Unerkannt und unbehindert

Anonym und störungsfrei im Netz -
Wie umgeht man Netzsperren, Zensur und Überwachungsmaßnahmen?

1. Voraussetzungen

'Arbeit im Internet' bedeutet, an einem Computer zu arbeiten, der oft zum Netz einer Firma oder Organisation gehört, das wiederum durch einen Internet Service Provider (ISP) mit dem Internet verbunden ist.
Alle hier geschilderten Methoden funktionieren nur dann, wenn Überwachung und Zensur nicht bereits 'im eigenen Hause' stattfinden, also auf dem eigenen Rechner, in der eigenen Firma, im Bereich des eigenen Internet Service Providers.
Beispiele: Einige Computerviren verhindern, dass man sich Hilfe holt: Sie kennen die Adressen der Hersteller-Websites von Antivirenprogrammen. Versucht man, eine solche aufzurufen, stürzt der Webbrowser ab. Einige Überwachungsprogramme (s.g. Keystroke-Logger) zeichnen jeden Tastaturdruck und jede Mausbewegung auf. Sie speichern alle Passwörter, jeden Text, bevor er verschlüsselt wurde, jede Mailadresse, mit der man Kontakt aufnimmt. Schließlich kann der Administrator eines Netzes alle Datenpakete überwachen, die von und zu einem Computer darin fließen.

Mit einem derart infizierten Rechner ist es selbstverständlich unmöglich, vertraulich oder anonym zu arbeiten. Das Erkennen und Entfernen solcher korrumpierenden Schadprogramme ist Expertenarbeit (die sichere Installation eines Computers hingegen nicht!). Arbeitet man mit dem eigenen Computer, sollte man ihn im Vorweg vor Angriffen und Kompromittierung schützen. Arbeitet man in einem Netz (z.B. einer Redaktion) sollte man sicherstellen, dass man dem Administrator vertrauen kann.

Internet-Cafes oder andere fremde Rechner können für das anonyme Arbeiten eine Hilfe sein, solange dort keine Personalisierung stattfindet (man z.B. keinen Ausweis vorzeigen muss). Man muss dabei einkalkulieren, dass man Schadprogramme auf fremden Rechnern (z.B. Keystroke Logger) weder feststellen noch verhindern kann.

2. Anonym surfen / Websperren umgehen

Es gibt drei Arten der Anonymisierung und die Pseudonymisierung:

- ✓ Anfangs-Anonymisierung: Auf dem Rechner, auf dem man arbeitet, sollen keine Spuren bleiben,
- ✓ End-Anonymisierung: bei den Rechnern, die man ansurft, sollen keine validen Spuren bleiben. Die schließt das Umgehen von Websperren ein,
- ✓ Ende-zu-Ende-Anonymisierung: In der gesamten Kette der Rechner, mit denen gearbeitet wird, sollen keine validen Spuren bleiben.

- ✓ Pseudonymisierung (z.B. Logins und Freemail-Adressen unter falschen Namen) sind wirksame Anonymsierung, wenn Ermittler nicht auf die Spuren der Pseudonymisierung zugreifen können (z.B. weil Provider dafür im Ausland sind).

Albrecht Ude
Lehderstraße 53 — 13086 Berlin — Germany
www.ude.de — albrecht@ude.de

13.09.2010

Es gibt keine Methode, die 100%ige Anonymität gegenüber jedem Beobachter bietet, daher muss man je nach Anlass verschiedene Methoden kombinieren. Entscheidend für die Wahl der Methoden ist die Frage, vor wem man etwas verbergen möchte:

- ✓ vor anderen Nutzern desselben Computers oder Programmes,
- ✓ vor dem Administrator des Computers oder Netzes,
- ✓ vor dem Internet-Service Provider,
- ✓ vor dem Betreiber eines Internet-Dienstes (z.B. Webauftrittes),
- ✓ vor Überwachern aus Staat, Wirtschaft ~~und~~ oder Kriminalität.

2.1 Anfangs-Anonymisierung

"Privater Modus" im Webbrowser : Diese Methode wird im Jargon "Pornomodus" genannt. Sie nützt, um Spuren vor anderen Nutzern desselben Browsers zu verbergen. Der Administrator eines Firmennetzes oder des ISPs können diese aber (bei Interesse) durchaus noch sehen.
Eine Studie über diesen Modus in verschiedenen Browsern kommt zu einem deprimierenden Ergebnis: "Man hinterlässt man mit dem Private-Browsing-Modus mehr Spuren auf dem Rechner und im Netz, als man denkt.", wie der heise.de-Newsticker zusammenfasst.

