

# Privacy Guide

Anleitung zur Wahrung der Privatsphäre im Internet



Version: 2.1

Autor: Marcus Möller

Lizenz: CC-BY

## Inhaltsverzeichnis

1.Freie Software.....	2
2.Spurenarmes Surfen.....	2
2.1.Do Not Track.....	3
2.2.3rd Party Cookies.....	3
2.3.Flash.....	3
2.4.NoScript.....	4
2.5.Tracker Blocker.....	4
2.6.User Agent String.....	4
2.7.Plugins.....	5
2.8.Safe Browsing.....	5
2.9.Referrer.....	5
2.10.Privater Modus.....	6
2.11.Suchmaschine.....	6
2.12.https.....	6
3.Anonymes Surfen.....	6
3.1.Tor.....	7
4.Email Verschlüsselung.....	7
4.1.S/MIME.....	7
Comodo.....	7
CAcert.....	8

# Einführung

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

Angeichts 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 Email Clients Thunderbird.

## 1. Freie Software

Bei freier Software handelt es sich um Programme, bei denen der Quelltext einsehbar ist und unter bestimmten Lizenzbedingungen verändert und weitergegeben werden darf. Dadurch entsteht die Möglichkeit, den Programmcode zu untersuchen und potentielle 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.

Sicherheitslücken wie «Heartbleed» haben dazu beigetragen, ein grösseres Bewusstsein für die Notwendigkeit von Softwareauditierungen zu schaffen und 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 hinterlassen Sie im Netz weniger Spuren.

## 2.1. Do Not Track

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

Im Firefox aktiviert man diese Einstellung indem man in den Settings unter dem Punkt *Privacy* die Option *Tell sites that I dont want to be tracked* wählt. Da es aber bisher weder in Europa noch in den USA einen 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 mit Hilfe 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* Einstellungen stellt man zunächst von *Firefox will Remember history* auf *Use Custom Settings for History* um. Danach kann man den Punkt *Accept third-party cookies* auf *Never* stellen.

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

## 2.3. Flash

Der Adobe Flash Player hat keine besonders ruhmreiche Vergangenheit, was Sicherheit anbelangt. Daher sollte man sich Fragen ob man nicht grundsätzlich darauf verzichten kann.

Viele Dienstanbieter wie youtube.com haben mittlerweile auf HTML5 Technologie zum Abspielen von Videos und Audiodateien umgestellt.

Mit dem HTML5 basierten Flashplayer Shumway<sup>1</sup> ist es möglich, rudimentäre Flash Inhalte ohne den Adobe Flash Player abspielen zu können.

Falls man dennoch nicht auf den Adobe Flash Player verzichten kann, sollte man den lokalen Cache deaktivieren. Die Flash Einstellungen kann man vornehmen, indem man mit der rechten Maustaste auf einen Flash-Inhalt klickt und dort *Global Settings* wählt.

Im Reiter *Storage* kann man dann den Punkt *Block all sites from storing information on this computer* wählen um die Cachefunktion abzuschalten.

---

1 <https://mozilla.github.io/shumway>

## 2.4. NoScript

Das Firefox AddOn NoScript bietet die Möglichkeit, 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 AddOns 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 haben, 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.

## 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 AddOn Privacy Badger<sup>2</sup>. Es wird von der EFF (Electronic Frontier Foundation) entwickelt, einer Organisation die sich für Grundrechte im Informationszeitalter einsetzt. Das AddOn benötigt nach der Installation keine besondere Konfiguration.

## 2.6. User Agent String

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

Anhand dieser und weiterer Informationen, wie die verwendete Bildschirmauflösung oder die auf dem System installierten Schriften (die z.B. mit Hilfe eines Java Scripts 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 AddOn Secret Agent<sup>3</sup>. Nach der Installation, kann in den Einstellungen des Plugins eine Liste der zu verwendenden User Agent Strings festgelegt werden. Die Standardliste enthält viele exotische Browser, die dazu führen, dass einige Webseiten nicht mehr korrekt dargestellt werden. Daher empfiehlt es sich, diese Liste um die nicht gängigen Browser zu bereinigen. Dazu öffnet man in den Plugineinstellungen das Tab *User Agents* und bearbeitet den Inhalt der Box *Stealth Mode*.

---

<sup>2</sup> <https://www.eff.org/privacybadger>

<sup>3</sup> <https://www.dephormation.org.uk/?page=81>

Der *Stealth Mode* kann daraufhin im Tab *Entropy* über den Punkt *Enable Secret Agent's Stealth Mode* aktiviert werden.

