DU HAST NICHTS ZU VERBERGEN?

DU HAST NICHTS ZU VERBERGEN?

Erste Schritte zur Digitalen Selbstverteidigung

Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

EDWARD SNOWDEN

Inhalt

SIE WISSEN, WO DU LETZTEN SOMMER IM URLAUB WARST. SIE WISSEN, WER DABEI WAR UND WAS IHR EINGEKAUFT HABT. SIE WISSEN AUCH, WER DICH SEITDEM NICHT MEHR ANRUFT.

DU HINTERLÄSST DATEN. DU WIRST ÜBERWACHT. DU KANNST ETWAS DAGEGEN TUN.

Einleitung

Wer nicht gegen Überwachung kämpft, akzeptiert die Einschränkung seiner Freiheit. Dieses Heft zeigt Dir, wie Du Dich dagegen wehren kannst und ist ein Beitrag für Deine Digitale Selbstverteidigung. Als eine einführende Sammlung und Informationsquelle richtet es sich insbesondere an alle, die sich bisher nicht ausführlich mit den Themen Datenschutz und Überwachung auseinandergesetzt haben.

Hier bekommst Du keine komplizierten Codes oder unverständliche Massnahmen vorgeschlagen. Es reichen wenige Programme und Einstellungen, die für Dich kaum Aufwand bedeuten. Diese kleinen Veränderungen merkst Du bei der Nutzung Deines Computers oder Smartphones kaum. Auch wenn es keine absolute Sicherheit gibt, machst Du es datenhungrigen Unternehmen oder Geheimdiensten wesentlich schwerer, Informationen über Dich zu sammeln.

Die hier vorgestellten Programme und Massnahmen bieten eine gute Grundlage, um in die Digitale Selbstverteidigung einzusteigen. Das komplette Spektrum kann hier allerdings nicht präsentiert werden.

Viel Spass beim Lesen.

Start To Protect Your Digital Identity!

Nichts zu verbergen?

Gerne wird Überwachung mit dem Argument hingenommen, man habe ja nichts zu verbergen. Doch bist Du Dir sicher? Tust Du nichts, was irgendjemanden da draussen interessieren könnte?
Dein Smartphone erzählt *Google* und *Facebook* wo Du wohnst, wann Du schlafen gehst, wann Du morgens wach wirst, ob Du auf dem Weg zur Arbeit im Stau stehst und an welchem Ort Du Dein Geld verdienst. Und Du selbst erzählst *Facebook*, welches Essen Du magst, welche Musik Du am liebsten hörst und wo Du am liebsten Shoppen gehst. Und die Geheimdienste wissen, was Du *Google* und *Facebook* erzählst.

Für die Diskussion rund um das Thema Überwachung ist es aber irrelevant, ob Du etwas zu verbergen hast. Es geht vielmehr darum, dass die Gesellschaft widerstandslos eine Massenüberwachung zulässt, ohne einen Blick in die Zukunft zu werfen. Was jemand zu verbergen hat, ist schliesslich abhängig vom Zeitgeist und der politischen Entwicklung. Was heute noch als normal gilt, kann morgen schon verdächtig und unmoralisch erscheinen. Unter dem Buzzword und Megatrend “Big Data” geben wir unachtsam alles preis. Dabei bezahlen wir für kostenlose Internetanwendungen mit unseren Daten.
Es ist wichtig zu verstehen, dass Du bei *Google*, *Facebook* und Co. nicht der Kunde, sondern das Produkt bist - dessen Daten weiterverkauft werden. Sie sind der Rohstoff

für Werbetreibende und Versicherungskonzerne.

Noch nie war eine vollständige Überwachung so billig und technisch so einfach umsetzbar wie heute. Noch nie konnten Staaten so problemlos und mit einer so einfachen Begründung wie der Terrorismusabwehr tief in Deine Privatsphäre vordringen. Spätestens seit den Enthüllungen Edward Snwodens im Jahr 2013 ist die Massenüberwachung durch staatliche Geheimdienste auch öffentlich belegt.

