Warum ist das Internet gefährlich?

Das Internet ist für viele Aktivist*innen mittlerweile unerlässlich geworden. Hier informiert mensch sich über Tierrechtsthemen, vernetzt sich mit anderen Aktivist*innen oder plant Aktionen mit der eigenen Gruppe. Kurzum das Internet ist ein hilfreiches Mittel um politische Arbeit zu leisten. Aber neben all den positiven Seiten gibt’s natürlich auch Nachteile. Durch die Überwachung eines Internetanschlusses lässt sich sehr viel über den/die BenutzerIn herausfinden. Jede Seite die besucht und jede Eingabe die gemacht wird kann mitgelesen werden. Insbesondere die Polizei und natürlich auch der Staatsschutz haben ein reges Interesse daran Aktivist*innen einschätzen zu können. Wird der Internetanschluss überwacht, lassen sich erstaunlich detailierte Persönlichkeitsprofile erstellen. Was isst die Person gerne, wofür interessiert sie sich, mit welchen anderen politischen Vereinigungen kann sie sich identifizieren, wie gewaltbereit ist die Person… Die Liste lässt sich beliebig lange in alle denkbaren Richtungen erweitern. Jeder Seitenaufruf im Internet liefert ein weiteres Puzzleteil , dass Polizei und Staatsschutz dabei hilft dich besser kennen zu lernen und wenn sie dich erst gut genug kennen, fällt es ihnen viel leichter dich an politischer Arbeit zu hindern oder es zumindest zu erschweren. Es sei denn du lässt dir beim Surfen nicht über die Schulter schauen.

Wie funktioniert die Überwachung im Internet?

Grundsätzlich gibt es zwei Möglichkeiten wie deine Freiheit durch staatliche Überwachung eingeschränkt werden könnte. Zum einen kann es passieren, dass dein kompletter Internetanschluss überwacht wird und zum anderen kann es passieren, dass eine Internetseite, die du besuchst, überwacht wird.

Die komplette Überwachung des Internetanschlusses:

Wenn du eine Seite im Internet aufrufst wirst du zuerst einmal mit deinem Internetanbieter verbunden. Der Internetanbieter leitet dich dann an die entsprechende Seite weiter. Er sieht also exakt welche Seiten du aufrufst und es ist ihm möglich alle Seitenaufrufe eines Benutzers zu speichern. Eine Überwachung deines Internetanschlusses wird über deinen Internetanbieter durchgeführt. Dieser speichert dann einfach sämtliche Verbindungsdaten, also zum Beispiel wann du welche Seiten aufgerufen hast, und leitet diese an die Behörden weiter.

Die Überwachung einzelner Seiten:

Es kann auch vorkommen, dass einzelne Seiten überwacht werden. Hier klinken sich die Überwachungsorgane direkt an der Seite ein und speichern alle Seitenbesucher. Genau genommen speichern sie die IP Adressen der Seitenbesucher. Über diese IP Adressen lässt sich mit Hilfe des Internetanbieters der genaue Internetnutzer feststellen welcher auf die Seite zugegriffen hat. Aber nicht nur staatliche Überwacher können dich anhand deiner IP-Adresse orten. Auch für Privatpersonen ist es technisch leicht möglich den Benutzer anhand seiner IP Adresse auf einem Gebiet mit dem Radius von 50 – 100 Metern zu orten. Das funktioniert über die Zurückverfolgung deines Verbindungsweges bis zum kleinsten Subnetz. Es ist aber nur möglich den ungefähren Standpunkt herauszufinden und nicht den einzelnen Nutzer, auch funktioniert das Verfahren noch nicht absolut fehlerfrei (Stand Juni 2010).