An analysis of private browsing modes in modern browsers / G. Aggrawal ; E. Bursztein ; C. Jackson ; D. Boneh (proceedings of Usenix Security 2010)
http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf (15 S., 509 KB)
Private-Browsing-Modus schützt nur unzureichend. - heise.de, 09.08.2010
http://www.heise.de/newsticker/meldung/Private-Browsing-Modus-schuetzt-nur-unzureichend-1052101.html .

Genauso verhält es sich mit dem Menüpunkt **"Neueste Chronik löschen"**, den einige Browser anbieten. Andere Nutzer desselben Gerätes können dann die angesurften Seiten nicht nachvollziehen, Admins des Firmennetzes und des ISPs könnten diese dennoch mitloggen.
Sicherer ist es, einen **Webbrowser auf einem USB-Stick** zu nutzen. Entstehende Spuren (Seiten im Browser-Cache, History, Cokies etc.) werden dann auf dem USB-Stick gespeichert, den man nach getaner Arbeit abzieht.
(Auch das hilft aber nicht gegen Beobachtung durch Admins, ISPs und installierte Paket-Logger).

2.2 End-Anonymisierung / Web-Sperren umgehen

Welche **Spuren beim Surfen im WWW** man bei den angesurften Webservern hinterlässt, kann man bei
http://tools-on.net/privacy.shtml
nachvollziehen. Diese Spuren können prinzipiell auch durch Web-Filter ausgelesen werden. Diese Seite kann man auch nutzen, um das Funktionieren von Proxies (s.u.) zu testen. Nach der Nutzung eines Proxys müssen dort andere Daten erscheinen, insbesondere "Reported remote address", "Client's address", "Client's hostname" und "Preferable mail server".

Zu den Spuren im Web zählt auch die **Konfiguration des eigenen Webbrowsers**. Oft ist diese durch Browser Plugins, Systemfonts (installierte Schriften) und Cookies einzigartig, so dass diese Spur reicht, um Computer (und damit Nutzer) zu identifizieren oder Profile zu erstellen. Ob die eigene Konfiguration einzigartig ist, kann man mit dem Projekt "Panopticlick" der Electronic Frontier Foundation (EFF) herausfinden:
http://panopticlick.eff.org/ .

Ein besonderes Problem sind "**aktive Inhalte**" von Webseiten, Technologien mit Namen wie JavaScript, Java, Flash und andere. Diese können eine Webseite interaktiv gestalten, aber ebenso dazu dienen, Besucher auszuforschen oder anzugreifen. Z.B. sammelt die Firma Google mit dem Dienst GoogleAnalytics Besucherprofile von vielen Websites, die eigentlich nichts mit Google zu tun haben. Der Nutzer bemerkt das normalerweise nicht.
Man kann mit jedem Browser diese aktiven Inhalte deaktivieren. Das ist sicher, aber einige Websites sind dann gar nicht mehr oder nur eingeschränkt nutzbar.
Für den Firefox-Browser gibt es das Addon "**NoScript**". Damit ist es möglich, alle "aktiven Inhalte" zu sperren, aber für einzelne Seiten freizuschalten oder auch nur temporär, für die jeweilige Sitzung, zuzulassen.
Mit einem hohen Maß an Sicherheit kann man also dennoch einzelne, vertrauenswürdige Sites nutzen. Ebenso kann man z.B. die eigentliche Website nutzen, aber GoogleAnalytics das Datensammeln verwehren.
http://noscript.net/ .

Wenn ein Web-Filter nach dem Listenprinzip arbeitet, der einfach den Zugang zu Seiten sperrt, die in einer "Black List" erfasst sind, helfen **Caches** und **Proxies**.

Als schnelle Lösung bieten sich die Caches der großen Suchmaschinen (Ask, Bing, Exalead, Google, Yahoo) an.
http://www.ask.com/ ,
http://www.bing.com ,
http://www.exalead.com/search/ ,
http://www.google.com/ ,
http://search.yahoo.com/ * Ob der Yahoo-Cache noch unabhängig vom Bing-Cache ist, ist derzeit unklar.

