

Internet-Anonymisierungsdienste im Test

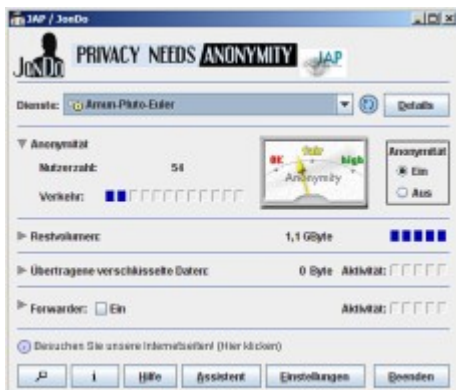
Nachdem ab 2009 auch Internetprovider zur 6-monatigen [Vorratsspeicherung](#) von [IP-Adressen](#) verpflichtet sind, ist es technisch möglich, das Surfverhalten jeden Nutzers 6 Monate lang und ohne Gerichtsbeschluss zu einem bestimmten Anschluss zurückverfolgen. IP-Adressen spielen für die Anonymität im Internet eine große Rolle, da es zu einem bestimmten Zeitpunkt internetweit eindeutige Anschlusskennungen sind, die zur Kommunikation erforderlich sind. Eine Maßnahme gegen die Aufzeichnung von IP-Adressen können kostenpflichtige Anonymisierungsdienste darstellen, die nicht nur die Kommunikation zwischen Rechner und Anonymisierungsdienst verschlüsseln, sondern den Nutzer nach außen hin unter veränderter IP-Adresse auftreten lassen. In diesem Fall hinterlassen Sie beim Surfen nur die IP-Adresse des Anonymisierungsdiensts, während Ihr Internetanbieter aber nur Ihre originäre IP-Adresse sehen und speichern kann, so dass eine Zuordnung von Surfspuren zu einem bestimmten Anschluss zumindest erheblich erschwert wird. Zwar gibt es auch zahlreiche kostenlose und anmeldefreie [Proxyserver](#), die quasi als Mittler zwischen Quell- und Zielrechner fungieren. Diese sind aber oft unzuverlässig und die Daten werden unverschlüsselt übertragen, so dass Ihre Daten einschließlich etwaiger Passwörter auf dem Weg dorthin und vom Proxyserver selbst beobachtet werden können. Bei vielen solcher Proxys handelt es sich außerdem um [von Kriminellen gekaperte](#) Rechner, denen Ihre Daten anzuvertrauen nicht ungefährlich ist. Ich habe deshalb im Januar 2009 17 internationale Anonymisierungsdienste insbesondere unter dem Aspekt der Anonymisierungsqualität und des Datenschutzes unter die Lupe genommen. Die Reihenfolge der getesteten Services beinhaltet keine Wertung.

Kurzübersicht

	Sitzland	Kein Logging irgendwelcher Verbindungsdaten, auch nicht teil-, orts- oder zeitweise	Keinerlei E-Mail-Sperren	Preis
1. Jondonym	International	✘	✓	ab 6,15 €/GB
2. Tor	International	✘	✓	0
3. Cyberghost	Deutschland	✘	✘	ab 0 €
4. Perfect Privacy	International	✓	✓	ab 10 €/Monat
5. Relakks	Schweden	✘	✘	ab 5 €/Monat
6. Internet Anonym VPN	Deutschland	✘	✘	ab 12 €/Monat u. 25 GB
7. Ivacy	Schweiz	✓	✓	ab 8,33 €/Monat od. 0,50 €/GB
8. Linkideo	Jersey	✓	✓	ab 2 €/Monat
9. Xerobank/ShadowVPN	Panama	✘	✓	ab 10 US\$/Monat u. 10 GB

10. SwissVPN	Schweiz	✘	✓	5 US\$/Monat
11. Safersurf	Deutschland	✘	✓	5,90 €/Monat
12. Witopia	USA	✘	✓	40 US\$/Monat
13. Trackbuster	Deutschland	✘	✓	5 €/Monat
14. Your Freedom	Deutschland	✘	✓	ab 0 €
15. Surfonym	Österreich	✓	✓	ab 4,90 €/Monat
16. BananaVPN	Zypern	✘	✓	ab 15 US\$/Monat
17. VPN Out	USA	✘	✘	ab 8,33 US\$/Monat u. 83 GB

1. Jondonym



Eine der besten Anonymisierungsqualitäten in diesem Test dürfte Jondos mit [Jondonym](#) bieten. In einem quelloffenen Java-Client kann der Nutzer die Route seiner Daten selbst bestimmen. Zur Verfügung stehen dazu sogenannte Mixkaskaden, also Ketten von bis zu 3 Servern weltweit verteilter Betreiber. Wer davon vorratsspeichert, soll in Kürze im Client angezeigt werden; derzeit findet noch keine Vorratsdatenspeicherung statt. Selbst mit Vorratsdatenspeicherung ist eine Aufdeckung, so Geschäftsführer und Diplom-Wirtschaftsinformatiker Rolf Wendolsky, nur dann möglich, wenn alle [Mixe](#) einer

Kaskade vorratsspeichern und der Zielsever, also etwa eine angesurft Webseite, die IP-Adresse des letzten Mixes und den Quellport der jeweiligen Serververbindung speichert. Auf den speichernden Mixes will Jondonym die Vorratsdaten derart verschlüsselt speichern, dass eine Entschlüsselung beim Mix nicht möglich ist. Diebstahl und [Beschlagnahme](#) blieben somit ergebnislos. Die Übertragung zu und zwischen den Mixen erfolgt mehrfach verschlüsselt. Auch kennt kein Mix sowohl den absendenden als auch den empfangenden Rechner. Daraus ergibt sich der Vorteil, dass eine - möglicherweise erzwungene - Überwachung ins Leere läuft, solange nicht die gesamte Mixkaskade betroffen ist. Hinsichtlich rechtlicher und technischer Aspekte der Vorratspeicherung befinden sich das Unternehmen sowie einzelne Betreiber noch in Diskussion mit den zuständigen Behörden. Bei Jondonym wurden akzeptable Geschwindigkeiten um 1.000-2.000 [KBit/s](#) regelmäßig nur mit den kostenpflichtigen Premiumservern und mit gemessener [Pingzeit](#) von über 300 ms erreicht. Selbst hier schwankt die Geschwindigkeit auf Grund der Serverkaskadierung relativ stark, was ebenfalls viele Anwendungen ausschließen wird. Die Premium-Anonymisierungsleistung bezahlt der Jondonym-Kunde jedoch auch mit einem Premiumpreis von über 6 € pro Gigabyte. Kundenanfragen wurden schnell, freundlich und kompetent beantwortet. Als Bezahlarten für Jondonym werden Bargeldversand, [Paysafecard](#), Überweisung und Paypal angeboten.

Technik-Exkurs: Jondonym vs. 1-Mix-Lösungen - Anonymität oder Geschwindigkeit?