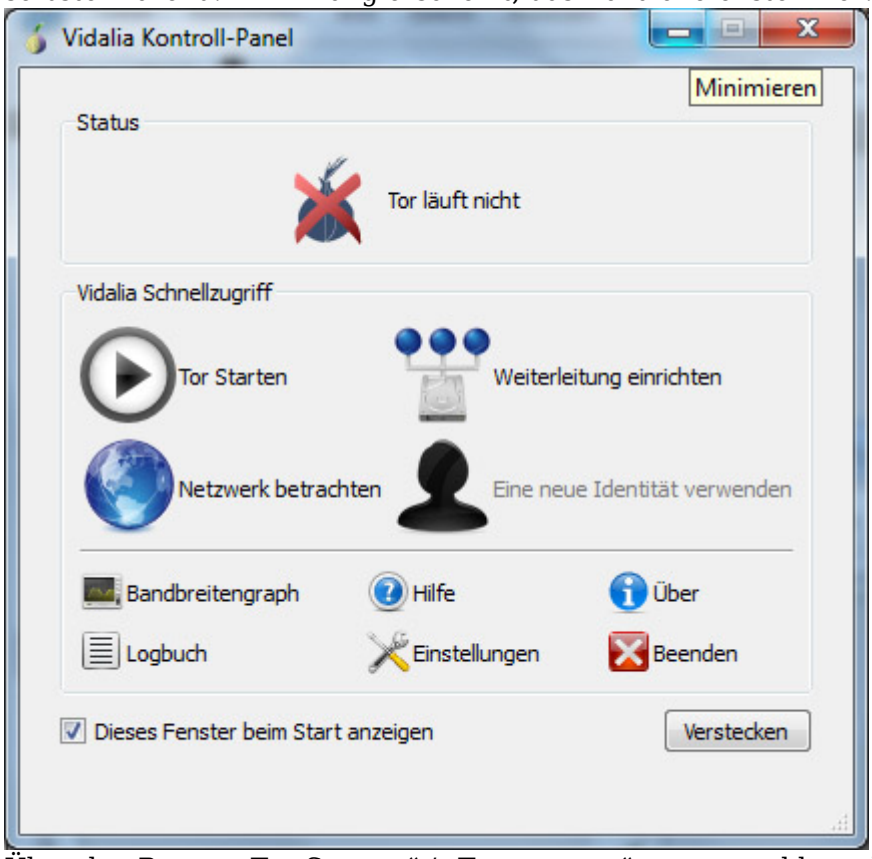
Was kann ich gegen die Überwachung unternehmen?

Eine sehr gute Möglichkeit die Überwachung deines Internetanschlusses zumindest erheblich zu erschweren ist die Verwendung eines Netzwerks zur Anonymisierung. Und das funktioniert

folgender Maßen. Über deinen Internetanbieter verbindest du dich mit dem Netzwerk, dort wirst du über drei Zwischenpunkte zur gewünschten Website weitergeleitet. Der Trick dabei ist, dass für den Internetanbieter nur der erste Zwischenpunkt sichtbar ist, alles was danach kommt, kann nicht mehr (oder nur extrem schwer) überwacht werden. Auch die Daten, die zum ersten Zwischenpunkt gesendet werden sind nicht verwertbar, da die Verbindung, über die diese Daten übertragen werden, verschlüsselt ist. Falls die Seite die du besuchst überwacht wird, bist du auch nicht identifizierbar. Du kannst nur bis zu dem dritten Zwischenpunkt verfolgt werden (wenn mensch von der besuchten Internetseite ausgeht der erste Zwischenpunkt). Lediglich die Zwischenpunkte könnten aufzeichnen von wem sie Daten erhalten und wohin sie die Daten weiterleiten. Solche Netzwerke zur Anonymisierung sind die wohl beste Möglichkeit sich gegen den Überwachungs- und Kontrollwahn zu wehren. Das gängigste kostenfreie Netzwerk ist TOR.

Wie verwende ich TOR?

Zu allererst muss die Software natürlich installiert werden. Windows Benutzer haben es hier leichter. Unter http://www.torproject.org/download.html.de gibt es das „Tor Browser Bundle für Windows“, ein Paket in dem alles Nötige enthalten und bereits vorkonfiguriert ist. Das Paket muss einfach installiert und dann gestartet werden. Vor dem Benutzen sollte mensch sich die Warnungen auf der Seite http://www.torproject.org/download.html.de#Warning durchlesen, damit mensch das Programm auch richtig bedient. Tor startet beim Einschalten des PC’s dann von selbst (oder ist in deiner Startleiste unter Vidalia Bundle -> Vidalia zu finden), die Bedienung ist relativ selbsterklärend. Am Anfang erscheint, das Kontrollefenster hier:



Über den Button „Tor Starten“ / „Tor stoppen“ startet und beendet mensch die Verbindung zum Tor-System.

Aber Achtung: Nur weil du Tor gestartet hast verwendest du nicht automatisch eine anonyme Verbindung. In deinem Internetprogramm (Firefox) siehst du unten rechts entweder „Tor deaktiviert“ oder „Tor aktiviert“. Durch klicken auf den Schriftzug kann in den jeweils anderen Modus geschalten werden. Nur wenn du Tor über das Kontrollfenster gestartet und den Modus im Internetprogramm auf „Tor aktiviert“ geschaltet hast surfst du anonym. Wenn du dir nicht sicher

