DIE BESTEN BROWSER FÜR IHREN DATENSCHUTZ

Wer ohne Vorsichtsmaßnahmen und Kenntnisse im Internet surft, gibt seine gesamte Persönlichkeit und Interesseren preis.

Vorwort

Liebe Anwenderinnen und Anwender,

auf neuen Laptops oder PCs ist in den allermeisten Fällen Windows vorinstalliert. Hier wiederum ist der eigene Browser „Edge“ von Microsoft mitgeliefert.

Also, im WLAN anmelden, auf „Edge“ klicken – und schon surfen wir im Internet. So weit, so gut, so unkompliziert.

Aber diese Bequemlichkeit hat einen Preis: Alles, was Sie im Internet sehen und tun, bekommen Microsoft, Facebook, Amazon und Co. mit.

Aber vielleicht haben Sie auch schon davon gehört, dass es alternative Browser wie **Chrome** oder **Firefox** gibt. Die sollen schneller oder datenschutzfreundlicher sein.

Als Antwort darauf kann ich leider nur sagen: „Denkste“.

In diesem Leitfaden zeige ich Ihnen, auf was Sie achten sollten, um den Datenschutz beim Surfen zu verbessern.

Ihr Kaner Etem

Datenschutz im Netz: Warum Sie diesen Punkt nicht ignorieren sollten

Das Surfen im Internet ist sehr bequem: Wir sind innerhalb von Sekunden über Geschenisse auf der Welt informiert, viele Einkäufe können wir vom Sofa aus erledigen, wir erreichen unsere Liebsten schnell per WhatsApp und Videochat, wir können online unseren Kontostand einsehen und Überweisungen tätigen.

Jedoch hat diese Bequemlicht einen erheblichen Preis: Da wir die meisten Dienste im Internet nutzen, ohne Geld dafür zu bezahlen, gibt es eine andere Währung, auf das die meisten Internetunternehmen aus sind: Unsere Daten.

Während Sie im Internet surfen, verraten Sie folgende Eigenschaften über sich:

- **Ihren gesamten Internetverlauf**
  Alle Internetbrowser zeichnen Ihren Verlauf auf. Das ist einerseits praktisch für Sie, da Sie einmal besuchte Seiten wieder nachschlagen können bzw. merkt sich der Browser, welche Seiten Sie oft aufrufen und schlägt diese bereits vor, wenn Sie den ersten Buchstaben der Webseite in das Adressenfeld tippen.

  Auf der anderen Seite jedoch senden einige Browser den gesamten Verlauf an den Browser-Entwickler. Speziell Google (Chrome) und Microsoft (Edge) sammeln diese Daten.

  Mit Ihrem Verlauf können unternehmen leicht feststellen, worin Ihre Interessen liegen.

  Übrigens: Auch der Incognito-Modus verhindert nicht, dass Daten an Webseiten und Browser-Entwickler gesendet werden. Dieser verhindert lediglich, dass der Verlauf während einer Incognito-Sitzung auf Ihrem Rechner gespeichert wird.

- **Ihre Suchanfragen (auch solche, die Sie nicht einmal abschicken)**

  Vorsicht: Alles, was Sie ins Adressfeld tippen, wird bereits an die Suchmaschine (in den meisten Fällen Google) gesendet. Dies dient dem automatischen Vorschlagen / Vervollständigen von Suchanfragen.

- **Ihren Standort**
  Durch Ihre IP-Adresse und Ihr WLAN-Netz kann jede Webseite bis auf wenige Meter genau Ihren Standort feststellen. Dadurch kann leicht festgestellt werden, ob Sie in einem teuren Stadtviertel oder auf dem abgeschiedenen Land wohnen.

- **Ihre Geräteinformationen**
  Betriebssystem, Geräteart (PC / Laptop), Bildschirmauflösung: All das erfährt jede Webseite von Ihnen.

  Warum das ebenfalls nicht gut für Sie ist? Nun, wenn Sie zum Beispiel für den nächsten Urlaub nach Flügen oder Hotels suchen, dann zeigen Ihnen viele Buchungsseiten höhere Preise, wenn Sie ein Apple-Gerät nutzen – da viele Käufer von Mac-Rechnern oder iPhones als wohlhabender gelten.

