Surfen, aber sicher!

Wie sich Sicherheit und Privatsphäre verbessern lassen durch optimierte Browsereinstellungen

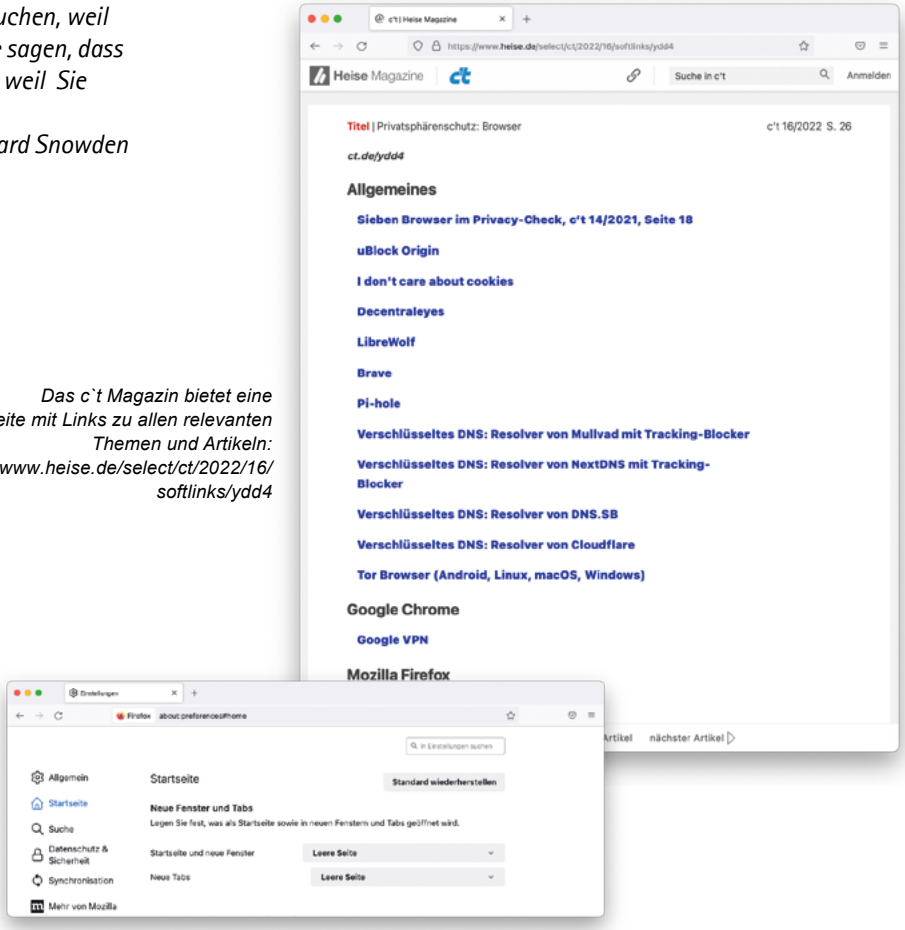
„Zu argumentieren, dass Sie keine Privatsphäre brauchen, weil Sie nichts zu verbergen haben, ist so, als würden Sie sagen, dass Sie keine Freiheit der Meinungsäußerung brauchen, weil Sie nichts zu sagen haben."

Edward Snowden

Die Privatsphäre beim Surfen im Internet ist bereits bedroht und tatsächlich ziemlich ausgehöhlt. Die Datenspuren, die wir bei der täglichen Nutzung hinterlassen, sind äußerst umfangreich. Die Gefahr für den Missbrauch entsteht vor allem auch aus der langfristigen Speicherung bei verschiedensten Diensten und dem Zusammenfügen unterschiedlichster Nutzungen zu Nutzerprofilen, die tief in das Verhalten blicken lassen. Ein ganzer Industriezweig hat sich um die Verfolgung von Nutzern entwickelt.

Welche Seiten und Inhalte werden wie lange und wie oft betrachtet? Was wird gekauft, was sind Vorlieben?

Es gibt zahlreiche Möglichkeiten, das zu ändern, doch nur, wer selbst das Steuer in die Hand nimmt und Optionen kennt und einsetzt, der profitiert auch davon.



Das c`t Magazin bietet eine Seite mit Links zu allen relevanten Themen und Artikeln: www.heise.de/select/ct/2022/16/softlinks/ydd4

Der Browser macht den Unterschied

Auch wenn sie ähnlich aussehen und fast identisch zu funktionieren scheinen, so unterscheiden sich die populären Browser Firefox, Safari, Chrome und Edge doch ganz erheblich in ihren Datenschutzmöglichkeiten. Gleich vorab seien daher als bessere Alternativen der Brave Browser und LibreWolf erwähnt, die ihre Existenz dem Schutz der Privatsphäre verdanken.

