Privacy Guide

Anleitung zur Wahrung der Privatsphäre im Internet

Version: 3.0

Autor: Lioh Möller

Inhaltsverzeichnis

Einführung

«Die gute Nachricht: Wir wissen jetzt, das wir nicht paranoid sind!
... die schlechte Nachricht: Wir werden alle überwacht. Jetzt und überall.»

Angesichts zunehmender Überwachung des Internets und Kooperationen von Firmen mit Geheimdiensten ist es an der Zeit, die eigene Privatsphäre selbst zu schützen.

Im Folgenden wird beschrieben was notwendig ist, um das Recht auf Privatsphäre auch im Internet zu wahren. Die Einstellungen, beziehen sich auf die englischsprachigen Versionen des Freien Webbrowsers Firefox und des E-Mail-Clients Thunderbird.

1. Freie Software

Bei Freier Software handelt es sich um Programme, bei denen der Quelltext einsehbar ist und die unter bestimmten Lizenzbedingungen verändert und weitergegeben werden dürfen. Dadurch entsteht die Möglichkeit, den Programmcode zu untersuchen und potenzielle Hintertüren zu entdecken. Bei proprietärer Software ist der Quelltext nicht einsehbar, wird aber auf Anfrage von einigen Herstellern zur Verfügung gestellt.

Grundsätzlich ist keine Software vor Infiltrierung durch Dritte geschützt. Bei grossen Projekten wie z.B. dem Linux Kernel muss der Programmcode durch eine oder mehrere Personen geprüft und freigegeben werden, bevor er veröffentlicht wird (das sogenannte Peer-Review).

In der Vergangenheit kam es auch im Umfeld Freier Software zu grösseren Sicherheitsproblemen, wie zum Beispiel der «Heartbleed»-Sicherheitslücke, die es Angreifern erlaubte, verschlüsselte HTTPS-Verbindungen abzuhören.

Eine Verfügbarkeit des Quelltextes alleine garantiert noch keinen Sicherheitsgewinn, sie ist aber eine wichtige Voraussetzung, um die Sicherheit in Software zu erhöhen.

Auch durch KI gefundene Sicherheitslücken haben dazu beigetragen, ein grösseres Bewusstsein für die Notwendigkeit von Softwareauditierungen zu schaffen, und sie haben vor Augen geführt, dass Sicherheit auch Geld kostet.

2. Spurenarmes Surfen

Beim Surfen im Internet hinterlässt man eine Vielzahl von Datenspuren, die von Diensteanbietern genutzt werden können. In erster Linie dienen sie zur Ermittlung von Vorlieben, um auf den Anwender zugeschnittene Werbung oder Suchergebnisse anzeigen zu können. Gerade bei der Online-Suche kann das schnell zu einer sogenannten «Filter Bubble» führen.

Isst man beispielsweise gerne asiatisch und hat in der Vergangenheit bei einem Suchanbieter wie Google nach asiatischen Restaurants gesucht, besteht eine sehr hohe Wahrscheinlichkeit, dass man in Zukunft in erster Linie asiatische Restaurants als Suchergebnis erhält.

Das mag zunächst harmlos klingen, in der Praxis erhält man allerdings fast nur noch Suchresultate, die bereits dem eigenen Interessensbild entsprechen, und erfährt möglicherweise gar nichts mehr von anderen Inhalten, die auch interessant sein könnten.

Mit den folgenden Einstellungen, hinterlässt man deutlich weniger Spuren im Netz.

2.1. Global Privacy Control (GPC)

Seit einigen Jahren gibt es die Möglichkeit, einem Webseitenbetreiber mitzuteilen, dass man nicht verfolgt werden möchte.

Im Firefox aktiviert man diese Einstellung, indem man in den **Settings** unter dem Punkt **Privacy & Security** die Option *Tell websites not to sell or share my data* wählt. In einigen US-Bundesstaaten wie Kalifornien, Colorado und Connecticut fungiert Global Privacy Control (GPC) als „Do Not Sell“-Mechanismus. Da es aber ausserhalb dieser Regionen keinen verbindlichen rechtlichen Rahmen für die Funktion gibt, respektieren nur wenige Seitenbetreiber diese Einstellung.

