Bild: Rudolf A. Blaha

Ein Browser für Datenschutzbewusste

Firefox-Sicherheitskompendium, Teil 1

Wer beim Surfen Wert auf Sicherheit und Privatsphäre legt, muss seinen Browser abschotten. Dies ist der Start einer Artikelserie, die zeigt, wie Sie Firefox gegen Unrat aus dem Netz abdichten. Holen Sie sich die Kontrolle und die Selbstbestimmung beim Surfen im Internet zurück!

Von Mike Kuketz

Ein Browser ist das Tor zur digitalen Welt, und zwar sowohl im privaten als auch im beruflichen Alltag. Er sollte daher keine Einfallsmöglichkeit für Sicherheitsprobleme bieten und die Privatsphäre schützen. Welche komplexen Prozesse im Hintergrund ablaufen müssen, um eine Webseite im Browser darzustellen, können viele Nutzer vermutlich nicht einmal erahnen.

Warum auch? Die dahinterliegende Technik arbeitet völlig geräuschlos und suggeriert einem Nutzer das Gefühl der Freiheit, jeden erdenklichen Informationsschnipsel der Webseite erreichen zu können und nichts auf der Webseite zu verpassen. Dabei ist nur den wenigsten bewusst, wie Webseitenbetreiber schon durch das Einbinden externer Ressourcen wie JavaScript, Schriftarten oder Social-Media-Buttons die Privatsphäre ihrer Besucher verletzen und ihre Sicherheit gefährden.

Diese Artikelserie gibt Ihnen ein Komplettpaket gegen aufdringliche Werbung, neugierige Tracker und Sicherheitsprobleme. Sie demonstriert die vielen Wege, auf denen persönliche Daten beim Surfen in fremde Kanäle abfließen, und zeigt, was Sie dagegen tun können. Auf dieser Basis können Sie selbst entscheiden, mit welchen Anbietern Sie ihre Daten teilen.

Als Basis dafür eignet sich der Browser Firefox am besten (siehe Kasten

„Surf-Rüstung“) – allerdings nicht im Auslieferungszustand. Neben vielen Tipps zur Konfiguration stellt diese Artikelserie Add-ons vor, die den Browser sicherer und datensparsamer machen.

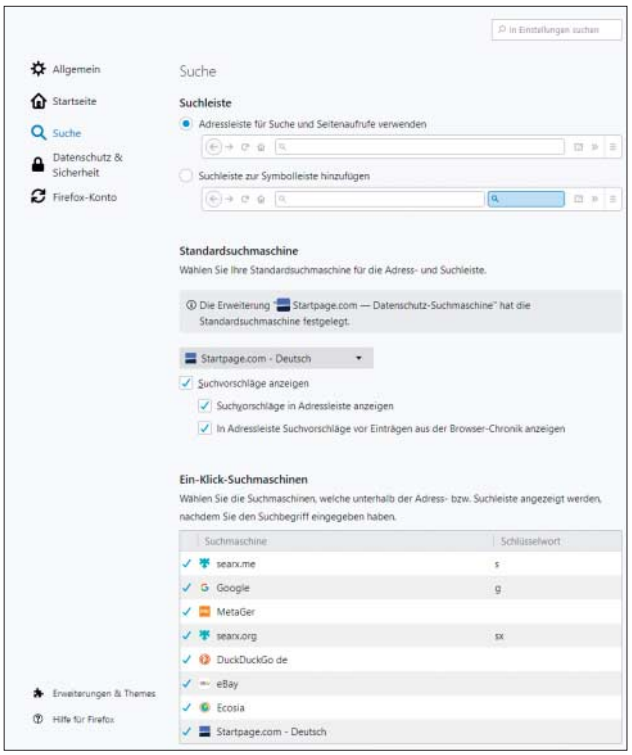
Suchmaschine anpassen

Starten Sie mit einem frisch installierten (und aktuellen) Firefox. Im Auslieferungszustand nutzt Firefox Google als Suchmaschine. Wenn Sie die Option „Suchvorschläge anzeigen“ aktiviert haben, werden ihre Eingaben ins Firefox-Adressfeld schon beim Eintippen von Suchbegriffen und URL-Anfängen an Google übertragen.

