SICHERES SURFEN

Viele Menschen glauben, dass das Surfen im Internet anonym sei und die abgerufenen und gesendeten Informationen sicher übertragen würden. Dies ist jedoch grundsätzlich erst mal nicht richtig: Jede/r InternetbenutzerIn hinterlässt andauernd Spuren im Netz, und genau genommen kann man sich meistens nicht vollständig sicher sein mit wem man da gerade Daten austauscht und dass die unterwegs aber auch nachdem sie schon angekommen sind niemand anderes mehr zu Gesicht bekommt.

Grundsätzlich muss unterschieden werden zwischen Privatsphäre und Sicherheit. Zur Privatsphäre zählt zum Beispiel die Möglichkeit, sich pseudonym oder gar anonym im Netz zu bewegen, während die Möglichkeit Informationen auf sicherem Weg zu übertragen, also ohne dass sie unterwegs verändert oder abgehört werden können, zum Bereich der Informationssicherheit gehört.

Für AktivistInnen ist je nach Anwendungsfall häufig beides wichtig, weshalb diese beiden Bereiche auch oft vermischt werden, die Privatsphäre aber häufig ganz besonders. So kann die Exekutive durch Anfragen bei ServerbetreiberInnen herausfinden, ob von einem bestimmten Internetzugang auf bestimmte Webseiten zugegriffen wurde und teilweise ist auch aus den Protkollen des Servers ersichtlich, welche Daten durch jemanden dorthin geschickt wurden. Wer Dateien ins Internet hochlädt sollte sich ausserdem bewusst sein dass diese häufig auf den ersten Blick nicht sichtbare zusätzliche Daten (‘Metadaten’) enthalten, die mitunter Rückschlüsse auf den/die UrheberIn zulassen.

SSL

Um erst mal kurz auf Informationssicherheit einzugehen: Verschlüsselung ist bei politischer Arbeit ein Muss- und das auch beim Surfen/Arbeiten im Netz. Eine Webseite ruft ihr dann verschlüsselt auf, wenn vorne HTTPS statt HTTP steht. Damit ist dann fast garantiert (hängt natürlich von der Serverkonfiguration ab), dass alle Daten, die ihr an den Server schickt und auch die, die ihr von dem Server holt (also welche Seiten ihr euch anseht!) über eine verschlüsselte Verbindung geführt werden. Somit wird dann eine Anfrage der Exekutive an eure InternetanbieterIn nur zu der Information führen, dass ihr auf einen gewissen Server zugegriffen habt, aber nicht, was ihr euch darauf angesehen habt.

Suchmaschinen

Da ohne Suchmaschinen die Recherche im Netz schwer möglich ist, können SuchmaschinenanbieterInnen auch bestens eure Daten sammeln. Nicht nur Google, sondern auch Bing von Microsoft oder Yahoo sammeln eure Suchanfragen und werten diese aus. Doch noch mehr: Google ist ja auch im Besitz von der Videoplattform Youtube, DoubleClick (einem der grössten AnbieterInnen von Onlinewerbung) sowie reCAPTCHA, das von andere Webseiten zur Spambekämpung verwendet wird (wobei dann wiederum Daten an Google übertragen werden). Ausserdem bietet Google ‘Google Analytics’ an, eine Software, die WebseitenbetreiberInnen in die eigene Website einbinden können, um Statistiken über die BesucherInnen zu erstellen. Auch hier werden die Daten wiederum an Google gesendet. Ein Drittel der grössten 500 Webseiten nutzt Google Analytics.

Die Gefahr von Datensammlung durch Suchmaschinen ist schon länger bekannt. Alternative Suchmaschinen sind zum Beispiel Ixquick (löscht IP-Adressen und andere personenbezogene Daten nach 48h und gibt die Daten nicht weiter), das deutsche Projekt Metager2, das von einem gemeinnützigen Verein betrieben wird, oder Scroogle, eine Website, die die Suchanfrage an Google weiterleitet, wobei sie anonymisiert wird. All diese Suchmaschinen werden auch über HTTPS angeboten, woduch dann sowohl die Informationssicherheit als auch der Schutz der Privatsphäre gewährt ist.

Browsererweiterungen, die das Leben im Netz etwas sicherer machen

Wir beschränken uns hier auf Erweiterungen für den Browser Firefox, da dieser Browser sehr weit verbreitet ist, es gibt ihn für viele Betriebssysteme und es existieren enorm viele Sicherheits- und Privacyerweiterungen dafür.

Wie oben schon erwähnt, sammelt Google eure Daten nicht nur über die Suchfunktion. Da ihr beim Surfen im Netz andauernd Spuren hinterlasst und Datenkrümel auf eurem Computer abgespeichert werden, die dann wiederum von Webseiten ausgelesen werden können, kann mit der Zeit ein genaues Profil von euren Surfgewohnheiten erstellt werden. Google merkt sich von welcher IP Adresse aus ihr diese Suche getätigt habt und speichert ein Cookie (eine Textdatei) auf eurem Computer, anhand derer Google euch auch dann noch ‘wiedererkennen’ kann, wenn sich eure IP-Adresse geändert hat.

Eine Erweiterung, die gegen diese Datensammelwut hilft ist ‘Google-Sharing’. Wenn Google-Sharing installiert ist, werden die Anfragen, die euer Browser an Google schickt zuerst an einen Server vom Google-Sharing Projekt geschickt und dort Anonymisiert (dies bezieht sich nur auf die Google Services, wo kein Login benötigt wird). Dann erst werden die Daten an Google weitergeleitet. Der Server, über den die Daten geleitet werden wird Proxyserver genannt. Das Riseup-Kollektiv bietet mittlerweile einen eigenen Google-Sharing Proxy Server an, den Link dazu findet ihr am Ende des Flyers.

