie vielfach zitiert „zur Aufklärung schwerer Straftaten“ (Terrorismus, Völkermord, etc.) genutzt werden, sondern „zur Aufklärung mittels Kommunikation begangener Straftaten“. Das kann im Ernstfall auch nur eine Beleidigung sein. Es muss davon ausgegangen werden, dass diese Regelung hauptsächlich der Medienindustrie nutzt und von dieser zur massenhaften Abmahnung von Urheberrechtsverletzungen genutzt wird.

Dabei hatte der deutsche Bundestag die Vorratsdatenspeicherung bereits abgelehnt. Über den „EU-Umweg“ kam sie jedoch unter Umgehung der demokratischen Institutionen mit dem Argument der Terrorismusbekämpfung dennoch zu Stande. Nicht nur anhand der konkreten Umsetzung der Richtlinie, sondern auch anhand der Äußerungen verschiedener Politiker wird in letzter Zeit klar, dass die Vorratsdatenspeicherung mit Terrorismusbekämpfung wenig bis nichts zu tun hat.

Klassische (bisherige) Überwachungsanordnungen

Bisher waren schon diverse Eingriffe in die elektronische Kommunikation seitens des Staates möglich: stets auf richterlichen Beschluss, oder bei nachträglicher solcher Genehmigung bei Gefahr im Verzug ausnahmsweise durch die Staatsanwaltschaft, können z.B. Telefonate abgehört (und damit natürlich ebenso die Partner der Telefonate nicht nur belauscht, sondern auch direkt ermittelt) werden, das Passwort der Email-Postfächer konnte vom Provider verlangt werden etc. Das alles erfordert aber stets einen konkreten Verdacht auf die Begehung schwerer Straftaten, den leider vorhandenen Fällen von Missbrauch wird jetzt aufgrund von Platz und Thema nicht weiter nachgegangen (nur eine Anmerkung: richterliche Genehmigungen werden typischerweise allzu leichtfertig erteilt, so dass man weitgehend der Gewissenhaftigkeit staatsanwaltlicher Anträge auf solche Maßnahmen vertrauen muss).

Wichtig an diesen bisher möglichen Maßnahmen ist, dass sie niemals nachträglich stattfanden (d.h. erst nach einem konkreten Anfangsverdacht begonnen wurden) und nur einen sehr kleinen Teil der Bevölkerung betrafen. Anhand des Anstiegs der Telefonüberwachung um 500% alleine in den Jahren 1995-2004 und einem sich fortsetzenden Trend lässt sich aber erkennen, dass solche Überwachungsmaßnahmen zunehmend inflationär verwendet werden. Dagegen betrifft die Vorratsdatenspeicherung zunächst einmal ausnahmslos jeden (über die Einschränkungen und deren Wirksamkeit später mehr).

IP-Adress-Speicherung

Die überwiegende Mehrheit der Internetnutzer erhält von einem Internet Provider zeitlich begrenzt eine IP-Adresse, die typischerweise bei jeder Einwahl bzw. maximal 24 Stunden („Zwangstrennung“) wechselt. Es gibt jedoch auch Provider wie QSC, bei denen zum Einen keine Zwangstrennung stattfindet und zum Anderen bei rascher Wiedereinwahl sogar dieselbe IP-Adresse wie zuvor vergeben wird, was einer statischen IP-Adresse schon recht nahe kommt; sie lässt sich Wochen, teils Monate aufrecht erhalten.

Insbesondere bei Internet-Flatrates durften diese IP-Adressen bisher überhaupt nicht gespeichert werden, was die meisten Provider leider schon heute nicht kümmert. Nur einige wenige Provider bieten Anschlüsse ohne Speicherung der Daten an. Die meisten Provider speichern die Daten schon heute bis zu 6 Monaten. Herabsenkungen der Speicherfristen waren hauptsächlich Notlösungen, da einzelne Provider von Anfragen durch Staatsanwaltschaften regelrecht überflutet wurden.

Im Laufe des Jahres 2008 soll dies im Zuge der Vorratsdatenspeicherung geändert werden: in Deutschland müssen diese Daten dann sechs Monate gespeichert werden.

Nur über diese IP-Adresse, die einem Anschluss und damit einer Person zugeordnet werden kann, können die meisten Internetdienste direkt Personen zugeordnet werden: z.B. bei Aufruf von Websites (www) ohne Login, Teilnahme am Filesharing wie z.B. BitTorrent, VoIP-Telefonie, IRC, Instant Messaging etc.

