Spurenvermeidung im Browser

Digitale Selbstverteidigung – NoName e. V.*

8. Mai 2017

Disclaimer: Alle Ratschläge haben wir nach bestem Wissen und Gewissen ausgewählt. Trotzdem können wir keinerlei Garantie übernehmen und haften insbesondere nicht für die genannte Software. Sinn dieser Empfehlungen ist, Privatsphäre und Sicherheit beim alltäglichen Surfen angemessen zu verbessern. Für hoch-sicherheitskritische Zwecke sind sie nicht gedacht.

Den folgenden Empfehlungen haben wir eine allgemeine Einführung und eine Demonstration der Problematik mit *Lightbeam für Firefox* (`https://www.mozilla.org/de/lightbeam/`) und *Panopticlick* (`https://panopticlick.eff.org/`) vorangestellt. Neben *Alternative Dienste* und *Tor-Browser* ist dies ein Themenblock zu *Spuren im Netz*.

1 Firefox

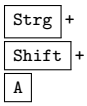
`https://www.mozilla.org/` (de, en, . . .)

Wir empfehlen *Mozilla Firefox* als Browser und beziehen uns im Folgenden darauf. (Andere Browser siehe unten.)

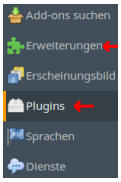
1.1 Einstellungen

Einstellungen → *Erweitert* → *Datenübermittlung*: alles deaktivieren.

1.2 Add-Ons entrümpeln



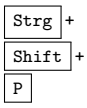
Add-ons können sinnvoll aber auch problematisch sein. Insbesondere Plugins geraten immer wieder wegen unbeabsichtigter Sicherheitslücken in Kritik. Vergangenen Herbst hat eine vermeintlich sinnvolle Erweiterung für Schlagzeilen gesorgt, weil diese detaillierte Browserverläufe von Nutzern ausgespäht hatte.



Erweiterungen, von denen man nicht so genau weiß, was sie tun, sollte man deinstallieren. Insbesondere dann, wenn sie vom Installationsprogramm irgendwelcher anderer Software ungefragt mitinstalliert wurden. Eventuell vorhandene Werbe-Blocker werden durch das unten empfohlene *uBlock Origin* überflüssig.

Plugins, von denen man sicher weiß, dass man sie nicht braucht, entfernen. Unnötig ist auf jeden Fall das *Adobe Reader Browser Plugin*. Bei allen anderen bereits installierten Plugins, wenn möglich, *Nachfragen, ob aktiviert werden soll* (*Click-to-Play*) einstellen. Neue Plugins nur installieren, wenn man sie wirklich braucht.

1.3 Der Private Modus



Der *Private Modus* im Firefox dient in erster Linie dazu, dass keine Informationen über das Surfverhalten (*Chronik*, *Cookies*) **auf dem eigenen Computer** gespeichert werden. Nur in beschränktem Umfang werden auch bekannte Tracker blockiert. Man sollte nicht zu viel vom privaten Modus erwarten.

1.4 Empfohlene Add-Ons

HTTPS-Everywhere (EFF)

`https://www.eff.org/https-everywhere` (en)

Sehr sinnvoll, auch wenn der Name ist etwas irreführend ist: es kann leider nicht magisch alle unverschlüsselten Verbindungen verschlüsseln, sondern prüft, ob von einer Seite bekannt ist, dass diese `https` unterstützt, und leitet ggf. von `http` auf `https` um. Die EFF gilt als sehr vertrauenswürdige Bürgerrechtsorganisation.

*Für den Termin *Spuren im Netz* am 08. und 10. Mai 2017 der Reihe Digitale Selbstverteidigung / Cryptoparty Heidelberg des NoName e. V.. Kontakt: crypto@noname-ev.de.

Self-Destructing Cookies https://addons.mozilla.org/de/firefox/addon/self-destructing-cookies/ (en)
Sorgt dafür, dass *Cookies* und ähnlich Daten gelöscht werden, sobald alle betreffenden Tabs geschlossen wurden. Ausnahmen lassen sich leicht einrichten. Regelmäßiges Leeren des *Cache* zur Vermeidung anderer Tracking-Methoden ist möglich.

uBlock$_0$ bzw. uBlock Origin https://github.com/gorhill/uBlock (en)
Universeller Blocker auf Basis wählbarer Filterlisten mit sinnvollen Standard-Einstellungen. Blockiert Tracking, Malware, Werbung, ...

