Jason Mason: Sicherheit bei Nutzung des Internets Teil 2 – Hier findet ihr einfache und kostenlose Methoden sowie Werkzeuge, um eure Computer, Laptops, Tablets und eure Privatsphäre vor Gefahren aus dem Internet zu schützen

Selbst wenn ihr nichts Falsches tut, werdet ihr beobachtet und protokolliert. Und die Speicherkapazität dieser Systeme nimmt jedes Jahr beständig um Größenordnungen zu… Sie können dieses System nutzen, um in der Zeit zurückzugehen und jede Entscheidung, die ihr jemals getroffen habt, jeden Freund, mit dem ihr jemals etwas besprochen habt, unter die Lupe zu nehmen und euch auf dieser Grundlage anzugreifen… Um aus einem unschuldigen Leben einen Verdacht abzuleiten und jeden im Kontext eines Übeltäters darzustellen. Edward Snowden Quelle

Spätestens dann, wenn man von der Corona-App und weiteren geplanten Aktionen, wie z.B. die Einführung des digitalen Euro, Supercomputern, Digitalisierung von Schulen, Künstlicher Intelligenz und digitaler Identität liest, wird einem wieder bewusst, wie wichtig die eigene Absicherung gegen die externe Kontrolle und das Ausspionieren ist.

Dank Jasons freundlicher Bereitschaft zur Zusammenarbeit mit Transinformation können wir euch seinen aktuellen Artikel zu dieser Thematik anbieten, der aus drei Teilen besteht. Teil 1 findet ihr hier.

Gerne könnt ihr auch unser mehrteiliges Interview mit Jason lesen, von dem bereits Teil 1, Teil 2, Teil 3a *und* Teil 3b *veröffentlicht wurden. Weitere werden noch folgen.*

Ich habe mich aufgrund einiger Anfragen zu diesem Thema entschlossen, einen neuen Artikel zu verfassen, bei dem sich alles um die Sicherheit im Internet bei Computern und Smartphones dreht.

Der Fokus liegt dabei auf den verbreiteten Windows-Rechnern und Android-Geräten. Ich stelle hier eine Reihe von Tools vor, die es ermöglichen, sicherer im Netz unterwegs zu sein und die eigene Privatsphäre vor Spähangriffen zu beschützen.

Datenschützer weisen ausdrücklich darauf hin, dass man von diesen meist einfach zu installierenden Tools Gebrauch machen sollte, um der vollständigen Überwachung aller Aktivitäten am Computer, Smartphone und im Netz entgegenzuwirken.

Sichere Internetbrowser und Browsererweiterungen für den PC

Das verbreitete und altbekannte Betriebssystem Windows von Microsoft ist kein sicheres oder gar privates Betriebssystem. Da Windows das verbreitetste PC-Betriebssystem der Welt ist, ist es auch das wichtigste Angriffsziel für Hacker, Viren und Malware.

Ausserdem gilt als bestätigt, dass Microsoft bei der Entwicklung von Windows mit Geheimdiensten wie der NSA und deren Projekt PRISM zusammenarbeitet, um Daten der Nutzer zu sammeln. Zuständig dafür sind sogenannte Spyware-Programme, die im Hintergrund des Betriebssystems arbeiten und den Nutzer ausspionieren.

Wikipedia PRISM Surveillance Program
PRISM (Überwachungsprogramm)

Microsoft NSA collaboration user data
Microsoft hat der NSA Zugang zu verschlüsselten Nachrichten gewährt.

PRISM Snowden and government surveillance
PRISM, Snowden und Regierungsüberwachung: 6 Dinge, die Sie wissen müssen.

NSA spying PRISM surveillance cheat sheet
Alles, was Sie über PRISM wissen müssen.

Datenschützer behaupten, dass Microsoft Windows 10 im Grunde ein Trojaner-Betriebssystem der NSA darstellt, das es Spionen ermöglicht, aus der Ferne die Computer und darauf befindlichen Dateien seiner Nutzer auszuspionieren.

Diese Daten werden, wie auch bei Android-Apps, durch die regelmässigen Updates übertragen. Diese Funktion kann von den meisten Nutzern nicht unterbrochen werden und übermittelt daher ständig eure aktuellen Daten an die Spionage-Organisationen.

Es hilft nichts, zu behaupten, dass jemand nichts zu verbergen hätte, oder keine illegalen Aktivitäten ausführt. Jedes eurer eingegebenen Wörter auf der Tastatur, jeder Mausklick, jede E-Mail, Message oder Skype-Übertragung sowie die Aktivitäten auf sozialen Medien werden durch diese Backdoor-Programme von Windows an Datenspione übertragen.

Microsoft gibt offen zu, diesen Diensten diese Hintertüren in ihrem Betriebssystem

offenzuhalten.

Diese Datenspionage betrifft nicht nur Privatpersonen, sondern vor allem auch Unternehmen und Regierungen.

Der NSA-Whistleblower Edward Snowden legte die Existenz viele dieser Überwachungsprogramme offen und die von ihm veröffentlichten Dokumente belegen die Methoden, mit denen Geheimdienste wie die NSA mindestens seit dem Jahr 2007 Windows-Nutzer legal ausspionieren.

Quelle

Diese geleakten Dokumente zeigen, dass sowohl Microsoft als auch Apple, Google, Yahoo, PalTalk, AOL, Facebook, YouTube, Skype und viele weitere Tech-Unternehmen der NSA direkten Zugang zu den Informationen und Daten ihrer Nutzer gewähren.

Als das Projekt PRISM im Jahr 2007 startete, war Microsoft der erste Partner der NSA in diesem Programm und der amerikanische Geheimdienst begann sofort, eine gigantische Menge an Daten von ihren Servern herunterzuladen und somit wurde PRISM zur wichtigsten Datenquelle für die NSA.