Störend wirkt die Schwerfälligkeit des Java-Clients in Jondonym, der außerdem nur die Verbindungen solcher Programme erfasst, in denen Jondonym als HTTP- oder [SOCKS](#)-Proxyserver eingetragen wird, was nicht bei allen Programmen möglich ist. Auch halten sich Flash- oder andere Plugins nicht immer an die Proxy-Einstellungen des Browsers, so dass sie am Anonymisierer "vorbeilaufen". Zur Linderung bietet das Unternehmen zwar den kostenlosen [Jondofox](#) an, einen speziell vorkonfigurierten Firefox, der aber externe Programme noch immer nicht erfasst. Anders als bei Diensten, die nur 1 Anonymisierungsserver zwischenschalten, ist es auf Grund der hohen Anonymität, aber niedrigen Geschwindigkeit auf Grund der Client-Software und nicht zuletzt wegen der hohen Preise nicht denkbar etwa VoIP-Telefonie mit Jondonym zu kombinieren. Auf der anderen Seite bergen 1-Mix-Lösungen ohne Serverkaskadierung, die dank verbreiteter [VPN](#)-Standards meist alle Verbindungen erfassen, das [Risiko](#), dass ein lokaler Beobachter im Netz des Nutzers (ISP, WLAN) durch Größen- und Zeitanalysen des verschlüsselten Datenstroms mit bis zu 90-prozentiger Trefferquote auf abgerufene Webseiten schließen kann. Gegen diese Angriffe hilft keine Verschleierung der IP-Adresse, von Identifizierungsgefahren durch Plugins, ActiveX, Webbugs, Cookies, Flash-Cookies und Browser-Header einschließlich Sprache, Browser und Betriebssystem abgesehen. Ferner erkaufte man sich die höhere Geschwindigkeit schnellerer 1-Mix-Lösungen ohne verschachtelte Verschlüsselung und -anonymisierung mit dem Nachteil, dass der Anonymisierungsanbieter den Nutzer einschließlich seiner Inhaltsdaten, womöglich unter behördlichem Druck, mit Leichtigkeit im Alleingang überwachen kann, was selbst bei Tor [möglich](#) ist. Das kann bei dubiosen Offshore-Anonymisierern eher der Fall sein als bei einem geregelten, vorratsdatenspeichernden Internetprovider. Problematisch an VPN-Lösungen gegenüber dem aktiv einzubindenden Jondonym-Client ist ferner, dass im Fall von VPN-Verbindungsabbrüchen Verbindungen unbemerkt am VPN-Tunnel "vorbeilaufen" können, wenn die Firewall dies nicht blockiert. Allein der Client des Anonymisierers [Ivacy](#) stoppt dieses Vorbeilaufen auf Wunsch.

2. Tor



[Tor](#) ist ein kostenloser, aber nicht zu verachtender Anonymisierungsdienst. Er wird mit den Programmen Privoxy, einer bedienungsfreundlichen Erweiterung für den Browser Firefox und der Tor-Benutzeroberfläche Vidalia ausgeliefert. Ähnlich wie bei Jondonym werden Verbindungen durch eine zufällig ausgewählte Kette von Rechnern geleitet und so anonymisiert. Diese Kette ist nicht statisch, sondern wechselt alle paar Minuten. Die Kommunikation zwischen den Serverknoten ist verschlüsselt und kein Server kennt sowohl Ausgangs- als auch Endserver. Tor hat keinen bestimmten Betreiber, sondern jedermann kann teilnehmen und Teil des Tor-Netzwerks werden. Auf Grund des sogenannten Onion-Routing-Prinzips der verschachtelten Mehrfachverschlüsselung (daher auch die Zwiebel im Tor-Logo) würde selbst ein Abhören mehrerer Knotenpunkte nicht ohne Weiteres den Nutzer offenbaren. Das dezentrale Konzept hat, ähnlich wie bei Peer-to-peer-Netzwerken, den Vorteil, dass es keine zentrale Stelle gibt, an der Sperr- oder Abhörmaßnahmen installiert werden könnten, die alle Nutzer betreffen würden. Auch führt ein Nichtfunktionieren einzelner Knoten nicht zur Unbenutzbarkeit des kompletten Diensts. Kritikpunkt von Tor ist die niedrige Geschwindigkeit. Nachteil des offenen Konzepts ist, dass man sich auf unbekannte Betreiber unter anderem des Endservers verlassen muss, der die übertragenen Dateninhalte wie etwa E-Mail-Passwörter zwangsläufig unverschlüsselt zu Gesicht bekommt, um sie ins Internet verschicken zu können. Das gilt jedenfalls dann, wenn der Nutzer keine Ende-zu-Ende-Verschlüsselung zum Zielsystem ähnlich SSL beim Onlinebanking einsetzt. Der schwedische Hacker Dan Egerstad wies nach, kann jedermann manipulierte Endserver aufsetzen und damit sensible Daten abfischen kann; so soll es ihm [gelingen](#) sein, zahlreiche Zugangsdaten von den Dienst nutzenden Diplomaten auszuspähen. Auch will Egerstad durch Geoanalysen [herausgefunden](#) haben, dass inzwischen ein beträchtlicher Teil solcher Server mutmaßlich von US-amerikanischen und chinesischen Nachrichtendiensten betrieben wird. 2006 wies der britische Forscher Steven Murdoch [nach](#), dass durch Zeitanalysen Tor-Knoten trotz Verschlüsselung wiedererkannt und der Weg der

Daten so nachvollzogen werden könne. Der Angriff soll allerdings nur funktionieren, wenn die sogenannten [hidden services](#) in Tor vom Nutzer aktiviert sind, über die der Angreifer künstliche Last erzeugt, um hieraus zeitliche Schlüsse zu ziehen.

3. Cyberghost



[Cyberghost](#) ist ein Angebot des Ulmer Softwarehauses S.A.D. Der Kunde ist dabei auf einen proprietären, etwas trägen und derzeit nur für Windows angebotenen VPN-Client angewiesen, der im Test auch in der kostenlosen Version (dafür mit werbeträchtiger Warteschlange beim Verbindungsaufbau) gute und konstante Geschwindigkeit um 2.000 KBit/s herum lieferte. Zahlenden Nutzern garantiert der Dienst diese Geschwindigkeit sogar. Die Installation des Windows-Clients, der eine virtuelle Netzwerkkarte installiert, erfordert [Microsoft .NET 3.0](#). Durch die VPN-Software werden alle Verbindungen erfasst und

verschlüsselt. Allerdings hat der Anbieter die gängigen E-Mail-Ports für Thunderbird, Outlook etc. gesperrt. Hier wird der Anbieter seinem Konzept untreu. Nicht beantwortet wurde die Frage, was die Sperrung eingehender Mails zur angeblichen Spam-Vermeidung beiträgt. Negativ fällt ferner auf, dass der Anbieter bei der Registrierung ohne Not eine zu verifizierende E-Mail-Adresse verlangt. Diese darf auch keine Wegwerfadresse sein; wer etwas Geduld mitbringt, wird allerdings fündig. E-Mail-Adressen zu speichern verpflichtet zu sein behauptet indes nicht einmal Cyberghost. Wie weit vom Anbieter geäußerte Pläne zur Errichtung einer Infrastruktur im Ausland gediehen sind, wurde gleichfalls nicht beantwortet. Als Zahlungsmöglichkeit bietet der Dienst Click&Buy und Paypal an, daneben lediglich den anonymen Kauf von Paketen in Geschäften wie Mediamarkt. Bei kostenpflichtiger Nutzung zahlt der Kunde 10 € für 40 GB, zahlungsunwillige Nutzer müssen sich mit 10 GB pro Monat und Account begnügen.

Entgeistert: Wie anonym ist Cyberghost?

Der seit 2009 vorrattsspeichernde Anbieter von Cyberghost, S.A.D., will die Anonymität seiner Nutzer dadurch wahren, dass sich mehrere Nutzer eine externe IP-Adresse teilen. "Das ist wie in der Weihnachtszeit: Wenn viele das selbe Nikolauskostüm anhaben, kann hinterher keiner sagen, wer hinter dem einzelnen Kostüm steckt. Auch, wenn der Kostümverleih aufschreibt, wer sich ein Kostüm ausgeliehen hat", erklärte S.A.D. auf Anfrage. So einfach ist es allerdings nicht: Mag eine behördliche Anfrage mit nur einem Nutzungsdatum als Anhaltspunkt (etwa einer aufgezeichneten IP-Adresse mit Zeit) noch zu Tausenden Verdächtigenführen, sieht dies bei Kombinationen mehrerer Nutzungsvorgänge anders aus. So [speichern](#) Ebay oder Amazon jeden Klick selbst unangemeldeter Besucher und können Surfer oftmals per Cookie unterscheiden; auch das Tauschprogramm Emule sendet jedes Mal einen gleichbleibenden Client-Hash, also eine eindeutige Prüfsumme. Doch nun vergab Cyberagent im Test 3 verschiedene IP-Adressen, so dass mit jedem neuen Nutzungsvorgang der Kreis der Verdächtigen etwa gedrittelt wird, geht man davon aus, dass der Gesuchte unter gleichbleibender Cyberghost-Benutzerkennung arbeitet. Da eine DSL-Verbindung regelmäßig alle 24 Stunden zwangsgetrennt wird, dauert ein Nutzungsvorgang maximal 1 Tag. Bei angenommenen 100.000 Cyberghost-Nutzern ist ein gesuchter Nutzer damit auch ohne Inhaltsspeicherung seitens CyberGhost nach 11 Nutzungsvorgängen, bei täglicher Nutzung mithin nach 11 Tagen eingekreist und kann dann über die seitens Cyberghost vorratsgespeicherte und herauszugebende Original-IP-Adresse endgültig identifiziert werden. Dabei müsste die Anonymisierung trotz Vorratsdatenspeicherung bei Weitem nicht so schlecht sein, würde Cyberghost die Benutzerkennungen zumindest nicht in

Verbindung mit den Vorratsdaten speichern, denn erst sie ermöglicht eine "Bündelung" der vorratgespeicherten IP-Adressen zu einem Benutzer, der schließlich anhand seiner Original-IP-Adresse ermittelt werden kann.