2.2. 3rd-Party-Cookies

Grundsätzlich kann man sagen, dass Cookies weder schlecht noch gefährlich sind. Sie dienen beispielsweise dazu, eine Sitzung aufrecht zu erhalten.

Beim Aufruf einer Webseite kann ein Cookie für die spätere Nutzung gesetzt werden. Beim nächsten Zugriff auf diese Webseite, schickt der Browser automatisch den Cookie mit. Der Anbieter kann mithilfe des Cookies den Nutzer eindeutig zuordnen.

Ein besonderer Fall sind 3rd-Party-Cookies. Dabei handelt es sich um reguläre Cookies, die aber nicht direkt zur aufgerufenen Webseite gehören.

Es wird zum Beispiel ein Facebook-Like-Button in eine Webseite eingebunden. Der Button wird direkt von Facebook geladen und muss nicht angeklickt werden, um den Cookie zu setzen. Der Prozess passiert im Hintergrund.

Wenn man 3rd-Party-Cookies deaktiviert, werden keine Cookies mehr für Webseiten gesetzt, die nicht direkt aufgerufen worden sind.

Die Option zum Deaktivieren von 3rd-Party-Cookies ist im Firefox etwas versteckt. In den **Privacy & Security** Einstellungen stellt man zunächst im Bereich **Enhanced Tracking Protection** von *Standard* auf *Custom* um. Danach kann man unter **Choose which trackers and scripts to block** bei **Cookies** entweder *Cross-site Tracking Cookies and Isolate other cross-site Cookies* wählen oder mit *All cross-site cookies* 3rd-Party-Cookies komplett deaktivieren.

Firefox bietet ausserdem die Option, alle Cookies beim Beenden des Browsers zu löschen, was aber zum Komfortverlust führen kann.

2.3. uBlock Origin

uBlock Origin[1] hat sich über die Jahre gewissermassen zum Standard-Adblocker gemausert. Damit lässt sich Werbung unterbinden und auch Tracking wird minimiert. Die Erweiterung lässt sich wie üblich über die Add-on-Verwaltung von Firefox installieren. Eine Konfiguration ist im Normalfall nicht notwendig, da das Add-on mit sinnvollen Standardwerten ausgeliefert wird. Sollte eine Webseite einmal nicht korrekt dargestellt werden, kann die Erweiterung für diese gezielt deaktiviert werden. Für alle beschriebenen Add-ons wird empfohlen, das Symbol für den einfachen Zugriff an die Adressleiste anzupinnen. Dazu klickt man auf das Puzzle Teil und wählt *Pin to Toolbar*.

1 https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/

2.4. NoScript

Das Firefox-Add-on NoScript[2] ermöglicht es, für jede Webseite gezielt einzustellen, ob aktive Elemente (sogenannte Scripts) ausgeführt werden sollen oder nicht. Dabei wird der Ansatz verfolgt, dass standardmässig alle Scripts verboten sind, und pro Webseite freigeschaltet werden müssen.

Nach der Installation des Add-ons findet man ein entsprechendes Symbol neben der Adressleiste. Sollten auf einer Seite Scripts blockiert worden sein, öffnet sich zusätzlich eine Benachrichtigung im unteren Bereich des Browserfensters.

Über einen Klick auf das Symbol öffnet sich eine Liste aller auf der Webseite eingebundener Scripts. Angegeben wird jeweils der Name der Webseite, von der versucht wird, das Script zu beziehen. Besucht man z.B. die Webseite der New York Times, wird in der Liste nicht nur nytimes.com aufgeführt, sondern auch eine Vielzahl weiterer Webseiten wie z.B. Google, von denen weitere Scripte bezogen werden. In den meisten Fällen kommen diese Scripts von Werbeanbietern oder Analyseseiten und werden zur Identifikation und zum Tracking genutzt.