Bei Emails, Internettelefonie und herkömmlicher Telefonie wird jeweils der Absender und Empfänger sowie der Zeitpunkt bzw. die Dauer der Kommunikation gespeichert. Im Falle mobiler Kommunikation (SMS, MMS oder Telefonieren mit dem Handy) wird zusätzlich jeweils die Funkzelle und damit der ungefähre Standort zum Zeitpunkt der Kommunikation gespeichert. Vor allem bei Vieltelefonierern lassen sich damit ohne Weiteres Bewegungsprofile erstellen.

Die Vorratsdatenspeicherung kann also dazu benutzt werden, das Kommunikationsverhalten einer Person über Mediengrenzen hinweg aufzuzeichnen und damit das soziale Umfeld und andere Tätigkeiten zu analysieren. Dies stellt auch das Hauptproblem dar, weswegen die Vorratsdatenspeicherung von eigentlich allen Datenschützern komplett abgelehnt wird. Sie stellt nicht nur einen schweren Eingriff in die Privatsphäre dar, sondern führt auch bisherige Vertrauensverhältnisse und Berufsgeheimnisse ad absurdum.

Dazu zählen etwa die Berufsgeheimnisse von Ärzten, Anwälten oder Geistlichen. Ebenso werden Journalisten Probleme haben, Kontakt zu Informanten aufzunehmen. Wenn diese damit rechnen müssen, dass ihre Kommunikation gespeichert wird, können sie nicht mehr unbefangen mit Journalisten kommunizieren und ihnen beispielsweise brisante Fakten mitteilen. Das Gleiche gilt für Drogenberatungsstellen und Telefonseelsorgedienste. Die Vorratsdatenspeicherung führt also in der Summe zur Totalüberwachung des Kommunikationsverhaltens sämtlicher in der EU-lebenden Menschen, schränkt die Pressefreiheit ein und verhindert, dass Menschen in Not geholfen werden kann.

Zusätzlich werden durch die konkrete Umsetzung der Vorratsdatenspeicherung in Deutschland Anonymisierungsdienste ebenfalls zur Speicherung von Verbindungsdaten verpflichtet. Abgesehen davon, dass ein Anonymisierungsdienst, der Verbindungsdaten speichert, nicht mehr anonymisiert und damit sinnlos ist, verarbeiten die Server dieser Dienste häufig tausende Anfragen pro Sekunde. Damit würde die Speicherung der Daten Unmengen an externem Speicherplatz benötigen. Die Regelung kommt damit einem Verbot von Anonymisierungsdiensten in Deutschland gleich. Zum jetzigen Zeitpunkt ist abzusehen, dass mindestens 90% der in Deutschland betriebenen Anonymisierungsserver abgeschaltet werden müssen oder ins Ausland auswandern werden, falls die Vorratsdatenspeicherung über das Jahr 2008 hinaus Bestand hat.

Stand und Inhalt der VDS in der EU-Richtlinie

Folgende Punkte der EU-Leitlinie erscheinen hier erwähnenswert:

- sie wurde am 15. März 2006 verabschiedet, trat zehn Tage später in Kraft, und muss bis spätestens 15. März 2009 von allen EU-Mitgliedsstaaten umbzw. durchgesetzt werden
- die Speicherfrist muss mindestens sechs Monate und darf höchstens zwei Jahre betragen
- die meisten Mitgliedsstaaten haben gemäß Paragraph 15, Absatz 3 der Richtlinie die Verlängerung der Frist zur Einführung entweder ohne genaue Zeitnennung, meistens aber mit 18 bis 36 Monaten (maximal möglich, vgl.o.) beantragt
- die Erfassung der Verkehrsdaten ist Pflicht, die Erfassung der Inhaltsdaten bleibt verboten
- die Mindestanforderungen sind: IP-Adresse und Zeitraum des Kunden des Providers für jeden sei-

ner Kunden für die Dauer der Frist, Telefonnummern und Standortdaten beider Teilnehmer für die Dauer eines Telefonats

- ein Gummiparagraph zur eigenen Ausgestaltung, entsprechend missbrauchsanfällig, ist die Formulierung, dass jeder Staat nur im Rahmen der europäischen Menschenrechtskonvention und nach Maßgabe seiner eigenen, innerstaatlichen Regeln den Zugriff auf die Verbindungsdaten regelt — besonders gefährlich wird dies, da weitergehende Regelungen zur Weitergabe der VDS-Daten an Drittstaaten damit nicht ausgeschlossen werden, was durch andere Regelungen indes ausdrücklich erlaubt bzw. verlangt wird (!)