Über diese Vorgänge sollte im Grunde jeder Windows-Anwender Bescheid wissen. Man sollte deshalb aber nicht gleich den Kopf hängen lassen, denn es gibt verschiedene Werkzeuge und Tools, mit denen man seine Privatsphäre vor dem Ausspionieren schützen kann.

Es folgt nun eine Auflistung einiger wichtiger Antispy-Werkzeuge für Windows 10.

Wichtige Antispy-Werkzeuge für Windows 10

Die grösste Sicherheit für Anwender entsteht immer durch eine Kombination aus Anti-Virus und

Anti-Spyware-Programmen. Ausserdem ist es absolut notwendig, die Datenschutz- und Privatsphären-Einstellungen von Windows 10 richtig einzustellen, auch wenn diese komplexen Einstellungen die Kenntnisse vieler normaler Anwender auf die Probe stellen, weil sie im System schwer zu finden sind.

Dafür gibt es aber, wie gesagt, einige Lösungen, die das alles selbständig erledigen können und mit deren Hilfe man sich vor der Spionage des Herstellers und seiner Partner einigermassen schützen kann.

Hier ausserdem ein paar Links zur richtigen Sicherheits-Einstellung von Windows 10:

Windows 10 Sicherheit: So sichern Sie es perfekt ab.

Windows 10: Die 10 besten Tipps zu Sicherheit, Datenschutz, Microsoft

Windows 10 sicher einstellen

Windows 10 nach der Installation sicherer machen

O&O ShutUp10

https://www.oo-software.com/en/shutup10

https://www.chip.de/downloads/O-O-ShutUp10_82318496.html

O&O ShutUp10 ist ein kleines, kostenloses Antispy-Werkzeug für Windows 10. Es erlaubt euch, selbst zu entscheiden, welche Datenweitergabe euch zu weit geht.

In einer einfachen Benutzeroberfläche könnt ihr regeln, wie weit Windows 10 eure Privatsphäre schützen soll. Viele dieser Dienste protokollieren, wie schon erwähnt, eure Tastatureingaben und teilen WLAN-Zugangsdaten oder verbinden euren Rechner ohne zu fragen mit ungeschützten öffentlichen Netzwerken, was ein Sicherheitsrisiko darstellt.

O&O ShutUp10 muss dabei nicht selbst auf dem Rechner installiert werden und kann direkt ausgeführt werden.

Win10 SpyStop

https://www.chip.de/downloads/Win10-SpyStop_82472610.html

Win10 SpyStop ist das nächste kostenlose Werkzeug, das die Übermittlung personenbezogener Daten an die Server von Microsoft verhindert. Dazu werden die Anfragen dieser Server einfach abgeblockt. Win10 SpyStop blockiert dabei die Internetverbindungsanfragen von Microsoft, zum Beispiel die der Wartungs-Server oder Diagnose-Server und verweigert ihnen dadurch den Zugriff auf das eigene Betriebssystem.

W10Privacy

https://www.w10privacy.de/

https://www.chip.de/downloads/W10Privacy_81892989.html

Mit diesem Werkzeug schränkt ihr die Zugriffe von Microsoft-Servern ebenfalls deutlich ein.

Win10Privacy kombiniert hierbei viele Optionen für den Erhalt der Privatsphäre, sorgt für eine Minimierung der Datenübertragung und schaltet zahlreiche Dienste einfach ab, die sich in vielen verschiedenen Einstellungen befinden, die man ansonsten erst mühsam im System suchen müsste.

SpyBot Anti-Beacon

https://www.safer-networking.org/products/spybot-anti-beacon/

https://www.chip.de/downloads/Spybot-Anti-Beacon_82797002.html

Das nächste kostenlose Tool ist SpyBot Anti-Beacon. Es sorgt dafür, dass Windows möglichst wenig über euer Nutzerverhalten herausfinden kann.

Über die Datenschutz-Einstellungen von Windows kann man verhindern, dass viele dieser personenbezogenen Daten übertragen werden. Anti-Beacon schaltet Spionage-Funktionen von Windows einfach ab und stoppt die Übertragung von sogenannten Telemetrie-Daten, die ansonsten nur per Kommandozeilen-Befehl deaktiviert werden kann.

Verhindert wird auch das automatische Teilen von WLAN-Passwörtern. Damit kann Windows ansonsten automatische Updates durchführen lassen und installiert selbständig Software.

Ausserdem senden die Standartbrowser Daten an die Windows-Server und auch vorinstallierte Programme senden Telemetrie-Daten nach Hause. Telemetrie bezeichnet hier einfach das Verfolgen des Nutzungsverhaltens von Personen.

Mit Anti-Beacon wird es möglich, dieses Tracking effektiv zu stoppen.

SpyBot – Search & Destroy

https://www.safer-networking.org/compare-spybot-editions/

https://www.chip.de/downloads/SpyBot-Search-Destroy_13001443.html

Ein weiteres wichtiges Tool für die Sicherheit von Windows 10 vom Unternehmen Spybot ist Search & Destroy. Diese Freeware entfernt geschickt Spyware von eurem Betriebssystem.

Es lassen sich auch Daten wie besuchte Webseiten, geöffnete Dateien, gestartete Programme oder Cookies löschen. Das erhöht die Schnelligkeit des Betriebssystems und räumt es auf.

DoNotSpy10

https://pxc-coding.com/donotspy10/

https://www.chip.de/downloads/DoNotSpy10-Do-Not-Spy-fuer-Windows-10_81727412.html

Das letzte hier vorgestellte Antispy-Werkzeug ist DoNotSpy10. Dieses verändert auf Wunsch ebenfalls die Einstellungen von Windows 10, um für mehr Privatsphäre zu sorgen und die Diagnosefunktionen zu blockieren.

Apps können daran gehindert werden, die Kamera oder das Mikrofon zu aktivieren, auch die Gesichtserkennung oder die Weitergabe von Handschrift-Daten kann ausgeschaltet werden.