- **Achtung: Sie werden über mehrere Webseiten hinweg verfolgt**
  Mit sogenanntem „Tracking“ und abgelegten „Cookie“-Dateien auf Ihrem Rechner können einzelne Webseiten auch Ihre Aktivitäten auf anderen Webseiten verfolgen. Das machen insbesondere Facebook und Twitter. Dadurch ist es möglich, all Ihre Interessen zusammenzufügen, wie bei einem Puzzle.

Wozu das exzessive Datensammeln führt

Dass die Unternehmen viele Daten über Sie sammeln hat auch reale Konsequenzen:

Viele Unternehmen wissen absolut alles über Sie: Durch Ihre Aktivitäten im Internet geben Sie Ihre Interessen und Ihre Persönlichkeit preis und diese werden „für immer“ auf den Daten fremder Server gespeichert bleiben.

Personalisierte Werbung: Sie bekommen auf Webseiten maßgeschneiderte Werbung zu sehen, die Ihren Interessen entsprechen. Dies führt dazu, dass Sie mehr Geld ausgeben, obwohl Sie das eigentlich nicht wollten.

Personalisierte Nachrichten und Vorschläge: Auch politische Parteien, Vereine und Lobbys nutzen die Daten der sozialen Medien für Werbekampagnen. Daher erhalten Sie auf Facebook und YouTube nur noch Inhalte, die zu Ihren Interessen und politischen Ansichten passen.

Dies führt jedoch zu einer „Echokammer“-Bildung. Inhalte oder Berichte, die die Gegenseite beleuchten oder ein Thema aus mehreren Blickwinkeln betrachten, erhalten Sie nicht mehr. Dies öffnet Tür und Tor für Radikalisierungen und für die Empfänglichkeit von Propaganda.

Die meisten Browser kommen von Google und kaum jemand weiß es

Es gibt anscheinend viele Browser-Alternativen, z. B.:

Name	Firma	Sitz	basiert auf	Open Source
Firefox	Mozilla	USA	Gecko	✓
Chrome	Google	USA	Chromium	✗
Edge	Microsoft	USA	Chromium	✗
Brave	Brave Software	USA	Chromium	✓
Vivaldi	Vivaldi Technologies	Norwegen	Chromium	✗
Safari	Apple	USA	Webkit	✗
Opera	Opera Software	USA, China	Chromium	✗

Was viele Anwender jedoch nicht wissen, dass die meisten Browser davon den Unterbau **Chromium** verwenden. Die Nähe zum Namen „Chrome“ ist kein Zufall: Beides kommt von Google.

Chromium ist als eigener Browser erhältlich und komplett Open Source – also quelloffen. Jedermann kann also in den Code des Browsers schauen, was dieser Browser macht, und auch welche Daten er sammelt und wohin sendet.

Chrome dagegen besteht aus Chromium **und** zusätzlichem Code von Google, der nicht Open Source ist. Hierdurch werden dem Browser die Services von Google hinzugefügt (z. B. Google Docs) – und eben auch das Datensammeln.

Chromium hat als Unterbau den Vorteil, dass er ein sehr schneller Browser ist.

Dadurch, dass es Open Source ist, ist es anderen Entwicklern und Unternehmen explizit erlaubt, Chromium selbst zu verwenden und daraus einen eigenen Browser zu erstellen.

Und das machen tatsächlich auch sehr viele Hersteller: Viele andere populäre Browser und selbst Microsoft, eigentlich ein direkter Konkurrent, verwenden Chromium für Ihre Browser.

Wie Sie in der Tabelle oben sehen können, gibt es nur zwei bekannte Browser, die nicht Chromium nutzen: Firefox und Safari.

Firefox nutzt als Unterbau die Eigenentwicklung namens „Gecko“, das ebenso Open Source ist.

Apple nutzt für Safari Webkit, das von Apple aus dem Code von KHTML weiterentwickelt wurde, das wiederum aus der Linux-Welt kommt. Safari ist allerdings nur für Mac-Rechner und iOS-Geräte (iPhone, iPad) verfügbar.

Warum die Dominanz von Google und Chromium so gefährlich ist

Würden alle Browser Chromium nutzen, kann Google leicht diktieren, welche Webstandards im Internet gelten sollen.

So ist es bereits heute der Fall, dass Google auf der Video-Webseite YouTube, das ebenfalls Google gehört, anderen Browsern das Leben schwer macht, indem ab und zu der YouTube-Player nicht richtig funktioniert – nur wenn Browser verwendet werden, die auf Chromium basieren, funktioniert YouTube einwandfrei.