Verbot der Speicherung von IP-Adressen durch Websites in Deutschland

Da „nur“ die Quell-IP-Adressen von Internetnutzern, nicht aber auch die Zieladressen von der Vorratsdatenspeicherung erfasst werden, hängt die Möglichkeit, Internetnutzern mittels Vorratsdatenspeicherung nachzuspionieren, vom Loggen der IP-Adressen durch die Webserver der besuchten Internetseiten ab. Nun ist dieses Loggen wie auch das der Benutzernamen nach einem Login zwar generell eingeschaltet, aber jüngst hat der im Arbeitskreis Vorratsdatenspeicherung aktive Jurist Patrick Breyer einen juristischen Erfolg erzielt, der mit einiger Wahrscheinlichkeit zu einem allgemeinen Verbot des Loggens dieser personenbezogenen bzw. oft personenbeziehbaren IP-Adressdaten in Deutschland führen wird: nicht nur das ursprüngliche Amtsgericht, auch schon ein Landesgericht entschied, dass das Bundesjustizministerium (!) die Besucher-IP-Adressen nicht einfach wie üblich mitloggen darf. Diese Sache dürfte mindestens bis zum BGH (Bundesgerichtshof), vielleicht sogar BVG (Bundesverfassungsgericht) gehen.

Leider würde dies nur in Deutschland und auch nur theoretisch den Vorratsdatenspeicherungs–Missbrauch durch Dritte weitgehend unterbinden. Andere Länder sind einstweilen nicht dazu verpflichtet, dies zu unterlassen; so hängt es von der Einstellung der Website-Betreiber ab, ob sie das Loggen abschalten oder nicht. In der Firma, in der einer der Autoren als Datenschutzbeauftragter arbeitet, haben wir unserem Webserver dieses Loggen bereits abgewöhnt; da es aber bequemer ist, die Standardeinstellung (Loggen) eingeschaltet zu lassen, sowie teils gesteigertes kommerzielles Interesse seitens der Betreiber an diesen Daten besteht (und wenn nur, um heraus zu finden, aus welchen Ländern die Zugriffe kommen), ist kaum zu erwarten, dass ein nennenswerter Teil des Internets auf diese Standardmaßnahme verzichten wird — teils gibt es auch Sicherheitsbedenken dagegen, weil DDoS (Distributed Denial of Service) Webangriffe so schwerer zu erkennen und zu vereiteln sind.

Auch muss man sich im Klaren sein, dass dies nur die Nutzung von Internetseiten weniger durchleuchtbar macht, Filesharer haben von einer solchen Entscheidung überhaupt nichts.

Der Arbeitskreis Vorratsdatenspeicherung hat kürzlich eine Kampagne gestartet, um Betreiber von Webseiten vom datenschutzgerechten Betrieb zu überzeugen. Jede Seite, die die Daten von Benutzern nicht speichert, kann sich mit einem Datenschutzsiegel schmücken. Weiteres zur Aktion und den Bedingungen findet sich unter wir-speichern-nicht.de

Anmerkung: die Kriminalisierung der Internet-Nutzung durch Staat und Medienkonzerne

Ein Vergleich von Briefen und Paketen mit Emails ist letztlich entlarvend, wenn man darüber nachdenkt: so findet bei Briefen und Paketen eben keine allgemeine Verkehrsdatenüberwachung statt. Und das, obwohl auch Erpresserschreiben, Briefbomben und andere illegale Dinge per snail mail bzw. klassischer Post verschickt werden, was aber selten ist. Im Internet ist es gar nicht möglich, direkt physisch schädigende Dinge per Email zu versenden, und auch da sind illegale Inhalte die Ausnahme (vom Spam-Problem einmal abgesehen, das hat aber hiermit wenig direkt zu tun). Dennoch soll hier eine Totalüberwachung der kommunizierenden EU-Bürger etabliert werden.

Folgende Motivationen erscheinen denkbar bis plausibel, warum hier mit zweierlei, geradezu inversem Maß gemessen wird:

- die überwiegend alten und wenig Internet-versierten Politiker in Machtpositionen hegen unbewusste Ängste gegen das Internet als Solches
- sowohl Politikern als auch etablierten Massenmedien und der Medienindustrie missfällt die Möglichkeit, die erst das Internet geschaffen hat, dass auch normale Bürger fast kostenlos in der Lage sind, selbst ohne Verleger oder andere Dritte eigene Beiträge zu veröffentlichen, eigene Kreationen zum Download anzubieten oder Meinungen zu verbreiten bzw. zu deren Verbreitung beizutragen: es ist unerwünschte Konkurrenz bzw. kaum zu kontrollierende Kritik
- da die elektronischen Medien — vom Telefon einmal abgesehen — noch relativ neu sind, genießen sie keinen so direkten Grundrechtsschutz wie z.B. die klassische Brief- und Paketpost
- das Abmahnunwesen in Gestalt skrupelloser Anwälte, die Formfehler ausnutzen, um sich an Internetusern persönlich durch Serienabmahnungen zu bereichern, brauchen die IP-Adressen, um ihr halblegales Geschäft betreiben zu können
- korrupte Politiker und Firmen erhoffen sich möglicherweise auch eine Einschüchterung von „Whistleblowern“ und Aktivisten durch die Vorratsdatenspeicherung

