Empfehlungen zum Firefox

Eine Sammlung von Informationen rund um Firefox

R. Niederhagen

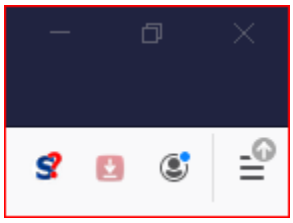
Stand: 02.07.19 17:23:59

Inhaltsverzeichnis

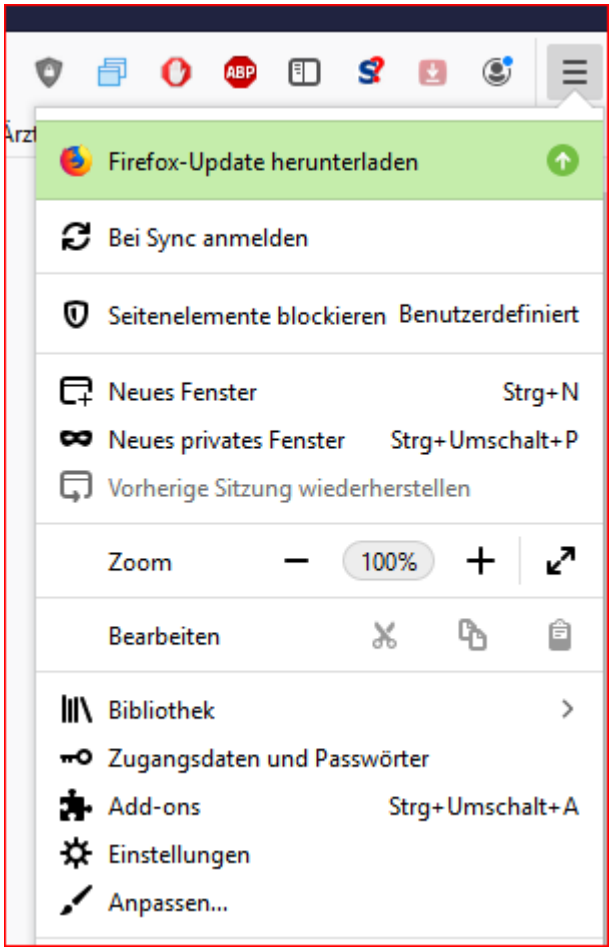
Dieses Dokument enthält Empfehlungen zu Einstellungen und Erweiterungen (AddOns) vom Firefox. Firefox ist ein Browser, den man im Gegensatz zu den Browsern Internet Explorer, Edge und Chrome recht gut an die eigenen Wünsche anpassen kann.

1 Einstellungen vom Firefox anpassen

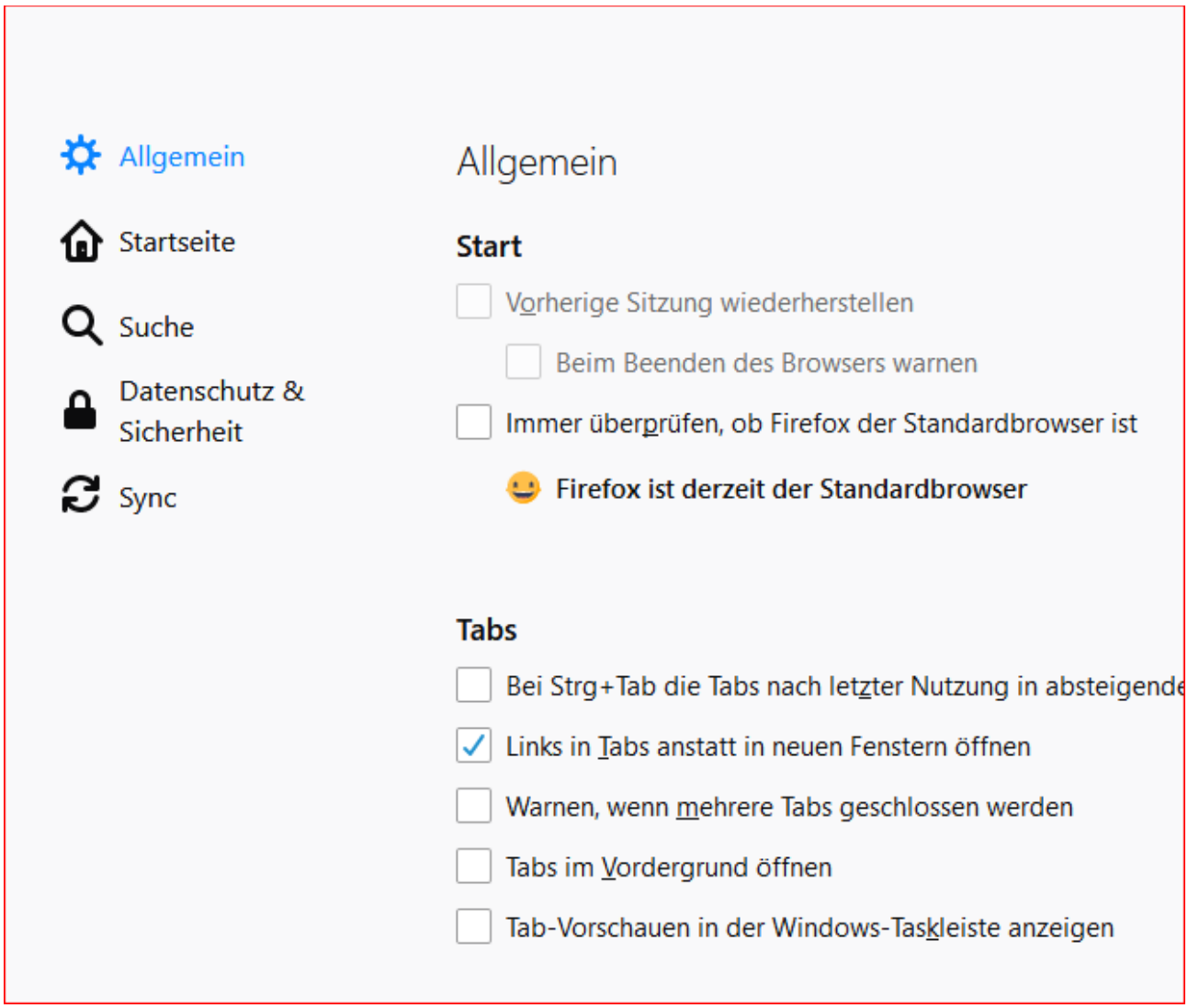
Über 'Extras' / 'Einstellungen' oder die drei waagerechten Striche rechts oben in einer recht aktuellen Version vom Firefox kommt man an die Einstellungen. Man muss auf die drei Striche klicken (linke Maustaste).