Sollte eine Webseite nicht mehr wie gewünscht dargestellt werden, kann man schrittweise Scripts von fremden Webseiten temporär zulassen, bis der Inhalt wieder korrekt dargestellt wird. Nachdem man so herausgefunden hat, welche Scripts freigeschaltet werden müssen, kann man diese permanent zulassen. Einstellungen bei NoScript gelten immer global. Es ist nicht möglich, den Zugriff auf z.B. googleapis.com für eine Webseite zuzulassen, für eine andere aber zu sperren. NoScript ist durch seinen sehr restriktiven Ansatz eher für erfahrene Anwender zu empfehlen, die auch aufwändigere Konfigurationseinstellungen nicht scheuen. Ist diese Hürde einmal gemeistert, bietet es einen sehr hohen Schutz.

2.5. Tracker Blocker

Tracker nutzen auf Webseiten eingebundene Elemente, um zu verfolgen, welche Webseiten besucht worden sind. Einen wirksamen Schutz gegen Tracker bietet das Add-on Privacy Badger[3]. Es wird von der EFF (Electronic Frontier Foundation) entwickelt, einer Organisation, die sich für Grundrechte im Informationszeitalter einsetzt. Das Add-on benötigt nach der Installation keine besondere Konfiguration und kann ebenfalls für einzelne Webseiten deaktiviert werden, sollten diese nicht wie erwartet dargestellt werden.

2.6. User-Agent-String

Bei jedem Aufruf einer Webseite werden der Name und die Version des verwendeten Browsers an den Webseitenbetreiber übermittelt, der sogenannte User-Agent-String.

Anhand dieser und weiterer Informationen, wie der verwendeten Bildschirmauflösung oder der auf dem System installierten Schriften (die z.B. mithilfe eines JavaScripts ausgelesen werden können), kann ein Benutzer sehr verlässlich identifiziert werden.

Eine mögliche Gegenmassnahme ist es, den User-Agent-String bei jedem Aufruf einer Webseite zu wechseln. Zu diesem Zweck eignet sich das Add-on Random User-Agent (Switcher)[4]. Das Plugin synchronisiert den User Agent standardmässig mit dem des verwendeten Browsers. Bei Firefox wird daher weiterhin Firefox als Browser signalisiert,

2 https://addons.mozilla.org/en-US/firefox/addon/noscript/
3 https://www.eff.org/privacybadger
4 https://addons.mozilla.org/en-US/firefox/addon/random_user_agent

das verwendete Betriebssystem jedoch zufällig entweder als Windows, macOS oder als Linux ausgegeben.

Sollte es Probleme mit der Darstellung einer bestimmten Webseite geben, kann die Erweiterung gezielt für einzelne Seiten deaktiviert werden.

2.7. CookieBlock

Das an der ETH Zürich entwickelte[5] Add-on CookieBlock bewertet Cookies automatisch anhand von vier Kategorien: „Notwendig“, „Funktionalität“, „Analytik“ und „Werbung“. In den Standardeinstellungen werden analytische Cookies und Werbungs- und Tracking-Cookies nicht akzeptiert. Bei Bedarf kann in den Einstellungen des Add-ons die Option *Cookie-Verlauf Erstellen* aktiviert werden. Damit wird ein separater Verlauf von Cookies gesammelt, welcher Websites und anderen Erweiterungen unzugänglich bleibt. Dieser Verlauf verlässt niemals den internen Speicher der Erweiterung, und ermöglicht es CookieBlock, die Genauigkeit der Kategorisierung zu verbessern.

2.8. I still don't care about cookies

Bei der Erweiterung *I still don't care about cookies*[6] handelt es sich nicht um eine eigentliche Sicherheitsverbesserung. Sie dient lediglich als Komfortfunktion, indem sie lästige Cookie-Banner ausblendet. Dabei stellt das Add-on nicht sicher, dass beim Beantworten des Cookie-Banners eine datenschutzfreundliche Auswahl getroffen wird. Daher ist *I still don't care about cookies* nur in Kombination mit CookieBlock zu empfehlen, welches das Speichern von unerwünschten Cookies tatsächlich unterbindet.

