Schutz vor den Überwachungs-Schaltzentralen der Eliten-Geheimdienste

Das Internet ist nur eine vergleichsweise geringe von den Geheimdiensten ermöglichte Schaltzentrale ist.

- **Das Internet macht nur 3 % vom Inhalt der gesamten Netze aus. Kennen Sie das *Deep Net* oder das *Dark Net* ?**

***

Google wird zum *BIG BROTHER*: höchste Zeit sich zu schützen

Veröffentlicht am 20.08.2017 von jason-mason.com

Der Internetgigant *Google* wird künftig Inhalte, die nicht den neuen Zensurbestimmungen folgen, automatisch aus seinen Suchanfragen entfernen oder ganz hinten auflisten. Das betrifft Webseiten und Suchanfragen, die nicht mit der „etablierten" wissenschaftlichen, medizinischen oder historischen Weltsicht übereinstimmen. Es gibt dazu ein neues Update der generellen Richtlinien von Google.

❖ Viele der Suchergebnisse von *Google* werden laut seinem *Mitarbeiter und Bilderberger-Mitglied Eric Schmidt* als „Programmfehler" betrachtet. Diese Ergebnisse will *Google* in seinem System eliminieren.

→ **Benutzer sollen nur mehr „richtige" Suchergebnisse geliefert bekommen. Die neuen Richtlinien stellen also eine generelle Zensurmaßnahme dar, die unerwünschte Webseiten und Inhalte herausfiltern.**

- Dadurch sollen nur mehr Inhalte zugelassen werden, die auf ihre „*hohe Qualität*" geprüft und als „*sichere Nachrichtenquellen*" („*Staats*"*-Medien bzw. Reuters*) bestätigt werden.

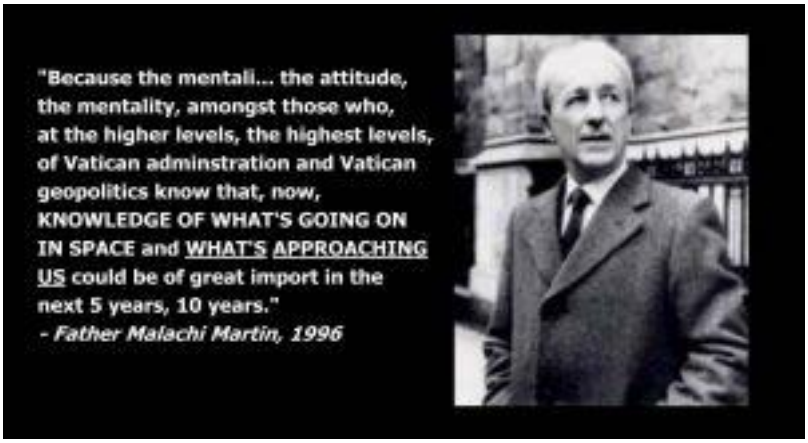
In den neuen Richtlinien wird ausdrücklich betont, dass sogenannte „*Verschwörungstheorien*" den niedrigsten Rang in den Suchergebnissen erhalten sollen.

- Das bedeutet wahrhaft eine Entwicklung in Richtung des „*Wahrheitsministeriums*". **Freie Meinung und freier Informationsfluss sollen unterbunden werden.**

Ein Blick auf die neuen Google-Richtlinien

Punkt 7.10 der Google-Richtlinie:

- „Substanzlose Verschwörungstheorien“ oder Beispiele von Webseiten mit der niedrigsten „Qualität“. Inhalte, die diese Bewertung erhalten, sind Google zufolge *„trügerische Webseiten die das Ziel verfolgen, substanzlose Verschwörungstheorien zu verbreiten“*. Die Begründung von *Google* lautet:
  → Webseiten, die in direktem Widerspruch zu „*etablierten historischen Fakten*“ stehen, stehen unter Verdacht, Nutzer „*falsch*“ zu informieren. Suchen Nutzer gezielt nach solchen Informationen, zeigt das, dass sie einen alternativen Standpunkt vertreten (also selbst „Verschwörungstheoretiker“ oder schlimmeres seien).