Quelle

Alternativen zum Windows-Betriebssystem

Es gibt eine Reihe von empfehlenswerten Alternativen und vor allem kostenlosen Betriebssystemen, um Windows zu ersetzen. Linux ist hierbei das wichtigste Open-Source-Betriebssystem, das im Grunde alles tun kann, was Windows auch kann.

Linux ist hingegen aber viel sicherer und Funktionen zum Schutz der Privatsphäre sind bereits eingebaut. Ausserdem sind die wichtigsten Windows-Programme und Anwendungen auch für Linux Betriebssysteme verfügbar.

Top 15 best windows emulators for Linux enthusiasts
Top 15 der besten Windows-Emulatoren für Linux-Enthusiasten

Es existieren ausserdem Windows-Emulatoren, um bestimmte Windows-Anwendungen auf einem Linux-Betriebssystem auszuführen.

Zu diesen Emulatoren zählen: Wine, VMware Workstation, CrossOver Linux oder VirtualBox.

Meist ist es allerdings nicht notwendig, zu solchen Emulatoren zu greifen, weil es in der Regel eine Linux-Alternative für diese Anwendungen gibt.

Oft ist Linux auch die einzige Möglichkeit, das Windows-Betriebssystem auf der vorhandenen PC-Hardware oder dem Laptop zu ersetzen und die nötigen Treiber sind online verfügbar. Linux arbeitet dabei viel sparsamer als Windows und läuft daher auch auf älteren Rechnern stabil.

Ähnlich wie bei Windows gibt es viele verschiedene Versionen an Linux-Betriebssystemen, die man auch als Distros bezeichnet. Wenn also der Schutz der Privatsphäre der wichtigste Grund für einen Wechsel auf Linux ist, dann garantiert dieses Betriebssystem sogar, dass ihr nicht ausspioniert werdet.

Eine sehr wichtige Funktion der wichtigsten Linux-Varianten sind bootfähige Live-USB-Betriebssysteme. Die Installation eines Linux-Systems auf einem bootfähigen USB-Stick macht es dadurch möglich, Linux direkt vom USB-Stick zu betreiben, ohne Windows dauerhaft zu deinstallieren oder Linux auf eurem Rechner zu installieren.

Linux Betriebssysteme sind sorgenfrei und dazu – im Gegensatz zu Windows – noch völlig unkompliziert. Deshalb arbeitet man damit durch seine vereinfachte Bedienung wesentlich müheloser und erhält dadurch ein alltagstaugliches, sorgenfreies Betriebssystem, das zudem völlig kostenlos ist.

Es gibt keine Lizenzschlüssel und es muss auch keine Software aktiviert werden, weil die wichtigsten Programme und auch ein Office Paket bereits im Lieferumfang enthalten sind und nicht nachgekauft oder heruntergeladen werden müssen.

In den vielen verschiedenen Linux-Distributionen gibt es Unterschiede im Funktionsumfang und der Bedienoberfläche. Die bereits enthaltenen nützlichen Programme umfassen Bürosoftware, Brennsoftware oder auch Bildbearbeitungs-Software und Spiele.

Linux lässt sich mittlerweile genauso einfach bedienen wie Windows XP und die Distributionen benötigen nur geringe Hardware-Anforderungen und können daher problemlos auch auf sehr alten Computern und Laptops installiert werden.

Durch Linux werden diese älteren Rechner in der Regel sehr viel schneller und können daher als Ersatz für Windows-Rechner neu aufbereitet werden. Die Distributionen mit den geringsten Systemanforderungen sind zum Beispiel Lubuntu oder Xubuntu.

https://lubuntu.net/downloads/

https://xubuntu.org/download

Aber auch die populärsten Distros namens Ubuntu und Mint benötigen geringe Hardware-Anforderungen. Das aktuelle Ubuntu läuft mit einem Prozessor mit 2 GHz, 2 GB RAM Arbeitsspeicher und 25 GB freiem Festplattenspeicher.

Mint braucht sogar nur 1 GB RAM und 15 GB freien Festplattenspeicher. Somit wird mehr Platz auf der Platte frei, wenn man vorher ein Windows-Betriebssystem installiert hatte. Ältere, immer noch verfügbare Linux-Versionen laufen mit noch weniger Ressourcen.

Auf Linux braucht man übrigens weder ein Anti-Viren-Programm noch eine Firewall, weil so gut wie alle Viren ausschliesslich für das Windows-Betriebssystem entworfen sind! Wenn man eine gefährliche .exe Datei herunterladen sollte, die für Windows schädlich ist, kann Linux sie nicht ohne Weiteres ausführen.

Alle diversen Linux Betriebssysteme kann man sich als ISO-Dateien gratis herunterladen. Diese Datenpakete müssen auf eine CD oder DVD gebrannt oder auf einen bootfähigen USB Stick installiert werden.

Ein einfaches, kostenloses Brennprogramm für diesen Zweck ist zum Beispiel der CD-Burner-XP.

https://www.chip.de/downloads/CDBurnerXP_13008371.html

Wenn ihr die mit der ISO-Datei gebrannte CD unter Windows ins Laufwerk einlegt, kann nun das Linux-Installationsprogramm gestartet werden. Danach erfolgen die meisten Installationsschritte fast automatisch. Es gibt drei Optionen:

1. Linux kann als Hauptbetriebssystem installiert werden und löscht Windows von eurem Rechner.
2. Linux kann als zweites Betriebssystem neben Windows installiert werden und bei jedem Start kann man zwischen beiden wählen. Das Windows-System bleibt dabei unverändert.
3. Linux kann auch direkt von einem bootfähigen USB Stick oder von der gebrannten CD/DVD als Live-Version betrieben werden, wenn man im Bootmenü die Bootreihenfolge im BIOS ändert.