Google ist ein Werbekonzern, der aus allen Informationen, die er erhält, Profile bildet: Ein Nutzer, der seine Privatsphäre schützen will, wird nicht ausgerechnet diesem Unternehmen seine Suchen anvertrauen wollen. Muss er auch nicht, denn es gibt reichlich Alternativen. Startpage zum Beispiel.

Der Suchmaschinenbetreiber hat sich den Datenschutz auf die Fahnen geschrieben und ermöglicht es, Trefferseiten über einen Proxy verschleiert anzusehen. Dabei sind die Suchergebnisse fast so gut wie die von Google, weil Startpage mit Google zusammenarbeitet. Es gibt von Startpage ein Firefox-Add-on. Es nennt sich „Startpage.com – Datenschutz-Suchmaschine“. Vorsicht, daneben tummeln sich noch einige ähnlich bezeichnete Add-ons von Fremdanbietern.

Im Suchmaschinen-Schwerpunkt aus c’t 6/2019 finden Sie ebenfalls Suchmaschinen-Alternativen, die Ihre Privatsphäre besser schützen als Google [1]. Die Suchmaschinen-Optionen finden Sie unter Einstellungen\Suche.



Die Standardsuchmaschine lässt sich in den Optionen festlegen.

Werbung abwehren

Online-Werber haben viele Methoden entwickelt, um Surfer auszuspähen. Mit Werbeblockern lassen sich viele Schnüffeleien unterbinden. Der Werbe- und Inhalteblocker uBlock Origin etwa filtert äußerst effektiv Werbung, Tracker und Social-Media-Gedöns wie Facebook- und andere Buttons aus. Das lässt den Browser weniger Inhalte laden und macht den Seitenaufbau schneller. Nicht zuletzt schützt uBlock Origin den Nutzer und seine Daten auch vor Malvertising, also Werbung, die Schadcode enthält.

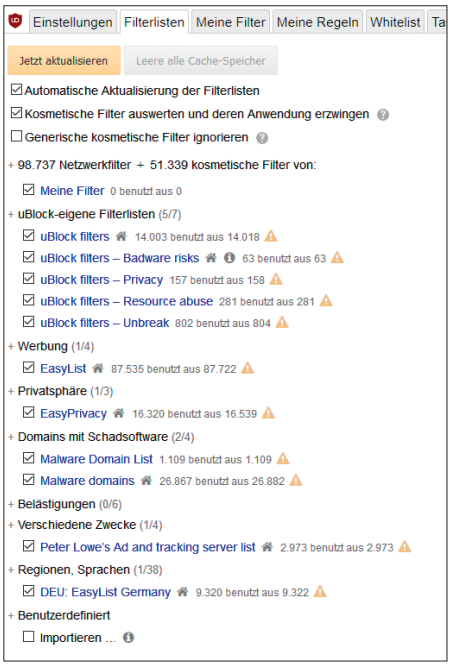
Unter dem Namen „uBlock Origin (von Raymond Hill)“ finden Sie das Add-on bei Mozilla (siehe ct.de/y433). Nach der Installation zeigt es sich durch ein Icon in der Symbolleiste rechts oben neben der Adresszeile. Ein Klick darauf bringt ein kleines Pop-up-Fenster zum Vorschein, das Dashboard. uBlock Origin arbeitet im Auslieferungszustand mit Standardeinstellungen, die schon eine Menge unnützer Inhalte wegfiltern.

uBlock Origin nutzt hauptsächlich Filterlisten. Ist zum Beispiel die Domain „www.werbung.com“ in einer der Filterlisten enthalten, blockiert uBlock Origin den Aufruf und Firefox wird keine Inhalte von der Domain laden.