Da aber gerade die Meinungsfreiheit durch das Internet enormen praktischen Aufschwung erfahren hat, gefährdet die Vorratsdatenspeicherung diese ganz massiv, indem sie die Internetnutzer durch permanentes Nachspionieren einschüchtert sowie z.B. tatsächlichen Versuchen aussetzt, ihre Freiheit auf Meinungsäußerung durch „Seitenangriffe“ auszuhebeln. Jemand, dem eine Meinungsäußerung nicht passt, wird zweifellos unter irgendwelchen Vorwänden versuchen, an die Vorratsdatenspeicherungs-Daten des Missliebigen zu gelangen, sei es legal oder nicht (z.B. Bestechen von Administratoren des Providers des "Gegners"). Das Missbrauchspotenzial ist hier ganz enorm. Gerade im Bereich der Korruptionsbekämpfung muss man hier das Schlimmste befürchten, eigentlich können die sogenannten Whistleblower (Mitarbeiter von Firmen, die Informationen über korrupte Praktiken in ihren Firmen weitergeben) in der EU nur noch in persönlichen Gesprächen oder Briefen ihre Infos an Korruptionsaufklärer weiterleiten, weil die Vorratsdatenspeicherung es zu gefährlich macht, dafür elektronische Medien zu nutzen!

Letztlich ist es ein generelles Problem, dass einmal bekannt gegebene Daten nicht mehr aus der Welt zu schaffen sind, was zweifellos ein wesentlicher Grund für die Vorgabe der Datensparsamkeit im Bundesdatenschutzgesetz (BDSG) war und immer noch ist. Der andere ist, wo keine Daten sind, können sie auch gar nicht erst missbraucht werden. Hier wird das BDSG auf den Kopf gestellt, indem fast unvorstellbare Datengebirge und ebenso umfangreiche Missbrauchsmöglichkeiten dafür geschaffen werden. Wer glaubt, die Internet- und Telefonprovider würden solche Daten auch nur halbwegs sicher verwahren, sei auf den Bericht des Bundesdatenschutzbeauftragten Peter Schaar verwiesen, der fast überall schlampigen und nicht gesetzeskonformen Umgang mit Kundendaten in größeren Unternehmen festgestellt hat.

Gegenmaßnahmen

Da selbst die Vorratsdatenspeicherung noch keine vollständige Überwachungsmaßnahme ist, obwohl sie sehr weit geht, gibt es natürlich Möglichkeiten, sich ihr zu entziehen. Und anders als manche Politiker glauben machen wollen, werden dies auch viele unbescholtene Bürger tun, die sich nicht bespitzeln lassen wollen.

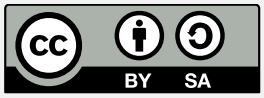
Der Umfang der geplanten Speicherung macht es zunächst sehr schwierig, sich der Pauschalüberwachung zu entziehen. Verschiedene technische Methoden und die Ausnutzung von Gesetzeslücken machen dies aber möglich. So könnte man auf lokale Mailboxen zurückgreifen, die nicht zur Speicherung verpflichtet sind, Anonymisierungsdienste mit Servern im Ausland benutzen, Remailer benutzen oder das Handy einfach mal ausschalten. Dabei sollte man sich nicht vom BKA einschüchtern lassen, das solche Maßnahmen in der Vergangenheit immer wieder als „konspiratives Verhalten“ gewertet hat. Weitere Möglichkeiten zur Umgehung der Vorratsdatenspeicherung und Wahrung

der Privatsphäre finden sich auf den folgenden Seiten.

Natürlich werden wir uns keineswegs mit der Vorratsdatenspeicherung abfinden. Zahlreiche Menschen (aktuell 30.000) haben sich unter dem Dach des Arbeitskreises Vorratsdatenspeicherung zusammen gefunden, um die bisher größte Verfassungsbeschwerde in der Geschichte der Bundesrepublik einzulegen. Irland klagt ebenfalls vor dem europäischen Gerichtshof gegen die Richtlinie. Das Land bezweckt zwar, damit längere Speicherfristen möglich zu machen, aber wenn die Richtlinie damit für ungültig erklärt wird, kann uns das nur recht sein.

Informationen:

Autoren: Stefan Urbat und Helmut Pozimski



Umgehung der Vorratsdatenspeicherung im Fall von Emails

Hintergrund

Die Vorratsdatenspeicherung bei Emails zu umgehen, stellt sich als relativ schwierig heraus; fast Jeder benutzt heutzutage ein Postfach bei einem der großen Freemailer oder seinem Internetprovider. Dort kann man sich eigentlich sicher sein, dass sie die Vorratsdatenspeicherung nicht nur in vollem Umfang umsetzen, sondern auch Strafverfolgungsbehörden und Geheimdiensten Abhörschnittstellen zur Verfügung stellen. Kleinere Anbieter werden zwar nur wenig benutzt, sind aber davon auch keineswegs ausgenommen.