***Google*, *Facebook* und *Youtube* arbeiten im Grunde zusammen und beschäftigen bereits jetzt ein Heer von „*Experten*“, die solche Inhalte identifizieren und herausfiltern sollen.**

Es gibt neue Scanprogramme, die auf ***K****ünstlicher* ***I****ntelligenz* (KI) beruhen und das bald selbst erledigen werden. **Federführend bei diesen Zensurmaßnahmen sind NGOs, also Nichtregierungsorganisationen.**

? Warum haben sie einen so starken Einfluss und wer steht hinter ihnen?

- Es wurden erst vor kurzem einige dieser NGOs namentlich bekannt gemacht. Die wichtigste von allen ist die *ADL* (*Anti-Defamation League*), gefolgt vom *No Hate Speech Movement* und dem *Institute for Strategic Dialogue*.

Forscht man ein wenig nach, stellt man fest, dass […] davon ausgegangen werden darf, dass die Medien und die politischen Eliten komplett korrupt sind, und von einfluss-reichen Quellen finanziert und gesteuert werden. Es gibt dafür sogar neue EU-Richt-linien, die kriminalisieren.

Um dieser Willkür entgegenzuwirken, ist es wichtig, sich von den großen Diensten wie *Google*, *Facebook* und *Youtube* zu trennen, um nicht automatisch ins Visier dieser Zensurbehörden zu gelangen. Der *NSA-Whistleblower* Edward Snowden gab einige Ratschläge heraus, um sich abzusichern:

Ratschlag 1 – Smartphones

Die meisten Menschen nutzen heute neben ihrem Computer hauptsächlich ihr *Smartphone* zur Kommunikation. Es gibt ein paar wichtige kostenlose Apps, um ihr Telefon sicherer zu machen. *Edward Snowden* empfiehlt ganz besonders Verschlüsselungsanwendungen. Dazu gehört das Verschlüsseln der Anrufe und Textnachrichten.

→ ***Signal – Sicherer Messenger.***

Signal funktioniert ähnlich wie *WhatsApp*. Mit *Signal* können Sie kostenlos telefonieren und in Echtzeit Nachrichten austauschen. Sie können Gruppen erstellen, um sich gleichzeitig mit mehreren Personen zu unterhalten sowie Multimediainhalte und Anhänge untereinander teilen. Das alles läuft absolut vertraulich. Die Entwickler und Betreiber von *Signal* haben zu keinem Zeitpunkt Zugriff auf Ihre Kommunikation und speichern keine Ihrer Daten. *Signal* nutzt ein fortschrittliches Verschlüsselungsprotokoll, um die Vertraulichkeit aller Kommunikation jederzeit sicherzustellen. *Signal* verwendet Ihre bestehende Rufnummer und Ihr Adressbuch. Es gibt keine zusätzlichen Anmeldungen, Benutzernamen, Passwörter oder PINs zu verwalten.

→ ***Sophos Mobile Security***

Gewinner der Auszeichnungen „*Best Android Security 2016*“ und „*Best Protection 2015*“. *Sophos Mobile Security* hat in den von AV-TEST durchgeführten Vergleichstest für Android Sicherheits- und Antivirus-Apps 14-mal in Folge (seit September 2014) die maximale Schutzquote von 100% erzielt. Alle Features, keine Werbung, völlig kostenlos. Diese App schützt Ihr Android-Gerät und Ihre Privatsphäre umfassend und ohne negative Auswirkungen auf die Leistung oder die Akku-Laufzeit. Apps werden automatisch mit Hilfe aktuellster *SophosLabs*-Informationen gescannt, um Sie vor Datenverlust und unvorhergesehenen Kosten zu schützen. Bei Verlust oder Diebstahl des Gerätes können Sie es ferngesteuert sperren oder zurücksetzen und so Ihre Daten schützen.

→ **Hola Kostenlose VPN**

Hola VPN ist ein Browser, um das Internet anonym zu nutzen. Virtual Private *Network* bezeichnet ein virtuelles privates Kommunikationsnetz. *Hola VPN funktioniert* durch die gemeinsame Nutzung der brachliegenden Ressourcen seiner Nutzer zum Wohle aller. *Hola* bietet Zugriff auf Websites, die durch Ihr Land blockiert sind. *Hola* beschleunigt *Browsing* durch die Wahl der schnellsten Quellen und reduziert Datenkosten und Gerätestrahlung. Verstecken Sie Ihre IP-Adresse, um das Internet privat und anonym zu nutzen. *Hola* ist 100% kostenlos. *Hola* bietet außerdem die App Fake GPS location. Damit können sie die GPS Überwachung austricksen.