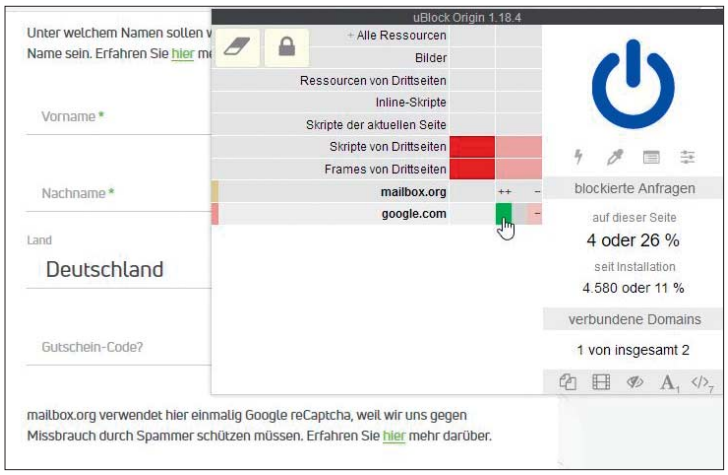
Filterlisten gegen die Werbeflut

Im Auslieferungszustand hat uBlock Origin bereits diverse Filterlisten mit Tausenden von Domains aktiviert, die für die Auslieferung von Werbung, Trackern und anderen unerwünschten Inhalten bekannt sind. Darüber hinaus bringt das Add-on noch weitere optionale Filterlisten mit, die Sie zusätzlich auswählen können. Zur Aktivierung müssen Sie zunächst das Dashboard aufrufen, dort auf das Icon mit den Schiebereglern klicken und anschließend auf den Reiter „Filterlisten“ wechseln.

Sowohl in der Kategorie „Werbung“ als auch in „Privatsphäre“ sind bereits ein paar Listen vorausgewählt. Setzen Sie in beiden Kategorien die fehlenden Häkchen bei allen Filterlisten. Weiterhin empfiehlt es sich, die Filterliste „DEU: EasyList Germany“ in der Kategorie „Regionen, Sprachen“ auszuwählen. Mit dieser von verschiedenen Adblockern genutzten Liste filtert uBlock Origin Inhalte von Werbedomains aus, die häufig auf deutschen Internetseiten anzutreffen sind.



Mit Listen können sie viele nervige Inhalte unterdrücken, zum Beispiel Social-Media-Buttons.



Eine Website funktioniert nicht mit uBlock Origin? Schalten Sie es mit dem blauen Schalter für diese Site ab.

Die Listen in der Kategorie „Belästigungen“ blockieren nervige Cookie-Hinweise oder Social-Sharing-Buttons (Facebook, Twitter & Co.). Mit jeder zusätzlichen Filterliste, die Sie aktivieren, steigt allerdings das Risiko, dass Inhalte blockiert werden, die für den Betrieb einer Webseite erforderlich sind.

Sollte der seltene Fall eintreten, dass uBlock benötigte Inhalte unterdrückt, deaktivieren Sie den Adblocker mit einem Klick auf den blauen Schalter für die betroffene Webseite. Damit verlieren Sie dort dann allerdings auch den Schutz vor schadhafter Online-Werbung und Trackern. Manchmal muss man uBlock Origin bei Seiten deaktivieren, die Maßnahmen gegen Werbeblocker getroffen haben.

Weitere Funktionen

Im Standardmodus, dem sogenannten „Easy mode“, bestehen die Einflussmöglichkeiten im Wesentlichen in der Auswahl von Filtern. Für ambitionierte Nutzer bieten sich im „Medium mode“ aber noch viele weitere Optionen.

Sie aktivieren ihn, indem Sie im Reiter „Einstellungen“ des Dashboards ein Häkchen vor „Ich bin ein erfahrener Anwender“ setzen. Im Medium mode können Sie das Nachladen von Skripten und Frames von externen Seiten deaktivieren – ein guter Kompromiss zwischen Nutzbarkeit einerseits und mehr Sicherheit und Privatsphäre andererseits. Dazu fügen Sie unter „Meine Filterlisten“ im Dashboard die folgenden Zeilen ein:

```
* * 3p-script block
* * 3p-frame block
```

Geben Sie sie zunächst rechts unter „Temporäre Regeln“ ein, speichern sie und übernehmen sie durch einen Klick auf „Dauerhaft speichern“ als permanente Regeln. Manchmal schießt man damit aber über das Ziel hinaus, etwa wenn Webseiten Google Captchas einsetzen. Mailbox.org nutzt ein solches Captcha zum Beispiel bei der Registrierung. uBlock Origin im Medium mode unterdrückt es und man kann die Registrierung nicht abschließen.