Da eine Nachricht immer erst vom Rechner an den Mailserver des eigenen Anbieters und anschließend wiederum von diesem an den Mailserver des Empfängers übertragen wird, besteht hier wenig Möglichkeit, die Speicherung zu verhindern. Eine Verschlüsselung der Email und die Nutzung von Anonymisierungsdiensten bietet zwar einen gewissen Schutz, kann aber nicht verhindern, dass Absender und Empfänger von beiden Servern gespeichert werden und möglicherweise (je nach Handhabung) den einzelnen Personen zugeordnet werden können. Selbst bei völliger Pseudonymisierung lassen sich immer noch Profile über die Häufigkeit und den Zeitpunkt der Kommunikation zwischen einzelnen Personen erstellen. Es gibt also kaum eine Möglichkeit, sich bei Beibehaltung der Adresse und des Anbieters der Vorratsdatenspeicherung zu entziehen; es existieren jedoch sowohl einfache als auch komplexe Methoden, die Vorratsdatenspeicherung in dem Bereich völlig oder teilweise zu umgehen.[1] [2]

Anbieter im Ausland

Das Nächstliegende ist es nun, einfach einen Anbieter außerhalb der EU zu wählen, der nicht zur Vorratsdatenspeicherung verpflichtet ist. Falls der Anbieter vertrauenswürdig ist, kann das eine Option sein. Einen ähnlichen Effekt hätte auch die Verwendung anonymer Mailsysteme wie i2pmail [3] oder das Betreiben eines eigenen Mailservers. Damit hätte man die Vorratsdatenspeicherung für die Senderseite abgeschaltet. Jedoch werden die meisten anderen Menschen weiterhin ihre Provider- oder Freemailerpostfächer verwenden. Sendet man eine Email an solche Adressen, greift die Vorratsdatenspeicherung wieder und beim Server des Empfängers werden die Daten wieder komplett gespeichert. Bei dieser relativ einfachen Methode hätte man also nur einen Teil der Vorratsdatenspeicherung umgangen und müsste entweder nur noch mit Menschen, deren Postfächer sich außerhalb der EU befinden kommunizieren oder die Speicherung hinnehmen.

lokale Mailboxen

Oftmals lassen Gesetze bei genauerem Hinsehen Lücken offen: eine davon ist das Betreiben lokaler Mailboxen. Dabei stellt man einfach ein Formular zur Verfügung, in das Nachrichten eingetragen werden können. Diese Nachrichten werden nicht etwa wie üblich versendet, sondern einfach lokal auf dem Server unter dem Namen des betreffenden Nutzers gespeichert; damit entfällt die sonst übliche Speicherpflicht. Ein solches System existiert bereits und erlaubt es völlig anonym mit den Mitgliedern der German Privacy Foundation zu kommunizieren.[4] Die Nachrichten werden dabei auch noch automatisch verschlüsselt, so dass sie nur der legitime Empfänger lesen kann. Für die Zukunft ist auch ein öffentliches System geplant. Der Nachteil dabei ist freilich, dass man bei einer Antwort auf eine Nachricht darauf angewiesen ist, dass der Empfänger wiederum eine lokale Mailbox oder eine andere vorratsdatenspeicherungsfreie Kommunikationsmöglichkeit zur Verfügung stellt. Erfolgt die Antwort über Email, schlägt die Vorratsdatenspeicherung wieder gnadenlos zu. Sind sowohl Empfänger als auch Absender jeweils vorsichtig, lässt sich die Vorratsdatenspeicherung aber komplett vermeiden.

andere Kommunikationssysteme

Obwohl im Gesetz festgelegt ist, dass die Anbieter „öffentlich zugänglicher Telekommunikationsdienste für Endnutzer“ zur Speicherung verpflichtet sind, existiert möglicherweise ein weiterer Weg, der Vorratsdatenspeicherung ein Schnippchen zu schlagen. Genaue Speicherungsvorschriften sind nämlich nur für „öffentlich zugängliche Telefondienste“, „elektronische Post“ und „Internetzugangsdienste“ vorhanden. Nicht ausdrücklich erfasst sind Instant Messanging Dienste wie etwa Jabber, ICQ oder AIM. Ob diese nun durch die fehlende

Speichervorschrift von der Vorratsdatenspeicherung befreit sind, werden möglicherweise bald Gerichte zu klären haben - es kann aber erstmal davon ausgegangen werden. Trotzdem sollte man auch hier mit der Auswahl des Anbieters extrem vorsichtig sein. Große Netzwerke wie ICQ oder AIM haben zwar viele Nutzer, sind aber nicht besonders freundlich gegenüber der Privatsphäre ihrer Nutzer. Man sollte deswegen auf eher dezentrale Netzwerke wie Jabber oder völlig serverlose wie etwa Retroshare [5] ausweichen. Im Falle von Jabber [6] kann man sich dann selber einen Server aufsetzen oder sich einen aussuchen, der von einer vertrauenswürdigen Institution betrieben wird. Natürlich sollte man immer auf ordentliche Verschlüsselung achten, sonst besteht auch weiterhin die Möglichkeit, überwacht zu werden.