2.9. Standort

Standortdaten sind wie das Öl in den Motoren der Werbeindustrie. Sie gelten als besonders wertvoll und daher wird mit allen möglichen Tricks versucht, den Standort zu ermitteln. Um es den Werbetreibenden etwas zu erschweren, kann man in Firefox im Bereich **Permissions** für **Location** den Punkt *Block new requests asking to access your location* aktivieren.

Leider reicht dies alleine nicht aus und daher empfiehlt sich die Verwendung des Add-ons Spoof Geolocation[7]. Damit ist es möglich, einen Fake-Standort zu setzen und diesen zu übertragen. Laut der Add-on-Dokumentation befüllt das Plugin das *navigator.geolocation*-Objekt mit dem Fake-Standort und überträgt dieses an die Webseite. Noch besser ist es allerdings, wenn man die Standortübermittlung ganz verweigert. Dazu klickt man auf das Erweiterungssymbol und deaktiviert den Haken bei *Share Location*. Bei jeder Standortanfrage wird dann das Add-on-Symbol rot eingefärbt.

2.10. Privater Modus

Firefox und viele andere Browser bieten an, ein Fenster im Privaten Modus zu starten. Im privaten Modus werden keine sensiblen Daten gespeichert und keine History angelegt. Sofern nicht explizit aktiviert, werden auch Add-ons im privaten Modus nicht genutzt.

5 https://www.research-collection.ethz.ch/server/api/core/bitstreams/72f5e7ed-4d01-4174-8b19-795e1d5ba7db/content
6 https://addons.mozilla.org/en-US/firefox/addon/istilldontcareaboutcookies
7 https://addons.mozilla.org/de/firefox/addon/spoof-geolocation

2.11. Suchmaschine

Die Anbieter Google und Bing haben sich bei der Suche im Internet stark durchgesetzt. Damit wissen sie viel über unsere Vorlieben und unser Surfverhalten. Es gibt alternative Anbieter, die zusichern, keine personenbezogenen Daten zu speichern und weiterzuverarbeiten. Dazu gehören die Suchmaschine DuckDuckGo[8], Startpage.com[9] oder die Metasuchmaschine metaGer[10], welche allerdings einen Lizenzschlüssel erfordert.

Startpage.com ist eine Suchmaschine, die im Hintergrund auf Google sowie Bing zugreift. Sie ist vollständig lokalisierbar. Es kommt keine personalisierte Suche zum Einsatz, wodurch die Gefahr einer «Filter Bubble» verringert wird.

2.12. HTTPS

Beim Zugriff auf Webseiten über HTTP werden alle Informationen unverschlüsselt übertragen, und können leicht von Dritten analysiert werden. Besonders eine Übertragung von Passwörtern über HTTP ist sehr kritisch.

Um HTTPS für möglichst viele Seiten zu forcieren, bietet Firefox einen HTTPS-Only Mode. In den Einstellungen wählt man dazu unter **Privacy & Security** den Punkt *Enable HTTPS-Only Mode in all Windows*.

2.13. DoH

DNS-Abfragen sind wie das Nachschlagen in einem Telefonbuch. Dabei wird in der Regel der DNS-Server des Internetanbieters kontaktiert. Die Übertragung erfolgt standardmässig unverschlüsselt. Protokolle von DNS-Servern sind auch bei Ermittlungsbehörden sehr begehrt, da diese auf einfache Weise wiedergeben, welche Webseiten oder Domains von einem Anschluss abgefragt wurden.

Es bietet sich an, einen DNS-Anbieter unabhängig vom eigenen Internetprovider zu nutzen, bei Bedarf auch in einem anderen Land. Anbieter wie Quad9[11] ermöglichen ausserdem die verschlüsselte Übertragung von DNS-Abfragen über DNS-over-HTTPS (DoH). Dabei werden Anfragen wie auch bei einem Besuch einer Webseite über HTTPS mittels SSL verschlüsselt.