Von unschuldig zu schuldig

Überwachung funktioniert wie die Geschichte vom heissen Wasser und dem Frosch: Er sitzt ruhig im Topf und merkt nichts, bis es zu spät ist. Wir werden immer stärker überwacht und spüren es genauso wenig. Im Gewöhnungseffekt liegt die Gefahr. Durch diese Entwicklung schränkt sich der Raum der Privatsphäre immer weiter ein. Die permanente Überwachung führt dazu, dass aus der Unschuldsvermutung eine Schuldvermutung wird. Für Deinen Staat bist Du potenziell verdächtig. Und deshalb lässt er seine Geheimdienste nach bestimmten Verhaltensmustern suchen. So interessiert er sich beispielsweise für Bewegungsprofile, die er vorher als verdächtig typisiert hat. Was verdächtig ist, bestimmen die Behörden selbst. Aufgrund solcher und unzähliger anderer Daten landeten mindestens 1,2 Millionen Menschen auf den Überwachungslisten der amerikanischen *National Security Agency (NSA)*.

Viele dieser Personen werden nicht einmal mehr verdächtigt, ihre Daten bleiben aber selbst dann gespeichert, wenn sie als nutzlos klassifiziert werden. Tatsächlich ist die Überwachung der eigenen Bevölkerung in den meisten demokratischen Ländern verboten. Umgehen lassen sich die Gesetze durch Kooperationen mit ausländischen Geheimdiensten. Und kommt es einmal zum Skandal, werden in aller Regel nicht die Geheimdienste sanktioniert, sondern das Fehlverhalten wird mit einer Gesetzesinitiative legalisiert.

Neben der staatlichen Überwachung durch Geheimdienste sind auch allerlei Unternehmen an Deinen Daten interessiert. Viele Verbindungen im Internet sind unverschlüsselt und ein Mitlesen der übertragenen Informationen ist für Internetanbieter und Webseitenbetreiber ein Kinderspiel.

Du musst aber gar nicht im Internet surfen, um eine Datenspur zu hinterlassen. In unserem Alltag entsteht eine Vielzahl von Daten. Das elektronische U-Bahn Ticket erfasst Ein- und Ausstiegsorte, Einkaufsbonusprogramme analysieren Deine Kaufkraft und die Bankkarte zeichnet Deine Bezahlvorgänge auf. Besonders Smartphones und andere Smart-Devices bündeln durch ihre vielseitigen Anwendungsbereiche Deinen Datenstrom. Gerade für Krankenkassen können Deine Bewegungsdaten interessant sein,

um Dir an Dein
Fitnesslevel angepasste
Versicherungstarife
anzubieten. Bei einigen
privaten Versicherungen
ist dieses Modell bereits
in der Praxis zu sehen.
Aus diesem Grund fördern
viele Krankenkassen
den Kauf sogenannter
“Wearables”. Dass dabei
Datenschutzrechte
missachtet werden,
wird selten beleuchtet.
So verkaufen einige
Unternehmen die
gewonnenen Nutzerdaten.
Diese können mit
anderen Daten verknüpft
und zu umfassenden
Profilen zusammengefügt
werden, die dann von
Datenhändlern verkauft
werden. US-amerikanische
Unternehmen sind
durch den “National
Security Letter” dazu
verpflichtet, mit der *NSA*
zusammenzuarbeiten. Die
Geheimdienste wissen
also, was Du tust.