Fazit

Es gibt viele Möglichkeiten, sich der Vorratsdatenspeicherung bei Emails zu entziehen. Jedoch gibt es keine Patentlösung, die einen völlig davon befreit. Schließlich erfordern einige Maßnahmen doch einiges an Aufwand und technischem Verständnis. Letztendlich muss man sich auch überlegen, inwieweit man die eigenen Kommunikationsmöglichkeiten aufgrund der Vorratsdatenspeicherung einschränken möchte. Es wird immer ein Spagat zwischen persönlicher Sicherheit bzw. Paranoia und Bequemlichkeit bleiben, den nicht alle Menschen zu machen bereit sein werden. Trotzdem sollte man nicht zu leichtfertig mit seiner Kommunikation umgehen und den Überwachern alles bereitwillig präsentieren. Letztendlich ist jeder selber dafür verantwortlich zu entscheiden, wie viel an Aufwand einem unbeobachtete Kommunikation wert ist.

weiterführende Informationen

[1] Ideen des AK-Vorrat, um die Vorratsdatenspeicherung zu umgehen: https://wiki.vorratsdatenspeicherung.de/VDS-umgehen

[2] Anleitung zur Benutzung von Remailern: http://www.anon.gildemax.de

[3] i2p-Maildienst (nur erreichbar über das i2p-Netzwerk): http://mail.i2p

[4] Nachrichtenbox der GPF: https://www.awxcnx.de/gpf/index.htm

[5] Retroshare-Webseite: http://retroshare.sourceforge.net

[6] Webseite von Jabber (Englisch): http://www.jabber.org

Informationen:

Autor: Helmut Pozimski

Umgehung der Vorratsdatenspeicherung durch Anonymisierungsdienste

Grundlage

Im Zuge der Vorratsdatenspeicherung soll unter anderem gespeichert werden, wer sich wann für welchen Zeitraum mit welcher IP-Adresse im Internet einwählt. Diese Daten könnten nun dazu genutzt werden, um die Aktionen eines Nutzers im Internet nachzuvollziehen. Schließlich hinterlassen wir bei der täglichen Internet-Nutzung überall Datenspuren. Immer wenn wir eine Webseite aufrufen oder andere Internet-basierte Dienste nutzen, wird zwangsläufig die IP-Adresse des Anschlusses übertragen. Das ist zwar an sich logisch, da der andere Server wissen muss, an wen er die Antwortpakete schicken muss, lässt aber auch zusammen mit den Daten aus der Vorratsdatenspeicherung eine Identifizierung des Nutzers zu. Gerade für Filesharer ist das ungünstig, da die Musikindustrie nun eine bessere Möglichkeit hat, Nutzer von Tauschbörsen zu identifizieren und zu verklagen, aber es gibt auch viele andere Situationen, in denen man nicht unbedingt identifizierbar sein will, etwa bei der Recherche zu politischen Themen. Um dies zu vermeiden, gibt es verschiedene technische Möglichkeiten, seine IP-Adresse zu verschleiern und so einen Rückschluss auf die eigene Person zu erschweren bis unmöglich zu machen.

Anonymisierungsdienste

Zunächst einmal gibt es die klassischen Anonymisierungsdienste, die meist nicht sehr komfortabel sind, aber eine nach momentanen Erkenntnissen gute Anonymität bieten. Einer der bekanntesten Vertreter dieser Gattung ist TOR. (The Onion Router [1]) Dieses Netzwerk wurde ursprünglich von Matej Pfajfar an der Universität Cambridge entwickelt. Später hat die Electronic Frontier Foundation die Entwicklung unterstützt, mittlerweile wird das Projekt durch Spenden finanziert und bietet es als freie Software allen Interessenten an. Bei TOR kommt das Prinzip des „Onion Routing“ („Zwiebel-Routing“) zum Tragen. Das heißt, der Benutzer nimmt zunächst mittels der TOR-Software Kontakt zu einer zufälligen Kaskade von 3 hintereinander geschalteten Anonymisierungsservern auf. Wenn der Benutzer eine Webseite aufruft, verschlüsselt die Software das Paket in mehreren Stufen. Jeder Server entschlüsselt nun eine Verschlüsselungsschicht und leitet das Paket an seinen Nachfolger weiter. Der dritte Server hat nun das unverschlüsselte Paket und leitet es an den Zielserver weiter. Dieser antwortet und die Kette leitet das Paket in umgekehrter Reihenfolge an den Nutzer zurück. Das hat den Vorteil, dass jeder Server der Kaskade nur seinen Vorgänger und Nachfolger kennt und man so zur Aufdeckung der Identität des Nutzers die Kontrolle über alle drei Server der Kaskade bräuchte.