Hier ein paar Links zur Installationshilfe:

Linux Mint installieren-so gehts

Linux Mint installieren

Linux Mint auf dem PC installieren

Auf Youtube:

Das ist Linux Mint 20 Ulyana

https://www.youtube.com/watch?v=Fap-6YqVbaY

Das ist Ubuntu 20.04

https://www.youtube.com/watch?v=vvFQeJ29vhg

TAILS

Edward Snowden gibt uns den Ratschlag, die Linux-Distro namens TAILS zu betreiben, um maximale Sicherheit und Privatsphäre zu garantieren.

Dieses Betriebssystem hinterlässt keine Spuren im Internet oder auf eurem Rechner, weil es als Live-USB-System betrieben wird. Als Windows-Ersatz ist es jedoch kaum geeignet und daher sollte eine andere Distro installiert werden, die dauerhaft in Verwendung bleiben kann.

Die einfache Installation auf einem USB-Stick oder einer Live-CD macht es möglich, verschiedene kostenlose Versionen von Linux zu testen. Die zwei wichtigsten und beliebtesten Distros (Distributionen) von Linux sind ohne Frage Ubuntu und Mint.

https://tails.boum.org/

https://www.chip.de/downloads/Tails_64248643.html

Das von Edward Snowden empfohlenes Betriebssystem namens TAILS muss hier aber noch genauer beschrieben werden.

Das ebenfalls kostenlose Betriebssystem TAILS soll Datenspionen das Leben so schwer wie möglich machen. TAILS steht für „The Amnesic Incognito Live System“ (Das gedächtnislose, unerkannte Live-System).

Der Download von TAILS erfolgt über eine Downloaderweiterung für Firefox oder den Tor-Browser. TAILS basiert auf Linux und kommt ohne eine fixe Installation aus. Für den Betrieb ist keine Festplatte nötig.

Viren, Trojaner und sonstige Schadprogramme, die man sich während der Nutzung einfangen kann, gefährden eure Windows-Installation nicht. Ihr vermeidet ausserdem, aufgrund von Schwachstellen und Sicherheitslücken eures Windows-Systems, unnötige Spuren im Netz zu hinterlassen.

Um unerkannt zu agieren und etwaige Sperren zu umgehen, durchlaufen alle Datenpakete bei TAILS das anonyme Tor-Netzwerk. Informationen, die während der Nutzung anfallen, speichert das System nur auf ausdrücklichen Wunsch. Um das, was bleibt, gegenüber Dritten abzusichern, hat TAILS wichtige Werkzeuge zur Verschlüsselung von Dateien, E-Mails und Instant-Messaging-Nachrichten installiert.

TAILS läuft auf USB-Sticks, DVDs und Festplatten. Am besten ist es, das Betriebssystem auf DVD zu brennen und von dort zu starten. Da die Disk nach dem Brennen keine neuen Daten aufnimmt, kann sich logischerweise keine Schadsoftware einnisten. Alternativ bietet sich die Möglichkeit, das Betriebssystem auf einem USB-Stick oder einer SD-Karte zu installieren.

Wer mit Windows im Internet unterwegs ist, muss immer mit gefährlichen Angriffen und Spionage rechnen. Dieser Gefahr geht man mit TAILS einfach aus dem Weg. Man muss sich um Viren, Spionage und Malware keine Sorgen mehr machen, denn TAILS agiert wie ein Schutzschild und ohne Einwilligung können keine zusätzlichen Daten im System gespeichert bleiben.

Bei jedem Start ist TAILS wieder so konfiguriert, dass man in der ursprünglichen Arbeitsumgebung landet. Wer hohen Wert auf Sicherheit legt, wird hier bestens bedient und TAILS ist vor allem entstanden, um sensible Aufgaben im Netz zu erledigen, ohne Spuren zu hinterlassen und um maximale Sicherheit für private Nutzer zu garantieren.

Ubuntu

https://www.chip.de/downloads/Ubuntu_42589318.html

https://www.chip.de/downloads/Ubuntu-32-Bit_22592231.html

https://www.chip.de/downloads/Universal-USB-Installer_56810883.html

Ubuntu ist ein kostenloses und einfach zu bedienendes Betriebssystem und ausgezeichnet für Umsteiger geeignet, denn alle nötigen Anwendungen zur alltäglichen Arbeit am Rechner bringt diese Version bereits mit.

Es gibt Ubuntu bislang als 32-Bit und 64-Bit Version zum Download, wobei die neueste Version nur noch mit 64-Bit zur Verfügung gestellt wird. Wer einen älteren Rechner mit 32-Bit besitzt, muss somit auf eine ältere Version zurückgreifen.

Die heruntergeladene ISO-Datei kann mit Tools wie dem Universal USB Installer auf einem USB-Stick installiert werden und startet dann, nach Umstellung der Boot-Einstellungen im Bootmenü eures Rechners, direkt vom USB-Stick.

Ihr könnt dieses Betriebssystem und alle anderen Linux Distros wie TAILS auf diese Weise auch auf beliebigen anderen Rechnern betreiben, die einen USB-Anschluss besitzen und es einfach auf Reisen mitnehmen.

Somit muss eine vorhandene Windows-Installation nicht ersetzt werden und Linux kann einfach im Live-Betrieb genutzt werden. Durch einen Boot-Manager können auch beide Betriebssysteme auf der Festplatte installiert werden und Ubuntu kann neben Windows als zweites Betriebssystem eingerichtet werden.

Neue Versionen von Ubuntu oder Mint erscheinen etwa alle sechs Monate. Somit ist Linux ein kostenloses und sicheres Betriebssystem für private Anwender oder auch Unternehmen.

Mint

https://www.chip.de/downloads/Linux-Mint-Ulyana-Cinnamon-64-Bit_39460086.html

https://www.chip.de/downloads/Linux-Mint-Tricia-Cinnamon-32-Bit_29494476.html

Die zweite kostenlose Alternative für Windows 10 ist Linux Mint 20, das dieses Jahr ebenfalls neu erschienen ist und optisch dem älteren Windows 7 ähnelt.