Metadaten

Die Daten, die staatliche Institutionen und Unternehmen speichern, sind überwiegend Metadaten. Befürworter der Überwachung sagen gerne, es handele sich ja "nur" um Metadaten. Doch genau diese geben einen detaillierten Einblick in Dein Leben. Also was genau sind Metadaten?
Metadaten sind "Daten über Daten". Nicht die Inhalte Deines Telefongesprächs werden erfasst, dafür aber der Ort, die Uhrzeit, die Dauer und Eure Telefonnummern. Anhand dieser Daten lassen sich komplexe Bewegungs- und Handlungsmuster erkennen. Auch Freundeskreise und die berufliche Kommunikation lassen sich erfassen. Weitere Metadaten sind zum Beispiel E-Mail Betreffzeilen, IP-Adressen, Empfänger und Sender von SMS und Mails. Metadaten lassen sich zählen, kategorisieren und in Datensätzen zusammenfassen. Das macht es einfach, sie auszuwerten. Teilweise entstehen Metadaten, um einen Service erst zu ermöglichen – ohne Handynummer kann ich keine SMS verschicken. Du kannst Metadaten weder verschlüsseln noch blockieren. Es braucht also gesetzliche Regelungen, um eine missbräuchliche Verwendung zu verhindern. Stattdessen verpflichten die Gesetze in Deutschland und der Schweiz die Anbieter von Telekommunikation und Internet sogar dazu, alle Daten ihrer Nutzer für eine bestimmte Zeit zu speichern, in der Schweiz für sechs Monate. In Deutschland wurde diese Praxis als verfassungswidrig erklärt. Daraufhin hat die Politik ein neues Gesetz verabschiedet: Heute gelten Speicherzeiten zwischen vier und zehn Wochen. Viele Apps und Anwendungen wie beispielsweise *Facebook* speichern die Daten ihrer Nutzer jedoch jahrelang. Sie werden unter anderem dazu verwendet, zukünftige Verhaltensweisen zu berechnen. Dank Edward Snowden wissen wir, dass auch die Geheimdienste Metadaten illegalerweise speichern.
Wer möglichst wenig Metadaten produzieren will, müsste auf Handygespräche und SMS verzichten und stattdessen auf verschlüsselte Internetkommunikation setzen.

WER HAT UNS VERRATEN?

METADATEN!

Passwörter und Passsätze

Passwörter sind die Schlüssel zu Deinen persönlichen Daten im Internet. Du brauchst also gute Passwörter, um Dich zu schützen. Ein gutes Passwort soll lang und kompliziert sein, Sonderzeichen, Zahlen und grosse sowie kleine Buchstaben beinhalten. Je länger, komplexer und ungewöhnlicher Dein Passwort ist, desto länger braucht ein Angreifer, um es zu ermitteln. Bei einem Passwort mit elf Stellen in ungewohnter Kombination benötigt ein Computer sehr lange, um den Passwortschutz zu durchbrechen.
Bei einem Angriff werden zunächst die bekanntesten Passwörter in verschiedenen Sprachen getestet. Zudem sollten keine persönlichen Daten wie Name oder Geburtstag im Passwort enthalten sein.

Xt87ko?,H7!"l?a6k wäre also ein gutes Passwort. Da Du aber für jeden Zugang ein anderes komplexes Passwort verwenden solltest, wird das ganz schön kompliziert.

Es gibt zwei einfache Lösungen für dieses Problem: Eine Möglichkeit sind Programme zum Managen und Erstellen von Passwörtern. Die andere Option ist, anstelle von Passwörtern Passsätze zu verwenden. Diese sollten auch Sonderzeichen und Zahlen beinhalten. Ein Passsatz lässt sich einfacher merken, als eine wirre Kombination einzelner Zeichen. Ab und an solltest Du Deine Passsätze auch wechseln. Und damit Du das nicht vergisst, wurde der "Change Your Password Day" ausgerufen. Er ist immer am 1. Februar.

Diceware

Diceware bezeichnet eine Methode, mit der Du auf spielerische Art und Weise ungewöhnliche und wirkungsvolle Passsätze erstellen kannst. Dafür brauchst Du einen Würfel und eine *Diceware* Wort- und Zeichenliste, die Du leicht im Internet findest. Jedes Wort oder Zeichen auf der Liste entspricht einer fünfstelligen Kombination der Ziffern 1 bis 6. Fünf Mal würfeln ergibt also immer ein Wort. Zum Beispiel entspricht die gewürfelte Kombination 16661 dem Wort "daten".

Empfohlen wird, mindestens fünf Wörter und ein Zeichen beziehungsweise eine Zahl zu erwürfeln. Dadurch erhältst Du einen einzigartigen, zufällig generierten und trotzdem leicht zu merkenden Passsatz wie beispielsweise "sechs olive kosmos moskau 1500 oz". Es wird empfohlen, zwischen die einzelnen Wörter ein Leerzeichen zu setzen. Auf die Gross- und Kleinschreibung kannst Du verzichten. Durch die grosse Zeichenanzahl ist ein *Diceware* Passsatz nur sehr schwer zu knacken.