Im Dashboard sieht man, dass die Domain google.com (rot) vollständig blockiert wird. Um diese Domain für Mailbox.org zuzulassen, klicken Sie in der rechten Spalte der Zeile „google.com“ ganz links auf das grüne Icon (siehe Screenshot oben). Nach einem Reload müssen Sie das für die Domain gstatic.com wiederholen. Damit werden Google-Inhalte für Mailbox.org erlaubt. uBlock Origin bietet noch viele weitere Feintuning-Optionen (siehe ct.de/y433). *(jo@ct.de)* c't

Surf-Rüstung

Warum Firefox? Der Mozilla-Browser stellt unter allen aktuellen Browsern das kleinste Übel dar. Er ist quelloffen, anders als zum Beispiel der am weitesten verbreitete Browser Chrome, dessen proprietären Bestandteile Google nicht veröffentlicht. Opera gibt seine Quelltextanteile ebenso nicht heraus. Apples Safari sowie Microsofts Browser Edge und Internet Explorer sind komplett Closed Source. Damit fehlt es bei diesen Browsern nach meiner Auffassung an der notwendigen Transparenz.

Aber auch das Open-Source-Projekt Chromium, die Basis von Chrome, sowie die vielen Chrome-Geschwister, die auf Chromium aufsetzen, kommen für Nutzer nicht in Frage, die ihre Privatsphäre konsequent schützen wollen. Denn auch Chromium ist eng mit Google verbandelt, was den Browser aus Datenschutzgründen nicht empfehlenswert macht.

Bleiben noch Forks als denkbare Alternative, also Abspaltungen vom Original-Projekt, die unabhängig weiterentwickelt oder verändert werden. GNU IceCat oder Waterfox sind solche Firefox-Forks, die besonders viel Wert auf den Datenschutz legen. Allerdings gibt es mit Forks ein generelles anderes Problem: Sie werden lediglich von wenigen Leuten (weiter-)entwickelt.

Die fehlende Manpower ist beim Thema Sicherheit allerdings höchst bedenklich. In der Vergangenheit ist es immer wieder passiert, dass Sicherheitsaktualisierungen, die in das Mutterprojekt eingeflossen sind, über Wochen oder auch Monate nicht eingepflegt wurden. Selbst GNU IceCat, das vom GNU-Projekt betreut wird, hinkt meist deutlich hinterher.

Auch Firefox ist unter Datenschützern nicht unumstritten. Mozilla hat seinem Browser in der Vergangenheit Funktionen spendiert, die das Image empfindlich angekratzt haben, weil sie sich negativ auf die Privatsphäre und die Sicherheit auswirken – angefangen beim Tracking via Google Analytics auf der about:addons-Seite über die Integration von Cliqz zur Sammlung der Surfaktivitäten bis zur Remote-Installation von Add-ons.

Ersteres hat Mozilla nach dem Protest der Nutzer wieder abgestellt und die beiden anderen Features lassen sich deaktivieren. Dennoch: Wer seinen Firefox dauerhaft möglichst datensparsam nutzen möchte, der muss einige Anpassungen vornehmen und bei jeder neuen Version oder bei jedem Update von Firefox genau hinschauen. Denn niemand kann garantieren, dass Mozilla in Zukunft nicht wieder fragwürdige Funktionen einbaut.

Literatur

[1] Jo Bager, Universalfahnder, Sechs Allzweck-Suchmaschinen im Vergleich mit Google, c't 6/19, S. 60

Blog und Add-ons: ***ct.de/y433***