Ebenso kann man die bei
http://www.faganfinder.com/urlinfo/
unter dem Punkt "Cache" aufgeführten, die Waybackmachine
http://www.archive.org/index.php
oder das Coral Content Distribution Network
http://www.coralcdn.org/
nutzen - jeweils vorausgesetzt, dass diese nicht selbst auf den "Black Lists" stehen.

Caches können nur anzeigen, was sie bereits vorher gespeichert haben. **Proxies** als 'zwischengeschaltete' Rechner surfen dagegen im Auftrag des Benutzers in Echtzeit.

Proxies findet man auf einschlägigen Listen, z.B.
A-Z Proxies
http://www.azproxies.com/

immer wieder in Weblogs, z.B.:

Albrecht Ude
Lehderstraße 53 — 13086 Berlin — Germany
www.ude.de — albrecht@ude.de

120+ Proxies For Browsing Web Anonymously And Accessing Blocked Websites
http://www.techdreams.org/tips-tricks/120-proxies-for-browsing-web-anonymously-and-accessing-blocked-websites/1258-20090130

oder durch eine intelligente Abfrage bei einer Suchmaschine, z.B.
Google.com, Suche nach **inurl:proxy.cgi "start browsing"**
http://www.google.com/search?hl=en&q=inurl%3Aproxy.cgi+%22start+browsing%22&aq=f&aqi=&aql=&oq=&gs_rfai= .

Ein besonders hervorhebenswerter Proxy ist Picidae.
http://pici.picidae.net/ .
Er wandelt Webseiten in Graphiken um - dadurch werden alle textbasierten Websperren "geblendet", weil die ausgelieferten Seiten keine Texte enthalten. (Hintergründe dazu unter **http://www.picidae.net/**).

Weitere Möglichkeiten

Neben Caches und Proxies gibt es weitere Möglichkeiten, listenbasierte Websperren zu umgehen, es sind sämtlichst simple Tricks.

Viele Websites haben RSS-Feeds. Diese kann man webbasiert abonnieren und wird so stets über Änderungen und Aktualisierungen informiert. Ein bekannter RSS-Aggregator ist **http://www.bloglines.com** .

Übersetzungsdienste können ebenfalls helfen, eine gesperrte Website anzusurfen:
http://babelfish.yahoo.com ,
http://translate.google.com .

Ferner gibt es spezielle Filterdienste, die für Surfer mit geringer Bandbreite gedacht sind: Sie filtern Hintergrundgraphiken u.dgl. aus und machen Webseiten dadurch "schlanker", z.B.
http://loband.org .

Schließlich gibt es die Möglichkeit, sich Webseiten via E-Mail zusenden zu lassen, z.B. hier: Web2Mail
http://web2mail.com/lite/welcome.php .

2.3 Ende-zu-Ende-Anonymisierung

Eine der besten (und einfachsten) Möglichkeiten zur völligen Anonymisierung ist das TOR-Netz. "TOR" steht für "The Onion Router" (Zweibelrouter), weil Verbindungen durch dies Netz drei Mal umgelenkt und dabei jedesmal verschlüsselt werden. Ein Überwacher müsste Zugriff auf alle drei (jeweils zufällig aneinandergeschalteten) Rechner haben, um den Weg der Daten verfolgen zu können. Da TOR ein internationales Netz ist, ist dies faktisch unmöglich. Einzelheiten (in vielen Sprachen) unter:
https://www.torproject.org/ .

Zudem beginnt bei TOR die Verschlüsselung bereits im eigenen Browser. Daher können auch der eigene Admin und der ISP die Kommunikation nicht mitloggen (solange keine Spionagesoftware lokal installiert ist).

Es gibt diverse **Firefox-Addons** für die bequeme Nutzung von TOR.
https://addons.mozilla.org/de/firefox/extensions/privacy-security/ .

Die einfachste Nutzungsmöglichkeit ist das **Privacydongle** des FoeBuD e.V.
https://privacydongle.de/ .
Die Software kann frei und umsonst aus dem Netz geladen werden. Sie wird einfach auf einen USB-Stick entpackt. Dieser enthält dann den Firefox-Browser und den TOR-Client, d.h. durch Start des Browsers auf dem Stick ist man bereits anonym im Netz.