Einen nachhaltigen Schutz gewährleistet Cyberghost selbst dann nicht, wenn man Anonymität im Sinne einer nur subjektiven Anonymität gegenüber angesurften Webseiten verstehen will. Etwa kann der Seitenbetreiber die Nutzeridentität im Wege der Akteneinsicht (§ 406e StPO) in Erfahrung bringen, wie es auch Rechteinhaber bei Tauschbörsennutzern seit jeher tun - mal mit mehr, mal mit weniger Erfolg. Um in den Genuss eines Ermittlungsverfahrens zu kommen, muss der Nutzer auch keine schwere Straftat begangen haben. Auf diese Mängel angesprochen, entgegnete S.A.D. zunächst, man könne sich keine Internetstraftat vorstellen, auf Grund derer selbst nach der einstweiligen Anordnung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung auch Original-IP-Adressen vom Anschluss des Nutzers herauszugeben seien. Als dies mit dem Beispiel der Verbreitung kinderpornografischer Schriften widerlegt wurde, verlagerte S.A.D. sich darauf, man sei gesetzlich nun mal zur Speicherung von Benutzerkennungen verpflichtet, was für nichtphysische Anschlusskennungen aber nicht zutrifft (BT-Drs. 16/6979 S. 46 zu § 111). Im Gegenteil könnte die Vorgehensweise sogar gegen § 113b TKG verstoßen, weil Vorrats- von Abrechnungsdaten, hier also den Benutzerkennungen, abzugrenzen sind (Frage 1). Hierauf äußerte S.A.D. nur noch, Straftäter wolle man ja nicht schützen. Dabei verkennt S.A.D., dass bis zur rechtskräftigen Verurteilung zu Recht das Menschenrecht der Unschuldsvermutung gilt; beispielsweise könnte im genannten Fall schlicht das ungeschützte WLAN des beschuldigten Anschlussinhabers missbraucht worden sein. Folglich schützt S.A.D. weder Schuldige noch Unschuldige konsequent. Das Unternehmen konnte im Anschluss auch nicht mehr schlüssig erläutern, welchen Anonymitätsvorteil Cyberghost vor diesem Hintergrund gegenüber beliebigen Internet Providern haben sollte, die ihre Kundendaten schließlich auch nicht wie sauer Bier feilbieten. Im Gegenteil kann man dort vermuten, dass sie sich über ihre datenschutzrechtlichen Pflichten qualifiziert haben beraten lassen, und dass juristische Beurteilungen nicht von Produktentwicklern getroffen werden, die zudem etwas versprechen, was es genauso wenig wie 100-prozentige Sicherheit geben kann: 100-prozentige Anonymität. Der Kundenservice des Unternehmens zeigte sich freundlich und kooperativ, solange keine kritischeren Fragen gestellt wurden.

4. Perfect Privacy

Perfect Privacy *solutions for independent people* Perfect Privacy hat kein Sitzland, sondern ist ein loser, internationaler Zusammenschluss von Privatpersonen. Angeblich arbeitet der Anbieter nichtkommerziell, und Einnahmen fließen fast ausschließlich in Infrastruktur und Rechtsverteidigung. Der Anbieter betreibt aktuell 20 voneinander unabhängig nutz- und verkettbare Server in 17 Ländern, viele davon außerhalb der EU, bei denen jeweils alle Nutzer unter derselben IP-Adresse surfen. Auf die Problematik angesprochen, dass auch der Berliner Server unabhängig vom Wohnsitz der Betreiberpersonen vorratsdatenspeicherpflichtig sein könnte (§ 3 Nr. 6 b TKG), äußerte Perfect Privacy, man sei auf den Berliner Server nicht angewiesen und werde ihn gegebenenfalls abziehen.

Nach ausdrücklicher Bestätigung speichert Perfect Privacy nach Verbindungsende weder IP-Adressen noch sonstige Logdaten. Allerdings soll Perfect Privacy dies schon einmal ernsthaft erwogen haben, nachdem mehrere Serververträge wegen Spam-Versands gekündigt worden waren. Auch behält sich der Anbieter ähnlich wie Jondonym vor, nach eigenem Ermessen im Verdachtsfall bei laufender Verbindung zurückzuverfolgen, wer sich mit bestimmten Servern verbindet. Der Kunde kann bei jeder Einwahl entscheiden, welchen Server er nutzen möchte, wobei wegen der stark variierenden Geschwindigkeiten für den Alltagsgebrauch regelmäßig nur ein kleiner Kreis in Frage kommen wird. So wurden in Hongkong oder Panama nur etwa 300 Kbit/s im Downstream erreicht, in Moskau oder Luxemburg dagegen bis zu 9.000 KBits/s bei einem Upstream von jeweils etwa 10% und einer Pingzeit zwischen 60 und 900 ms. Der Server in Roubaix, Frankreich war im Test ausgefallen und Teheran

steht nur Jahresabonnenten zur Verfügung. Im Schnitt erzielten alle Server gemeinsam ordentliche 2.800 KBit/s. Portsperrern, insbesondere im Mailbereich, bestanden nicht. Angeboten wird neben [PPTP](#) auch ein [SSH](#)-Zugang mit vorkonfiguriertem, auch auf Dauerverbindung einstellbarem Client. PPTP-Verbindungen werden von Windows von Haus aus unterstützt; man braucht lediglich in den Netzwerkverbindungen eine VPN-Verbindung einrichten. PPTP ist schnell, jedoch ist die dort eingesetzte Verschlüsselung [MPPE](#) schwach, weswegen empfohlen wird, ein mindestens 12-stelliges Passwort zu wählen. Einmal kam es beim Berliner Server zu einem Verbindungsabbruch, im Übrigen zeigten sich Geschwindigkeit und Verbindung über mehrere Server auch im mehrwöchigen Test als recht stabil. Ein optionaler [OpenVPN](#)-Client mit passenden Konfigurationsdateien für Windows und Mac steht Kunden zur Verfügung, ferner Zugangsmöglichkeiten über [Squid](#) und Socks 5.

Im Mitgliederbereich stellt Perfect Privacy zahlreiche nützliche Tipps zur Geschwindigkeitsoptimierung bereit. Auch Port-Forwarding wird auf Anfrage angeboten. Die Server scheinen nur teilweise verschlüsselt zu sein, so dass bei Beschlagnahmen oder Diebstahl eine Liste der Pseudonyme und verschlüsselten Passwörter [auslesbar](#) ist. Für eine Monatsflatrate zahlt der Nutzer je nach Laufzeit 10 bis 25 Euro für unbegrenzte Nutzung, wobei Perfect Privacy an seine Nutzer appelliert, im Schnitt nicht viel mehr als 100 GB monatlich zu verbrauchen. Dies wird allerdings (auch mangels Logdaten) nicht überprüft. Bei einzelnen, schwach angebundenen Servern wird besonders um maßvolle Nutzung gebeten. Als Zahlungsmöglichkeiten stellt Perfect Privacy Bargeldversand nach Neuseeland, Paysafecard, Paypal, Kreditkarte, [Liberty Reserve](#) und [Webmoney](#) zur Verfügung. Dabei gestaltete sich die Paysafecard-Zahlung abenteuerlich: Nach der Anmeldung, die immehrin über Wegwerfadressen erfolgen kann, musste man auf eine manuelle Bestätigungsmail warten. Als diese nach einigen Stunden kam, sollte der Paysafecode gemailt werden, der dann offenbar wiederum von einem Mitarbeiter nach einem weiteren Tag manuell eingelöst wurde und zur Übersendung der Zugangsdaten führte. Eine kostenlose Testnutzung bietet Perfect Privacy nicht an. Auf E-Mails wurde teils schleppend, aber freundlich und kompetent geantwortet. Es existiert auch ein deutscher Ansprechpartner. Perfect Privacys E-Mail schloss mit der schönen Losung: "If privacy is outlawed, only outlaws will have privacy."