Ein Menü wird geöffnet und das sieht dann so aus:

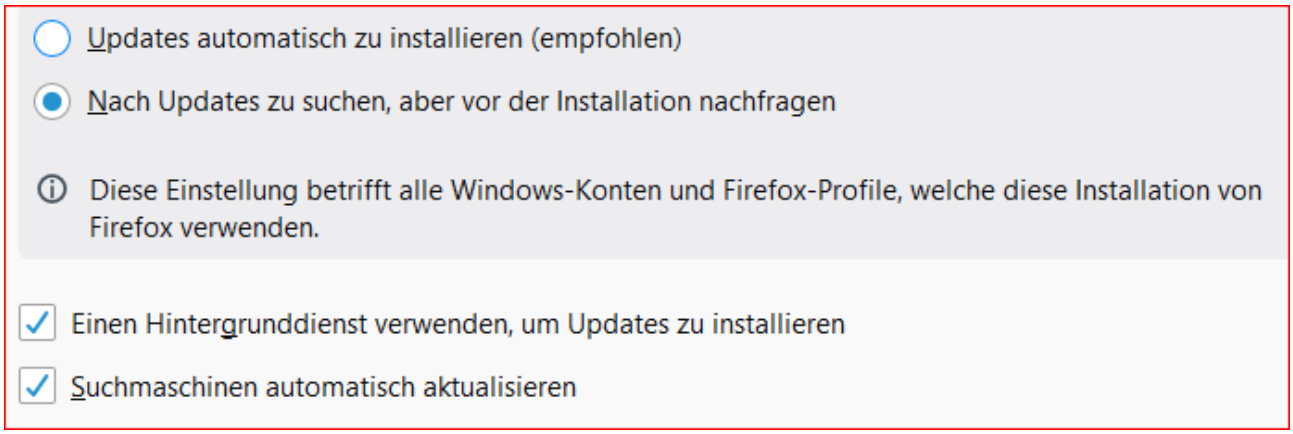


Wenn man auf 'Einstellungen' klickt, öffnet sich ein neuer Reiter und folgendes wird angezeigt:



1.1 Seite 'Allgemein' in den Einstellungen

Die meisten Einstellungen unter 'Allgemein' (ausgewählt links, hier blau) kann man nach Geschmack einstellen. Ich empfehle 'Updates automatisch zu installieren' abzuschalten und stattdessen 'Nach Updates zu suchen, aber vor der Installation nachfragen' zu aktivieren. Dann kann die Updates installieren lassen, wenn es einem passt – **aber bitte die Updates immer so schnell wie möglich einbauen lassen!**

