Privacy Guide

Anleitung zur Wahrung der Privatsphäre im Internet

Version: 2.0

Autor: Marcus 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 erfahren Sie was notwendig ist, um Ihr Recht auf Privatsphäre auch im Internet zu wahren.

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 allerdings durch eine oder mehrere Personen geprüft und freigegeben werden, bevor er veröffentlicht wird (das sogenannte Peer-Review).

Projekte wie das Betriebssystem OpenBSD oder das von diesem Projekt entwickelte OpenSSH (für den sicheren Remotezugriff), werden besonders strengen Sicherheits-prüfungen unterzogen.

In der Vergangenheit kam es allerdings auch im Umfeld Freier Software zu grösseren Sicherheitsproblemen, wie zum Beispiel der «Heartbleed»-Sicherheitslücke, die es Angreifern erlaubte, verschlüsselte https Verbindugen 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 uns vor Augen gehalten, dass Sicherheit auch Geld kostet.

2. Spurenarmes Surfen

Beim Surfen im Internet hinterlassen wir 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. Essen Sie beispielsweise gerne Asiatisch und haben in der Vergangenheit bei einem Suchanbieter wie Google verstärkt nach asiatischen Restaurants gesucht, ist es wahrscheinlich, dass Sie in Zukunft in erster Linie asiatische Restaurants als Suchergebnis erhalten. Auch wenn Sie an diesem Tag lieber gutbürgerlich Essen gehen würden. Das mag zunächst harmlos klingen, in der Praxis erhalten Sie allerdings fast nur noch Suchresultate, die bereits Ihrem Interessensbild entsprechen und erfahren möglicherweise gar nichts mehr von anderen Inhalten (die Sie aber auch interessieren 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 ge-tracked werden möchte.

Im Firefox finden Sie diese Einstellung in den Settings unter dem Punkt *Privacy*. Aktivieren Sie dort den Punkt *Tell sites that I dont want to be tracked*. Da es aber bisher in der Schweiz und auch in den USA keine 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.

Ein Cookie wird dabei wie folgt gesetzt: Sie fordern mit Ihrem Browser eine Webseite an. Die Webseite bietet den Cookie für die spätere Nutzung an (z.B. um die Sitzung aufrecht zu erhalten). Beim nächsten mal wenn Sie auf die Webseite zugreifen, schickt Ihr Browser automatisch den Cookie beim mit. Der Anbieter kann Sie mit Hilfe des Cookies 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 die Webseite eingebunden. Der Button wird direkt von Facebook geladen und muss nicht angeklickt werden um den Cookie zu setzen. Das ganze passiert im Hintergrund.

Wenn Sie 3rd Party Cookies deaktivieren, werden keine Cookies mehr für Webseiten gesetzt, die Sie nicht direkt aufgerufen haben.

Die Option zum Deaktivieren von 3rd Party Cookies ist im Firefox etwas versteckt. In den *Privacy* Einstellungen stellen Sie bitte zunächst von *Firefox will Remember history* auf *Use Custom Settings for History* um. Danach können Sie den Punkt *Accept third-party cookies* auf *Never* stellen.

Firefox bietet ausserdem die Option alle Cookies beim Beenden des Browsers zu löschen.

2.3. Flash

Der Adobe Flash Player hat keine besonders ruhmreiche Vergangenheit, was Sicherheit anbelangt. Daher sollten Sie sich Fragen ob Sie grundsätzlich darauf verzichten können.

Viele Dienstanbieter wie youtube.com bieten mittlerweile HTML5 Zugriff, (https://www.youtube.com/html5) mit dem sich die meisten Videos abspielen lassen.

Mit dem HTML5 basierten Flashplayer Shumway ist es möglich, Flash Inhalte ohne den Adobe Flash Player abspielen zu können.

Falls Sie dennoch nicht auf den Flash Player verzichten könnten, empfiehlt sich das Deaktivieren des lokalen Caches. Die Flash Einstellungen können Sie vornehmen, indem Sie mit der rechten Maustaste auf einen Flash-Inhalt klicken und dort *Global Settings* wählen. Im Reiter *Storage* können Sie dann den Punkt *Block all sites from storing information on this computer* wählen.

