Internetsicherheit

Der Zugang zum Netz wird in den meisten offensichtlichen [1)] Fällen über einen Browser hergestellt. Diesem soll deswegen auf dieser Seite besondere Aufmerksamkeit gewidmet werden.

Klick mal hier, um selbst zu sehen, was Dein Browser so alles über Dich mitteilt [2)]:

http://www.zendas.de/service/browserdaten.html

Konsequenzen:

- Meide den InternetExplorer - er sitzt zu tief in Windows, ist an vielen Stellen Teil des Betriebssystemkerns selbst. Durch seine weite Verbreitung lieben ihn Viren- und Trojanerprogrammierer.
- Meide Google Chrome - er ist immer auch dazu da, seinem Hersteller zu dienen. Nutze, wenn es denn schon sein muss, die bereinigte Alternative Chromium.

Nutze diese Seite, um Dich über die aktuellen Einstellungen Deines Browsers und die Technologie dahinter zu informieren: http://www.heise.de/security/dienste/Browsercheck-2107.html

Da **Firefox** OpenSource ist, sich durch PlugIns erweitern lässt, er für alle Plattformen verfügbar und außerdem der Standardbrowser im KvFG Netz ist, wird nun gezeigt, wie sich dieser sicherer betreiben lässt:

Grundlagen

Stelle Deinen Firefox so ein, dass dieser Webseiten mitteilt, dass Du nicht verfolgt werden willst. Zwar hält sich nicht jede Seite an diese Einstellung - aber es werden immer mehr.

Cookies

Weiter solltest Du die Cookie-Verwaltung des Firefox so konfigurieren, dass Cookies von Drittanbietern überhaupt nicht angenommen werden, da Dich sonst alle auf der von Dir besuchten Webseite eingebundenen Dienste ebenfalls mit Keksen befüllen. „Cookies von Drittanbietern akzeptieren“ sollte demnach auf „Nie“ stehen.

Auch sollten Cookies spätestens dann gelöscht werden, wenn Du das Browserfenster zu machst. Stelle Firefox deswegen so ein, dass bei „Behalten, bis“ steht: „Firefox geschlossen wird“.

Für noch härtere Gangarten gegenüber Cookies (also z.B. bestimmten Seiten verbieten, Cookies überhaupt auf Deinem Rechner abzulegen) eignen sich die in Firefox eingebauten Funktionalitäten nur bedingt. Lies für dieses Szenario weiter unten weiter.