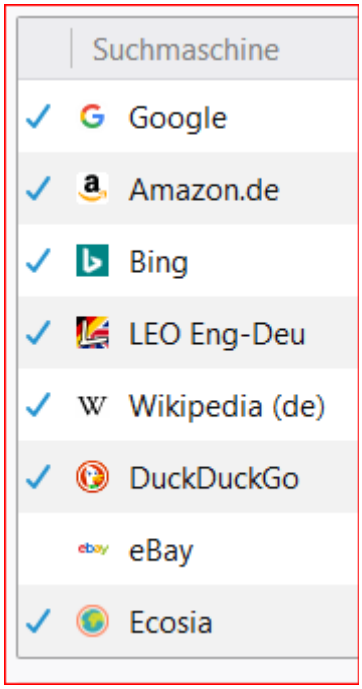


1.2 Seite 'Startseite' in den Einstellungen

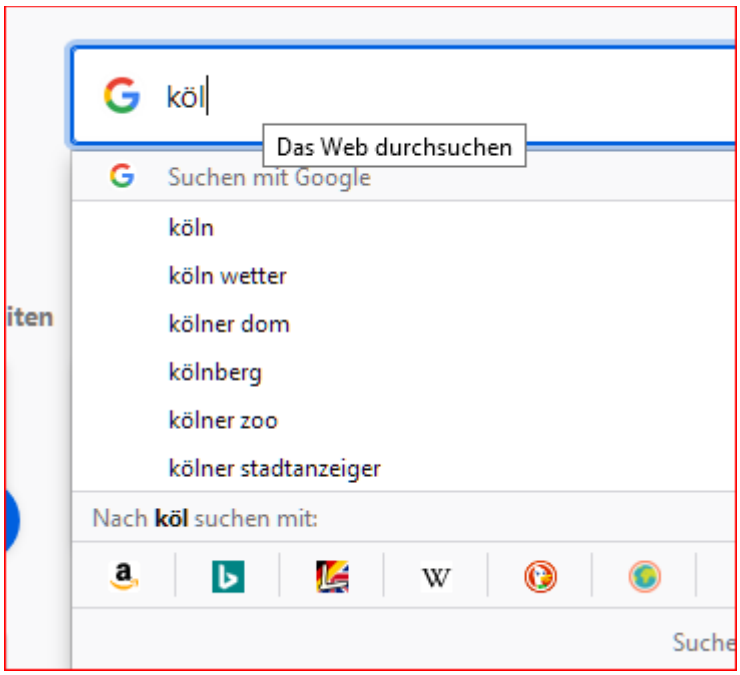
Hier kann man die Startseite festlegen (eventuell Startpage.com oder Google oder was auch immer man möchte und oft nötig hat). Der Startbildschirm kann man auch unterschiedlich aussehen lassen, zum Beispiel 'wichtige Seiten' oder 'zuletzt besuchte Seiten' – je nach Geschmack. Einfach mal damit spielen, passieren kann da nichts.

1.3 Seite 'Suche' in den Einstellungen

Ich mag die untere Adressleiste, weil dann da ein Suchfeld angeboten wird, in das man Stichworte eingeben kann und danach entscheiden kann, an welche Seite der Text geschickt wird. Möglich ist dann dort so einiges:



Wenn man den Haken bei 'Suchvorschläge anzeigen' macht und Google als Standardsuchmaschine hat, dann wird das, was man tippt schon beim Tippen an Google geschickt. Ist ganz nett, aber man muss sich überlegen, ob man das will. Ich habe nur 'köl' eingegeben, das Ergebnis ist dann auf dem nächsten Bild zu sehen.