Shortfacts

Was ist Diceware?
Eine einfache Methode, um sichere Passsätze zu erstellen.

Hintergrundinformationen und Wortlisten:
www.world.std.com/~reinhold/diceware.html

Zeitaufwand je Passsatz:
5 Minuten

1Password

Ein Kennwort-Manager ermöglicht es Dir, Benutzernamen, Anmeldeinformationen und komplexe Passwörter sowie Passsätze zu erstellen und zu speichern. Geschützt sind Deine Daten durch ein Masterpasswort. Dementsprechend sollte dieses möglichst komplex sein. Darüber hinaus gibt es die Möglichkeit, die gespeicherten Kennwörter zwischen verschiedenen Geräten zu synchronisieren. Du solltest jedoch beachten, dass die

Synchronisation mithilfe eines Cloud-Dienstes erfolgt, der von einem Drittanbieter betrieben wird. Dadurch gelangen Deine Daten ins Internet. Sicherer wäre es, die Passwortdaten nur lokal auf einem Gerät zu speichern. Der Nachteil eines Passwort-Managers ist, dass Schadsoftware, die Dein Masterpasswort abgreift, auch Zugriff auf alle anderen Passwörter erhält. Dennoch bieten Dir Kennwort-Manager bei richtiger Anwendung eine komfortable Möglichkeit, Deine Passwörter zu verwalten.

Das Programm *1Password* bietet einen sehr grossen Funktionsumfang, wie das Erstellen komplizierter Passwörter oder die Prüfung Deiner Passwörter auf ihre Stärke. Es erinnert Dich auch daran, besonders alte oder doppelt benutzte Passwörter zu ändern. *1Password* ist sehr einfach zu bedienen, kann in alle gängigen Browser integriert und zwischen verschiedenen Geräten synchronisiert werden. Es ermöglicht Dir, nach der Eingabe des Masterpasswortes online Anmeldefelder mit einem Klick auszufüllen. Allerdings handelt es sich bei *1Password* um ein kommerzielles Angebot, das Du entweder einmalig oder monatlich bezahlen musst und dem Du Deine Daten anvertraust. Gute und geprüfte Open-Source-Alternativen mit ähnlichen Funktionen sind beispielsweise *KeePass* oder *Password Safe*, allerdings sind sie in der Anwendung etwas weniger nutzerfreundlich.

Shortfacts

Was ist 1Password?
Ein Programm zum Passwörter erstellen und verwalten.

Wo bekomme ich 1Password?
www.1password.com

Plattformen: alle

Lizenz: kommerziell

Zeitaufwand: 15 Minuten

Open-Source-Alternativen:
www.pwsafe.org
www.keepass.info

The sheer size of data is too large, and in spite of all intricate programs for detecting suspicious messages, computers that register billions of data are too stupid to interpret and evaluate them properly, ridiculous mistakes where innocent bystanders are listed as potential terrorists occur necessarily – and this makes state control of communications even more dangerous.

SLAVOJ ŽIŽEK

Verschlüsselt kommunizieren

Die meisten Deiner Daten sind unverschlüsselt unterwegs. Das ist so, als würdest Du sie in einem durchsichtigen Briefumschlag versenden. Die Internetanbieter und Serverbetreiber, die als elektronische Briefträger an der Kommunikation beteiligt sind, können genauso einfach mitlesen, wie andere Angreifer und Schnüffler. Doch Du kannst etwas dagegen unternehmen. Ein Programm zur Verschlüsselung Deiner E-Mails ist in wenigen Minuten eingerichtet, für verschlüsselte Verbindungen zu Webseiten braucht es nur ein Add-on im Browser und für Chats und Internettelefonie bieten sich ebenfalls verschiedene Programme an. Die Verschlüsselung funktioniert dabei wie der Briefumschlag um einen Brief.

Während Unternehmen und Geheimdienste, bei unverschlüsselten Nachrichten den Inhalt sehen, wissen sie bei verschlüsselten Nachrichten nur noch, *dass* Du etwas versendet hast, nicht mehr *was*. Nur der Empfänger kann mit dem richtigen Schlüssel die Nachricht öffnen.