Sowohl in Firefox als auch in Thunderbird kann DoH über den Punkt **DNS over HTTPS** aktiviert werden. Dazu muss zunächst im Bereich **Enable DNS over HTTPS using:** auf *Increased Protection* umgestellt werden. Erst dann besteht die Möglichkeit, über den Punkt **Custom** einen eigenen DoH-Server zu hinterlegen. Eine Liste der empfohlenen Einstellungen findet man auf der Quad9-Webseite[12]. Zur Nutzung von Quad9 kann im Feld **Custom** die folgende URL hinterlegt werden: *https://dns.quad9.net/dns-query*

3. Anonymes Surfen

Beim Surfen im Internet kann ein Nutzer eindeutig einem Rechner und einer IP-Adresse zugeordnet werden. Falls immer möglich, empfiehlt sich die Nutzung eines offenen, anonymen W-LAN Zugangs (z.B. in einem Café). Beachten sollte man hierbei, dass nur verschlüsselte Verbindungen über solche Verbindungen aufbauen sollten. Eine Alternative

8 https://duckduckgo.com
9 https://www.startpage.com
10 https://metager.de
11 https://quad9.net
12 https://quad9.net/news/blog/doh-with-quad9-dns-servers

bietet die Nutzung eines Anonymisierungsnetzwerkes.

3.1. Tor

Eines der bekanntesten Netzwerke, die anonymes Surfen ermöglichen, ist Tor[13]. Dabei werden Verbindungen über die einzelnen Tor-Knoten, die auf Rechnern in der ganzen Welt laufen, geleitet. Man kann Tor als Client nutzen, oder auch selbst einen Knoten anbieten, über den andere Teilnehmer surfen können. Die Verbindung zwischen den Knoten wird verschlüsselt. Die einzelnen Teilnehmer haben keinen Einblick in die übermittelten Daten. Am Endpunkt, also am Übergang zum angefragten Zielserver, muss die Verbindung wieder entschlüsselt werden. Dieser Knoten, hat Zugriff auf die übertragenen Daten. Es ist also auch hier sehr zu empfehlen, nur verschlüsselte Verbindungen aufzubauen.

Die einfachste Möglichkeit, Tor zu nutzen, ist der vom Projekt bereitgestellte Tor-Browser. Dabei handelt es sich um eine modifizierte Firefox-Version, die alle für Tor notwendigen Komponenten bereits enthält.

Alternativ kann man eine spezialisierte Linux-Distribution wie Tails[14] nutzen, die einfach auf einen USB-Stick gespielt und von dort aus gestartet und genutzt werden kann. Tails bietet ausserdem einen Windows-Tarnmodus an, in dem sich das System gegenüber Servern im Internet wie ein Windows-Rechner verhält.

Tails eignet sich hervorragend für den Einsatz auf fremden PCs, da es ein abgeschlossenes System ist, das auf dem damit gestarteten Rechner keinerlei Spuren hinterlässt.

4. E-Mail Verschlüsselung

Standardmässig werden E-Mails unverschlüsselt übertragen und können theoretisch auf allen Knotenpunkten auf dem Weg zum Ziel mitgelesen werden. Es gibt verschiedene Möglichkeiten, sich dagegen zu schützen. Die meisten E-Mail-Programme unterstützen das SSL-basierte S/MIME zur Signatur und Verschlüsselung. Eine Alternative stellt die Verschlüsselung mittels GnuPG dar.

4.1. S/MIME

Bei S/MIME handelt es sich um ein etabliertes Verfahren, bei dem SSL-Zertifikate zum Einsatz kommen. Bei einem Zugriff auf HTTPS-Webseiten, wird eine ähnliche Technologie verwendet. Es gibt verschiedene Anbieter von S/MIME Zertifikaten, nur wenige davon stellen allerdings kostenlose Zertifikate zur Verfügung.

Actalis

Einer der Anbieter für kostenlose E-Mail S/MIME Zertifikate ist die Firma Actalis aus Italien. Über die Webseite des Anbieters lässt sich ein kostenfreies, für 1 Jahr gültiges S/MIME-Zertifikat beantragen[15].