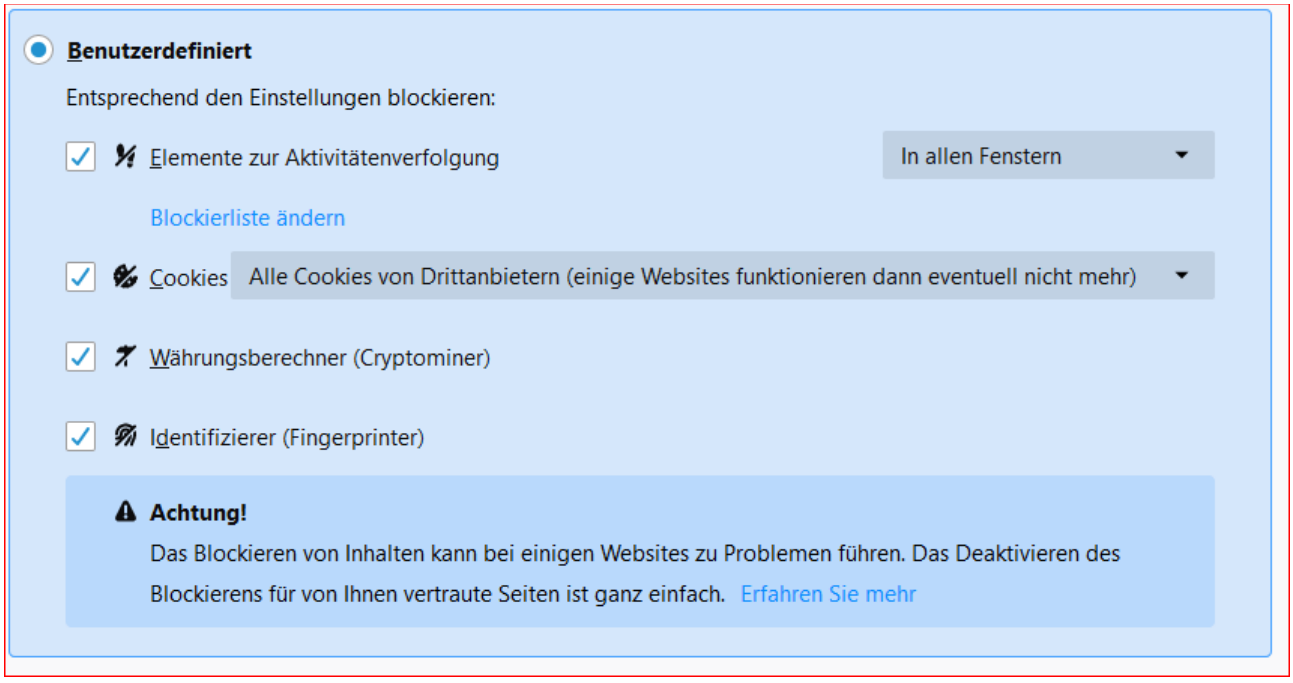


1.4 Seite 'Datenschutz & Sicherheit' in den Einstellungen

Hier ist das Wichtige für Sicherheit und Datenschutz versteckt.

1.4.1 'Seitenelemente blockieren'

Ich empfehle 'Benutzerdefiniert', und dort folgendes:

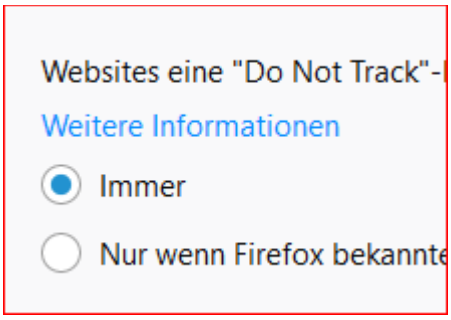


Wenn man Cookies blockiert, kann das zur Folge haben, dass manche Webseiten nicht mehr angezeigt werden. Eventuell muss man das wieder 'raus nehmen, wenn man sehr oft auf dieses Problem stößt. Wichtig ist das Häkchen bei "Währungsberechner (Cryptominer)', das verhindert,

dass eine Webseite auf unserem Rechner Bitcoins berechnet. Auch das Häkchen bei 'Identifizierer (Fingerprinter)' führt dazu, dass Webseiten, die mich über Cookies nicht mehr erkennen auch die charakteristischen Einstellungen meines Browsers nicht mehr dazu nutzen können, mich wieder zu erkennen.

1.4.2 'Do Not Track'

Kann man einstellen, aber das nützt nicht immer, da Webseiten nicht verpflichtet sind, auf den Wunsch mich nicht zu tracken (d.h. zu verfolgen) einzugehen. Es schadet aber auch nicht, die Einstellung zu machen.



1.4.3 'Cookies und Webseite-Daten'

Cookies beim Verlassen des Browsers zu löschen ist eigentlich ganz sinnvoll. Es kann sein, dass Firefox immer im privaten Modus arbeitet und das dann Standard ist.

1.4.4 'Zugangsdaten & Passwörter'

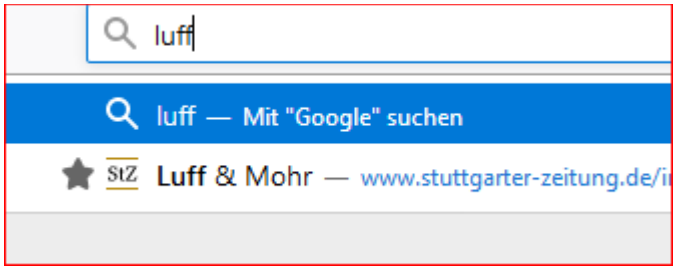
Es ist angenehm, Zugangsdaten und Passwörter im Firefox abzuspeichern, aber: ohne Master-Passwort kann man die problemlos auslesen – vermutlich auch entsprechend präparierte Webseiten könnten das. Also: entweder ein Master-Passwort verwenden (und nicht vergessen!) oder keine Zugangsdaten oder Passwörter im Browser abspeichern.

1.4.5 'Chronik'

Wenn man eine Chronik anlegen lässt, dann können die zuletzt / häufig benutzten Webseite auf der Startseite angezeigt werden. Ist nett – muss man sich halt überlegen, ob man das will.