5. Relakks



[Relakks](#) soll ein seit 2006 bestehendes Unternehmen der schwedischen [Piratenpartei](#) sein und sie [mitfinanzieren](#). 50.000 Nutzer will der Dienst bereits haben. Gesurft wurde im Test unter einer schwedischen IP-Adresse des Netzbetreibers Labs2.

Hinsichtlich des E-Mail-Verkehrs wurde eine Sperre auf [Port 25](#), nicht aber [465](#) festgestellt. Bei der Anmeldung forderte Relakks eine E-Mail-Adresse, für die auch eine Wegwerfadressen genutzt werden konnte. Im Übrigen war nicht zu ermitteln, welche Daten Relakks wie lange vorrattsspeichert. Anfragen an Relakks, an die schwedische Piratpartei sowie an den Netzbetreiber Labs2 blieben unbeantwortet. Die Angaben auf der Internetseite, wonach Verkehrsdaten an die Behörden herausgegeben würden, sobald ein Nutzer einer nach schwedischem Recht mit mindestens 2 Jahren Freiheitsstrafe bewehrten Straftat verdächtig ist, deutet auf eine Vorratsdatenspeicherung hin. Auch gegenüber anderen Kunden soll der Anbieter eine Vorratsdatenspeicherung [ingeräumt](#) haben; die Speicherfrist variiert zwischen 1 und 6 Monaten. Vor dem Hintergrund der umstrittenen [Beschlagnahme der Stockholmer Piratebay-Server 2006](#) scheint dies nicht ohne Risiko für Kunden. Im Geschwindigkeitstest wurden gute 4.000 KBit/s im Downstream und 600 KBit/s im Upstream bei einer Pingzeit von etwa 115 ms erreicht. Um zu bezahlen, musste man sich jedoch erst durch einen schwedischen Bezahl-dialog des Dienstleisters Paynova quälen. Bezahlt werden kann mit schwedischen Konten oder per Kreditkarte. Es liegen keine Informationen über Vorkehrungen vor, wonach Vorratsdaten nicht mit Bezahl-daten zusammengeführt werden könnten. Relakks kostet 5 € pro Monat oder 50 € für 1 Jahr. Der Service bewegte sich leider auf der Nulllinie.

6. Steganos



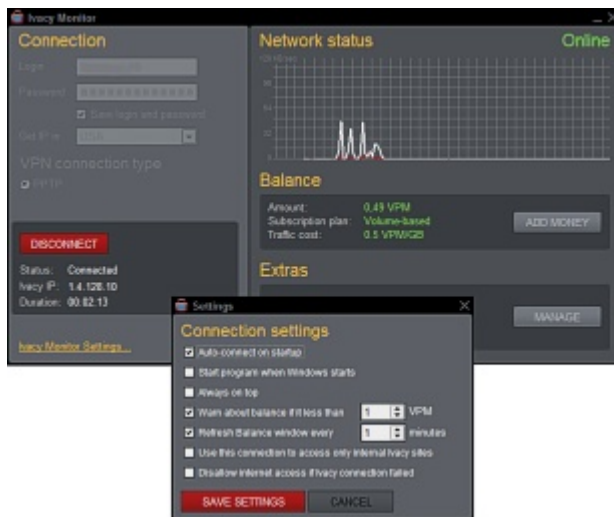
[Internet Anonym VPN](#) ist die Anonymisierungssoftware des Frankfurter Anbieters Steganos. Sie ist zu unterscheiden vom eingestellten Vorgängerprodukt Internet Anonym und wird im Gegensatz zu [Cyberghost](#) nicht über Ladengeschäfte vertrieben, wohl aber im Onlinehandel. Ohne die für Windows und Mac verfügbare Software, die weniger träge als jene von S.A.D. ist, ist das Produkt nicht nutzbar. Wie Cyberghost installiert die Software eine virtuelle

Netzwerkkarte. Im Test musste nicht nur die Seriennummer in die Software eingegeben und online abgeglichen werden, sondern vorher auch noch auf der Steganos-Website unter zwingender Eingabe einer gültigen E-Mail-Adresse aktiviert werden. Wegwerfadressen sind gesperrt; wie bei Cyberghost ist aber auch hier das Glück mit dem Tüchtigen.

Nach Aktivierung betrug die Datenrate im Test ca. 800 KBit/s im Down- (nachts mehr) und Upstream bei einer Pingzeit von ca. 90 ms. Während der Mail-Empfang uneingeschränkt funktionierte, war der Mailversand auf Port 25 (nicht aber 465) gesperrt, nachdem Steganos [angeblich](#) wegen Spamversands auf eine Blacklist gesetzt worden war. Die im Test zugewiesenen IP-Adressen, die sich alle Nutzer eines Servers teilten, stammten von 1&1. Steganos' Client zeigt in einer Hinweisbox ehrlicherweise an, dass Vorrats gespeichert wird und eine objektive Anonymität nicht erreicht wird. Die Verbindung zu Steganos' Servern ist 128-Bit-SSL-verschlüsselt. Gespeichert werden auf Grund der Vorratsdatenspeicherung Quell- und Ziel-IP-Adressen und Zeiten. Benutzernamen wie bei Cyberghost werden nicht mitgeloggt. Zwar werde die Summe des Datenvolumens gemeinsam mit der Seriennummer gespeichert, spätestens 45 Minuten nach Verbindungsende werde der Zusammenhang zwischen den Verbindungsdaten und der Seriennummer gelöscht, so dass danach nicht von einer IP-Adresse auf Benutzer oder Seriennummern geschlossen werden könne. Auch ein ["Einkreisen"](#) gesuchter Nutzer ist trotz Vorratsdatenspeicherung allenfalls anhand der Onlinezeiten möglich, weil ohne an die Verbindungsdaten gekoppelte Benutzernamen oder Seriennummern das Suchkriterium von verbindungsübergreifend gleichbleibenden Benutzernamen oder Seriennummern entfällt. Einem gleichbleibenden Benutzernamen steht es natürlich gleich, wenn der Kunde einen Internetzugang mit statischer Original-IP-Adresse verwendete, wie es bei manchen Kabel-, aber auch [DSL-Internetanbietern](#) der Fall ist, und dies bekannt ist oder geraten wird. Eine statische IP-Adresse bedeutet, dass die vom Internetanbieter dem Rechner zugewiesene, für die Zeit der Verbindung internetweit eindeutige Kennung in Form der IP-Adresse auch bei der nächsten Verbindung die gleiche ist, was auch unabhängig von der Anonymität Hackerattacken und gezielte Sperrungen durch Seitenbetreiber begünstigt. Benutzer statischer IP-Adressen sollten daher zur Sicherheit generell auf Anonymisierungsanbieter mit Vorratsdatenspeicherung verzichten. Was den Preis betrifft, bietet Steganos für Internet Anonym VPN 5 verschiedene Modelle an, die zwischen 1 Monat mit 25 GB für 12 € und 12 Monaten ohne Trafficlimit für 300 € rangieren.