Privacy Badger (EFF) https://www.eff.org/privacybadger (en, fr, es, tr)
Privacy Badger versucht, solche Inhalte von Dritten zu blockieren, die Nutzer über verschiedene Websites hinweg ausspionieren. Welche dies sind, lernt Privacy Badger mit der Zeit automatisch. Die EFF pflegt eine Liste mit Ausnahmen, damit Nützliches nicht unter die Räder kommt. Social-Media-Buttons werden durch lokal gespeicherte Grafiken und Links ersetzt.

Da *uBlock$_0$* und *Privacy Badger* ein ähnliches Ziel verfolgen, halten wir es für ausreichend, eines von beiden zu installieren. Je mehr Erweiterungen installiert sind, umso langsamer der Browser, umso großer das Risiko von Problemen und umso schwieriger ggf. eine Fehlersuche. Prinzipiell ist es aber möglich, beide parallel zu nutzen. Mehr dazu am 17. Mai bei *Privatsphäre schützen*.

2 Andere Desktop-Browser

Was zu Firefox gesagt wurde, gilt größtenteils auch für die Firefox-basierten Browser *Iceweasle*, *Icecat* und *Pale Moon*.

2.1 Chrome und Chromium

Auch für *Chrome* bzw. *Chromium* gibt es *HTTPS-Everywhere*, *uBlock Origin* und *Privacy Badger*. Man sollte für diese Erweiterungen nach der Installation den Haken bei „*Im Inkognitomodus zulassen*“ setzen. *Self-Destruction Cookies* gibt es nicht für Chrome. *Tab Cookies* soll ähnliche Funktionalität bieten, wurde aber zuletzt im Juni 2011 aktualisiert. Wir haben dieses Add-On nicht getestet und können daher keine konkrete Empfehlung geben.

2.2 Safari unter macOS / OS X

Leider gibt es keines der oben empfohlenen Add-Ons für *Safari*. Einen passablen Tracking-Schutz bietet am ehesten *Disconnect Safe Browsing*: Diese Browser-Erweiterung ist quelloffen und Kooperationspartner von Disconnect sind u. a. Mozilla, das Tor-Projekt und die EFF, was einen vertrauenswürdigen Eindruck macht. Wir haben dieses Add-On nicht getestet und können daher keine konkrete Empfehlung geben. https://disconnect.me/freeprotection (en)

3 Smartphones

Die Auswahl an Browser-Add-Ons ist geringer und wegen der schwächeren Hardware können möglicherweise nur wenige Add-Ons gleichzeitig genutzt werden.

Android und verwandte Systeme: Wir empfehlen *Firefox for Android* mit *uBlock Origin*, *HTTPS-Everywhere* und *Self-Destructing Cookies*. Leider gibt es *Privacy Badger* (noch) nicht für die mobile Firefox-Variante. Was für die Desktop-Variante von *Chrome* gesagt wurde, gilt auch für *Chrome* unter Android.

iOS: Unter *iOS* gibt es *Mozilla Firefox Klar* als eigenen Browser oder Tracking-Blocker im Hintergrund für *Safari*. Wir haben dies nicht getestet und können daher keine konkrete Empfehlung geben.

4 Weitere Informationen

- http://heise.de/-3046195 (de)
  Ronald Eikenberg *Security-Checkliste Web-Browser*, c't, 23. Dezember 2015 (allgemeinverständliche Empfehlungen).
- https://donottrack-doc.com/ (de, en, fr)
  Personalisierte Web-Serie über das Geschäft mit unseren Daten, Arte, Bayerischer Rundfunk und ONF (Kanada).
  Achtung: Um Tracking begreifbar zu machen, setzt diese Seite selbst Tracking ein!
- https://digitalcourage.de/digitale-selbstverteidigung (de)
  Digitale Selbstverteidigung von Digitalcourage e. V. (deutsche Bürgerrechtsorganisation).
- https://ssd.eff.org/ (en)
  Surveillance Self-Defense Guide der Electronic Frontier Foundation (Bürgerrechtsorganisation, USA).
- https://support.mozilla.org/de/products/firefox/protect-your-privacy (de, en, ...)