1.4.6 'Adressleiste'

Ich habe da 'Einträge aus den Lesezeichen' angehakt, dann bekomme ich abgespeicherte Links zu Webseiten schnell angeboten. Beispiel:

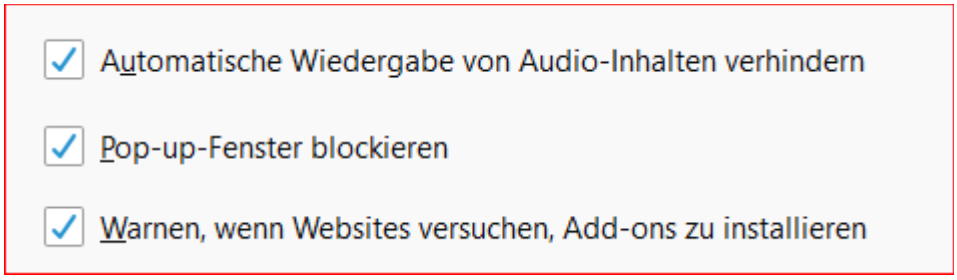


'Luff & Mohr' sind die Karikaturisten der Stuttgarter Zeitung – ich mag deren Karikaturen.

1.4.7 'Berechtigungen'

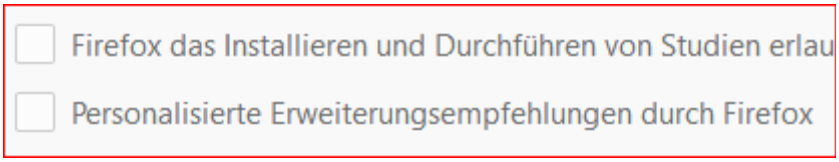
Da sollte alles abgeschaltet sein, wenn man Webseiten nicht auf Standort, **Kamera (!) und Mikrofon (!)** zugreifen lassen will. Das ist eigentlich der Standard. Man müsste dann gezielt eine Webseite dazu berechtigen (falls der Zugriff mal nötig sein sollte), was ich sehr sinnvoll finde. Wenn man in den Windows Einstellungen Programmen (Apps) verboten hat, auf Standort, Kamera und Mikrofon zu zu greifen, dann muss man das dann dort noch dem Firefox erlauben.

Die folgenden Häkchen finde ich sinnvoll:



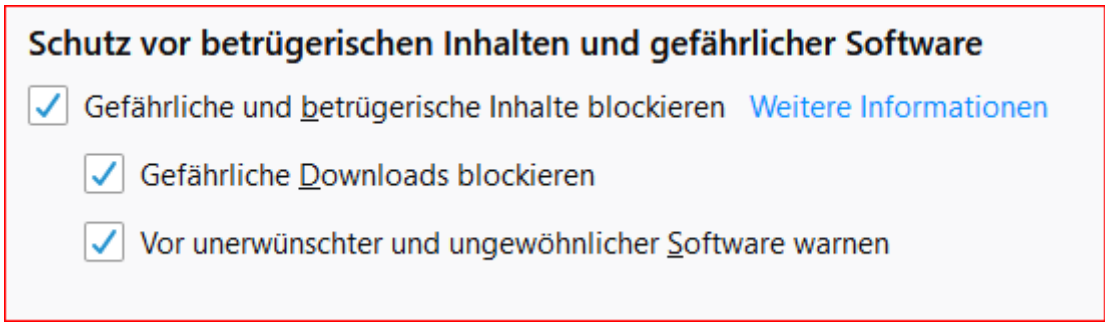
1.4.8 'Datenerhebung durch Firefox und deren Verwendung'

Im Gegensatz zu Google, Microsoft und Co. lebt Firefox (Mozilla, die Community, die Firefox und Thunderbird programmiert) nicht von Werbung. Es ist also nicht ganz so kritisch, denen Daten zu technischen Details zu geben. Muss jeder selbst wissen. Ich möchte auf jeden Fall aber nicht, dass bei mir was ohne Genehmigung installiert wird oder Studien durchgeführt werden:



1.4.9 'Schutz vor betrügerischen Inhalten und gefährlicher Software'

Das macht auch ein Virenscanner wie Kaspersky oder Windows Defender (der aber nur dann, wenn man ein paar magische Befehle kennt, bei Bedarf bei mir nachfragen). Es schadet aber nicht, wenn noch jemand aufpasst. Ich empfehle die drei Häkchen zu machen.



1.4.10 'Zertifikate'

Ehrlich gesagt weiß ich nicht so recht, wo drauf sich das bezieht. Hab 'Jedes Mal fragen' und 'Aktuelle Gültigkeit... bestätigen lassen' aktiviert.

1.5 Seite 'Sync' in den Einstellungen

Damit kann man Lesezeichen usw. über mehrere Geräte gleich (synchron) halten. Ist Geschmackssache.