7. Ivacy

Im Alpenland Schweiz hat die Potesta Steuerberatung AG ihren Sitz und betreibt über eine Tochtergesellschaft den Anonymisierungsdienst [Ivacy](#). Ivacy ermöglicht die VPN-Einwahl bei drei Servern in Großbritannien, USA und Russland. Zu allen Servern kann man sich per PPTP einwählen, zum russischen auch per OpenVPN und IPSec, wobei Letzteres im Test meist nicht funktionierte. Der russische Server kann auch mit IPSec genutzt werden, war im Test aber meist ausgefallen. Für PPTP und [IPSec](#)-Verbindungen kann optional der für Windows, Mac und Linux verfügbare Client verwendet werden, der auch so eingestellt werden kann, dass im Fall eines Verbindungsabbruchs keine Verbindungen am VPN-Tunnel vorbeilaufen. Port 25 ist gesperrt, 465 (SMTP über SSL) jedoch nicht;



für zahlende Nutzer fällt die Sperre weg. An Daten speichert Ivacy nach eigenen Angaben nur Benutzerkennung und nur im Fall eines Volumentarifs die Gesamtsumme des im Abrechnungszeitraum vom Nutzer verbrauchten Datenvolumens; Verbindungsdaten wie insbesondere IP-Adressen werden laut Ivacy nicht gespeichert. Auf eine Schweizer Verpflichtung zur Vorratsdatenspeicherung angesprochen, hieß es, sobald eine Behörde Ivacy zur Vorratsdatenspeicherung verpflichten wolle, werde die Betreibergesellschaft das Sitzland wechseln; an genehmen Ländern habe die Steuerberatung eine ganze Reihe zur Auswahl. Alle Nutzer eines Servers surfen unter derselben

externen IP-Adresse.

Im Geschwindigkeitstest über PPTP schnitten die Server unterschiedlich ab: am besten der britische Server mit 2.000-4.000 KBit/s im Down- und 600 KBit/s im Upstream bei einer Pingzeit von etwa 110 ms, am schlechtesten mit nur etwa halb so guten Werten der amerikanische. Ein Radiostream mit 256 KBit/s lief aber stets flüssig. Neben [Port-Forwarding](#), was für File-Sharer interessant sein kann, bietet Ivacy auch kostenlosen Usenet-Zugang. Seinen Nutzern bietet Ivacy außerdem ein Firefox-Plugin an, mit dem auch auf solchen Rechnern über Ivacy gesurft werden kann, auf denen kein Client installiert werden kann oder die Firewall VPN-Verbindungen verhindert; leider kam im Test keine Verbindung zustande. Zum Schnuppern bietet Ivacy kostenlose Testaccounts mit 100 MB Datenvolumen an. Bei der Anmeldung zeugt Ivacy beispielhaft, welche Kundendaten *wirklich* zur Bereitstellung eines VPN-Dienstes erforderlich sind: Benutzername und Passwort - mehr nicht. Zahlenden Nutzern offeriert Ivacy 3 Tarife: 1 Monat Flatrate für 10 €, 3 Monate Flatrate für 25 € und für Wenignutzer 0,50 € pro GB ohne Verfall. Das Unternehmen betont, dass es echte Flatrates anbiete und Vielnutzer nicht [diskriminiere](#). Bezahlt werden kann mit Paypal, Kreditkarte oder [Ukash](#). Der Kundenservice reagierte mit unterschiedlicher Geschwindigkeit, aber freundlich und aufgeschlossen. Aktuell denkt der Anbieter über den Aufbau eines SIP-Servers nach, über den anonyme Voice-over-IP-Telefonie möglich sein soll.

8. Linkideo



Im preislichen Spitzenfeld liegt der Anonymisierungsdienst [Linkideo](#). Sitz des Linkideos ist die Insel [Jersey](#), die zwar im Besitz der englischen Krone steht, aber nicht EU-Mitglied ist. Im Rahmen eines unbefristeten Sonderangebots bietet Linkideo einen VPN-Zugang mit echter Flatrate für nur 2 € Monatspreis an. Obwohl nur der kleinste Tarif mit nominellem Geschwindigkeitslimit von 512 KBit/s gebucht und bezahlt wurde, wurde offenbar der unlimitierte größte Tarif freigeschaltet, in dem zwischen 2.000 und 3.000 KBit (tagsüber weniger) im Down- und 800 KBit im Upstream bei einer Pingzeit von 70 ms erreicht wurden. Andere Kunden berichteten dasselbe. Auf die Speicherung personenbezogener Daten angesprochen erklärte Linkideo, es würden bei der Nutzung keinerlei Logdaten, insbesondere keine IP-Adressen gespeichert. Allerdings würden die Bezahl-Dienstleister und Linkideo die Zahlungsdaten speichern und eine Verknüpfung zwischen Benutzername und Bezahltdaten sei nicht denkbar.

Linkideos drei nutzbare Server in den Niederlanden, Großbritannien ([uk.linkideo.com](#)) und den USA ([usa.linkideo.com](#)) warte der Anbieter selbst. Alle Nutzer eines Servers seien unter derselben externen IP-Adresse unterwegs. Portsperrern, insbesondere auf 25 und 465, konnten im Test nicht festgestellt werden, allerdings neigte der niederländische Server im Test an manchen Tagen zu Verbindungsabbrüchen. Im größten (und bezahlten) Tarif für 10 € monatlich bietet der Anbieter

neben auch offiziell unbegrenzter Geschwindigkeit Port-Forwarding an. Zur Zeit bietet Linkideo nur Zugang per PPTP, also dem in Windows eingebauten VPN-Standard an. Bei entsprechender Nachfrage stehe man aber OpenVPN ebenso aufgeschlossen über wie datenschutzfreundlicheren Bezahlmöglichkeiten. Einstweilen kann nur über den kanadischen Zahlungsdienstleister Alertpay bezahlt werden, der Zahlung per Kreditkarte und wohl auch Überweisung auf EU-Konten anbietet. Beim kleinsten Tarif steht außerdem die Bezahlung per Anruf bei internationalen Premiumnummern einschließlich deutschen 0900-Nummern zur Verfügung, was im Test gelang, und was beispielsweise auch von einer [anonymen Prepaidkarte](#) aus denkbar wäre. Eine kostenlose Testnutzung ist nicht vorgesehen. Die Suche nach ungesperrten Wegwerfadressen für die Anmeldung erspart der Anbieter dem Kunden. Der Support reagierte teilweise träge, aber freundlich und fachkundig.

9. Xerobank; ShadowVPN



Ein 18-stufiges Anonymisierungskonzept verfolgt das Produkt [Xerobank](#) des gleichnamigen in Panama ansässigen Anonymisierungsspezialisten. Kunden stehen dafür Server in 28 Ländern zur Verfügung. Mehrfache gleichzeitige Nutzung eines Zugangs ist erlaubt, allerdings ist der monatliche Traffic auf 75 GB limitiert. Jede Verbindung passiert 3 der Server, von denen sich bei jeder Verbindung mindestens 2 in verschiedenen Staaten und mindestens 1 außerhalb der EU befinden. Die Route kann je nach Port oder anderen Kriterien ähnlich wie bei Tor auch verbindungsimmanent unterschiedlich sein. Alle Server kommunizieren untereinander komprimiert und verschlüsselt, dabei werden teilweise nach dem Zufallsprinzip Verbindungen in andere zusammengefasst. Die IP-Adressen werden intern mehrfach ausgetauscht, wobei kein Server alle Tauschschlüssel kennt. Zum Schutz der Nutzer werden nur mit OpenVPN oder IPSec verschlüsselte Einwahlen akzeptiert. Um Analysen von Zeit oder verschlüsselten Daten zu erschweren, generiert jeder Server auch künstlichen Datenverkehr und sendet mit zufälliger Verzögerung; Letzteres ist auch vom Kundenrechner aus möglich, der zudem Paketgrößen zufällig ändern kann. Kunden surfen unter denselben IP-Adressen, wobei externe IP-Adressen teils auch bei laufender Session transparent ausgetauscht werden. Alle beteiligten Datenträger seien datei- und partitionsweise verschlüsselt, so der Betreiber. Servermanipulationen lösten stufenweise eine Software- bis Hardware-Selbstzerstörung der Anonymisierungsserver aus. Entscheidungen und Zugriffsmöglichkeiten seien auch unternehmensintern vertraglich dezentral verteilt, um ungute Machtansammlungen zu vermeiden. Weitere Anonymisierungsvorrichtungen erklärt der Anbieter in einem [Whitepaper](#).