Leider ist der Marktanteil von allen Browsern zusammen, die Chromium nutzen, weltweit bei etwa 82 % (Stand Juli 2023), in Deutschland bei etwa 65 %.

Deswegen sollten Sie nach Möglichkeit einen Browser verwenden, der nicht Chromium nutzt, um die Dominanz von Google nicht weiter zu festigen.

Welche Browser schützen Ihre Daten?

Auf der Seite www.privacytests.org können Sie sehen, welche Browser Ihre Daten schützen.

Für den Datenschutz sind insbesondere die Kategorien **Fingerprinting resistance tests**, **Tracking query parameter tests, Tracker content blocking tests und Tracking cookie protection tests** wichtig.

Hierbei handelt es sich um Methoden der Webseiten, Ihren Rechner eindeutig identifizieren zu können (sodass Ihr Rechner auch im Incognito-Modus erkannt wird oder selbst dann, wenn Sie Ihren Browser wechseln) sowie durch Cookies und Skripte Ihre Aktivitäten im Netz aufzuzeichnen.

Achtung: Hierbei bewertet die Webseite die Datenschutzeinstellungen **beim Auslieferungszustand der Browser** – also frisch nach der Installation mit den Standardeinstellungen des Browser-Entwicklers.

Obwohl zum Beispiel Firefox relativ schlecht abschneidet, kann der Datenschutz in den Einstellungen signifikant erhöht werden.

Die Browser mit dem besten Datenschutz

Platz 1: LibreWolf

Obwohl ziemlich unbekannt, ist LibreWolf ein sehr guter Browser mit der Mischung aus standardmäßigem hohem Datenschutz und Komfort. LibreWolf ist ein „Fork“, also eine Abspaltung oder Weiterentwicklung, von Firefox.

LibreWolf ist im Grunde ein Firefox-Browser, der auf maximalen Datenschutz getrimmt wurde und Webseiten effektiv daran hindert, Daten über sie zu sammeln.

LibreWolf ist außerdem schon von Beginn an mit dem besten Werbeblocker ausgestattet, **uBlock Origin** (hier als Erweiterung für Firefox: tiny.cc/firefox-werbeblocker)

Die Entwickler von LibreWolf sind auch sehr fleißig: Sobald Firefox ein Update erhält, ist das entsprechende LibreWolf-Browserupdate in der Regel 24 bis 72 Stunden nach Firefox verfügbar.

Download: https://librewolf.net/

Nachteile:

Aus Datenschutzgründen ist LibreWolf auf Englisch eingestellt, das verhindert nämlich effektiver das Fingerprinting, also das Feststellen Ihrer Identität. Da die meisten Internetnutzer weltweit die englische Sprache nutzen, gehen Sie mit einem englischsprachigen Browser ebenso in der Masse unter. Stellen Sie den Browser auf Deutsch um, machen Sie sich ein Stück weit identifizierbarer. Aber natürlich können Sie die Sprache trotzdem auf Deutsch umstellen: Über die Menü-Schaltfläche oben rechts -> **Settings** (Einstellungen) -> **General** (Allgemein) -> (etwas weiter herunterscrollen) **Language** (Sprache).

Von Haus aus werden keine Passwörter gespeichert. Dies können Sie wieder aktivieren unter der **Menü**-Schaltfläche oben rechts -> **Einstellungen** -> **Datenschutz & Sicherheit** -> **Fragen, ob Zugangsdaten und Passwörter gespeichert werden sollen.**

Platz 2: Brave

Brave ist ein Rundum-Sorglos-Browser, der bereits von Haus aus Ihre Daten sehr effektiv schützt und einen eigenen Werbeblocker mitbringt. Auch dieser Browser ist Open Source.

Download: https://brave.com/de/

Nachteile:

Standardmäßig ist die eigene Brave-Suchmaschine voreingestellt, die Werbung anzeigt – hierüber finanziert sich allerdings die Firma, weshalb dieser Schritt nachvollzogen werden kann. In den Einstellungen können Sie aber problemlos eine andere Suchmaschine einstellen, wie etwa DuckDuckGo oder Startpage.