- Zusätzlich sollte man sein Smartphone noch mit einem App-Lock versehen, um fremden Zugriff auf das Telefon zu verhindern. Wenn sie diese oder ähnliche Dienste nutzen, verbessern Sie Ihre Sicherheit bereits enorm. Sogenannte Signal-Blocking-Hüllen schirmen Ihr Smartphone ab, wenn Sie auf Reisen sind

oder etwas Wichtiges zu erledigen haben und nicht gestört oder geortet werden wollen.

Ratschlag 2 – Sichere Internetbrowser und Erweiterungen

Edward Snowden empfiehlt auch, seinen 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* und *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 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 bzw. 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 weiterbetreiben bzw. kopieren kann. Somit trägt man seinen privaten Browser in Form eines USB-Sticks immer bei sich und er scheint nicht im eigentlichen Betriebssystem auf.

Download Chrome Portable Download Firefox Portable

Es folgt eine Auflistung der wichtigsten Erweiterungen, um diese Browser sicherer zu machen. Man muss sie direkt im jeweiligen Browser installieren. Klicken Sie dazu auf die Links.

→ AdBlocker Ultimate

Adblocker Ultimate ist mit dem einzigen Ziel konzipiert, alle Werbeanzeigen zu löschen, sodass Sie sich auf Ihre gewünschten Inhalte konzentrieren können. *Adblocker Ultimate* blockiert Schadsoftware und Tracking und 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 Ihrer Webseite beschleunigen und die CPU- und Speichernutzung verringern.

→ **AnonymoX**

Mit *AnonymoX* kann man seine virtuelle Identität mit nur einem Mausklick wechseln. Installieren und aktivieren Sie dieses kostenfreie Add-on für *Firefox* oder *Chrome*. Anschließend kann man sich eine IP und das Land aus dem man surfen will auswählen. Werden Sie ein Teil dieses Anonymisierungsnetzwerks. Mit 0,7 Millionen geschützten Nutzern bietet *AnonymoX* einen hervorragenden Schutz. Man kann unter den 0,7 Millionen Nutzern nicht mehr erkannt werden. Bleiben Sie anonym. Umgehen Sie viele Arten von Zensur, indem Sie eine virtuelle Identität in einem anderen Land annehmen und so *GEO-IP*-Sperren umgehen.

→ **Canvas Defender**

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 nichtlöschbarer Cookie-Nachfolger betrachtet. Mit dem *Canvas Defender* wird eine Störung im Fingerprinting erzeugt. Damit kann ein Browser nicht mehr einem speziellen Computer zugeordnet und zurückverfolgt werden.

→ **Click&Clean** (für Chrome) + **Clear Recent History** (für Firefox)

Diese Erweiterungen löschen Ihren Browsing-Verlauf, wenn der Browser geschlossen wird und verhindern die Verfolgung Ihrer Online-Aktivitäten.

→ **Ghostery**

Ghostery spürt Tracking-Technologien auf und blockiert sie, beschleunigt so den Aufbau der Internetseiten, macht sie übersichtlicher und schützt Ihre Daten. *Ghostery* sieht das „unsichtbare" Web und erkennt *Tracker, Web Bugs, Pixel* und *Beacons*, die von *Facebook*, *Google*, mehr als 500 weiteren Werbenetzwerken, Anbietern von Verhaltensdaten und Web-Publishern (d.h. von Unternehmen, die sich für Ihre Aktivität interessieren) eingesetzt werden. Das ist einer der aktuell wichtigsten Sicherheitserweiterungen.

→ **Mercury Reader** (für Chrome) und **Tranquility Reader** (für Firefox)

Diese Erweiterungen entfernen alle Werbeanzeigen und andere störende Elemente auf einer Webseite und lässt nur den Text und die Bilder übrig. Damit kann man unübersichtliche Webseiten endlich sauber und entspannt lesen.

→ **Mod Header** (für Chrome) + **Modify Headers** (fürFirefox) –

Sie sind Add-ons, mit dem sich der HTTP-Request-Header verändern, hinzufügen und filtern lässt. Eine von ihnen gewählte IP-Adresse wird auf ihre echte aufgesetzt. Sie müssen 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 *Facebook* oder *Google* vor seine eigene setzten und ist damit getarnt. 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 eine Liste mit falschen ID-Adressen anlegen.