2 Firefox absichern

2.1 Informationen aus c't 20/2017

In Browsern kann man Passworte abspeichern. Bei Edge und Crome (der speichert die Passworte sogar im Klartext in der Cloud) sollte man das auf keinen Fall machen. **Bei Firefox sollte man ein Master-Passwort benutzen. Dann werden die anderen Passworte verschlüsselt abgelegt.** Man sollte das Master-Passwort aber auf keinen Fall vergessen!

Im Firefox findet man unter 'Einstellungen', dort unter 'Datenschutz & Sicherheit' diverse Punkte zum Absichern des Browsers.

Weiterhin sollte man bei allen Browsern:

- Auto Updates aktivieren – am Besten nach Rückfrage
- Aktive Inhalte einschränken, d.h. JavaScript abschalten (am besten per AddOn) – das hat aber auch Nachteile, man muss JavaScript dann immer manuell für Webseiten frei schalten, damit sie angezeigt werden können
- Flash und Java abschalten
- SSL-Verschlüsselung forcieren
- Tracking unterbinden
- Telemetriefunktionen abstellen
- Firefox kann mit user.js gehärtet werden, das hat aber auch Nachteile, da dann sehr vieles abgeschaltet wird

Folgende AddOns sollten **gelöscht** werden:

- Flash Player
- Java Runtime
- WOT (Web Of Trust)

Folgende AddOns sollten **installiert** werden:

- HTTPS Everywhere
- uBlock Origin
- Decentraleyes

Webseite zu diesen Informationen findet man in dem Artikel von c't: http://ct.de/y5eb, es folgen die im Artikel erwähnten ADD-ONs.

2.1.1 NoScript

Add-on für Firefox, das in Webseiten eingebettete JavaScript-Programme blockiert, bis Sie die Freigabe erteilen. Das hat einmaligen Mehraufwand zur Folge bei den Webseiten, die man mit JavaScript anzeigen möchte, da sonst nichts zu sehen ist.

2.1.2 HTTPS Everywhere

Das für Firefox und Chrome erhältliche Add-on HTTPS Everywhere klinkt sich in die Webseiten-

Abfrage und wählt - sofern vorhanden - auch dann die HTTPS-gesicherte Variante, wenn der Anwender sie nicht explizit abruft. Per Opt-in kann es das Nachladen von unverschlüsselt übertragenen Elementen (etwa Werbe-Banner) oder sogar unverschlüsselte Verbindungen generell blockieren.

2.1.3 uBlock Origin

Das Add-on uBlock Origin von Raymond Hill ist ein Adblocker, der das Anzeigen unerwünschter Werbung verhindert. Es nutzt nach eigenen Angaben weniger Ressourcen als Adblock Plus und filtert Werbung, Werbetracker und Malvertising-Angriffe anhand mehrerer Filterlisten heraus. uBlock Origin ist für Firefox, Chrome und Edge erhältlich. Manche Webseiten werden dann aber nicht mehr angezeigt (z.B. Spiegel Online).

2.1.4 Decentraleyes

Bei jedem Abruf lädt der Browser die Bibliotheken von diesen Dritten nach, die ihn tracken können. Firefox- und Chrome-Nutzer haben mit dem Add-on Decentraleyes die Möglichkeit, ihren Browser gegen derlei Tracking zu schützen. Das Add-on speichert die Bibliotheken lokal und blockiert Abrufe beispielsweise von Google Hosted Libraries, Microsoft Ajax CDN und dem Cloudflare CDN.

2.1.5 LastPass

Passwort-Manager als Add-on für Firefox, Chrome oder Edge, der Passwörter verschlüsselt entweder lokal oder in der Anbieter-Cloud ablegt (Alternative zu den unsicheren Passwort-Managern der Browser selbst).

2.1.6 user.js-Projekt von pyllyukko (englischsprachig)

Für fortgeschrittene Anwender: Die user.js-Datei des finnischen Entwicklers pyllyukko überschreibt die Präferenzen des Firefox-Anwenders und ist deshalb auch dazu geeignet, fremde Systeme von eher unbedarften Nutzern - etwa in der Familie - zu härten, ohne viel Komfort einzubüßen. Kopiert man die user.js ins Firefox-Hauptverzeichnis, wirkt sich die Änderung auf alle Profile aus. Es ist auch möglich, sie in ein einzelnes Profilverzeichnis zu kopieren, um sie erst einmal zu testen oder sich eine temporär sicherere Surf-Umgebung zu schaffen. Die user.js von pyllyukko ändert mehr als 200 Parameter im Browser, schaltet etwa nicht benötigte APIs ab.

2.2 Firefox Sicherheitskompendium 1 aus c't 7/2019

Die Computerzeitung c't hat eine Reihe von Artikeln herausgegeben, aus denen ich einige wichtige Punkte im Folgenden zusammen gefasst habe.