bist ob du alles korrekt gemacht hast, kannst du einfach diese (leider englischsprachige) Seite hier besuchen: http://check.torproject.org/. Dort wird dir dann angezeigt ob du Tor verwendest oder nicht (durchgestrichene Zwiebel = Tor wird nicht verwendet; grüne Zwiebel = Tor wird verwendet). Da aber zum Glück nicht alle Menschen nur Windows benutzten gibt es hier zwei Konfigurationsanleitungen mit denen auch mit OSX und UNIX unerkannt gesurft werden kann.
Tor unter OSX: http://www.torproject.org/docs/tor-doc-osx.html.de
Tor unter UNIX: http://www.torproject.org/docs/tor-doc-unix.html.de
Falls ihr keinerlei Internetseiten aufrufen könnt, habt ihr zwar Tor im Internetprogramm (Firefox) aktiviert, aber über das Startfenster (Vidalia) noch keine Verbindung zum Tor-Netzwerk aufgebaut.

Gibt es Nachteile an TOR?

Natürlich gibt es auch bei TOR Nachteile. Da du die Internetseiten über 3 Zwischenpunkte aufrufst, dauert auch die Datenübertragung entsprechend länger. Konkret heißt dass, du musst länger warten bis dein Computer die Internetseite, die du besuchst, geladen hat. Da optimalerweise aktive Inhalte deaktiviert wurden (mehr dazu später) hat das zur Folge, dass diese auch nicht mehr genutzt werden können. Betroffen sind unter anderem:

- das Anzeigen und Abspielen von Videos, die auf der Seite eingebunden sind
- das Öffnen von PDF-Dokumenten im Internetprogramm selbst (PDF-Dateien werden alternativ einfach heruntergeladen und auf dem PC gespeichert)
- das sogenannte Java-Script, das zum Beispiel für die Konfigurationsleiste bei Forenbeiträgen verwendet werden kann, sowie für viele andere dynamische Seiteninhalte
- das Flash-Format was teilweise auf Fotogalerieseiten eingesetzt wird

Diese aktiven Inhalte sind bei der Verwendung von Tor standartmäßig deaktiviert und müssen erst durch den Benutzer aktiviert werden (wovon wir abraten).
TOR baut keine verschlüsselte Verbindung zur aufgerufen Seite auf (die Verschlüsselung beschränkt sich auf das Tor-Netzwerk). Das hat zur Folge, dass alle Eingaben, die dort getätigt werden am letzten Zwischenpunkt von TOR mitlesbar sind, wenn eine unverschlüsselte Seit angefordert wird. Problematisch ist das eigentlich nur wenn mensch sich auf der Seite mit Benutzername und Passwort registrieren muss. In diesem Fall sind die Anfrage und die Antwort auf diese Anfrage zwischen dem letzten Knotenpunkt und dem Server mitlesbar. Bei E-Mail-Anbietern die keine verschlüsselte Verbindung verwenden (verschlüsselte Verbindungen sind erkennbar an **https:**\\beispielwebseite.de) ist hier auch der komplette Inhalt der Mails zu lesen. Zum Umgang mit E-Mails gibt es hier einen Artikel, der auch eine Lösung für dieses Problem bietet. Dort wird jedoch nur auf das Verschlüsseln von E-Mail-Inhalten eingegangen, ein anonymes Abrufen von E-Mails ist über Tor möglich (jedoch nicht gerade eine der am leichtesten zu nutzenden Funktionen). Wer technisch etwas versierter ist, kann natürlich auch seine Mails anonym abrufen, im Allgemeinen sollte aber eine Verschlüsselung (so wie im oberen Link beschrieben) für einen sicheren E-Mail-Verkehr sorgen.

Gibt es Möglichkeiten wie ich trotz TOR identifiziert werden kann?

Kooperation der Netzwerkbetreiber

Zu allererst ist zu sagen, dass TOR im Allgemeinen einen sehr hohen Sicherheitsstandart hat aber natürlich gibt es auch hier Risiken. In der Vergangenheit ist es bereits vorgekommen, dass die Betreiber von Netzwerken zur Anonymisierung mit Überwachungsorganen kooperiert haben. Das

heißt, sie haben den Behörden offengelegt wo sie den Benutzer innerhalb ihres Netzwerkes weitergeleitet haben. Dadurch konnte dann sozusagen der Verschleierungseffekt aufgehoben werden. Dagegen ist Tor relativ gut gewappnet, da es keinen Betreiber im eigentlichen Sinne gibt. Die Zwischenpunkte gehören weder einem Betreiber noch sind sie für diesen einsehbar. Zwischenpunkte sind oft Rechner von Einzelpersonen, die dann die Weiterleitung übernehmen. Für diese Einzelpersonen wäre es möglich festzustellen woher die Daten kommen und wohin sie gehen. Eine Überwachung ist also nur möglich wenn die Daten über 3 Zwischenpunkte geschleust werden, die erstens ausgewertet werden und zweitens untereinander vernetzt sind. Die Wahrscheinlichkeit, dass dies passiert ist aber verschwindend gering. An technisch Versierte können wir nur die Bitte aussprechen ihren Rechner dafür zur Verfügung zu stellen und ein weltweites anonymes Internet zu unterstützen.