→ **Privacy Badger**

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

→ **ProxFlow** (für Chrome) und **ProxTube** (für Firefox)

Diese 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.

ScriptSafe (Chrome) und **NoScript** (Firefox)

ScriptSafe und NoScript erlauben das Ausführen von JavaScript, Java und anderen Plugins nur bei vertrauenswürdigen Domains Ihrer Wahl (z.B. Ihrer 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.

→ **ZenMate VPN** (für Chrome) + **ZenMate VPN** (für Firefox)

Das Add-on von *ZenMate* verschlüsselt Ihre Netzwerkverbindungen einfach und effektiv. Auch unerfahrene Nutzer erhalten so mehr Privatsphäre im Internet und dürfen auf ausländische, in Deutschland gesperrte Dienste, wie das US-Netflix oder Youtube-Videos, zugreifen. Zur Auswahl stehen Server aus Deutschland, Rumänien, den USA und Hong Kong. Für Premium-Nutzer kommen außerdem Server an den Standorten Frankreich, Schweiz, Kanada, der Westen der USA, Singapur und Großbritannien hinzu.

→ **All-in-One Sidebar** (für Firefox)

Diese Sidebar ermöglicht die Anzeige diverser Fenster als Paneele in der Sidebar und macht so Schluss mit dem Chaos! Zusätzlich zu den Lesezeichen und der Chronik lassen sich nun auch die Downloads und Add-ons in der Sidebar von *Firefox* anzeigen.

→ **BetterPrivacy** (für Firefox)

Dank *BetterPrivacy* schließen Sie ein bisher wenig beachtetes Sicherheitsloch in *Firefox*. Mit der Firefox-Erweiterung BetterPrivacy schützen Sie sich effektiv vor sogenannten Super-Cookies. Wer viel im Internet surft, setzt sich Gefahr aus, beim Abspielen von Flash-Animationen ein *Local Shared Object* (LSO) einzufangen. Dabei handelt es sich um ein langlebiges Cookie, das beliebige Daten auf Ihrem PC sammeln, speichern und versenden kann, ohne dass Sie etwas davon bemerken. Mit der Erweiterung *BetterPrivacy* für *Firefox* können Sie je nach Einstellung diese LSOs bei jedem Browser-Start oder -Ende oder nach zeitlichen Intervallen diese Objekte löschen lassen.

→ **Disconnect** (für Firefox)

Disconnect zeigt und blockiert unsichtbare Webseiten, die Ihr Suchverhalten verfolgen und speichern. *Disconnect* wurde im Jahr 2016 zum besten Browser-Sicherheitstool gewählt.

→ **HTTPS Everywhere**

HTTPS Everywhere wird von *Edward Snowden* als eine der wichtigsten Erweiterungen überhaupt bezeichnet. Mit dem kostenlosen Add-on „*HTTPS Everywhere*“ verschlüsseln Sie Webseiten und surfen anonym im Internet. „*HTTPS Everywhere*“ bewirkt den Wechsel von einer unverschlüsselten zu einer verschlüsselten Datenübertragung per HTTPS.

Random User-Agent (für Chrome) und **Random Agent Spoofer** (fürFirefox)

Diese Erweiterungen täuschen falsche Browser aus unterschiedlichen Betriebssystemen vor und können so eingestellt werden, dass sie zufällig rotieren. Das erschwert die Verfolgung ihres Surfverhaltens im Netz.

→ **Self-Destructing Cookies** (für Firefox)

Diese Erweiterung löscht alle Cookies automatisch, sobald der Browser geschlossen wird. Sie schützt außerdem gegen Tracker und Zombie-Cookies.

→ **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* benötigen *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.

***

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

***

Ratschlag 3 – Sichere Suchmaschinen

→ **DuckDduckGo**

Es gibt auch sichere Alternativen zur Suchmaschine von *Google*. Da wäre einmal *DuckDuckGo*, eine Suchmaschine, die besonderen Wert auf Privatsphäre legt. Das Hauptaugenmerk bei *DuckDuckGo* wurde aber auf das Thema Datenschutz und Privatsphäre gelegt. Die Suchmaschine speichert keine IP-Adressen, protokolliert keine Informationen über Besucher und verwendet Cookies nur in überschaubaren Maßen. *DuckDuckGo* hat sich im Laufe der letzten Jahre zu einer konkurrenzfähigen Suchmaschine zu *Google* entwickelt.

