Spurenvermeidung im Browser

NoName e.V., 22.07.2018

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 Einführung zu technischen Hintergründen und eine Demonstration der Problematik mit *Lightbeam™ für Firefox* (https://www.mozilla.org/de/lightbeam/) und *Panopticlick* (https://panopticlick.eff.org/) vorangestellt.

1 Mozilla Firefox

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

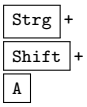
Wir empfehlen *Mozilla Firefox*® als Browser und beziehen uns im Folgenden darauf. (Andere Browser siehe 2.)

1.1 Einstellungen

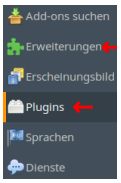
Einstellungen → *Datenschutz & Sicherheit* → *Schutz vor Aktivitätenverfolgung*: Wir empfehlen dies auf *Immer* zu stellen, sollte man *nicht* das später noch aufgeführte Ädd-on *uBlock Origin* verwenden. Andernfalls ist sie nicht notwendig. Man kann unter *Ändern der Blockierliste* den Umfang der Aktivitätenverfolgung auch noch weiter erhöhen. „Do Not Track“ sollte immer mitgesendet werden.

Einstellungen → *Datenschutz & Sicherheit* → *Datenerhebung durch Firefox und deren Verwendung*: Wir empfehlen erstmal eine Abschaltung aller Optionen dieser Sektion. Informationen zu den einzelnen Punkten sind daneben verlinkt, man kann dort nachlesen, was diese Dinge tun, falls man sie ggf. wieder aktivieren möchte.

1.2 Add-Ons entrümpeln



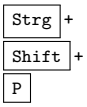
Add-ons können sinnvoll aber auch problematisch sein. Insbesondere Plugins geraten immer wieder wegen unbeabsichtigter Sicherheitslücken in Kritik. Im Herbst 2016 hat eine vermeintlich sinnvolle Erweiterung für Schlagzeilen gesorgt, weil diese detaillierte Browserverläufe von Nutzern ausgespäht hatte.



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 bspw. 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



Im *Privaten Modus* Firefox greift in der Standardeinstellung auch der native Schutz vor Aktivitätenverfolgung in seiner Grundvariante (siehe oben, *Einstellungen*), dieser Modus dient aber in erster Linie dazu, dass keine Informationen über das Surfverhalten (*Chronik*, *Cookies*) **auf dem eigenen Computer** gespeichert werden. Dies sollte man bei der Verwendung im Hinterkopf behalten, um ihn nicht mit falschen Annahmen zu verwenden.

1.4 Empfohlene Erweiterungen oder Add-Ons

Erweiterungen lassen sich im Firefox installieren über das Menü, → *Add-ons* → *Erweiterungen*, dann lässt sich oben rechts nach installierbaren Erweiterungen suchen.

uBlock Origin https://github.com/gorhill/uBlock (en)

Universeller Blocker auf Basis wählbarer Filterlisten mit sinnvollen Standard-Einstellungen. Blockiert Tracking, Werbung, etliche Malware-Infektionskanäle,. . .

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

Leitet von (unverschlüsseltem) `http` auf (verschlüsseltes) `https` um, wenn in HTTPS-Everywhere hinterlegt ist, dass die Seite auch eine verschlüsselte Version besitzt. Funktioniert allerdings nur für dort eingetragene Webseiten. Bietet die Möglichkeit, alle unverschlüsselten Verbindungen zu verbieten, was für unvertrauenswürdige Netze sehr praktisch ist.

Decentraleyes https://decentraleyes.org (en)

Ersetzt einige extern nachgeladene Ressourcen, die von Webseiten benötigt, aber z.B. von Google nachgeladen werden, durch lokale Kopien.

Cookie AutoDelete https://addons.mozilla.org/de/firefox/addon/cookie-autodelete/ (en)

Sorgt dafür, dass *Cookies* und ähnlich Daten gelöscht werden, sobald alle betreffenden Tabs geschlossen wurden. Dies sorgt im Normalfall auch dafür , dass man aus Webseiten ausgeloggt wird oder Einstellungen vergessen werden, wenn man den entsprechenden Tab schließt. Will man dies verhindern, kann man die entsprechende Seite über das Icon von Cookie AutoDelete auf der entsprechenden Seite *whitelisten*. Wichtig: *Aktiven Modus* über das Icon des Add-Ons einschalten, es fängt nicht automatisch an zu funktionieren, damit Seiten für Logins oder Einstellungen vorher zur Whitelist hinzugefügt werden können, wenn man das möchte.

First Party Isolation https://addons.mozilla.org/en-US/firefox/addon/first-party-isolation/ (en)

First Party Isolation reduziert die Möglichkeiten, über verschiedene Webseiten hinweg als dieselbe Person wiedererkannt zu werden. Manchmal führt dies zu Problemen, z.B. bei 3rd-party-Loginsystemen („Login with Google“, „Login with Facebook“ o.Ä.), daher ist das Feature bei Bedarf auch per Knopfdruck abschaltbar.

2 Andere Desktop-Browser

2.1 Chrome und Chromium

Auch für *Chrome* bzw. *Chromium* gibt es alle der oben empfohlenen Erweiterungen. Man sollte für diese Erweiterungen nach der Installation den Haken bei „*Im Inkognitomodus zulassen*“ setzen.

2.2 Safari unter macOS / OS X

uBlock Origin ist auch für Safari verfügbar, allerdings noch im Teststadium. https://github.com/el1t/uBlock-Safari (en)

Eine Alternative könnte auch *Disconnect Safe Browsing* sein. https://disconnect.me/freeprotection (en)

Wir haben diese Add-Ons nicht getestet und können daher keine konkrete Empfehlung geben.Entsprechungen für *Cookie AutoDelete* und *HTTPS Everywhere* für *Safari* sind uns keine bekannt.

3 Smartphones

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*, *Cookie AutoDelete* and *Decentraleyes*. Was für die Desktop-Variante von *Chrome* gesagt wurde, gilt auch für *Chrome* unter Android. Es gibt auch *Mozilla Firefox Klar* als eigenen Browser neben dem regulären Firefox. Dieser ist bereits von Haus aus mit eingebautem Trackingschutz ausgestattet und legt keinerlei Historie über die besuchten Seiten an.

iOS: Auch unter *iOS* gibt es *Mozilla Firefox Klar* als eigenen Browser oder Tracking-Blocker im Hintergrund für *Safari*. Desweiteren gibt es auch *Mozilla Firefox* auf iOS, aufgrund von Apples Regeln für iOS-Apps sind hier allerdings keine Add-Ons verfügbar. Wir haben beides 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, . . .)