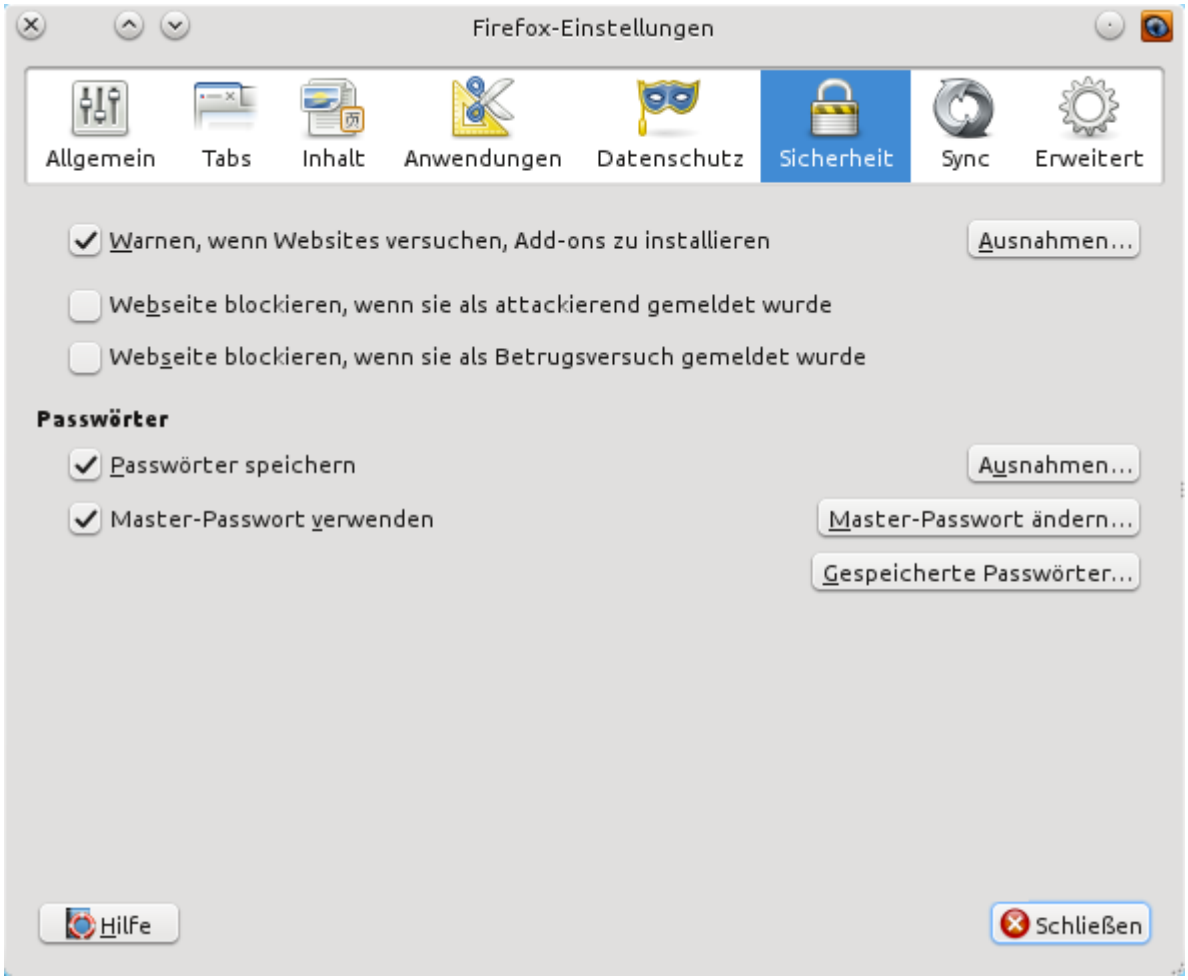
Lösche beim Surfen regelmäßig den lokalen Cookie-Cache Deines Firefox ([Strg] [Umschalten] [Entf] zeigt Dir die Option). Nach einem Besuch bei Facebook kannst Du so leicht alle Cookies auf einmal loswerden.

History

Klick mal hier: http://www.zendas.de/service/browserdaten/css_hack.html

Und jetzt überlege Dir, ob Du nicht lieber regelmäßig Deine Browser-History (Chronik) löschen willst. Im Einstellungsfenster oben siehst Du hierzu eine entsprechende Checkbox, die ich bei mir nicht aktiviert habe: ich mach das lieber (un)regelmäßig von Hand, weil ich zu häufig in meiner Browser-History nach Webseiten suche, auf denen ich relevante Informationen fand.

Passwörter



Wenn Du Deine Passwörter in Firefox speicherst, dann lege auf jeden Fall ein Masterpasswort ausreichender Komplexität fest.

Ent-Google-n

Das Bild oben enthält schon einige weitere evtl. auch für Dich richtige Einstellungen: Die beiden

Funktionen

- Webseite blockieren, wenn sie als attackierend gemeldet wurde
- Webseite blockieren, wenn sie als Betrugsversuch gemeldet wurde

bedeuten nichts anderes, als dass Firefox sich jede Stunde eine Datei herunter lädt, die die Domain-Namen mit Malware enthält und dann prüft, ob Du Dich gerade auf diesen „bösen Seiten“ herumtreibst. Die im obigen Bild zu sehenden Einstellungen sind, weil Firefox lediglich lokale Überprüfungen durchführt, somit nur für fortgeschrittene Paranoiker angeraten, die die Übertragung der eigenen IP an Mozilla im Kontext des Downloads verhindern wollen.