Logdaten speichert Xerobank über das Sessionende hinaus nicht, mit Ausnahme von E-Mail-Verbindungsdaten auf Port 25, die zur Spam-Vermeidung 2 Tage dezentral aufbewahrt werden. Auf Nachfrage räumte Xerobank ein, etwa Spammer damit zwar sperren, gewöhnlich aber selbst nicht identifizieren zu können; die Speicherung wirke vor allem präventiv. Darüber hinaus wird das tägliche Datenvolumen für 7 Tage gespeichert. Auf Behördenanordnungen aus anderen Ländern, insbesondere den USA, Großbritannien reagiere Xerobank grundsätzlich nicht. Keine der seit der Gründung anno 2004 360 eingegangenen internationalen Verfügungen und Gerichtsentscheidungen habe irgendeine Wirkung gezeitigt. Für die Anonymisierung von Kundenzahlungsdaten vor sich selbst habe Xerobank eine Schweizer Bank unter Vertrag genommen, die für jeden Kunden ein anonymes Nummernkonto einrichte, unter dem Xerobank seine Kundenkonten ausschließlich führe. Im Test wurden Verbindungen über den downloadbaren Client OpenVPN aufgebaut, was unproblematisch funktionierte. Allerdings zeigte sich, dass die Serienschaltung der Server und sonstigen Feinheiten des Betreibers ihren Tribut von der Leistung fordern: Die Geschwindigkeit betrug nur etwas über 300 KBit/s im Down- und etwas über 200 KBit im Upstream bei Pingzeiten von über 300 ms. Eine [Traceroute](#)-Abfrage führte von den Niederlanden über Schweden in die USA. Es wurden alle Verbindungen und Ports erfasst und auch beim Mailversand zeigten sich keine Probleme.

Wem Geschwindigkeit und Preis wichtiger als Anonymität sind, dem bietet das Unternehmen alternativ das Produkt [ShadowVPN](#) an. Hierbei sind keine gleichzeitigen Mehrfach-Logins möglich. Der monatliche Traffic ist auf 10 GB limitiert. Der Zugang erfolgt ebenfalls über ein OpenVPN-Programm. Die Geschwindigkeit dieses abgespeckten Produkts betrug im Test immerhin um 1.000 KBit/s im Down- und 200 KBit/s im Upstream bei einer Pingzeit von 160 ms. Die Serverkaskadierung und die sich daraus ergebenden Vorteile entfallen, im Übrigen kommt dieselbe Infrastruktur zum Einsatz.

Xerobank ist inklusive geschütztem Onlinespeicherplatz für stattliche 35 US\$ monatlich erhältlich, ein Testaccount wird für 1 US\$ angeboten. Die "Light"-Variante ShadowVPN (vorkonfigurierter Client erhältlich für Windows, Mac und Linux) ist für 10 US\$ monatlich erhältlich. Vor allem Geschäftskunden und Regierungen bietet das Unternehmen ferner das hier nicht getestete Produkt "Onyx" an, das sich durch noch mehr Anonymisierungsfeatures als Xerobank, höhere Geschwindigkeit, Hardwarerouter sowie je nach Traffic 4- (180 GB) bis 7-stellige Monatspreise (150 TB) auszeichnet. Bezahlt werden kann mit Kreditkarte und bei Jahresabonnements nach Absprache auch per Bargeldversand. Der Support antwortete schnell, freundlich, fachkundig und in erfrischend richtigem Englisch. Geschäftsführer Steve Topletz war Mitentwickler des Anonymisierungsprodukts Torpark und lehrt Privacy software design an der University of Texas. Für 2009 plant das Unternehmen starke Ende-zu-Ende-Echtzeitverschlüsselung für Mobilfunktelefonie und VoIP auf den Markt zu bringen, außerdem laufen Betatests anonymen, verschlüsselter Jabber-Server.

10. Swiss VPN

Nicht primär als Anonymisierungsdienst, sondern vor allem als Schutz in ungeschützten Umgebungen wie offenen WLANs versteht sich der Schweizer Dienst [SwissVPN](#). Verkehrsdaten und IP-Adressen werden 6 Monate lang auf Vorrat gespeichert und nach [Schweizer Recht](#) an dortige Behörden herausgegeben. Der Dienst basiert auf mehreren in der Schweiz untergebrachten Servern und die Nutzer erhalten Schweizer IP-Adressen. Unterstützt werden nur PPTP ohne eigenen Client und das eher exotische [EAP-TTLS](#); die Unsicherheit der PPTP-Verschlüsselung will SwissVPN dadurch ausgleichen, dass den Kunden sichere, unveränderliche Passwörter zugeteilt werden. Eine anbieterseitige Serverkaskadierung findet nicht statt. SwissVPN ist nicht auf bestimmte Protokolle beschränkt und es werden keine Mail-Ports gesperrt. Da der Anbieter keinen kostenlosen Testaccount zur Verfügung stellen wollte, wurde auf einen Geschwindigkeitstest verzichtet; jedoch könnte eine VPN-Testverbindung allein zum SwissVPN-Webserver auf eine gute Geschwindigkeit hindeuten. Zwar werden für die Anmeldung selbst überhaupt keine Bestandsdaten wie Benutzererkennung, Passwort oder E-Mail-Adresse abgefragt, jedoch ist Zahlung nur per Kreditkarte und Paypal möglich. Nach Anbieterauskunft können diese Daten auch mit Vorratsdaten zusammengeführt werden. Die Kosten betragen 5 US\$ monatlich, wobei der Kunde seine Vertragslaufzeit von 1-12 Monaten selbst festlegen kann. Der Support reagierte rasch und leidlich freundlich.

11. Safersurf Anonympaket

The screenshot shows the Safersurf.com website interface. On the left, there are four service packages listed: 'Schutzpaket' (Not purchased), 'Speedpaket' (Not purchased), 'Anonympaket' (Purchased), and 'Komplettpaket' (Not purchased). Below these is a 'Safersurf ist aktiv' indicator and a 'Deaktivieren' button. On the right, there is a 'Globale Safersurf Statistik (Stand: Woche 21.08)' table showing traffic statistics for the last 24 hours, week, month, and year.

	Gestern 08.07.2009	Woche 2.100	Monat Statistik	Jahr 2009
Abgeholte Webseiten	3.312.731	3.793.464	7.402.373	7.402.373
Abgeholte eBooks	16.714	38.407	78.826	78.826
Informa Videopakte	54	130	446	446
Informa eMails	17	38	73	73
Unversuchte eMails	6.185	12.776	24.812	24.812

Das [Safersurf](#) Anonympaket arbeitet offenbar als Proxy, der in die Browser eingetragen werden kann, aber nicht muss. Es zeigte sich, dass sich Safersurf daher auch nicht mit bereits vorhandenen Proxys zur Werbefilterung verträgt. Im Test ersetzte Safersurf die IP-Adresse nach außen hin durch eine eigene und entfernte Betriebssystem und Referrer aus den übermittelten Daten. Nach Herstellerangaben werden außerdem Trackingdaten von Google, Doubleclick, IVW und anderen entfernt, die

zur Erstellung von Benutzerprofilen verwendet werden können. Obwohl der HTTP- und E-Mail-Proxy grundsätzlich alle Ports erfassen soll und keine gesperrt oder gedrosselt werden sollen, erfolgte bei Empfang und Versand von E-Mails über [POP3](#) und [SMTP](#) (z.B. Thunderbird, Outlook) keine Anonymisierung. Laut Beschreibung soll der anonyme E-Mail-Versand wohl so funktionieren, dass E-Mails über einen Mailserver von Safersurf versendet werden, der daraufhin die Absenderadresse durch eine solche ersetzt, die Antworten 10 Tage lang an den Absender zurückleitet und spätere Antworten zurückweist. Auch Emule wurde nicht anonymisiert, so dass die Anonymisierung letztlich offenbar nur HTTP-Verkehr sowie über Safersurf gesendete E-Mails erfasst.

Die gemessene Web-Geschwindigkeit lag bei 1.000-2.000 KBit/s im Down- und 300 KBit/s im Upstream. Die Pingzeit betrug meist über 300 ms. Der nach eigenen Angaben 10 deutsche Server betreibende Anbieter aus Leipzig speichert gemäß der Vorratsdatenspeicherung IP-Adressen und Zeit. Statische Benutzernamen wie bei [Cyberghost](#) werden nicht gespeichert. Das getestete "Anonympaket" kostet 5,90 € monatlich bei einer Mindestlaufzeit von 3 Monaten, die der Kunde per Lastschrift oder Kreditkarte begleichen kann. Der Service antwortete schnell und freundlich. Meldungen wie [diese](#) oder der [bizarre Formen](#) annehmende Krieg gegen den Heise-Zeitschriftenverlag lassen den Nutzer allerdings etwas ratlos hinsichtlich der Seriosität des Anbieters zurück.