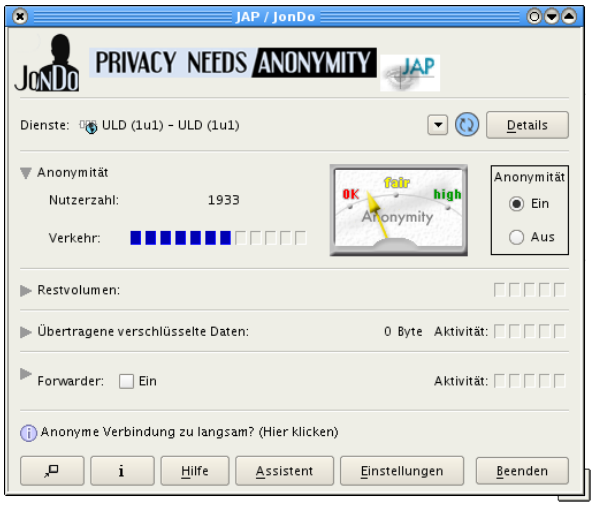
Vidalia-Konfigurationswerkzeug für TOR unter GNU/Linux

Um dies unwahrscheinlich zu machen wird die Kaskade zusätzlich alle 10 Minuten geändert. Die Möglichkeit, dass Geheimdienste eine größere Anzahl TOR-Server betreiben könnten und somit Kontrolle über alle Server der Kaskade erlangen könnten besteht zwar, die Wahrscheinlichkeit eines Erfolgs ist aber gering und sinkt mit der steigenden Zahl der Server. Neben dem reinen Surfen erlaubt TOR auch anonyme Kommunikation über IRC und weitere Protokolle.

TOR bietet in der aktuellen Version schon ein gutes Maß an Anonymität, jedoch wurden in der Vergangenheit mehrere Angriffsmöglichkeiten bekannt, die doch zur Identifizierung des Nutzers führen könnten. Zudem ist bei der Benutzung von TOR äußerste Vorsicht geboten, da die Daten ja beim letzten Server (Exit-Node) unverschlüsselt vorliegen. Man sollte daher tunlichst darauf achten, keine Daten unverschlüsselt über das System zu schicken, die doch eine Identifizierung ermöglichen könnten oder sonstwie vertraulich sind. Besonders Passwörter und andere sensiblen Informationen sollten nur

verschlüsselt übertragen werden.

Dem Problem des Vertrauens zu den Serverbetreibern nimmt sich JonDo (früher JAP [2]) an. Die JAVA-Software ist ebenfalls frei und wird von mehreren Universitäten in Zusammenarbeit mit dem unabhängigen Datenschutzzentrum Schleswig-Holstein entwickelt. Sie funktioniert ähnlich wie TOR, verwendet jedoch feste Kaskaden, deren Betreiber bekannt sind und eine Selbstverpflichtung unterschrieben haben. Das hat den Vorteil, dass die Möglichkeit der Übernahme durch Geheimdienste nicht besteht und die Verbindung tendenziell schneller ist.



Hauptfenster der JAP/JonDo-Software unter GNU/Linux

Dafür kostet die Benutzung von JonDo in der aktuellen Version jedoch eine monatliche Gebühr und anonymisiert nur Webseitenaufrufe. Es gibt zwar auch kostenlose Kaskaden, diese bieten aber nicht die volle Anonymität. Bisherige Betreiber von Servern sind neben den Initiatoren des Projekts auch der bayerische Landesverband der Piratenpartei, der Foebud und der Chaos Computer Club. Damit bietet JonDon theoretisch ein hohes Maß an Anonymität; als Zugeständnis an das deutsche Recht musste jedoch eine Abhörschnittstelle eingebaut werden, die im Fall schwerer Straftaten die Identität von Nutzern aufdecken kann. Davon musste bis jetzt jedoch erst einmal Gebrauch gemacht werden.