Hier lässt sich auch festlegen, in welchem Abstand der *User Agent String* rotiert werden soll. Alle weiteren Einstellungen des Plugins, können auf den Standardwerten belassen werden. Sollte es Probleme mit der Darstellung einer bestimmten Webseite geben, kann diese in der *Host Whitelist* eintragen werden. Etwas störend wirkt die *Secret Agent Toolbar*. Sie kann bei Bedarf über *View / Toolbars / Secret Agent Toolbar* ausgeblendet werden.

## 2.7. Plugins

Firefox bietet die Möglichkeit, dass Plugins erst nach Bestätigung aktiviert werden. Unter *Tools / Add-Ons* im Bereich *Plugins* kann dazu die Option *Ask to activate* gesetzt werden.

## 2.8. Safe Browsing

Die meisten aktuellen Browser bieten eine sogenannte *Safe Browsing* Funktion an. Dabei werden aufgerufene Webseiten und heruntergeladene Dateien mit einer Liste von als schädlich eingestuft Seiten und Downloads verglichen. Firefox aktualisiert diese Liste regelmässig.

Bei einer Übereinstimmung schickt Firefox Teile der Webseite an den *Safe Browsing Service* von Google. Dort wird der Inhalt weiter analysiert und der Zugriff auf die Webseite gegebenenfalls unterbunden. Es besteht weiterhin die Möglichkeit, den Inhalt der Seite dennoch anzeigen zu lassen, was vom Anwender allerdings explizit bestätigt werden muss.

Die *Privacy Policy*<sup>4</sup> von Google beschreibt, wie Google mit den gewonnenen Daten umgeht.

Google speichert die IP Adresse, ein oder mehrere Cookies sowie die verdächtigen Daten für zwei Wochen. Erst danach werden sie anonymisiert weiterverarbeitet und die Rohdaten werden gelöscht.

Wenn man nicht möchte, dass Google diese Daten speichert, kann man die Abgleich-funktion deaktivieren. Dazu gibt man in der Adressleiste *about:config* ein und sucht nach der Option *browser.safebrowsing.reportURL*. Nach einem Doppelklick auf den Wert kann man die URL löschen. Für den Konfigurationsschlüssel *browser.safebrowsing.malware.reportURL* geht man gleichermassen vor.

## 2.9. Referrer

Beim Aufruf eines Links auf einer Webseite wird der Zielseite automatisch über einen sogenannten Referrer im HTTP Header mitgeteilt, von welcher Seite die Anfrage kam. Hat man z.B. auf Google nach dem Wort *Windows* gesucht und klickt auf einen Treffer von Microsoft, dann bekommt Microsoft die Information, dass man zuvor auf Google war und dort nach dem Wort *Windows* gesucht hat.

Diese Funktion kann für Webseitenbetreiber sehr sinnvoll sein um Webseiten strukturell besser aufzubauen. Denn damit kann auch ermittelt werden, wie Links am häufigsten aufgerufen werden. Auf der anderen Seite verraten Referrer, welche Suchworte eingegeben wurden um auf eine Seite zu gelangen.

---

4 <https://www.google.com/intl/en/chrome/browser/privacy/whitepaper.html>

Da sich ein generelles Deaktivieren negativ auf den Surfkomfort auswirken kann, empfiehlt sich das Zulassen von Referrern innerhalb einer Seite und das De-aktivieren von Referrern beim Wechsel auf eine andere Seite. Leider bietet Firefox selbst diese Einstellmöglichkeit nicht an. Dazu eignet sich das AddOn RefControl.

Nach der Installation des AddOns und dem Neustart des Browsers, findet man im *Tools* Menü einen Eintrag zur Konfiguration der RefControl Optionen. Dort müssen keine einzelnen Seiten hinzugefügt werden. Stattdessen klickt man neben *Default for sites not listed* auf *Edit* und stellt dort *Block* als Standardaktion ein. Durch das Setzen des Hakens bei *3rd Party requests only* stellt man sicher, dass die Einstellung nur für den Aufruf neuer Seiten gilt.

## **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.

## **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 weiter zu verarbeiten. Dazu gehören die Suchmaschine DuckDuckGo, Startpage.com oder die schweizerische Metasuchmaschine eTools.ch.