2.4. NoScript

Das Firefox AddOn NoScript bietet Ihnen 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 finden Sie 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. Besuchen Sie 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 Scripts 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, lassen Sie bitte schrittweise Scripts von fremden Webseiten temporär zu, bis der Inhalt wieder korrekt dargestellt wird. Nachdem Sie so herausgefunden haben, welche Scripts Sie freischalten müssen, können Sie diese permanent zulassen. Beachten Sie bitte, dass Einstellungen bei NoScript immer global gelten. 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 Sie besucht haben. Einen wirksamen Schutz gegen Tracker bietet das AddOn Privacy Badger. Es wird von der EFF (Electronic Frontier Foundation) entwickelt, einer Organisation die sich für Grundrechte im Informationszeitalter einsetzt. Zur Installation des AddOns besuchen Sie bitte die Webseite: https://www.eff.org/privacybadger und klicken auf Install. Firefox wird sie auffordern, die Installation zu bestätigen. Das AddOn benötigt 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. Anhand dieser und weiterer Informationen, wie die verwendete Bildschirmauflösung oder die auf dem System installierten Schriften (die z.B. mit Hilfe eines Flash Scripts ausgelesen werden können), kann ein Benutzer sehr verlässlich identifiziert werden.

Eine mögliche Gegenmassnahme ist es, den sogenannten *User Agent String* bei jedem Aufruf einer Webseite zu wechseln. Zu diesem Zweck eignet sich das AddOn *Secret Agent,* das Sie von der Webseite des Entwicklers https://www.dephormation.org.uk/?page=81 herunterladen können. Nach der Installation, können Sie in den Einstellungen des Plugins eine Liste der zu verwendenden User Agent Strings festlegen. Die Defaultliste enthält viele exotische Browser, die dazu führen, dass einige Webseiten nicht mehr korrekt dargestellt werden. Eine User Agent Liste zur Verwendung mit Firefox finden Sie hier:

https://raw.githubusercontent.com/MarcusMoeller/privacyguide/master/User_Agents.txt

Kopieren Sie diese und fügen Sie sie in den Plugineinstellungen im Tab *User Agents* in der Box *Stealth Mode* ein.

Den Stealth Mode können Sie daraufhin im Tab *Entropy* über den Punkt *Enable Secret Agent's Stealth Mode* aktivieren. Hier können Sie auch festlegen, in welchem Abstand der User Agent String rotiert werden soll. Alle weiteren Einstellungen des Plugins, können Sie auf den Standardwerten belassen. Sollten Sie Probleme mit der Darstellung einer bestimmten Webseite haben, können Sie diese in der *Host Whitelist* eintragen. Etwas störend wirkt die Secret Agent Toolbar. Sie können diese bei Bedarf über *View / Toolbars / Secret Agent Toolbar* ausblenden.

2.7. Plugins

Firefox bietet die Möglichkeit, dass Plugins nur nach Bestätigung aktiviert werden. Unter *Tools / Add-Ons* im Bereich *Plugins* können Sie die Option *Ask to activate* setzen.

2.8. 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. Haben Sie z.B. auf Google nach dem Wort *Windows* gesucht und klicken auf einen Treffer von Microsoft, dann bekommt Microsoft die Information, dass Sie zuvor auf Google waren und dort nach dem Wort *Windows* gesucht haben.

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

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, finden Sie im Tools Menü einen Eintrag zur Konfiguration der RefControl Optionen. Sie müssen keine einzelnen Seiten Hinzufügen. Klicken Sie stattdessen neben *Default for sites not listed* auf *Edit* und stellen dort Block als Standardaktion ein. Durch das Setzen des Hakens bei *3rd Party requests only* stellen Sie sicher, dass die Einstellung nur beim Aufruf neuer Seiten aktiv ist.

2.9. 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.

2.10. 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, 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.

2.11. https

Beim Zugriff auf Webseiten über http werden alle Informationen unverschlüsselt übertragen, und können von Dritten analysiert werden. Besonders bei der Übertragung von Passwörtern ist das sehr kritisch. Viele Webseitenanbieter lassen zwar https-Anfragen zu, bieten aber defaultmässig http an, da für unverschlüsselte Verbindungen weniger technischen Ressourcen benötigt werden.