» https://brave.com
» https://librewolf.net

In sieben Schritten zum sicheren Browser

Da Firefox bereits sehr gute Voraussetzungen bietet, was den Schutz der Privatsphäre angeht, seien hier nur dessen optimierte Sicherheits-Einstellungen aufgeführt, zu erreichen im Firefox-Menü unter „Einstellungen".

1. Unter „Allgemein", ganz unten bei Verbindungseinstellungen, auf „Einstellungen" klicken. Wiederum unten „DNS über HTTPS" wählen (hausinterne Server können damit eventuell nicht mehr angezeigt werden).

2. Links „Startseite" anklicken und am besten für „Startseite und neue Fenster" sowie für „Neue Tabs" „Leere Seite" wählen.

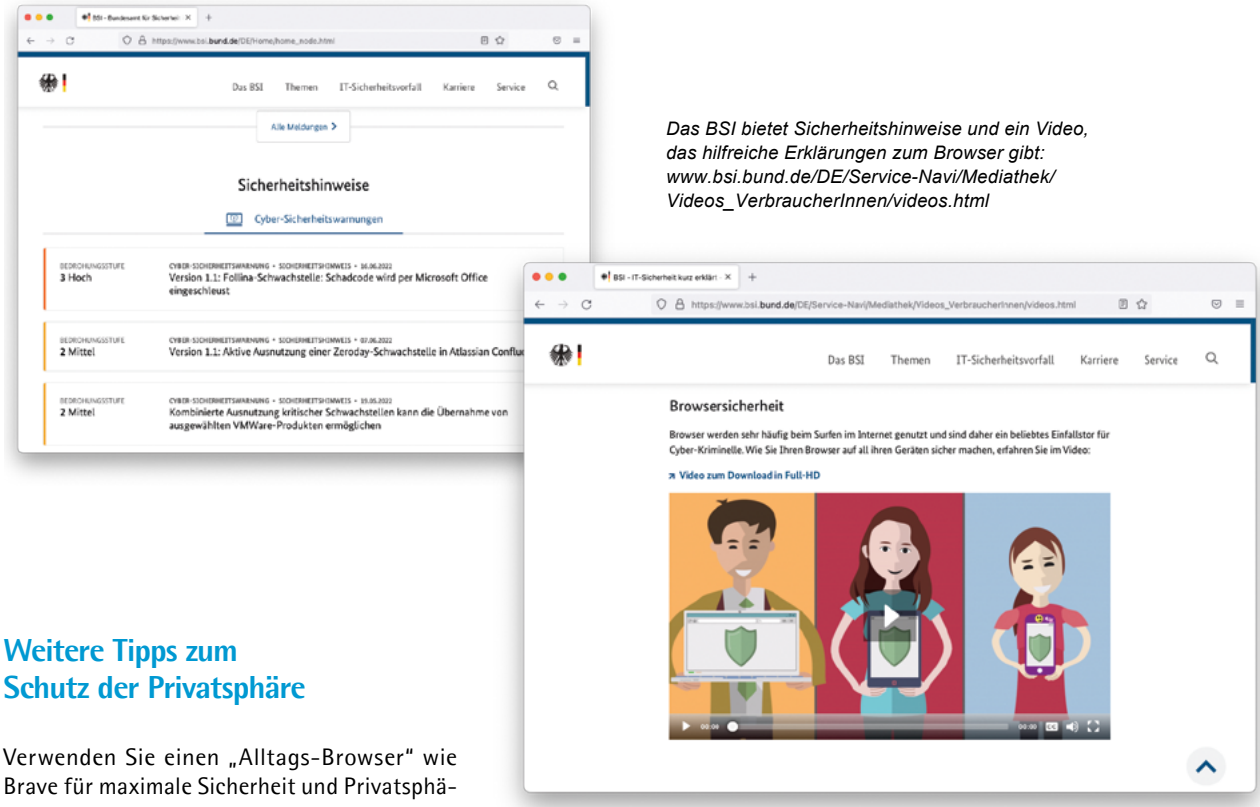
3. Links unter „Suche" statt Google eine datenschutzfreundliche Suchmaschine wie DuckDuckGo auswählen. „Suchvorschläge anzeigen" deaktivieren, um die Übertragung an die Suchmaschine bereits beim Tippen zu vermeiden.