Die Erweiterung ‘HTTPS-Everywhere’ hilft bei der Informationssicherheit. Sie macht die Datenübertragung insofern sicherer, dass sie dafür sorgt, dass Seiten immer über eine verschlüsselte Verbindung aufgerufen werden. Dies geht jedoch nicht einfach überall, sondern es müssen händisch Regeln dafür geschrieben werden, was aber momentan schon sehr intensiv von engangierten AktivistInnen gemacht wird. So werden zum Beispiel die Server von Wikipedia, Google oder Facebook nach Installation der Erweiterung nur noch verschlüsselt aufgerufen.

Ein weiteres Problem im Netz sind sogenannte Skripte. Das sind kleine Programme, die in Webseiten eingebaut werden und die euer Browser dann herunterlädt, um sie auf eurem Computer auszuführen. Dies kann ein grosses Sicherheitsrisiko darstellen. Die Erweiterung ‘NoScript’ sorgt dafür dass solche Skripte nur noch von Seiten kommen dürfen, von denen ihr das vorher ausdrücklich erlaubt habt.

Die Erweiterung ‘Adblock Plus’ versucht, die ganze Werbung, mit der ihr beim Surfen zugemüllt werdet, zu unterbinden. Dies schützt nicht nur eure Nerven, denn somit wird Onlinewerbung von externen Servern oft gar nicht mehr geladen, so dass Werbenetzwerke nicht mehr Cookies setzen und Cookie-unabhängig Profile bilden können.

Die Erweiterung ‘Beef Taco’ unterbindet das Abpseichern von Cookies für über 100 verschiedene Werbenetzwerke.

Wer nicht jedes mal, wenn eine Webseite besucht wird, mitteilen möchte, welcher Webbrowser und welches Betriebssystem und welche Versionen davon verwendet werden, kann die Erweiterung ‘User Agent Switcher’ nutzen.

Weitere Erweiterungen (für Privatsphäre): BetterPrivacy, CookieSafe, FoxyProxy, RequestPolicy; Erweiterung für Informationssicherheit: Certificate Patrol, Force-TLS

Um zu überprüfen, wie wiedererkennbar euer Browser ist, könnt ihr die Webseite panopticlick.eff.org der Electronic Frountier Foundation, die ‘Fingerabdrücke’ von Browsern vergleicht. Eine weitere Webseite, die aufzeigt, welche Daten euer Browser preisgibt, ist browserspy.dk

Metadaten – Daten in den Daten

Wenn ihr Dateien im Internet veröffentlicht, seien es Fotos, Videos, Texte, etc, dann lauft ihr Gefahr, mehr von euch preiszugeben als euch lieb ist. Wenn ihr mit eurer Digitalkamera ein Photo macht, dann speichert die Digitalkamera nicht nur das Photo, sondern in dem Photo werden zusätzlich auch vermerkt, welches Kameramodell das Photo gemacht hat, zu welcher Uhrzeit an welchem Tag, wie die Belichtung war- manche Kameras mit GPS speichern sogar den Ort. Dasselbe passiert natürlich wenn ihr mit eurem Handy Photos macht. Diese Daten nennen sich Metadaten, im Falle von Photos gibt es dafür einen Standard namens Exif (Exchangable Image File Format), ein anderer heisst IIM (Information Internchange Model). Oft wird bei Photos auch ein Vorschaubild als Metadatum abgespeichert- wenn ihr dann in eurem Bildbearbeitungsprogramm die Gesichter auf den Fotos der letzten Aktion unkenntlich macht, bleiben sie in den Metadaten unverändert! Um zu sehen, welche Metadaten in euren Fotos vorhanden sind, könnt ihr Fotoverwaltungsprogramme oder die Webseite regex.info/exif, mit der ihr auch Metadaten von Fotos im Web ansehen könnt, verwenden.

Auch bei Videos kann es sein, dass abgespeichert wird, mit welcher Software das Video bearbeitet wurde. Wenn ihr solche Dateien ins Internet stellt, dann ist es nötig, dass ihr vorher darauf achtet, welche Metadaten in den Dateien drin sein können und wie ihr sie entfernen könnt. Durch die Metadaten können Rückschlüsse auf eure Identität gezogen werden!

Auch bei PDF Dateien können Metadaten drin sein, so speichert zum Beispiel OpenOffice bei der Erstellung eines PDFs als Metadatum ab, dass das PDF mit OpenOffice erstellt wurde und wie euer BenutzerInnenname lautet. Textverarbeitungsprogramme wie Microsoft Word haben immer wieder Aufmerksamkeit erregt, da die ganze Erstellungsgeschichte des Dokuments mitabgespeichert wurde. So war es sogar möglich, gelöschte Passagen aus Dokumenten wieder erscheinen zu lassen.

Also macht euch schlau, bevor ihr Dateien ins Netz stellt und durch unvorsichtigen Umgang euch und andere gefährdet.

Suchmaschinen:
https://www.ixquick.com
https://www.metager2.de
https://ssl.scroogle.org
Riseups Googlesharing Service
https://we.riseup.net/riseuphelp/googlesharing
Spuren, die ihr hinterlasst
https://panopticlick.eff.org
http://browserspy.dk
Metadaten in Fotos
http://regex.info/exif

tear the system down - bit. by. bit. mailto:bitbybit@riseup.net
technologie in linksradikalen kontexten https://we.riseup.net/bitbybit