12. Witopia Personal VPN



Der VPN-Anbieter [Witopia](#) aus Virginia sieht sein Angebot vor allem als Schutz in ungesicherten WLANs. Der Kunde kann sich über PPTP oder OpenVPN einwählen. Verbindungsdaten einschließlich IP-Adressen werden für 1 Woche auf Vorrat gespeichert, eine Herausgabe erfolgt nach US-amerikanischem Recht. Mehrere Nutzer teilen sich eine öffentliche IP-Adresse. Die Daten der Nutzer laufen über zwei Server in Kalifornien und Nordvirginia, wobei die Standorte nach Geschwindigkeit der Anbindung ausgewählt wurden. Eine Sperrung bestimmter Ports findet laut Anbieter nicht statt. Eine Bestellung erfordert die Angabe einer vollständigen Post- und E-Mail-Adresse. Kurioserweise werden dabei Wegwerf-, nicht aber Hotmail-Adressen akzeptiert. Eine Zusammenführung der auf Vorrat gespeicherten Verkehrsdaten mit Zahlungsdaten ist möglich. Wegen technischer Schwierigkeiten, die aber nicht zwangsläufig beim Anbieter liegen müssen, konnte ein Test leider nicht erfolgreich durchgeführt werden. Der Preis beträgt 40 US\$ für jede Monatsflatrate. Akzeptierte Zahlungsmethoden sind Paypal und Kreditkarte. Der Support reagierte schnell und freundlich.

13. Trackbuster



Ausschließlich auf den Zugangsstandard OpenVPN setzt der deutsche Anonymisierungsanbieter [Trackbuster](#). Als vorratsspeicherungspflichtiges Unternehmen speichert Trackbuster die Original- und die ausgewechselte IP-Adresse sowie Start- und Endzeitpunkt der Verbindung. Immerhin werden keine Benutzerkennungen wie bei Cyberghost gespeichert, die eine Einkreisung in Frage kommender Original-IP-Adressen [erleichtern](#) könnten. Auch ist es nach Anbieterangaben nicht möglich, Verkehrs- mit Zahlungsdaten zusammenzuführen. Gleichwohl ist der Anonymisierungsgrad auf Grund der Vorratsdatenspeicherung zwangsläufig geringer. Das Unternehmen beteiligt sich an unserer [Verfassungsbeschwerde gegen die Vorratsdatenspeicherung](#). Alle maßgeblichen Server, die sich nach Anbieterangabe ausschließlich in Deutschland befinden, werden vom Anbieter selbst gewartet. Die Serienschaltung mehrerer Server ist nicht vorgesehen. Der Dienst ist nicht auf HTTP-Verkehr beschränkt und es werden auch keine Ports gesperrt, was im Test bestätigt werden konnte. Weiter wurden im Test angenehme Geschwindigkeiten von gut 3.000 KBit im Down- und 800 KBit/s im Upstream bei erfreulichen Pingzeiten um 70 ms gemessen. Die zugewiesene IP-Adresse stammte aus Deutschland, wo nach Angaben des Anbieters sämtliche Server stehen. Für seine Dienste berechnet das Unternehmen monatlich 5 € ohne Zeit- oder Volumenbegrenzung. Pflichtangaben bei

der Anmeldung sind nur Benutzername und Passwort, optional eine E-Mail-Adresse. Positiv ist, dass der Kunde seine Vertragslaufzeit monatsgenau (1-12) selbst auswählen kann. Als Zahlungsmittel werden Banküberweisung und Paypal akzeptiert. Der Service antwortete schnell und freundlich.

14. Your Freedom



Eher als Ausweg gegen sperrende und zensierende Netzanbieter sieht sich der Anbieter [Your-freedom](#). Als in Deutschland ansässiger Anbieter werden die vorgeschriebenen Verbindungsdaten auf Vorrat gespeichert, wobei alle Nutzer eines Servers unter gleicher externer IP-Adresse surfen. Derzeit betreibt der Anbieter weltweit 21 Server in Deutschland, Frankreich, Großbritannien, den USA, Kanada, in Kürze auch in der Schweiz und in Singapur. Auf jedem Server hielten sich Nutzer in dreistelliger Zahl auf. Die Standorte und Anbindungen wurden auf Geschwindigkeit optimiert. Eine Kaskadierung der Server ist nicht vorgesehen. Die Nutzung erfolgt entweder über OpenVPN oder über einen proprietären Client mit eigener, zugegebenermaßen schwachen Verschlüsselung ähnlich WEP. Neben der Vorratsdatenspeicherung blockiert der Anbieter eine ganze Reihe von Ports, namentlich 37, 135, 137-139, 161 und 162 UDP sowie 37, 135, 139, 445, 6667 und 8080 TCP. Gesperrt ist auf den US-Servern ferner Filesharing und allgemein IRC. Hinsichtlich E-Mails sperrt der Anbieter Port 465 gesperrt; E-Mails auf Port 25 (unverschlüsselt) werden vom anbieter-eigenen Server auf Viren und Spam hin überprüft, außerdem die Empfängerzahl begrenzt und die E-Mails werden gegebenenfalls ausgebremst. Bei der Anmeldung wird neben Benutzername und Passwort eine E-Mail-Adresse abgefragt und überprüft, für die Wegwerfadressen verwendet werden können. Je nach Bandbreite verlangt der Anbieter für eine Flatrate ein Monatsentgelt zwischen 0 und 20 €, wobei zwischen verschiedenen Laufzeiten zwischen 1 und 12 Monaten gewählt werden kann. Als Zahlungsmittel bietet der Anbieter vor allem Kreditkarte, Paypal und Liberty Reserve, aber auch Ukash an. Auch hier reagierte der Service schnell und freundlich.

15. Surfonym



[Surfonym](#) nennt sich ein Anonymisierungsanbieter mit Sitz in Wien. Da Österreich die Europäische Richtlinie zur Vorratsdatenspeicherung derzeit noch nicht umgesetzt hat, speichert der Anbieter keinerlei Logdaten. Alle Nutzer eines der 5 in Österreich stehenden Server surfen normalerweise unter derselben externen IP. Durch Anhängen eines Suffixes an den Benutzernamen ist es möglich, eine eigene dynamische IP zu erhalten. Unterstützt wird OpenVPN. Ein Test war wegen technischer Schwierigkeiten, die aber nicht sicher beim Anbieter liegen, leider nicht möglich. Ein Blockieren von Ports ist ebenso wenig vorgesehen wie eine kaskadierte Serverstruktur. Bei der Anmeldung werden Name und eine funktionierende E-Mail-Adresse abgefragt, wobei es auch eine Wegwerfadresse tut. Die Kosten betragen 4,90 € für eine Monatsflatrate. Bezahlt werden kann nur mit Paypal und [Egold](#). Der Betreiber von Surfonym antwortete schnell und freundlich.

16. BananaVPN



IP-Adressen, Verbindungszeiten und Datenvolumina für die Dauer eines Monats speichert der zyprische VPN-Anbieter [BananaVPN](#). Dabei sieht sich der Anbieter nicht primär als Anonymisierer, sondern will wohl die IP-Adressen auswechseln, so dass in einigen Ländern gesperrte Internetseiten und ähnliches betreten werden können. Nutzern eines Servers wird dieselbe externe IP-Adresse zugewiesen. Serverkaskadierung wird nicht unterstützt. Der Anbieter räumt ein, schon auf Polizeianfrage alle gewünschten Daten herauszugeben. Das bei BananaVPN bevorzugte Einwahlprotokoll ist PPTP, laut Website auch IPSec. Es ist auch möglich, Verkehrsdaten mit Zahlungsdaten in Verbindung zu bringen. Blockiert sollen lediglich einige ungenannte P2P-Ports

sein. Einen kostenlosen Testaccount gewährte der Anbieter nicht, weswegen auf einen Test verzichtet wurde. Nennenswert mag noch sein, dass der Anbieter Server und IP-Adressen in Großbritannien (15 US\$ monatlich), den USA und in Deutschland (jeweils 20 US\$ pro Monat) anbietet. Für 25 € wird außerdem ein separater US-Server mit eigener dynamischer IP-Adresse angeboten, der vor allem für eine reibungsfreie VoIP-Erreichbarkeit vorgesehen ist. Etwas Banane ist leider auch der Datenschutz bei der Anmeldung, bei der Name, E-Mail- und Postadresse und auch noch die Telefonnummer abgefragt werden. Als Zahlungsmittel stehen nur Kreditkarten zur Verfügung. Eine kostenlose Testnutzung für Kunden ist nicht vorgesehen, in den ersten 3 Tagen will der Anbieter aber bei Unzufriedenheit den vollen Preis zurückerstatten. Auf Anfragen wurde schnell, etwas missmutig und mit mittelmäßiger Sachkunde geantwortet.