4. Bei „Datenschutz & Sicherheit" den „Schutz vor Aktivitätenverfolgung" von „Standard" auf „Streng" für maximale Sicherheit erhöhen. Das Schutzschild in der Adressleiste ermöglicht es diesen Schutz für eine einzelne Webseite zu deaktivieren, falls diese sonst nicht funktioniert.

5. Weiter unten kann man „Cookies und Website-Daten beim Beenden von Firefox löschen" lassen. So bleiben keine Datenspuren übrig, die bei der nächsten Nutzung abgefragt werden können. „Ausnahmen verwalten ..." hilft einzelne bevorzugte Seiten davon auszunehmen.

6. Bei „Datenerhebung durch Firefox und deren Verwendung" alles deaktivieren, um die Weitergabe ihrer Nutzung zu unterbinden.

7. „Nur-HTTPS-Modus in allen Fenstern aktivieren", um vor unverschlüsselt übertragenen HTTP-Webseiten gewarnt zu werden.



Das BSI bietet Sicherheitshinweise und ein Video, das hilfreiche Erklärungen zum Browser gibt: www.bsi.bund.de/DE/Service-Navi/Mediathek/Videos_VerbraucherInnen/videos.html

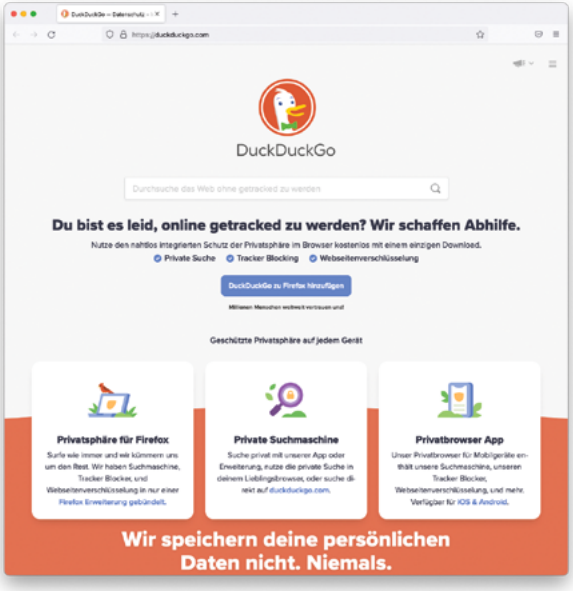
Weitere Tipps zum Schutz der Privatsphäre

Verwenden Sie einen „Alltags-Browser" wie Brave für maximale Sicherheit und Privatsphäre, der so eingestellt ist, dass er keine History speichert sowie mit generell restriktiven Einstellungen. Nehmen Sie als Standardsuchmaschine entweder DuckDuckGo oder Startpage, weil diese nicht mit anderen Diensten vernetzt sind (im Gegensatz zu Google). Vermeiden sie Google Dienste und Google-Logins, da diese eine Verfolgung über ihre gesamte Nutzung ermöglichen. Für dedizierte Recherche schalten Sie dann um auf Firefox mit obigen Einstellungen, damit man zum Beispiel auf gefundene Artikel oder Suchergebnisse wieder zugreifen kann. Da er nur für bewusste Recherche verwendet wird, ist die History reduziert und weniger privat.

Vermeiden sollte man die Unsitte, jede Webseite – auch bekannte – jedes Mal als Suche einzugeben. Besser ist es, sich häufige Adressen zu merken und direkt in die Adresszeile einzugeben oder als Bookmark zu speichern. Das erspart die Suchanfrage und damit auch CO_2 und Energie im Rechenzentrum der Suchmaschine.

Es lohnt sich, das wahrscheinlich am häufigsten verwendete Programm, den Browser, näher kennenzulernen und die verfügbaren Einstellungen durchzugehen. Vieles lässt sich an die eigenen (Sicherheits-)Bedürfnisse sinnvoll anpassen und manches dabei auch vereinfachen und sogar beschleunigen.

Wie immer gibt es auch diesen Artikel als PDF mit Links zum Anklicken: www.bayerisches-aerzteblatt.de/aktuelles-heft.html



Damit ist schon viel erreicht: Umstellung auf leere Startseite, um beim Start Fremdanbieterinhalte zu vermeiden. Alternativ kann auch DuckDuckGo als Startseite dienen. DuckDuckGo ist die Suchmaschine, die die Privatsphäre schützt und keine Daten weitergibt oder speichert. https://duckduckgo.com/

Autor

Dr. Marc M. Batschkus

Arzt, Medizinische Informatik,
Spezialist für E-Health, E-Learning,
Datenmanagement & macOS

E-Mail: mail@batschkus.de