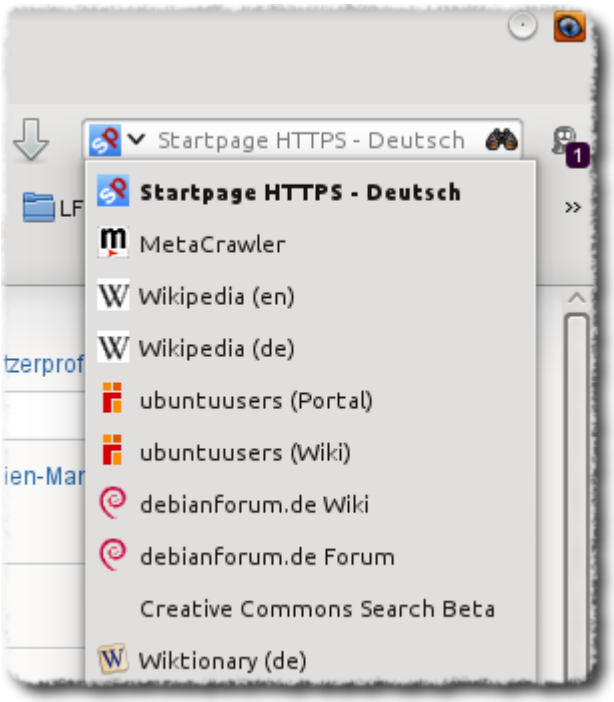
Vergiss nicht, die **Startseite Deines Browser** umzustellen. Empfohlen werden kann https://startpage.com, das sich als Vermittler zwischen Deinen Browser und Google einklinkt. Die Google Suche wird dann von Startpage übernommen und Google bekommt Deine Daten nicht mehr zu sehen. Du findest die Funktion

- unter Windows: /Extras /Einstellungen /Allgemein /Startseite
- unter Linux: /Bearbeiten /Einstellungen /Allgemein /Startseite

Weiter sollte man die **GEO Informationsdienste** abzuschalten, die ebenfalls an Google hängen. Verfahre wie folgt:

- In der URL Zeile eingeben: about:config
- Die Warnmeldung abnicken
- In die Filterzeile eingeben: geo.enabled
- Doppelklick auf den Eintrag geo.enabled

Dieser Eintrag sollten nun von „true“ auf „false“ umgeschaltet sein.



Wer das **Suchfeld** rechts oben in Firefox nutzt, sollte dieses ebenfalls bearbeiten und Startpage als Default-Suchmaschine einrichten. Die Einträge für Google und Bing sowie Yahoo kann man über die Funktion „Suchmaschinen verwalten …“ löschen. Ganz einfach erhält man den Eintrag für Startpage durch Aufruf der folgenden Seite:

https://startpage.com/deu/download-startpage-plugin.html

Wer die Suchfunktion direkt aus der **URL Zeile** nutzt, sollte diese von Google auf Startpage umschalten. Wie das geht, steht hier:

https://startpage.com/deu/company-faq.html#q13

Kurzbeschreibung:

- about:config
- keyword.URL

und hier entweder den auf Google zeigenden Eintrag ändern in:

```
https://startpage.com/do/search?language=deutsch&cat=web&query=
```

oder den Eintrag keyword.URL als string selbst neu anlegen, wenn dieser in Deiner Version des Firefox nicht vorhanden ist.

Erweiterungen

Um Angriffe von Webseiten auf Deine persönlichen Daten und das Abgreifen dieser Daten zu verhindern - oder zumindest: zu erschweren - solltest Du die folgenden PlugIns (Erweiterungen, AddOns) für Firefox installieren und mit Umsicht auch nutzen.

Weich

https://addons.mozilla.org/de/firefox/addon/ublock-origin/

uBlock Origin verhindert die Anzeige der meisten Werbebotschaften und damit auch, dass diese Seiten Dein Surfverhalten beobachten. Diese Erweiterung spart darüber hinaus (vor allem wichtig bei mobilen Endgeräten) Bandbreite, beschleunigt so das Surfen und stellt das Internet wieder so dar, wie es sein sollte. Diese Erweiterung ist ein echter Gewinn an Komfort! [3)].

https://addons.mozilla.org/de/firefox/addon/privacy-badger-firefox/

Alternativ zu Ghostery, das zunehmend im Verruf kommt, weil die Firma mit dem Add-on kommerzielle Interessen verfolgt, kann auch der einfachere Privacybadger eingesetzt werden.

https://addons.mozilla.org/de/firefox/addon/canvasblocker/

Canvas Fingerprinting ist eine Tracking Technik die hier auf Wikipedia näher beschrieben wird und sich mit dem Addon **CanvasBlocker** in den Griff bekommen lassen könnte / sollte.