17. VPN Out



Einer der wenigen ansatzweise datenschutzfreundlichen US-amerikanischen VPN-Anbieter ist [VPN Out](#). Der Zugang erfolgt ausschließlich über den Standard OpenVPN, also verschlüsselt. Auch alle drei Server des Anbieters mit Standort USA, die vom eigenem Personal gewartet werden, sind verschlüsselt. Es werden jeweils einen Monat lang Logdateien mit den Verbindungsinformationen aufgezeichnet, die sich auch auf allerdings frei wählbaren Benutzernamen beziehen. Nicht gespeichert werden Original-IP-Adressen der Nutzer, und allen Nutzern eines Servers wird dieselbe externe IP-Adresse zugewiesen. Bei der Anmeldung abgefragte Informationen sind Benutzername, Passwort, Name und E-Mail-Adresse, bei der auch Wegwerfadressen funktionierten. Der Anbieter ermutigte dazu, falsche Namen anzugeben. Er räumt ein, dass die geloggtten Benutzernamen nachträglich mit personenbezogene Zahlungsdaten verbunden werden können, so dass sich das Nichtspeichern der Original-IP-Adressen unter Umständen als nutzlos erweist, weil eine Identifizierung über die Bezahlungen vorgenommen werden kann. VPN Out blockiert Port 25, nicht aber 465. Im Test zeigte der US-Server eine gute Geschwindigkeit von über 6.000 KBit/s im Down- und etwa 600 KBit/s im Upstream bei einer ebenfalls guten Pingzeit von nur 60 ms. Der Anbieter bietet 4 Tarife an, die von 15 GB über 3 Monate für 25 US\$ bis hin zu 1 TB über 12 Monate für 100 US\$ reichen. Die Bezahlung kann leider nur per Paypal erfolgen. Bei der Beantwortung der Fragen bewies der Betreiber große technische und rechtliche Kenntnisse.

Fazit

Schlimmer als keine Sicherheit ist falsche Sicherheit. Behalten Sie deshalb immer im Hinterkopf, dass es absolute Anonymität nicht gibt, auch mit den besten Anonymisierungsdiensten. Vielmehr gehen Sie mit Anonymisierungsdiensten ein neues Risiko ein, indem Sie dem Anonymisierer, der womöglich im Ausland sitzt und dessen rechtlich kaum haftbar zu werden ist, Ihre Daten anvertrauen. Verwenden Sie, wo immer möglich, Ende-zu-Ende-Verschlüsselung wie SSL oder PGP, so dass auch der Anonymisierungsanbieter nicht mitlesen kann. Forschungen der Universität Regensburg haben ergeben, dass selbst bei sicherer Verschlüsselung und Anonymisierung der IP-Adresse durch eine Zeit- und Volumenanalyse allein des verschlüsselten Verkehrs an nur einem Punkt zwischen Rechner und Anonymisierer (z.B. bei Ihrem Internetprovider) das Ansurfen bestimmter vermuteter Webseiten mit großer Wahrscheinlichkeit zugeordnet werden kann. Bei den üblichen VPN-Implementierungen wie OpenVPN und IPsec soll die Erfolgswahrscheinlichkeit dessen bei über 90% liegen.

Im Übrigen sind Sie bei keinem Anonymisierungsdienst anonym, solange Sie eingewählt sind. Denn für die Dauer der Verbindung ist der Weg zu Ihnen technisch auf jeden Fall zurückverfolgbar, andernfalls könnten sie keine Daten empfangen. Im Übrigen müssen bei Vorliegen der rechtlichen Voraussetzungen auch Anonymisierungsdienste alle greifbaren Benutzerdaten an Behörden herausgeben, woran auch die Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung nichts ändert. Lassen Sie sich nicht einreden, ein Anonymisierungsanbieter gebe gespeicherte Daten nicht heraus: Angesichts drohender Maßnahmen wie Beschlagnahme, Verhängung von Zwangs- und Bußgeldern, Inhaftierung der Geschäftsführung, Zwangstilllegung,

Gewerbeuntersagung oder gar einem Strafverfahren wegen Strafvereitelung werden Anonymisierungsanbieter behördlichen Anordnungen realistischere Folge leisten, soweit möglich. Vielmehr deuten solche heroischen Ansinnen auf fehlenden juristischen Sachverstand hin, der ihre Daten stärker in Gefahr bringen kann als ein seriöser Provider mit Vorratsdatenspeicherung. Achten Sie deshalb darauf, dass der Anbieter von vornherein so wenig wie möglich speichert. Werden Sie hellhörig, wenn Ihnen ein Anbieter Dinge wie 100%-ige Anonymität im Internet verspricht, die es nicht gibt. Bezahlen Sie kein Geld dafür, dass URLs oder sonstige Verbindungsinhalte nicht gespeichert werden - das geschieht auch sonst nicht.

Bedenken Sie außerdem bei der Benutzung von Anonymisierungsdiensten, dass eBay- und Paypal-Konten teilweise wegen Hackingverdachts gesperrt wurden, nachdem deren rechtmäßiger Inhaber über Anonymisierungsserver darauf zugriff. Im Test verweigerte GMX die Anmeldung eines E-Mail-Kontos über Perfect Privacy. Auch sonst kann es sein, dass Seitenbetreiber Zugriffe über Anonymisierungsdienste mit der Begründung blockieren, diese würden häufig zu missbräuchlichen Zwecken genutzt. Handeln Sie auch bei hohem Anonymitätsgrad verantwortungsvoll im Internet. Alles andere erschwert Ihrem Anonymisierungsanbieter das Leben, erhöht dessen Preise und ist Wasser auf die Mühlen von (Un-)Sicherheitspolitikern.

Sichern Sie Ihren Browser und nutzen Sie Software, um dessen Header mit Browserbezeichnung, Sprache und anderen Informationen bei jedem Seitenaufruf zu entfernen. Löschen Sie Flash- und sonstige Cookies regelmäßig. Meiden Sie nach Möglichkeit datenhungrige Seiten und geben Sie Ihre Daten nur dort an, wo unbedingt nötig. Ein Anonymisierungsdienst auf dem höchsten technischen Niveau nützt nichts, wenn Sie Ihre Daten durch diesen freiwillig herausgeben. Sichern Sie Ihren Rechner mit restriktiv eingestellten Software- und Router-[Firewalls](#), Antiviren- und [Spyware](#)-Programmen. Bedenken Sie beim Ausprobieren von Free- und Shareware, dass sich kostenlose Programme zunehmend durch Spyware finanzieren, also ihr Nutzerverhalten ausspionieren und verkaufen. Eine häufige Quelle von Schadsoftware jeder Art sind auch ohne ausreichenden Schutz genutzt illegale Raubkopien und Tauschbörsen. Schützen Sie sich vor Diebstahl, Beschlagnahme oder sonstigen [Fremdzugriffen](#) durch Vollverschlüsselungsprogramme wie etwa das quelloffene und kostenlose [Truecrypt](#).

Diese Übersicht soll zumindest sporadisch aktualisiert und erweitert werden. Vorschläge können Sie gerne in das unten genannte Forum schreiben.

Jonas

21.01.09

[Kontakt über Forum auf daten-speicherung.de...](#)