Viele Windows-7-Nutzer entscheiden sich aus Support-Gründen auf Linux umzusteigen und Linux Mint ist eine gute Möglichkeit, das zu tun, denn es läuft stabil und schnell. Auch hier wird aktuell keine 32-Bit-Variante mehr angeboten und Nutzer mit älteren Rechnern müssen zur Vorgängerversion greifen, die noch bis 2023 unterstützt wird.

Quelle

Sichere Internetbrowser und wichtige Browsererweiterungen

Edward Snowden empfiehlt auch, den jeweiligen Internetbrowser mit sogenannten Erweiterungen oder Add-ons sicherer zu machen.

Die meisten dieser Erweiterungen werden direkt im Browser installiert. Gängige moderne Internetbrowser, für die es solche Erweiterungen gibt, sind Mozilla Firefox oder Google Chrome.

Diese Internetbrowser sind Open-Source-Software, und unabhängige Entwickler können Erweiterungen dafür zu Verfügung stellen.

Die Meinungen, welcher Browser besser oder sicherer ist, gehen hierbei auseinander. Auf jeden Fall bieten sowohl Google als auch Mozilla ihre Browser auch als installationsfreie Portable-Browser an.

Das heisst, man kann sie auf einer anderen Partition oder einem USB-Stick oder einer SD-Karte installieren. Der Vorteil dabei ist, dass man diese Portable-Browser mit all ihren Einstellungen, Erweiterungen und Lesezeichen im Bedarfsfall einfach abziehen und an beliebig vielen anderen Computern einfach weiter betreiben bzw. dorthin kopieren kann.

Somit trägt man seinen privaten Browser in Form eines USB-Sticks immer bei sich und er erscheint nicht im eigentlichen Betriebssystem.

Die meisten Datenschützer raten eher dazu, den vertrauenswürdigeren Mozilla Firefox-Browser statt Google Chrome zu verwenden. Firefox Portable gibt es als 32-Bit und 64-Bit Version. Den Browser Firefox gibt es seit mehr als einem Jahrzehnt und er hat sich den Ruf erworben, die beste Datenschutzwahl unter den beliebten Browsern zu sein.

Firefox Portable: https://www.chip.de/downloads/Firefox-Portable_29186641.html

Ungoogled Chromium Portable: https://portapps.io/app/ungoogled-chromium-portable/

Bevor wir zu den wichtigsten Browsererweiterungen für Mozilla Firefox kommen, will ich noch einige andere sichere Browser für Windows oder Linux vorstellen. Die meisten dieser Browser sind auch für Android und Apple verfügbar.

Brave Browser

https://brave.com/

https://www.chip.de/downloads/Brave-Browser_90204622.html

Der Brave Browser bietet viele Funktionen für Sicherheit und Datenschutz und bietet daher viel Privatsphäre. Er nutzt HTTPS und blockiert automatisches Anzeigen und Script sowie Cookies. Auch Tracker können gemeinsam mit Malware blockiert werden.

Ungoogled Chromium

https://github.com/Eloston/ungoogled-chromium

https://www.chip.de/downloads/Ungoogled-Chromium_101325413.html

Freunden des Browsers Google Chrome kann man als Ersatz Chromium bzw. Ungoogled Chromium nahelegen. Das deshalb, weil der Quellcode von Chromium nicht von Google kontrolliert wird und somit nicht der Datenerfassung des Tech-Giganten unterliegt.

Speziell die Version Ungoogled Chromium legt grossen Wert auf den Schutz der Privatsphäre. Man kann hier ausserdem viele normale Browsererweiterungen für Chrome installieren, um zusätzliche Sicherheit zu erhalten und ausserdem gibt es diesen Browser ebenfalls als Portable-Version für den USB-Stick.

Ungoogled Chromium verzichtet hierbei auf jegliche Google-Codes und das kommt auf jeden Fall dem Schutz der Privatsphäre zugute und es werden keine Google-Server kontaktiert. Als Suchmaschine ist hierbei DuckDuckGo voreingestellt und nicht Google.

Epic

https://www.epicbrowser.com/

https://www.chip.de/downloads/Epic-Privacy-Browser_75452475.html

Auch der Epic Browser legt grossen Wert auf Datenschutz und sendet automatisch

Do-Not-Track-Anfragen, um Tracking zu verhindern.

Er blockiert ausserdem Cookies, Anzeigen und Analysesysteme. Der Epic Browser verwendet ebenfalls DuckDuckGo als Suchmaschine. Viele andere Funktionen anderer Browser sind ebenfalls abgeschaltet und damit garantiert er eine extreme Privatsphäre.

Es werden im Browser keine History, Login-Daten oder andere Informationen gespeichert und auch die IP-Adresse wird nicht übermittelt.

Wichtige Browsererweiterungen für Mozilla Firefox und Chromium

Bevor die wichtigen Browsererweiterungen für sicheres Surfen im Netz installiert werden, ist es sinnvoll, auch den Firefox oder Chromium Browser auf Sicherheit einzustellen und zu optimieren.

Anleitungen dazu gibt es zum Beispiel hier:

Firefox sicher machen: 9 Tipps

Firefox Tuning: So machen Sie Ihren Browser schöner, schneller und sicherer

Firefox: privacy and security

Google Chrome absichern Tipps

Acht Surfkomfort-Tipps für Firefox und Chrome

So machen Sie Google-Chrome sicher

Es folgt eine Auflistung der wichtigsten Erweiterungen, um diese Browser sicherer zu machen. Man muss sie direkt bei den Einstellungen im jeweiligen Browser installieren.

Auch Google Chrome-Nutzer können diese Erweiterungen installieren. Das funktioniert sogar beim Tor-Browser, weil er auf Firefox basiert. Man sollte jedoch genau überlegen ob man im Tor-Netzwerk derartige Erweiterungen nutzen möchte, weil man damit möglicherweise im Netz zu identifizieren ist.