Obwohl es technisch einfach ist, werden Nachrichten selten verschlüsselt. Ein Problem ist sicher, dass viele Menschen denken, Verschlüsselung sei eine komplizierte und aufwändige Sache. Oder sie denken, dass sie selbst nichts zu verbergen hätten und dass Menschen die verschlüsseln verdächtig sind. Der Einsatz von Verschlüsselungen dient aber dem Schutz Deiner Privatsphäre.

Achte bei der Auswahl Deiner Verschlüsselungssoftware darauf, dass es sich um eine Ende-zu-Ende-Verschlüsselung handelt. Nutze Open-Source-Software, denn nur diese kann unabhängig auf Hintertüren geprüft werden.

Überlege Dir, neben Deiner Kommunikation auch Datenträger wie Festplatten oder USB-Sticks zu verschlüsseln. Sowohl *Apple* als auch *Windows* bieten Optionen für Verschlüsselungen von Festplatten. Aber auch hier wäre eine Open-Source-Alternative, wie beispielsweise *veraCrypt*, die erste Wahl.

Signal

Ein grosser Teil der alltäglichen Kommunikation findet in verschiedenen Instant Messengern statt. Die mit Abstand meisten Nutzer verzeichnet dabei die Facebook-Tochter *WhatsApp*. Und obwohl *WhatsApp* heute Deine Nachrichten verschlüsselt, gibt es zwei zentrale Argumente, die für andere Messenger sprechen. Zum einen kannst Du die Weitergabe Deiner persönlichen Daten an *Facebook* nicht verhindern. Zum anderen ist *WhatsApp* keine Open-Source-Software.

Als Alternative lässt sich die *Signal-Private Messenger* App nutzen. Der Dienst ist ein Open-Source-Projekt und gilt bei gleichem Funktionsumfang als sehr zuverlässig. Einer der grossen Fürsprecher von *Signal* ist Edward Snowden. Auch *Apples iMessage* oder der Schweizer Messenger *Threema* bieten Ende-zu-Ende-Verschlüsselungen an. Beide Dienste sind jedoch kommerzielle Software und der Quellcode nicht überprüfbar.

Shortfacts

Was ist Signal?
Ein Instant Messenger für verschlüsselte Chats und Telefonate.

Wo bekomme ich Signal?
www.whispersystems.org

Plattformen:
iOS und Android

Lizenz: Open Source

Zeitaufwand: 5 Minuten

E-Mails verschlüsseln

Das Verschlüsseln von E-Mails sollte ein zentraler Bestandteil Deiner Digitalen Selbstverteidigung sein. Als das wichtigste Verfahren für Verschlüsselungen gilt *OpenPGP* mit *GPG*. Open steht in diesem Fall für Open Source, *PGP* für "Pretty Good Privacy". Mit *OpenPGP* ist die Open-Source-Variante einer kommerziellen Verschlüsselungstechnik gemeint. *GPG* wiederum steht für "GNU Privacy Guard" und ist ein Programm, das den *OpenPGP* Standard verwendet.

Das Ganze klingt komplizierter als es ist. Stell Dir vor, Du bekommst ein Schlüsselpaar um Deine Mails zu versenden. Einen öffentlichen Schlüssel, den Du mit jedem teilst, der Dir schreiben will. Er liegt in einer kleinen Datei vor, die Du auf Deinem Blog oder in Deinem E-Mail-Anhang teilen kannst. Der zweite Schlüssel ist Dein privater Schlüssel. Wenn Dir jemand eine verschlüsselte Nachricht senden will, braucht er Deinen öffentlichen Schlüssel, um die Mail zu chiffrieren und Du nutzt Deinen privaten Schlüssel, um die Nachricht zu dechiffrieren. Der Vorteil dieser asymmetrischen Methode ist, dass nur die öffentlichen Schlüssel ausgetauscht werden und die privaten Schlüssel geschützt bleiben. Für Fremde ist es unmöglich, Eure Nachrichten zu lesen.