Aktive Inhalte

Wie oben schon erwähnt sollten aktive Inhalte deaktiviert werden da diese dazu gebracht werden können Informationen über deinen Rechner oder dein Internetprogramm (Browser: Firefox, Internet Explorer, Opera, …) preiszugeben. Anhand dieser Informationen ist es möglich den verwendeten Rechner relativ eindeutig zu identifizieren. Wenn also dein PC beschlagnahmt wird oder sich Überwachungsorgane in ihn einklinken, können sie die Daten, die sie aus den aktiven Inhalten haben, mit deinem Rechner vergleichen und mit relativer Genauigkeit feststellen ob du die entsprechenden Seiten aufgerufen hast. Aktive Inhalte sind in der vorkonfigurierten Version von Firefox (aus dem Tor Browser Bundle für Windows) standartmäßig deaktiviert.

Cookies

Cookies sind Dateien, die eine Internetseite auf deinem Rechner ablegt wenn du sie besuchst. Durch ein Auslesen der Cookies ist es möglich festzustellen welche Seiten du besucht hast. Internetseiten können in der Regel nur Cookies auslesen, die von ihnen selbst stammen, manchmal kann es passieren, dass über sogenannte „tracking cookies“ auch Cookies ausgelesen werden können, die nicht von der Internetseite selbst stammen. Dadurch ist es möglich genau festzustellen für was sich der / die NutzerIn noch so interessiert. Alle Cookies sind ganz normal auf dem PC abgelegt und können daher im Falle einer Beschlagnahmung oder ähnlichem auch ausgewertet werden. Wenn also die Cookies und die sogenannte History (eine weitere Auflistung der besuchten Seiten) über längere Zeit nicht gelöscht wurden, ist das eine lückenlose Auflistung aller besuchten Seiten mit konkreter Angabe wann diese besucht wurden. Leider ist es im Falle einer Beschlagnahmung auch möglich bereits gelöschte Daten wiederherzustellen. Deshalb empfehlen wir euch dazu, das How To zum sicheren Umgang mit Daten (www.kreaktivisten.org Leitfaden befindet sich derzeit noch in Arbeit) durchzulesen, was euch im Falle einer Beschlagnahmung sicherlich auch weiterhelfen sollte. Vermeiden lässt sich das ansammeln von Cookies zum einen durch ein regelmäßiges Löschen der Cookies (ansonsten sammeln sich bis zu 3.000 Cookies an bis diese automatisch überschrieben werden). Manche Internetprogramme bieten die Möglichkeit Cookies direkt beim Schließen des Programmes zu löschen. Diese Einstellung ist auf jeden Fall sinnvoll und sollte getätigt werden, da so nur die Seiten ausgelesen werden können, die seit dem Programmstart besucht wurden. Für Firefox funktioniert das Einstellen folgendermaßen: Firefox öffnen -> auf „Extras“ klicken -> dort „Einstellungen…“ auswählen -> in der Kategorie „Datenschutz“ auf den Button „Einstellungen…“ klicken -> ein Häkchen in alle Kästchen, die man automatisch löschen lassen will, setzen > alle Fenster durch den OK Button schließen. Wir empfehlen in jedes Kästchen ein Häkchen zu setzen, da so auch die entsprechenden Spuren gelöscht werden und nicht gleich zurückverfolgt werden kann was du die letzten Jahre so im Internet getrieben hast. Es besteht auch die Möglichkeit das Speichern von Cookies generell zu deaktivieren. Dadurch können aber einige Seiten nicht mehr aufgerufen oder fehlerfrei angezeigt werden. Durch ein komplettes Deaktivieren der

Cookiespeicherung ist also mit erheblichen Einschränkungen zu rechnen, die in Hinsicht auf das Sicherheitsrisikio, das entsteht nicht in Relation stehen.

Genauere Informationen

Wer sich über die exakte Funktionsweise von Tor informieren will, kann das unter http://www.torproject.org/overview.html.de#thesolution tun. Bei unserer Beschreibung handelt es sich nur um eine vereinfachte Beschreibung des gesamten Prozesses, die aber ausreichen sollte, um mit Tor sicher arbeiten zu können.