Startpage.com ist eine Suchmaschine die im Hintergrund auf Google 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 sich das Firefox AddOn HTTPS everywhere<sup>5</sup> der Electronic Frontier Foundation an. Nachdem die Installation erfolgt ist und der Browser neu gestartet wurde, findet man neben der Adressleiste ein Symbol, über das sich das Plugin steuern lässt. Ob eine Verbindung https verschlüsselt ist, kann man am Schloss-Symbol in der Adressleiste erkennen.

# **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 bietet die Nutzung eines Anonymisierungsnetzwerkes.

---

5 <https://www EFF.org/https-everywhere>

### 3.1. Tor

Eines der bekanntesten Netzwerke, die anonymes Surfen ermöglichen, ist Tor<sup>6</sup>. 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 Zielsever, 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<sup>7</sup> 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 sehr gut für den Einsatz auf fremden PCs an, da es ein abgeschlossenes System ist, das auf dem damit gestarteten Rechner keinerlei Spuren hinterlässt.

## 4. Email Verschlüsselung

Standardmässig werden Emails unverschlüsselt übertragen und können theoretisch auf allen Knotenpunkten auf dem Weg zum Ziel mit gelesen werden. Es gibt verschiedene Möglichkeiten sich dagegen zu schützen. Die meisten Email-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.

#### Comodo

Einer der Anbieter für kostenlose Email S/MIME Zertifikate ist die Firma Comodo. Dabei handelt es sich um die weltweit zweitgrösste Zertifizierungsstelle. Über die Webseite des Anbieters lässt sich ein kostenfreies S/MIME Zertifikat beantragen<sup>8</sup>.

Im Formular muss der Vornamen, Nachnamen und die Email-Adresse angegeben werden, für die ein Zertifikat erstellt werden soll. Das Herkunftsland muss entsprechend definiert werden; die Verschlüsselungsstärke sollte auf *High Grade* belassen werden. Mit Hilfe des angegebenen Revocation Passwort, lässt sich das Zertifikat zu einem späteren Zeitpunkt wieder zurückziehen. Nachdem das Formular abgeschickt wurde, erhält man einen Link, über den man das persönliche Zertifikat beziehen kann.

---

<sup>6</sup> <https://www.torproject.org/>

<sup>7</sup> <https://tails.boum.org/>

<sup>8</sup> <https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate>

Da das Zertifikat im eigenen Browser erzeugt wird, muss der Vorgang bestätigt werden. Nach erfolgreicher Installation, findet man das Zertifikat in den erweiterten Einstellungen unter *Certificates / View Certificates*. Dort sollten man im Reiter *Your Certificates* das COMODO Zertifikat sehen können. Das Zertifikat muss zunächst exportiert werden, um es danach in einem eMail Programm wie Thunderbird importieren zu können. Dazu klickt man das Zertifikat an, und wählt den Punkt *Backup*. Beim Exportvorgang wird man aufgefordert ein Passwort zu vergeben. Dieses Passwort sollte man sich gut merken und die Zertifikatsdatei sollte man langfristig an einem sicheren Ort aufbewahren.

Im Thunderbird klicken man auf *Account Settings* und wählt dort im entsprechenden Email-Konto den Punkt *Security*. Dort klickt man zunächst auf *View Certificates*. Dadurch öffnet sich die Thunderbird Zertifikatsverwaltung, die der von Firefox zwar optisch ähnelt, aber getrennt gehalten wird. Unter dem Reiter *Your Certificates* klickt man auf *Import* und wählt die Zertifikatsdatei aus.

Beim Einlesen wird das zuvor vergebene 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 digital zu unterschreiben, da so die Kommunikationspartner in den Besitz des Public Keys kommen kann.

Thunderbird verschlüsselt Nachrichten nicht automatisch, auch wenn der Public Key des Empfänger bekannt ist. Über *Extras / AddOns* lässt sich zu diesem Zweck die Erweiterung *Encrypt if possible* installieren. In den Einstellungen des Plugins kann man festlegen, ob eine Nachfrage erscheinen soll, bevor eine Mail automatisch verschlüsselt wird.

## CAcert

Bei CAcert<sup>9</sup> 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 Email-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.

Bisher liefern nur sehr wenige Browser und Email-Clients das CAcert Stammzertifikat mit aus. Es lässt sich aber sehr leicht nachträglich importieren<sup>10</sup>.

---

9 <https://cacert.org>

10 <http://www.cacert.org/?id=3>