2.2.1 Suchmaschine

Die Standardsuchmaschine ist Google, Startpage verfolgt den User nicht. Startpage nutzt Google, geht über einen Proxy, um die Trefferseiten anzusehen.
Ich empfehle www.startpage.de als Suchmaschine.
Weitere Suchmaschinen findet man in c't 6/2016.

2.2.2 Werbung abwehren mit uBlock Origin

Mit dem ADD-ON 'uBlock Origin' wird Werbung abgeblockt. Auch Tracker und Social-Media-Gedöns wie Facebook und andere Buttons werden unschädlich gemacht. Die Social-Media Filter müssen manuell aktiviert werden (uBlock Origin Icon im Browser anklicken, dann auf die Schieberegler, dann dort auf Filterlisten, dann alles aktivieren, unter Belästigungen erst aufklappen).

Es kann aber passieren, dass man zu viel blockiert und Webseiten nicht mehr angezeigt werden. In dem Fall kann man den Blocker für einzelne Webseiten deaktivieren.

Der 'Medium Mode' bietet noch mehr Möglichkeiten, man kann das Nachladen von Scripten und Frames von externen Seiten deaktivieren. Dazu muss man unter 'Meine Filter' folgendes eintragen:

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

2.3 Firefox Sicherheitskompendium 2 aus c't 8/2019

In dem Artikel geht es um Tracker-Sperren.

2.3.1 JavaScript-Frameworks

JavaScript-Frameworks werden gerne von Webseitenprogrammieren benutzt. Diese Frameworks werden von Google bzw. Cloudflare bereit gestellt. Durch die Nutzung wird aber die IP-Adresse an Google & Co. Übermittelt. Das Add-ON 'Decentraleyes' verhindert das. Details dazu im Artikel ct.de/yrqu.

Wenn das ADD-ON installiert ist, kann man es über http://decentraleyes.org/test/ testen.

Wenn man 'uBlock Origin' installiert hat, muss man folgende Ausnahmen dort eintragen:

```
* ajax.googleapis.com * noop
* ajax.aspnetcdn.com * noop
* ajax.microsoft.com * noop
* cdjns.cloudflare.com * noop
* code.jquery.com * noop
* cdn.jsdelivr.net * noop
* yastatic.net * noop
* yandex.st * noop
* apps.bdimg.com * noop
* libs.baidu.com * noop
* lib.sinaapp.com * noop
* upcdn.b0.upaiyun.com * noop
* cdn.bootcss.com * noop
* sdn.geekzu.org * noop
* ajax.proxy.ustclug.org * noop
```

2.3.2 First Party Isolation

Hier geht es um Site-übergreifendes Tracking mit Drittanbieter-Cookies. Schutz davor bietet das ADD-ON 'First Party Isolation'.

Man kann die First Party Isolation auch über 'about:config' im Firefox aktivieren. Der Eintrag heißt:
`privacy.firstparty.isolate = true`

Mit dem ADD-ON kann man die Funktion aber leicht ein- und ausschalten.
Wenn der LOGON auf Webseiten nicht funktioniert, kann es an dem Parameter liegen. Dann kann

man den Schutz etwas aufweichen, indem man den Parameter setzt:
`privacy.firstparty.isolate.restrict_opener_access = false`

2.3.3 Drittanbieter Cookies

Standardmäßig akzeptiert Firefox Cookies von Drittanbietern. Dies kann man im Firefox unter 'Einstellungen / Datenschutz & Sicherheit' unter 'Seitenelemente blockieren' mit 'Benutzerdefiniert' unter Cookies mit der Einstellung 'Alle Cookies von Fremdanbietern …' ändern.

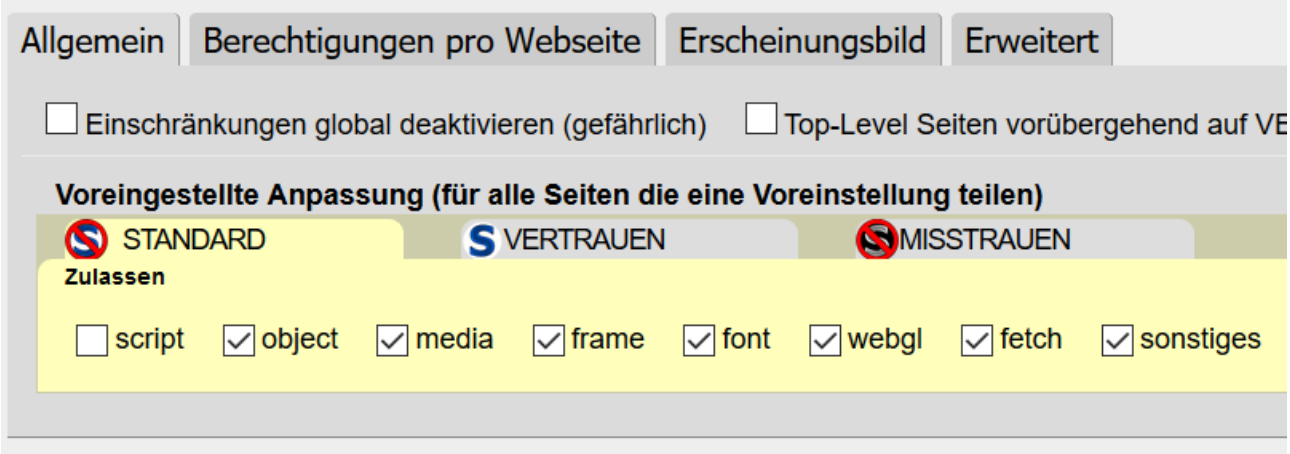
2.4 Firefox Sicherheitskompendium 3 aus c't 9/2019