→ **Startpage**

Eine andere Alternative ist die Suchmaschine *Startpage*. Mit *Startpage* nutzen Sie die Suchmaschine *Google*, ohne dass der Internetkonzern Sie tracken kann. Dafür anonymisiert der Dienst Ihre Anfragen und schickt sie dann erst an *Google*. Somit profitieren Sie von dem starken *Google*-Suchalgorithmus und schützen gleichzeitig Ihre Privatsphäre. Jetzt hat sich der Funktionsumfang von *Startpage* noch einmal vergrößert. Die anonyme Suchmaschine kommt jetzt auch mit interaktiven Karten zurecht und liefert Ihnen *Wikipedia*-Sofortantworten.

Ratschlag 4 – Verschlüsselung von Ordnern, Partitionen, Betriebssystemen und Festplatten

Besonderen Wert legt Edward Snowden auch auf die komplette Verschlüsselung des ganzen Computersystems. Es gibt hier verschiedene Möglichkeiten, je nachdem, welches Betriebssystem man nutzt. Am besten ist es, die ganze Festplatte zu verschlüsseln. Wenn der Computer gestohlen oder konfisziert wird, ist es fast unmöglich, an Ihre privaten Daten zu gelangen. Da die meisten Leute immer noch ein *Windows*-Betriebssystem nutzen, bieten sich hier folgende Möglichkeiten:

→ **TrueCrypt**

TrueCrypt ist eine Software zur Datenverschlüsselung, insbesondere zur vollständigen oder partiellen Verschlüsselung von Festplatten und Wechseldatenträgern. Das Programm läuft unter Windows ab der Version 2000 bis zur Version Windows 8. Laut einer Meldung auf der offiziellen Website wurde die Entwicklung von *TrueCrypt* im Mai 2014 eingestellt. Bei *TrueCrypt* wurden anscheinend Sicherheitslücken entdeckt. Viele Benutzer schwören heute immer noch auf die sichere Version *TrueCrypt 7.1a***.**

→ **VeraCrypt**

Veracrypt ist ein Nachfolger von *TrueCrypt*. Die Entwickler behaupten die bisher entdeckten Sicherheitslücken behoben zu haben. *VeraCrypt* wird laufend weiterentwickelt. *VeraCrypt* bietet die Möglichkeit, gesamte Systeme, einzelne Partitionen oder sogenannte „Container" zu verschlüsseln. Bei letzterem handelt es sich um spezielle Dateien mit fester Größe, die nach dem Entschlüsseln wie virtuelle Laufwerke behandelt werden. Durch die Verschlüsselung ihres Systems mit *Veracrypt* sind Sie gegen Ausspähungen von Regierungen und Konzernen gewappnet.

→ **BitLocker**

BitLocker ist eine Festplattenverschlüsselung von *Microsoft*, die in den Ultimate- und Enterprise-Versionen von Windows 7-10 enthalten ist. Da *BitLocker* nicht Opensource basiert ist, stellt sich die Frage nach Sicherheitsmängeln. *Microsoft* hat in seine Software mit Sicherheit Hintertüren eingebaut. Auch Edward Snowden stellte 2013 Dokumente bereit, die bestätigen, dass die NSA mit *Microsoft* zusammenarbeitet und so diese Verschlüsselungstechnik umgehen konnte.

- Im Zweifelsfall fällt die Wahl immer auf VeraCrypt. Es wird ständig weiterentwickelt und ist als sicher eingestuft.