Um die Suche nach diesen Erweiterungen zu vereinfachen, führe ich hier die Direktlinks auf. Klickt zur Installation einfach auf die folgenden Links.

AdBlocker Ultimate

https://addons.mozilla.org/de/firefox/addon/adblocker-ultimate/

https://chrome.google.com/webstore/detail/adblocker-ultimate/ohahllgiabjaoigichmmfljhkcfikeof?hl=de

AdBlocker Ultimate ist mit dem einzigen Ziel konzipiert, alle störenden Werbeanzeigen zu löschen, sodass ihr euch auf eure gewünschten Inhalte konzentrieren können.

Adblocker Ultimate blockiert Schadsoftware, Tracking, verbessert die Browserleistung und ist kostenlos.

Es gibt umfangreiche Filter, die einen angemessenen Schutz gegen lästige Anzeigen, YouTube-Werbung und anderes anbieten. Das Blockieren von Anzeigen wird die Ladegeschwindigkeit eurer Webseite beschleunigen und die CPU- und Speichernutzung verringern.

Canvas Defender und Canvas Blocker

Canvas Fingerprinting ist ein Sammelbegriff für eine Reihe von Nutzerverfolgungs-Techniken, um Online-Benutzer ohne Verwendung von Cookies eindeutig zu identifizieren. Sobald die Identifizierung möglich ist, kann beispielsweise das Internetnutzungsverhalten beobachtet und analysiert werden.

Canvas Fingerprinting kann mit Standardeinstellungen des Browsers nur schwer verhindert werden und wird als ein nicht löschbarer Cookie-Nachfolger betrachtet.

Mit dem Canvas Defender oder Canvas Blocker wird eine Störung im Fingerprinting erzeugt. Damit kann ein Browser nicht mehr einem speziellen Computer zugeordnet und zurückverfolgt werden!

https://addons.mozilla.org/de/firefox/addon/canvasblocker/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://addons.mozilla.org/de/firefox/addon/no-canvas-fingerprinting/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/canvas-blocker-fingerprin/nomnklagbgmgghhjidfhnoelnjfndfpd?hl=de

https://chrome.google.com/webstore/detail/canvas-fingerprint-defend/lanfdkkpgfjfdikkncbnojekcppdebfp?hl=de

Click & Clean + History Cleaner

Diese Erweiterungen löschen euren Browser-Verlauf, den Cache und Cookies usw., wenn der Browser geschlossen wird. Das verhindert somit die weitere Verfolgung eurer Online-Aktivitäten.

https://addons.mozilla.org/de/firefox/addon/history-cleaner/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://addons.mozilla.org/de/firefox/addon/browser-cleaner-pro/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/clickclean/ghgabhipcejejjmhhchfonmamedcbeod?hl=de

https://chrome.google.com/webstore/detail/super-history-cache-clean/afelaengidkffdcabnhdoeojoeoonfcn?hl=de

Ghostery

Ghostery spürt Tracking-Technologien auf und blockiert sie, beschleunigt so den Aufbau der Internetseiten, macht sie übersichtlicher und schützt eure Daten.

Ghostery sieht das „unsichtbare“ Web und erkennt dort Tracker, Web Bugs, Pixel und Beacons, die von Facebook, Google und mehr als 500 weiteren Werbenetzwerken, Anbietern von Verhaltensdaten und Web-Publishern (d.h. von Unternehmen, die sich für eure Aktivität interessieren) eingesetzt werden.

Ghostery ist eine der aktuell wichtigsten Sicherheitserweiterungen für euren Browser!

https://addons.mozilla.org/de/firefox/addon/ghostery/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/ghostery-%E2%80%93-privacy-ad-blo/mlomiejdfkolichcflejclcbmpeaniij?hl=de

Mercury Reader und Tranquility Reader

Mercury Reader (Chrome) und Tranquility Reader (Firefox) – Diese Erweiterungen entfernen alle Werbeanzeigen und andere störende Elemente auf einer Webseite und lassen nur den Text und die Bilder übrig. Damit kann man unübersichtliche Webseiten endlich sauber und entspannt lesen.

https://chrome.google.com/webstore/detail/mercury-reader/oknpjjbmpnndlpmnhmekjpocelpnlfdi?hl=de

https://addons.mozilla.org/de/firefox/addon/tranquility-1/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

Mod Header und Modify Headers

Mod Header (Chrome) + Modify Headers (Firefox) – sind Add-ons, mit denen sich der HTTP-Request-Header verändern, hinzufügen und filtern lässt.

Eine von euch gewählte IP-Adresse wird dadurch auf eure echte aufgesetzt. Ihr müsst dazu eine real existierende IP-Adresse angeben. Die IP-Adresse von jeder beliebigen Webseite lässt sich durch „anpingen“ herausfinden.

Man kann auf diese Weise z.B. die IP von beliebigen anderen Webseiten vor seine eigene setzten und ist damit im Netz getarnt und sicherer unterwegs. Das ist praktisch, wenn man etwa auf Dienste im Internet zugreifen will, die normalerweise nur im Ausland verfügbar sind, oder um eine beliebige falsche IP-Adresse vorzutäuschen.

Man kann sich mit diesen Erweiterungen eine ganze Liste mit falschen ID-Adressen anlegen

und diese abwechselnd benutzen.

https://addons.mozilla.org/de/firefox/addon/modheader-firefox/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://addons.mozilla.org/de/firefox/addon/modify-header-value/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/modify-headers-for-google/innpjfdalfhpcoinfnehdnbkglpmogdi?hl=de

https://chrome.google.com/webstore/detail/modheader/idgpnmonknjnojddfkpgkljpfnnfcklj?hl=de

Um seine eigene IP-Adresse herauszufinden oder mit einer dieser Erweiterungen zur Sicherheit veränderte IP-Adressen zu prüfen, gibt es zum Beispiel diese Dienste, die auch den Standort, das Betriebssystem und den Browser identifizieren können:

https://whatismyipaddress.com/

https://www.whatismyip.net/

https://www.whatismyip-address.com/?check

Privacy Badger + Privacy Possum

Die Erweiterung Privacy Badger sorgt für mehr Privatsphäre und weniger Werbung im Internet. Sie unterdrückt die gängigsten Werbe-Tracker und verhindert so, dass euer Surf-Verhalten aufgezeichnet wird. Damit könnt ihr den Privacy Badger als Adblocker nutzen und gleichzeitig für weniger aufgezeichnete Daten sorgen.