Thema des Artikels ist 'Smart gescriptet'. JavaScript wird von der Werbebranche genutzt, um den Benutzer per Browser Fingerprinting wiederzuerkennen. Außerdem ist JavaScript ein potenzielles Sicherheitsrisiko (vgl. ct.de/ymqh). Abhilfe schaffen folgende ADD-ONs.

2.4.1 NoScript

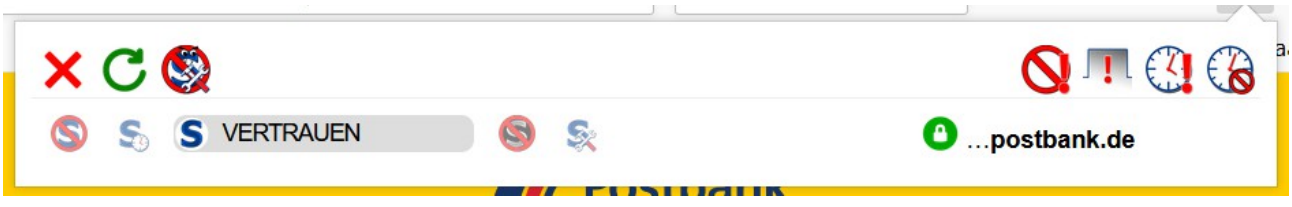
Nach der Installation zeigt es sich durch ein S-Icon in der Adresszeile.
Heise empfiehlt, NoScript folgendermaßen anzupassen:

Einstellungen von NoScript öffnen, dort unter dem Tab 'Allgemein / Standard' alle Häkchen außer bei Script setzen:



Wenn eine seriöse Webseite wegen abgeschaltetem Script meckert oder nicht funktioniert, erst mal Script temporär frei geben. Wenn es dann klappt, dann nur für diese Seite permanent frei geben.

Das grüne Schloss zeigt, dass die Webseite JavaScript TLS verschlüsselt überträgt:



2.4.2 Smart Referer

Beim Aufrufen einer neuen Seite wird die Information, von wo man kommt an die neue Webseite

übertragen. Das können auch Fremdanbieter nutzen, um Werbung anzupassen.
Das ADD-ON 'Smart Referer' verhindert das. Falls Webseiten mit Smart Referer nicht mehr funktionieren, lassen sich Ausnahmen definieren.

Selbst dann, wenn man zum Beispiel eine Seite bei Spiegel online aufruft, erfährt Google davon, weil Spiegel online JavaScript von www.googletagmanager.com einbindet, da 'von wo' in die Anfrage eingebunden wird! Manchmal werden so sogar personenbezogene Daten übermittelt (zum Beispiel e-Mailadresse). Smart Referer baut das Referer-Feld um und verhindert so das Weitergeben von Informationen.
Falls Webseiten nicht mehr funktionieren, kann man Smart Referer temporär deaktivieren. Es können auch feste Ausnahmen für Webseiten definiert werden.

2.5 Firefox Sicherheitskompendium 4 aus c't 10/2019

In diesem Beitrag geht es um die Bereinigung von URLs. Zur Behinderung von Werbung können Tracking-Informationen unterbunden werden.

2.5.1 Neat URL

Das ADD-ON 'Neat URL' verhindert die Weitergabe von Tracking Parametern (siehe ct.de/yh7b).

2.5.2 Skip Redirect

URLs enthalten manchmal versteckte Umleitungen. Speziell Google nutzt das. Zum einen ist das in Hinsicht auf den Datenschutz problematisch, zum anderen verlangsamt das den Aufbau der Seite.

Skip Redirect verhindert das. Es kann jedoch zu Problemen kommen, wenn Webseitenbetreiber zum Abschluss eines Kaufvertrages mit externen Zahlungsdienstleistern zusammen arbeiten. Dann kann man für diese Seite Skip Redirect deaktivieren bzw. die Seite in die Blacklist eintragen.

Man kann auch eine Whitelist anlegen, d.h. die Webseiten eintragen, dann wird nur für diese Webseiten die Umleitung entfernt.

Alphabetischer Index