Ein weiterer Ansatz zur Anonymisierung ist i2p [3]. Es ist ebenfalls freie Software und in JAVA geschrieben. Im Gegensatz zu JonDon und TOR anonymisiert es nicht einfach den Webtraffic, sondern stellt ein eigenes anonymes Netzwerk im Internet dar. Deswegen ist es auch nicht an Server gebunden, sondern jeder Nutzer leitet Pakete für andere Nutzer weiter. Das Grundprinzip ist ähnlich dem „Onion-Routing“ von TOR, jedoch fasst i2p zusätzlich Pakete von verschiedenen Leuten zusammen, verschlüsselt diese zusätzlich und schickt sie erst dann als größeres Paket weiter. Dieses auch als „Garlic-Routing“ bekannte Prinzip stellt sicher, dass nicht aufgrund der Verbindungen Rückschlüsse auf einzelne Nutzer möglich werden. Durch das geschlossene System kann man mit i2p aber auch nur speziell dafür geschriebene Anwendungen benutzen. Davon gibt es einige, unter anderem ist es möglich sich eine anonyme Emailadresse einzurichten, (die allerdings beim Senden auf 20 Mails pro Tag beschränkt ist, um Spam zu vermeiden) Dateien über eMule, Bittorent und Gnutella zu tauschen, sich anonym an Usenet-Diskussionen zu beteiligen und ein anonymes Blog zu führen. Die Anonymität mit i2p gilt als gut, jedoch besteht auch hier äußerste Vorsicht bei der Preisgabe persönlicher Informationen, sonst können am Ende doch noch Rückschlüsse auf die eigene Person möglich sein.

VPNs

Während die schon genannten Anonymisierungsdienste alle gemeinsam haben, dass sie ziemlich langsam sind und damit kaum für Filesharing oder ähnliches taugen, bieten anonymisierende Proxys bzw. VPNs teilweise schnellere Verbindungen, die sich auch schon mal zum Download von größeren Dateien wie Filmen eignen. Ein bekanntes Beispiel für einen solchen Proxy ist der Dienst Relakks [4], der von der schwedischen Piratenpartei betrieben wird. Dabei wird grundsätzlich erst mal eine VPN-Verbindung (Virtual Private Network) zu einem Server des Dienstleisters aufgebaut. Über diesen Server werden nun sämtliche Verbindungen geleitet. Aufgerufenen Webseiten gegenüber erscheint also nur die Adresse des Servers. Der zu betreibende Aufwand ist abgesehen von den monatlichen Kosten relativ gering, die Anonymität leider auch. Dieses steht und fällt mit der Integrität des Betreibers, der bei solchen Diensten den einzigen Mittelsmann darstellt und damit jederzeit die Anonymität aufheben kann. Für Filesharer könnte sich dieses Modell dennoch als praktikable Lösung herausstellen.

Fazit

Mit der perfekten Anonymität ist es wie mit der absoluten Sicherheit, es gibt sie einfach nicht. Dennoch gibt es einige Methoden, die einem relativ guten Schutz gewähren. Jeder sollte sich zumindest mit den entsprechenden Technologien vertraut machen, um in der Lage zu sein, seine Privatsphäre vor dem nicht zu stillenden Datenhunger des Staates zu schützen. In Zukunft wird man wohl zunehmend auf Server im Ausland ausweichen müssen, weil das Gesetz zur Vorratsdatenspeicherung auch Anonymisierungsdienste zur Speicherung von Verbindungsdaten verpflichtet.

weiterführende Informationen

[1] deutschsprachige TOR-Webseite: https://www.torproject.org/index.html.de

[2] JAP-Webseite: https://anon.inf.tu-dresden.de/index.html

[3] I2P-Webseite: https://www.i2p2.de

[4] Relakks-Webseite (Englisch): https://www.relakks.com/?lang=eng&cid=gb

Informationen:

Autor: Helmut Pozimski

Impressum

Das Piratenmagazin ist eine regelmäßig erscheinende Zeitschrift

Herausgeber (nach §8 (1) des baden-würtenbergischen Landespressegesetzes):

Piratenpartei Deutschland
Postfach 1223
70773 Filderstadt

verantwortlicher Redakteur (nach §8 (2) des baden-würtenbergischen Landespressegesetzes):

c/o Kim-Sun Mo
Postfach 1223
70773 Filderstadt

Emailadresse für Feedback:
feedback@piraten-magazin.de
vorratsdatenspeicherungsfreie Mailbox

Urheberrechte

Bildnachweis

Titelseite:
Zusammenstellung: Kim-Sun Mo
Grablichter und Todesanzeige: Sandra Hepp
restliche Bilder: Arbeitskreis Vorratsdatenspeicherung

Mitarbeiter

Redaktion: Kim-Sun Mo, Helmut Pozimski
Layout: Rebecca Breu, Helmut Pozimski

Danke auch an die Nichtgenannten Helfer, die uns im Vorfeld bei der inhaltlichen und äußerlichen Gestaltung im Wiki unterstützt haben.