Hart

https://addons.mozilla.org/de/firefox/addon/noscript

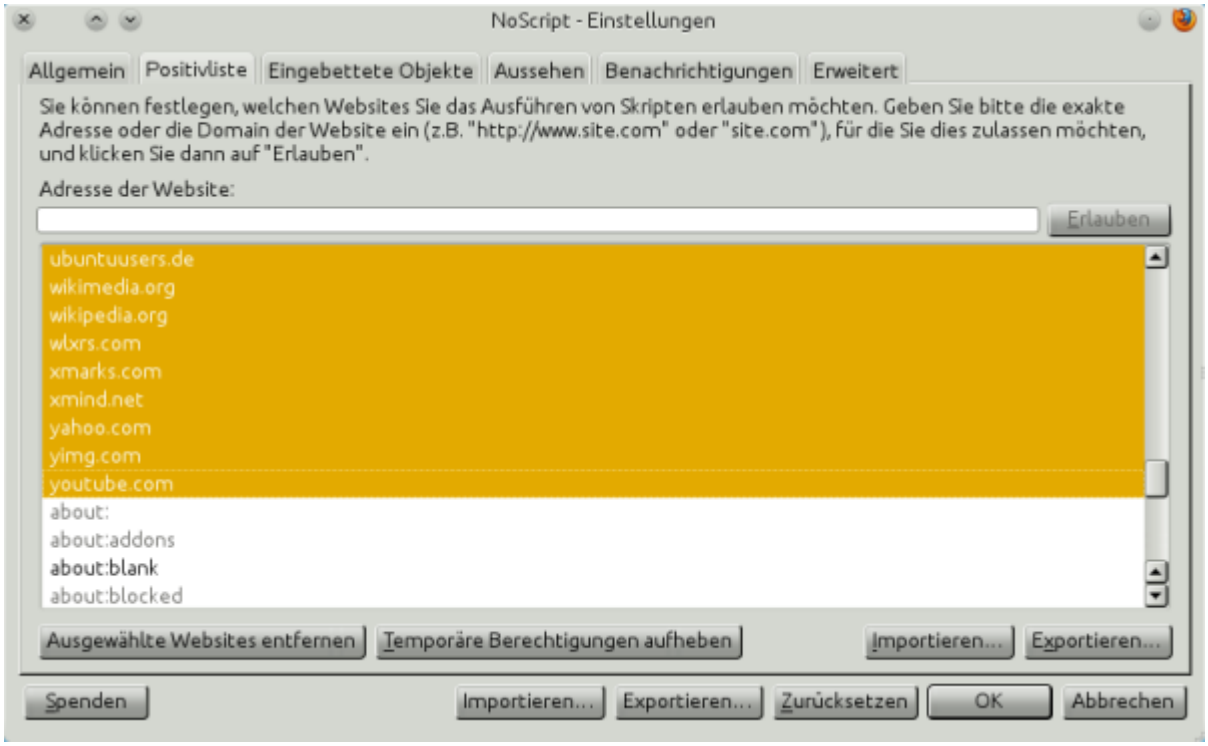
NoScript verhindert die Ausführung von **Scripten** in Deinem Browser und erlaubt es Dir, die Ausführung von Scripten nur ganz bestimmten Anbietern komplett oder zeitlich beschränkt zu erlauben. Mit diesem PlugIn erschwerst Du die Installation von bösartiger Software auf Deinem Rechner und die Verfolgung Deines Nutzerverhaltens.

Du musst allerdings sehr restriktiv mit der Freigabe von Scripting-Rechten verfahren und nicht etwa gleich Google-Analytics oder Facebook erlauben, Scripte auszuführen. Schalte immer zuerst nur temporär genau die Domain frei, auf der Du gerade bist (vergleiche also mit der URL, die Du im Browser in der Navigationsleiste oben ablesen kannst), und probiere aus, ob das nicht reicht, um die Webseite zu nutzen. Gehe Schritt für Schritt vor!

In vielen Fällen macht die Funktion von NoScript Sinn, einer Webseite lediglich temporär die Ausführung von Scripten zu erlauben. Nur / Erst wenn Du regelmäßig die Seite nutzt und dieser auch vertrauen kannst, solltest Du die Ausführung von Scripten für diese Webseite komplett freigeben.