Um eine Verschlüsselung erstmalig einzurichten, benötigst Du ungefähr 30 Minuten. Nachdem Du die Software einmal eingerichtet hast, funktioniert sie fast von alleine. Um zu beginnen, besuchst Du als Mac-Nutzer die Seite von *GPG Tools* oder als Windows-Nutzer die Seite von *Gpg4win*. Dort lädst Du Dir die entsprechende Software herunter und befolgst die Anweisungen des Installationsprogramms. Beide Programme bieten einfache Erklärungen und Einsteigertipps auf ihren Webseiten an. Die folgenden Schritte beziehen sich auf die Mac-Variante, *GPG Tools*. Die Schritte für die Windows-Software sind jedoch sehr ähnlich. Zunächst musst Du Dir ein eigenes Schlüsselpaar erstellen. Du wählst also "Neu" aus und füllst das

Feld mit Name, E-Mail und einer neuen Passphrase aus. Ist Deine Passphrase zu einfach, weist Dich das Programm darauf hin. Nach Eingabe der Informationen wirst Du gebeten, die Maus zu bewegen, um Zufallswerte zu erzeugen. Diese werden benötigt, um Deinen Schlüssel zu bilden. Danach ist Dein Schlüsselpaar bereits erstellt.

Anschliessend kannst Du mit dem Mailprogramm von *Apple*, einem öffentlichen Schlüssel und der entsprechenden E-Mail-Adresse verschlüsselte Nachrichten versendet. Die Option zum Verschlüsseln wird Dir in Deinem Mailprogramm angezeigt.
Die Schlüssel Deiner Kontakte speicherst Du einfach in der *GPG Keychain*. Das ist das Programm, mit dem Du auch Deinen eigenen Schlüssel erstellt hast und Deinen öffentlichen Schlüssel exportieren und versenden kannst.
Wenn Du ein anderes E-Mail-Programm verwendest, benötigst Du eventuell noch ein kleines Zusatzprogramm, das sich über eine Suche im Internet aber leicht finden lässt.

Shortfacts

Was ist OpenPGP mit GPG?
Eine einfache Methode zum Verschlüsseln und Entschlüsseln von E-Mails.

Wo bekomme ich GPG:
www.gpgtools.org (MacOS)
www.gpg4win.de (Windows)

Lizenz: Open Source

Zeitaufwand: 30 Minuten

EINE E-MAIL OHNE VERSCHLÜSSELUNG IST WIE EIN BRIEF IN EINEM DURCHSICHTIGEN BRIEFUMSCHLAG.

Unterwegs im Internet

Bekannte Browser wie *Safari*, *Google Chrome* oder der *Internet Explorer* sind Produkte grosser IT-Konzerne. Im deutschsprachigen Raum wird mittlerweile auch der Open-Source-Browser *Firefox* häufig genutzt.

Unabhängig von der Wahl des Browsers, werden Deine Daten wie Bilder, Suchanfragen oder Passwörter häufig unverschlüsselt übertragen. Der Grund dafür ist das "Hypertext Transfer Protocol" kurz HTTP. Es ist die Sprache, mit der Dein Browser und der Server, auf dem die Webseite hinterlegt ist, miteinander sprechen.
So wie Du darauf achtest, dass niemand auf den Bildschirm schaut, während Du Dein Passwort eingibst, solltest Du auch darauf achten, dass niemand entlang der Leitung Deine Daten lesen kann.
Das geht ganz einfach durch die Verwendung von HTTPS, also dem "Hypertext Transfer Protocol Secure", das viele Webseiten unterstützen. Am einfachsten verwendest Du HTTPS, indem Du Dir das Add-on *HTTPS Everywhere* installierst.

Um sicher zu surfen, solltest Du einige weitere Einstellungen vornehmen, die auf den nächsten Seiten erklärt werden.
Wenn Du wirklich anonym surfen möchtest, kannst Du den *Tor Browser* verwenden. Dieser ist allerdings etwas langsamer als andere Browser.

Einstellungen im Browser

Bestimmte Einstellungen solltest Du unabhängig vom verwendeten Browser vornehmen. Damit lassen sich einige Datenlöcher ganz einfach verschliessen. Zwei wichtige Einstellungen betreffen die Cookies.