Hinweis: Um Inkompatibilitäten mit installierten Add-ons zu vermeiden, empfiehlt es sich, das Zertifikat in einem privaten Browserfenster zu beantragen.

Nach der Erstellung des Kontos beim Anbieter und der Bestätigung der E-Mail-Adresse

13 https://www.torproject.org
14 https://tails.net
15 https://www.actalis.com/de/s-mime-zertifikate

kann das Gratis-S/MIME-Zertifikat zum Warenkorb hinzugefügt werden. Im Bestellformular müssen entgegen der Angaben, das Individuum, das Land, der Vorname, der Nachname, die Adresse sowie die Telefonnummer angegeben werden, für die ein Zertifikat erstellt werden soll. Nach erfolgter Bestellung muss das Zertifikat aktiviert werden. Dazu klickt man in der Bestätigungsmail auf *Activate Now*. Im Folgenden wird die E-Mail-Adresse angegeben, für die das Zertifikat ausgestellt werden soll. Daraufhin kann mit der Verifikation begonnen werden. Dazu muss die angegebene E-Mail-Adresse bestätigt werden. An diese Adresse wird auch das Passwort geschickt, welches später zum Einbinden des Zertifikates benötigt wird.

Nach einer Zeit und gegebenenfalls einem Klick auf *Refresh Certificate Status* kann im Dashboard von Actalis das Zertifikat im .p12-Format heruntergeladen werden.

Daraufhin kann es in einem E-Mail-Programm wie Thunderbird importiert werden. Dazu wählt man in Thunderbird den Punkt *Account Settings* und wählt dort im entsprechenden E-Mail-Konto den Punkt *End-to-End Encryption*. Dort klickt man auf *Manage S/MIME Certificates*. Dadurch öffnet sich die Thunderbird-Zertifikatsverwaltung.

Unter dem Reiter *Your Certificates* klickt man auf *Import* und wählt die Zertifikatsdatei aus.

Beim Einlesen wird das per E-Mail versandte Passwort angefordert. Wenn der Vorgang erfolgreich war, klickt man auf *Ok* und wählt in den S/MIME-Einstellungen das Zertifikat für die digitale Unterschrift und die Verschlüsselung aus. Es wird empfohlen, alle Nachrichten über den Punkt *Sign unencrypted Messages* digital zu unterschreiben, da so die Kommunikationspartner in den Besitz des Public Keys kommen können.

CAcert

Bei CAcert[16] handelt es sich um eine von einem Verein betriebene Zertifizierungsstelle. Sie bietet kostenfreie X.509-Zertifikate an und betreibt ein eigenes Vertrauensnetzwerk (Web of Trust). Dazu kommt ein Punktesystem zum Einsatz. Nutzer können sich mit sogenannten Assurern persönlich treffen, ihre Identität prüfen lassen und diese gegenüber CAcert bestätigen.

Nachdem man sich bei CAcert ein Konto erstellt hat und die E-Mail-Adresse verifiziert wurde, kann man über den Punkt **Client Certificates** / **New** ein neues S/MIME Zertifikat beantragen. Die Einbindung des Zertifikates in Thunderbird erfolgt wie zuvor beschrieben.

5. Veröffentlichungen

Der vorliegende Privacy Guide wurde in unterschiedlichster Form publiziert und wird fortlaufend überarbeitet und an die aktuellen Gegebenheiten angepasst.

https://www.pcwelt.de/article/1151579/der-grosse-privacy-guide-fuer-ihre-daten-datenschutz.html

http://www.freiesmagazin.de/mobil/freiesMagazin-2015-03-bilder.html#fm_15_03_privacy_guide

https://gnulinux.ch/privacy-guide

Mit einer Spende[17] unterstützt du den Privacy Guide und machst die digitale Welt ein Stück sicherer

16 https://cacert.org
17 https://gnulinux.ch/spenden-spenden-spenden