Kombiniere NoScript mit Facebook-Clients (z.B. friendica oder Diaspora), um zu vermeiden, beim Aufenthalt auf Facebook erst alle Scripte freigeben zu müssen und dies dann nachher bei Deinen weiteren Streifzügen durchs Netz nicht wieder zurück zu nehmen.

Der Umgang mit diesem PlugIn erfordert Einarbeitungszeit und auch einiges an Gewöhnung. Lass Dir Zeit und setze dieses nach ein paar Wochen mal wieder auf seine Grundeinstellungen zurück, um Anfangsfehler bei der Konfiguration los zu werden.



Gehe hierzu zu Extras - Addons und klicke bei NoScript auf Einstellungen. Wähle die Registerkarte Positivliste und markiere alle Domaineinträge (meist bis youtube). Klicke dann auf Ausgewählte Websites entfernen.

https://requestpolicycontinued.github.io/

bzw.

https://addons.mozilla.org/de/firefox/addon/requestpolicy

Das Add-on **Request Policy** (Continued) arbeitet ähnlich wie NoScript, bezieht sich jedoch nicht auf Scripte an sich, sondern auf das Verhalten von Webseiten, von weiteren Seiten Inhalte nachzuladen. Das können harmlose Cloud Speicher des Domain-Inhabers sein, weniger harmlose Fonts von Google oder auch über Werbung eingeschleuste Inhalte Dritter.

Die Pflege des Add-ons ist ähnlich aufwändig und auch umständlich wie bei NoScript. Dafür ist jedoch der Sicherheitsgewinn groß.

Knallhart

https://addons.mozilla.org/de/firefox/addon/cookies-manager-plus

oder

https://addons.mozilla.org/de/firefox/addon/cookie-monster

Der Umgang mit **Cookie**-Managern erfordert noch mehr Disziplin. Du musst beim Einsatz derartiger Erweiterungen damit rechnen, dass sich das Internet zu Beginn komplett anders anfühlt - weil erst einmal fast nichts mehr wie gewohnt funktioniert. Einerseits ist dies ein deutlicher Hinweis darauf, wie Cookie-verseucht das Netz inzwischen ist - andererseits sind Cookies aber auch nötig, damit Webseiten überhaupt funktionieren: z.B. sorgen Cookies dafür, dass Du Dich nicht nach jedem Klick in unserem Moodle neu anmelden musst, sondern Dein Browser von sich aus der Webseite mitteilt, dass Du wirklich Du bist.

Probiere einige Cookie-Manager wenigsten ein paar Tage am Stück aus, bevor Du Dich endgültig für oder gegen deren Einsatz entscheidest. Der Zugewinn an Privatsphäre ist heftig - aber eben auch die gefühlten Veränderungen im Netz.

Weitere

Weitere Plugins und Erweiterungen für Firefox, die dazu dienen, Deine **Sicherheit im Netz** zu erhöhen und Deine Privatsphäre zu schützen findest Du in dieser Kategorie:

https://addons.mozilla.org/de/firefox/extensions/privacy-security/

Die Erweiterungen **HTTPS Everywhere** der Electronic Frontier Foundation sorgt dafür, dass Du sicherer surfst. Informiere Dich und nutze den Dienst als PlugIn für Deinen Firefox:

https://www.eff.org/https-everywhere

Die Erweiterung **User Agent Switcher** verbirgt Deine Spuren im Netz dadurch, dass Du die Informationen über Dein Betriebssystem und Deinen Browser schlicht fälschst. Wer regelmäßig umschaltet bringt die eine oder andere Auswertungsroutine so ins Straucheln.

https://addons.mozilla.org/de/firefox/addon/user-agent-switcher/

Konsequent

Wenn Du wirklich weitgehend **anonym im Netz** unterwegs sein willst (oder musst), dann informiere Dich über Tor und Onion-Routing: https://de.wikipedia.org/wiki/Tor_%28Netzwerk%29

https://www.torproject.org

Um Dein privates Netz [4)] vor Angriffen von Außen (also aus dem Internet) zu schützen, reichen Programme auf Deinem Computer nicht aus. Du brauchst hierzu eine dedizierte **Firewall**, um Dein internes Netz vom Internet abzutrennen. Diese filtert - von Dir einstellbar wie umfangreich - dazu noch den ganzen Netzdreck gleich mit raus. Eigentlich sollten Deine Eltern sich um diesen Punkt kümmern - schließlich ist das Internet erst frei ab 18.