Um https für möglichst viele Seiten zu forcieren bietet sich das Firefox AddOn *HTTPS erverywhere* der Electronic Frontier Foundation an. Zur Installation des Plugins öffnen Sie bitte die Webseiten https://www.eff.org/https-everywhere und klicken auf den Punkt *Install in Firefox*. In dem sich öffnenden Hinweis klicken Sie bitte auf *Allow*. Nachdem die Installation erfolgt ist und der Browser neu gestartet wurde, finden Sie neben der Adressleiste ein Symbol, über das sich das Plugin steuern lässt.

3. Anonymes Surfen

Beim Surfen im Internet können Sie 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 Sie hierbei bitte, dass Sie nur verschlüsselte Verbindungen über solche Verbindungen aufbauen sollten. Eine Alternative bietet die Nutzung eines Anonymisierungsnetzwerkes.

3.1. Tor

Eines der bekanntesten Netzwerke, die anonymes Surfen ermöglichen, ist Tor. Dabei werden Verbindungen über die einzelnen Tor-Knoten, die auf Rechnern in der ganzen Welt laufen, geleitet. Sie können 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 (der nicht immer der gleiche ist), hat Zugriff auf die übertragenen Daten. Es ist also auch hier sehr zu empfehlen, dass Sie nur verschlüsselte Verbindungen aufbauen.

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 nutzen Sie eine spezialisierte Linux Distribution wie Tails dar, 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.

Das Aussehen der Desktopoberfläche wurde in diesem Modus an Windows angeglichen. 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. Sollten Sie sich für GnuPG interessieren, empfiehlt sich der Einsatz des Thunderbird Plugins Engimail, was im folgenden aber nicht näher beschrieben wird.

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 dieser Anbieter ist die Firma Comodo. Dabei handelt es sich um die weltweit zweitgrösste Zertifizierungsstelle. Über die Webseite des Anbieters:

https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate

lässt sich ein kostenfreies S/MIME Zertifikat beantragen. Geben Sie in dem Formular bitte Ihren Vornamen, Nachnamen und die Email-Adresse an, für die Sie ein Zertifikat erstellen möchten. Definieren Sie das Herkunftsland entsprechend, und belassen Sie die Verschlüsselungsstärke auf *High Grade*. Definieren Sie ein Revocation Passwort, mit dem Sie bei Bedarf das Zertifikat auch wieder zurückziehen können.

Nachdem Sie das Formular ausgefüllt haben, erhalten Sie einen Link, über den Sie Ihr persönliches Zertifikat beziehen können.

Da das Zertifikat in Ihrem Browser erzeugt wird, müssen Sie den Vorgang bestätigen. Nach erfolgreicher Installation, finden Sie das Zertifikat im Zertifikatsspeicher Ihres Browsers. Bei Firefox ist dieser in den erweiterten Einstellungen unter *Zertifikate* / *Zertifikate anzeigen* zu finden. Dort sollten Sie im Reiter *Ihre Zertifikate* das COMODO Zertifikat sehen können. Klicken Sie es bitte an, und wählen *Backup*. Das Zertifikat muss zunächst exportiert werden, um es danach in einem eMail Programm wie Thunderbird importieren zu können. Beim Exportvorgang werden Sie aufgefordert ein Passwort zu vergeben. Merken Sie sich dieses Passwort gut und heben Sie die Zertifikatsdatei langfristig an einem sicheren Ort auf.

Im Thunderbird klicken Sie bitte auf *Konten-Einstellungen* und wählen dort in Ihrem Email-Konto den Punkt S/MIME-Sicherheit aus. Klicken Sie dort bitte zunächst auf *Zertifikate verwalten*. Dadurch öffnet sich die Thunderbird Zertifikatsverwaltung, die der von Firefox zwar optisch ähnelt, aber getrennt gehalten wird. Unter dem Reiter *Ihre Zertifikate* klicken Sie bitte auf *Importieren* und wählen Ihre Zertifikatsdatei aus.

Beim Einlesen wird das zuvor vergebene Passwort angefordert. Wenn der Vorgang erfolgreich war, klicken Sie bitte auf *Ok* und wählen 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 Ihre Kommunikationspartner in den Besitz Ihres Public Keys kommen kann, mit dem sie später Emails an Sie verschlüsseln können.

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 können Sie festlegen, ob eine Nachfrage erscheinen soll, bevor eine Mail automatisch verschlüsselt wird.