Privacy Possum sorgt dafür, dass kommerzielle Tracking-Methoden verdreht werden und verfälschte Daten an die Tracking-Unternehmen und Spyware-Organisationen übermittelt werden.

https://addons.mozilla.org/de/firefox/addon/privacy-badger17/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://addons.mozilla.org/de/firefox/addon/privacy-possum/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/privacy-badger/pkehgijcmpdhfbdbbnkijodmdjhbjlgp?hl=de

https://chrome.google.com/webstore/detail/privacy-possum/ommfjecdpepadiafbnidoiggfpbnkfbj?hl=de

ProxFlow + ProxTube

ProxFlow (Chrome) und ProxTube (Firefox) – helfen beim Entsperren von Inhalten, die durch

Ländersperren nicht zugänglich sind. Sie umgehen damit auch alle Ländersperren von YouTube und man kann sich endlich alle Videos ansehen.

https://addons.mozilla.org/de/firefox/addon/proxtube/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/search/Proxflow?hl=de

SriptSafe + NoScript

ScriptSafe (Chrome) und NoScript (Firefox) – ScriptSafe und NoScript erlauben das Ausführen von JavaScript, Java und anderen Plugins nur bei vertrauenswürdigen Domains eurer Wahl (z.B. eurer Homebanking-Website). Der auf einer Positivliste basierende präventive Ansatz zum Blockieren von Skripten verhindert das Ausnutzen von bekannten und unbekannten Sicherheitslücken ohne Verlust an Funktionalität.

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

https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijlflahbdbdgdf?hl=de

VPN Dienste als Browsererweiterung

Bleibt anonym, gesichert sowie uneingeschränkt und entsperrt jede Website mit VPN. Diese Erweiterungen sind weltweit verfügbar und damit kann man Beschränkungen aufheben, Blockierungen umgehen und die echte IP-Adresse wird geschützt sowie verborgen, um sicher im Netz zu surfen. Alle diese Dienste sind zudem noch kostenlos.

https://addons.mozilla.org/de/firefox/addon/hoxx-vpn-proxy/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://addons.mozilla.org/de/firefox/addon/zenmate-free-vpn-best/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://addons.mozilla.org/de/firefox/addon/uvpn-unlimited-vpn/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/touch-vpn-secure-and-unli/bihmplhobchoageeokmgbdihknkjbknd?hl=de

https://chrome.google.com/webstore/detail/zenmate-free-vpn%E2%80%93best-vpn/fdcgdnkidjaadafnichfpabhfomcebme?hl=de

https://chrome.google.com/webstore/detail/uvpn-free-and-unlimited-v/jaoafpkngncfpfggjefnekilbkcpjdgp?hl=de

Quelle

Google & Facebook Container

Hindert Google und Facebook daran, euch durch das Internet zu verfolgen.

Mit dem Google- und Facebook-Container Add-on für Firefox übernehmt ihr die Kontrolle und könnt ganz einfach eure Aktivität im Netz von der auf Facebook isolieren. Google und Facebook Container packen eure Identität in einen separaten Behälter. So ist es für Google und Facebook schwerer, eure Besuche auf anderen Websites mit Drittanbieter-Cookies zu verfolgen.

Die Add-ons hindern diese Dienste aber nicht daran, Informationen, die sie bereits über euch gesammelt haben oder die sie bereits an Dritte weitergegeben haben, zu missbrauchen. Diese Container Erweiterungen gibt es nur für Mozilla Firefox!

Die Social-Networking-Webseiten sind dafür bekannt, Benutzer im ganzen Web zu verfolgen. Ja, Facebook verfolgt euch, auch wenn ihr euch abgemeldet habt. Dies geschieht durch die Verwendung von sogenannten Drittanbieter-Cookies.

Das Facebook-Container-Add-on von Mozilla soll das verhindern. Es ermöglicht Firefox, die Website in einem separaten Container oder Sandbox-Tab zu öffnen. Wie Google monetarisiert Facebook eure Daten und verkauft sie an Werbetreibende.

Doch nicht nur auf ihren Webseiten legen diese Social-Media-Riesen eure gesammelten Daten auf. Jede Website, die eine Social-Login-Option bietet, verkauft eure Daten ebenfalls weiter. Die Erweiterung Searchonymous hindert Google oder die NSA daran, eure Suchanfragen zu verfolgen. Wenn installiert, werden bei der Suche keine Tracking-Cookies mehr gesendet.

https://addons.mozilla.org/de/firefox/addon/google-container/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://addons.mozilla.org/de/firefox/addon/facebook-container/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

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

https://chrome.google.com/webstore/detail/searchonymous/onhfdppooafpnnigbmnpnnjmbajggekc

DuckDuckGo Privacy Essentials

DuckDuckGo Privacy Essentials bietet mehr Privatsphäre beim Surfen im Netz und verhindert und blockiert versteckte Werbe-Tracker, die man selbst nachverfolgen kann.

Optimierter Verschlüsselungsschutz, Suche im Privatsphäre-Modus, Selbstzerstörungsknopf der persönlichen Browserdaten, App-Verriegelung – DuckDuckGo ist die auf Datenschutz orientierte Alternative zur Google-Suche.