Im Abschnitt Firewall findest Du mehr Informationen zum Thema.

Wenn Du Dich, Deine Daten und Deine Rechner absichern willst, dann solltest Du auf ein **Betriebssystem** umsteigen, das nur wenige auf dem Desktop nutzen und das deswegen von Viren- und Trojaner-Programmierern ignoriert wird und sich darüber hinaus komplett (also inklusive aller installieren Programme) selbst auf dem neuesten Stand hält: Dein Kühlschrank nutzt es, Dein Smartphone verwendet es wahrscheinlich auch, rund 2/3 der Server im Internet nutzen es und 99% der Supercomputer. Dieses System bringt darüber hinaus eine sehr gute Sicherheitsarchitektur mit:

Im Abschnitt Linux findest Du mehr Informationen zum Thema.

Googlen?

Um es kurz zu machen: Wer großen Wert auf Sicherheit im Sinne von Privatsphäre legt, meidet diesen Dienst (siehe oben zu alternativen Suchmaschinen). Wer Kompromisse eingeht - für den sind die folgenden Tipps gedacht:

Du kannst z.B. Startpage verwenden. Das ist nicht mehr als ein Frontend für Google - mit dem Vorteil, dass Google aber nur die IP von Startpage zu sehen bekommt und nicht die Deine:

https://startpage.com/

Wenn Du trotzdem unbedingt Google verwenden willst, dann melde Dich nicht mit Deinem **Google-Benutzerkonto** an, wenn Du nur Suchen willst. Auch Dein Firefox merkt sich, auf welchen Webseiten Du warst und informiert Dich mit [Strg] [H] über Deine Onlinegeschichte - allerdings ohne dass Du hierdurch entrechtet würdest. Die Google History benötigst Du nicht.

Deaktiviere die History-Funktionen in Deinem Google-Profil und überprüfe die Einstellungen Deines Profils regelmäßig.

Wenn Du unbedingt Google nutzen willst, dann tu dies über die folgende Seite, die weitere Sicherheitsmechanismen implementiert:

https://encrypted.google.com/

Diese Funktionen schützen Dich dann zwar nicht vor Google, aber vor vielen anderen, die auf der

Leitung zwischen Dir und Google ihr Ohr haben.

Smartphone und Verwandte

Beachte, dass Du mit der Nutzung der in Deinem Smartphone verbauten Browser meist gleich in der Cloud Deines Anbieters hängst und somit diesem die Daten über Dein Onlineverhalten mitgibst. Nutze deswegen auch auf Deinem Smartphone alternative Browser wie Firefox, Dolphin HD, Opera und dergleichen.

Informiere Dich über Datenschutzeinstellungen Deines Smartphones und schalte alles ab, was Du nicht unbedingt brauchst - z.B. geoinformation und location based services, wenn Du in der Schule sitzt.

Nutze auch auf Deinem Smartphone überwiegend freie Dienste und Programme. Anstatt z.B. Google Maps steht Dir auch OpenStreetMap zur Verfügung. Statt Google Reader kannst Du freie Reader - z.B. Sage in Firefox - nutzen und statt den Google-Mail-Client unter Android z.B. das mächtigere K9.

Lies für Android hier weiter: http://fsfe.org/campaigns/android/android.de.html

Weiter: Soziale Netze

1)
Es gibt noch viele, nicht so offensichtliche Fälle: Viele Programm nehmen „von sich aus“ und oft ungefragt immer mal wieder Verbindung mit dem Hersteller auf, blasen Daten ins Netz oder suchen nach Updates. Dies soll hier nicht Gegenstand der Betrachtung sein.
2)
ZENDAS ist die Datenschutzstelle der Unis in BaWü. Man sollte der Seite vertrauen dürfen.
3)
Selbstverständlich ist dieses PlugIn nicht Nebenwirkungsfrei für die Betreiber der Seiten, die ihren Service ja über Werbung auch finanzieren, weswegen man sich überlegen sollte, ob man das Adon auf regelmäßig gelesenen Seiten deaktivieren sollte
4)
Gemeint ist hiermit das Netz in Deinem Haus und nicht Dein Rechner / ein einzelner Rechner in diesem Netz.