Platz 3: Tor-Browser / Mullvad

Beide Browser sind Open Source und im Grunde gleich, nur dass der Tor-Browser beim Surfen im Internet zusätzlich das Tor-Netzwerk verwendet, dass durch das Umleiten über mehrere „Nodes“ (private Rechner im Tor-Netzwerk) Ihre Herkunft so verschleiert, dass die Webseite auch Ihren Standort und Ihre IP-Adresse nicht mehr sieht.

Dadurch surfen Sie tatsächlich sehr anonym im Netz (nur die erste Tor-Schnittstelle erhält Ihre IP-Adresse, alle anderen Stationen dahinter nicht mehr), aber dadurch kann Ihre Internetgeschwindigkeit niedriger sein als gewohnt.

Mullvad nutzt Ihre normale Internetverbindung, sodass Sie wie gewohnt über Ihren Internetanbieter im Netz surfen.

Beide Browser speichern keinerlei Daten über Ihre Aktivitäten. Es gibt also keinen Browserverlauf, keine Cookies oder sonstige Protokolle. Dadurch werden aber auch keine Logins auf Webseiten oder Online-Shops gespeichert.

Betrachten Sie daher beide Browser eher für Aktivitäten, die Sie nur einmalig erledigen wollen, um Ihre Identität zu verschleiern (Tor-Browser) oder keine Spuren auf dem Rechenr zu hinterlassen (Mullvad).

Download Tor-Browser: https://www.torproject.org/de/

Download Mullvad-Browser: https://mullvad.net/de

Nachteile: Der Mullvad-Browser ist nur in englischer Sprache.

Andere Browser

Was den Datenschutz angeht, sind folgende Browser schnell „abgefrühstückt“:

Edge und Chrome: Edge kommt von Microsoft und Chrome von Google. Hier können Sie sich nur aussuchen, von welchem Unternehmen Sie Ihre Daten sammeln lassen wollen.

Opera: Opera ist nicht Open Source und es kann daher nicht geprüft werden, welche Daten gesammelt und/oder versendet werden. Im Jahr 2016 hat ein chinesisches Konsortium 90 % der Opera-Firmenanteile gekauft. Daher kann aus datenschutztechnischer Sicht nur von Opera abgeraten werden.

Vivaldi: Vivaldi ist ein guter Browser, der durch seine große Anpassungsmöglichkeiten besticht. Allerdings ist Vivaldi nicht Open Source. Daher kann aus datenschutztechnischer Sicht nicht unabhängig geprüft werden, welche Daten Vivaldi sammelt und versendet.

Achtung: Internetsurfer mit hohen Datenschutz-einstellungen werden von Webseiten „bestraft“

Beachten Sie bei der Nutzung dieser Browser, dass viele Webseiten hohe Datenschutzeinstellungen bestrafen.

Das äußert sich darin, dass einige Webseiten schlicht nicht richtig funktionieren, wenn ein Browser bestimmte Cookies oder Skripte zur Nachverfolgung nicht zulässt.

Einige Webseiten können Ihnen auch „den Zutritt verwehren“, wenn Werbe- oder Trackingblocker erkannt werden – zum Beispiel machen das Nachrichtenseiten recht häufig, da sie auf die Einnahmen durch Werbeanzeigen angewiesen sind.

Den Datenschutz beim Firefox-Browser verbessern

Da viele Anwender Firefox nutzen, können Sie einfach mit diesen Schritten den Datenschutz bei Firefox signifikant verbessern:

Installieren Sie die beiden Erweiterungen Origin uBlock (Werbe-blocker) und Privacy Badger (Tracking-Blocker):

tiny.cc/firefox-werbeblocker

tiny.cc/firefox-skriptblocker

Unter der **Menü**-Schaltfläche oben rechts -> **Einstellungen** -> **Datenschutz & Sicherheit** stellen Sie zusätzlich den Daten-schutz von **Standard** auf **Streng**.

Aber Achtung: Auch hier gilt der Hinweis, dass Webseiten dann nicht richtig funktionieren oder Webseiten Ihnen den Zutritt verwehren. In dem Fall können Sie diese Einstellung dann einfach wieder rückgängig machen.

Impressum: Computerwissen, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theo-dor-Heuss-Straße 2-4, 53177 Bonn, Vorstand: Richard Rentrop, Bonn, Redaktionell Verantwortliche: Patricia Sparacio, VNR Verlag für die Deutsche Wirtschaft AG, Adresse s.o., Redaktion, Satz & Layout: Kaner Etem, München