Wenn Google eure Daten verwendet, um euch gezielte Werbung zu schalten, macht DuckDuckGo das Gegenteil. Wenn ihr einen sofortigen Datenschutz-Boost wollt, ist der Wechsel zu DuckDuckGo für eure Internet-Suchen eine grossartige und einfache Option.

Ihr könnt jedoch noch einen Schritt weiter gehen und die Erweiterung DuckDuckGo Privacy Essentials auch bei Chrome installieren. Die Privacy Essentials-Erweiterung bietet Optionen für Script- und Tracker-Blockierung, stellt sicher, dass ihr immer die HTTPS-Version einer Website besucht und führt eine praktische Datenschutzbewertung für jede Website ein, die ihr besucht.

https://addons.mozilla.org/de/firefox/addon/duckduckgo-for-firefox/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/duckduckgo-privacy-essent/bkdgflcldnnnapblkhphbgpggdiikppg?hl=de

Disconnect

Disconnect zeigt und blockiert unsichtbare Webseiten, die euer Suchverhalten verfolgen und speichern. Disconnect wurde im Jahr 2016 zum besten Browser-Sicherheitstool gewählt. Es existiert ausserdem eine eigene Disconnect-Suchmaschine, die grossen Wert auf Privatsphäre legt.

https://addons.mozilla.org/de/firefox/addon/disconnect/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/disconnect/jeoacafpbcihiomhlakheieifhpjdfeo?hl=de

https://search.disconnect.me/

HTTPS Everywhere

HTTPS Everywhere wird von Edward Snowden als eine der wichtigsten Browser-Erweiterungen überhaupt bezeichnet. Mit dem kostenlosen Add-on HTTPS Everywhere verschlüsselt ihr Webseiten und surft anonym im Internet. HTTPS Everywhere bewirkt den Wechsel von einer unverschlüsselten zu einer verschlüsselten Datenübertragung per HTTPS.

https://addons.mozilla.org/de/firefox/addon/https-everywhere/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=de

Random User Agent

Random User-Agent (Chrome) und Random Agent Spoofer (Firefox) – Diese Erweiterungen täuschen beim Surfen im Netz falsche Browser und unterschiedliche Betriebssysteme vor und können so eingestellt werden, dass sie zufällig rotieren. Das erschwert die Verfolgung eures Surfverhaltens im Netz.

Das Ändern eines Benutzer-Agenten kann nützlich sein, um Zensur zu umgehen, z. B. wenn ein Inhalt nur von einem Mobiltelefon oder einer bestimmten Plattform verfügbar ist.

Eine Erweiterung mit noch mehr Auswahlmöglichkeiten, um ein Profil zu spoofen, nennt sich Chameleon und ist nur für Firefox verfügbar. Sie enthält einige zusätzliche Optionen zur Verbesserung der Privatsphäre.

https://addons.mozilla.org/de/firefox/addon/user-agent-string-switcher/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://addons.mozilla.org/de/firefox/addon/random_user_agent/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://addons.mozilla.org/de/firefox/addon/chameleon-ext/

https://chrome.google.com/webstore/detail/random-user-agent/einpaelgookohagofgnnkcfjbkkgepnp?hl=de

Cookie Auto Delete

Diese Erweiterung löscht alle Cookies automatisch, sobald ein Tab oder der Browser geschlossen werden. Sie schützt ausserdem gegen Tracker und Zombie-Cookies. Cookies, die nicht benutzt werden, werden automatisch gelöscht.

https://addons.mozilla.org/de/firefox/addon/cookie-autodelete/?utm_source=addons.mozilla.org

&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/cookie-autodelete/fhcgjolkccmbidfldomjliifgaodjagh?hl=de

uBlock Origin

uBlock Origin ist eine freie, plattformübergreifende Erweiterung zum Filtern von Webinhalten wie beispielsweise Werbung. Es ist eine Weiterentwicklung des inzwischen eingestellten uBlock.

Gegenüber Adblock Plus benötigt uBlock Origin laut eigener Analyse deutlich weniger Arbeitsspeicher und CPU-Zyklen bei vergleichbarem Funktionsumfang. Die Chrome-Version hatte Ende 2016 über 6 Millionen, die Firefox-Version mehr als 2 Millionen tägliche Nutzer und diese Zahlen sind in den letzten Jahren noch einmal sprunghaft angestiegen. Ublock Origin ist selbst beim Tor Browser vorinstalliert.

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

https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=de

Decentraleyes

Decentraleyes enthält eine lokale Bibliothek mit häufig verwendeten JavaScript- und CSS-Bibliotheken. Viele Websites fordern eine JavaScript- oder CSS-Datei von einem externen Server an.

Wenn dies geschieht, blockiert Decentraleyes diese Verbindung. Stattdessen wird die Anforderung mithilfe einer eigenen lokal gespeicherten Bibliothek bedient. Daher muss euer Browser mit einer geringeren Anzahl von verschiedenen Servern kommunizieren. Das soll eure Online-Privatsphäre schützen und gleichzeitig die Ladezeiten der Seiten verbessern.

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

https://chrome.google.com/webstore/detail/decentraleyes/ldpochfccmkkmhdbclfhpagapcfdljkj?hl=de

TrackMeNot + Don’t track me Google

Das sind Browser-Erweiterungen, um die Privatsphäre bei Suchmaschinen zu erhöhen. Es werden dabei zufällige falsche Daten an gängige Suchmaschinen übermittelt, die das Suchprofil verändern und somit ein Tracking verhindern.

https://addons.mozilla.org/de/firefox/addon/trackmenot/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

https://chrome.google.com/webstore/detail/dont-track-me-google/gdbofhhdmcladcmmfjolgndfkpobecpg

Das war ein kurzer Überblick über derzeit sinnvolle Sicherheitserweiterungen. Eine Kombination dieser Anwendungen reicht aus, um einen relativ sicheren Browser einzurichten. Man kann euch dann nicht mehr so einfach am Computer und im Netz ausspionieren.