Weitere Anonymisierungsdienste sind **JonDonym** und das Invisible Internet Project **I2P**:
https://anonymous-proxy-servers.net/ .
http://www.i2p2.de/ .

3. Anonyme E-Mail

3.1 Pseudonymisierung

Bei einem Freemail-Provider (ggfs. im Ausland) eine nichtssagende Mailadresse einzurichten, kann sehr hilfreich sein. Bei Abruf der Mails via WWW kann man Proxies oder TOR nutzen, um weitere Spuren zu verwischen.

3.2 Anonyme E-Mail empfangen

Um anderen die Möglichkeit zu geben, E-Mails anonym abzusetzen, sollte man eine Privacybox bei der German Privacy Foundation (GPF) einrichten:
https://privacybox.de/ .

Nach Einrichtung werden dort abgesetzte E-Mails anonym zugestellt. Auch hier kann die Anonymität erhöht werden, indem man das Web-Formular via TOR oder Proxy aufruft. Besonderer Vorteil: Man kann in der eigenen Privacybox den eigenen, öffentlichen PGP-Key einbauen. Dann werden alle so beförderten E-Mails auch noch verschlüsselt, ohne dass der Absender sich um Verschlüsselung kümmern muss.

3.3 Anonyme E-Mails versenden

Anonym E-Mails versenden kann man einem anderen Service der GPF:
http://www1.privacyfoundation.de/anon-email.htm .
Wer der GPF nicht traut (und warum sollte man?), kann das Web-Formular via TOR oder Proxy aufrufen. Dann weiß nicht einmal die GPF, wer ihr Angebot nutzt.

4. Verschlüsseln

4.1 Speichermedien verschlüsseln

Die derzeit beste Methode, um Festplatten, USB-Sticks und andere Speichermedien zu verschlüsseln, ist das kostenfrei nutzbare Open-Source-Programm Truecrypt:

Albrecht Ude
Lehderstraße 53 — 13086 Berlin — Germany
www.ude.de — albrecht@ude.de

http://www.truecrypt.org/ .
Mit dem Programm kann man auch wirkungsvoll Dateien verstecken (Steganographie).

4.2 Nachrichten verschlüsseln

Um E-Mails zu verschlüsseln, bieten sich PGP und als kostenfreie Variante GnuPG an. Problem: Alle Kommunikationsteilnehmer müssen Programme installieren und Schlüssel austauschen, was in der Praxis ein echtes Hindernis ist. Dennoch: Journalisten sollten PGP/GnuPG installieren, um ggfs. damit arbeiten zu können.
PGP
http://www.pgpi.org/ .
GnuPG
http://www.gnupp.org/start.html ,
http://www.gpg4win.org/ .

5. Weitere Informationen

Gute Hinweise und Anleitungen zum Themengebiet findet man auf der Homepage von Kai Raven
http://hp.kairaven.de/ .

und im Privacy-Handbuch der GPF
http://www1.privacyfoundation.de/handbuch_11.htm ,
Kapitel "Anonymisierungsdienste nutzen"
https://www.awxcnx.de/handbuch_22.htm .

Internet censorship wiki
http://en.cship.org/wiki/Main_Page .

AnonWiki
http://anonymitaet-im-inter.net/wiki/ .

Einige Proxy-Tools von Scusi
https://scusiblog.org/?page_id=2137 .

Der Chef surft mit : Technische Möglichkeiten der Mitarbeiterinnen- und Mitarbeiter-Kontrolle bei der Internet- und E-Mail Nutzung und wie man sich davor schützen kann / Gerrit Wiegand ; Andreas Friedel
Offenbach: mainis IT-Service GmbH, © 2002
http://www.onlinerechte-fuer-beschaeftigte.de/page.php?k1=main&k2=kontrolle&k3=ratgeber&view=&lang=1&si=4c8a05f110c72 ,
http://www.onlinerechte-fuer-beschaeftigte.de/upload/s480e1c9f6be9d_verweis1.pdf (PDF, 25 S., 407 KB)

Zensur im Internet und Umgehung von Zensur
German Privacy Foundation, 16.06.2009 (Vortragsfolien der Veranstaltung "Digitales Aikido")
https://www.awxcnx.de/download/digitales_aikido_zensur.pdf .

Albrecht Ude
Lehderstraße 53 — 13086 Berlin — Germany
www.ude.de — albrecht@ude.de

13.09.2010