***

Ratschlag 5 – Der Tor-Browser

Wem die bisher aufgezählten Sicherheitsmaßnahmen noch nicht ausreichen, der kann noch schwerere Geschütze auffahren. Das *Tor*-Browser-Paket ermöglicht anonymeres Surfen im Internet mit dem Open-Source-Browser *Firefox*. Sobald Sie im Internet unterwegs sind, hinterlassen Sie jede Menge Spuren. Das kostenlose Tor-Browser-

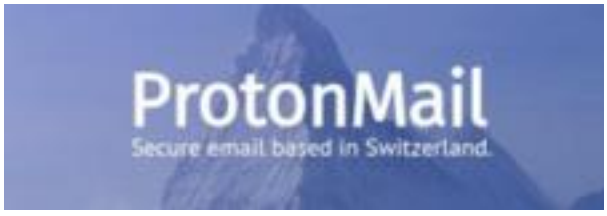
Paket beugt dem vor, indem es Sie über das verschlüsselte Tor-Netzwerk ins Internet bringt. *Tor* steht für „The Onion Router“ (der Zwiebel Router). Er wurde so benannt, weil er mehrere Sicherheitsebenen besitzt. Mit dem *Tor*-Browser sind Sie immer anonym im Internet unterwegs.

Wenn Sie die Sicherheit noch weiter erhöhen wollen, nutzen Sie einen zusätzlichen VPN-Client. Diese Software leitet ihren Datenverkehr auf verschiedene Server im Ausland um, und sie erhalten automatisch eine andere IP-Adresse. Wenn Sie VPN aktivieren und erst danach den *Tor*-Browser starten, bemerkt niemand, dass Sie das *Tor*-Netzwerk benutzen.

Der beste kostenlose VPN-Client ist derzeit CyberGhost. In der Basic-Version kann *CyberGhost* jeweils drei Stunden am Stück verwendet werden und unterbricht dann kurz. Man muss einige Sekunden warten, bis man wieder verbunden ist. Das lässt sich aber verkraften. Die Nutzung selbst ist unbegrenzt. Mit *CyberGhost*können Sie auch mit herkömmlichen Browsern wie *Firefox* oder *Chrome* anonym im Internet surfen.

Es gibt auch ein spezielles, von *Edward Snowden* empfohlenes Betriebssystem namens Tails. Das kostenlose Betriebssystem *Tails* soll Datenspionen das Leben so schwer wie möglich machen. *Tails* steht für „**T**he **A**mnesic **I**ncognito **L**ive **S**ystem“. 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 Ihre Windows-Installation nicht. Sie vermeiden außerdem, aufgrund von Schwachstellen und Sicherheitslücken Ihres Windows-Systems, unnötige Spuren im Netz zu hinterlassen. Um unerkannt zu agieren und etwaige Sperren zu umgehen, durchlaufen alle Datenpakete 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 einen USB-Stick oder eine SD-Karte zu installieren.

→ **ProtonMail**



Auch im normalen Internet gibt es die Möglichkeit, verschlüsselte online-Konten zu benutzen.
Viele *Tor*-Nutzer vertrauen auf diese Möglichkeit. *ProtonMail* gehört einem Unternehmen in der Schweiz, das kostenlose Konten anbietet. *ProtonMail* hat den Hauptsitz in Genf und wird von *Proton Technologies* geführt. Ihre Server befinden sich an zwei Standorten in der Schweiz, außerhalb der EU- und US-Rechtsprechung. *ProtonMail* wurde im Jahr 2013 wegen

der Enthüllung der Snowden-Affäre gegründet. Ende 2016 lag die Nutzerzahl bei rund fünf Millionen.

In den Jahren 2015/2016 wurde *ProtonMail* in Suchresultaten von *Google* unterdrückt, wodurch *ProtonMail* weniger zahlende neue Nutzer gewann als geplant. Wenn sie ein sicheres Email-Konto benötigen, wählen sie das kostenlose *ProtonMail*.

***Edward Snowden* glaubt, dass *Tor* die derzeit wichtigste Technologie zum Schutz der Privatsphäre im Netz darstellt.** Er selbst nutzt ausschließlich *Tor*. Er meint, wenn man jetzt selbst noch kein *Tor* nutzt, man das schleunigst ändern sollte. Es wird in Zukunft zu schweren repressiven Maßnahmen im Netz kommen. **Jede Webseite, die man heute ansurft, stiehlt Nutzerdaten von Ihnen. Diese Informationen werden abgefangen, gesammelt, analysiert und von in- und ausländischen Regierungen und Konzernen gespeichert.** Indem man sich durch ein paar einfache Schritte schützt, kann man dieser Entwicklung entgegenwirken, seine Privatspäre schützen und zu keinem gläsernen Bürger werden