Cookies sind kleine Dateien, die Webseiten im Browser abspeichern und die Informationen über Dich und Dein Surfverhalten beinhalten. Auf manchen Webseiten finden sich dazu noch Cookies, die von fremden Anbietern hinterlegt werden. Besonders die Cookies von Drittanbietern solltest Du blockieren. Zudem kannst Du einstellen, dass Cookies gelöscht werden, sobald Dein Browser geschlossen wird. Damit verhinderst Du, dass Dein Verhalten im Internet von bestimmten Webseiten verfolgt wird. Beide Optionen bieten alle gängigen Browser an und sind leicht im Menüpunkt "Einstellungen" zu finden.

Eine weitere Einstellung ist die Aktivierung von *Do Not Track*, die ebenfalls von allen Browsern unterstützt wird. Damit teilt Dein Browser der besuchten Webseite mit, dass Du nicht getracked werden möchtest. Allerdings handelt es sich dabei um einen freiwilligen Standard, an den sich die Webseiten nicht halten müssen.

Eine weitere Möglichkeit weniger Informationen an *Google* preiszugeben ist die Verwendung alternativer Suchmaschinen. *DuckDuckGo* (www.duckduckgo.com) ist beispielsweise eine Suchmaschine, die Deine Privatsphäre respektiert.

Zwei Plug-ins, die immer wieder mit Sicherheitsproblemen zu kämpfen haben, sind *Flash* und *Java*. Du kannst zwar beide deaktivieren, es gibt jedoch einige Webseiten, die diese Programme benötigen. Du hast aber die Möglichkeit einzustellen, dass Dein Browser Dich für jede Webseite fragt, ob er *Java* oder *Flash* verwenden soll. Zuletzt solltest Du darauf achten, dass Du Deinen Browser in der neusten Version verwendest, denn viele Updates dienen dem Schliessen von Sicherheitslücken.

uBlock Origin

Bei *uBlock Origin* handelt es sich um einen sogenannten Ad-Blocker. Das Programm ist Open Source und verhindert zuverlässig, dass Du mit Werbung belästigt wirst. Im Gegensatz zum am häufigsten verwendeten Ad-Blocker *AdBlock Plus*, sind die Datenschutzbedingungen bei *uBlock Origin* besser. *AdBlock Plus* ermöglicht es zudem Unternehmen, sich von der Liste der geblockten Werbung freizukaufen.

Shortfacts

Was ist uBlock Origin?
Ein Ad-Blocker, der Dich vor Werbung beim Surfen schützt.

Wo bekomme ich uBlock Origin?
www.github.com/gorhill/uBlock
Oder auf den Add-on Seiten von Chrome, Firefox und Opera

Lizenz: Open Source

Zeitaufwand: 3 Minuten

HTTPS Everywhere

HTTPS Everywhere ist aus einer Zusammenarbeit des *Tor-Projects* und der *Electronic Frontier Foundation (EFF)* entstanden. Es prüft bei jeder Webseite, die Du besuchst, ob diese HTTPS unterstützt. Wenn sie das tut, sorgt *HTTPS Everywhere* dafür, dass Dein Browser eine sichere Verbindung zu dieser Webseite aufbaut. Dabei ist es egal, ob Du die URL selbst eintippst oder einen Link anklickst. Das Programm arbeitet unauffällig im Hintergrund und muss nach seiner Installation nicht mehr beachtet werden.

Shortfacts

Was ist HTTPS Everywhere?
Ein Add-on, das dafür sorgt, dass immer HTTPS anstelle von HTTP verwendet wird, sofern die besuchte Webseite das unterstützt.

Wo bekomme ich HTTPS Everywhere?
www.eff.org/Https-Everywhere

Lizenz: Open Source

Zeitaufwand: 3 Minuten

Privacy Badger

Privacy Badger ist ein von der *Electronic Frontier Foundation* zur Verfügung gestelltes Add-on, das Software blockiert, die Dich über mehrere Webseiten hinweg verfolgt. Damit *Privacy Badger* funktioniert, musst Du nichts weiter tun, als das Programm zu installieren. Angeboten wird das Add-on für alle gängigen Browser.

Shortfacts

Was ist Privacy Badger?
Ein Add-on, das Dich gegen verschiedene Tracker schützt.

Wo bekomme ich Privacy Badger?
www.eff.org/de/privacybadger

Lizenz: Open Source

Zeitaufwand: 3 Minuten

Lieber nicht.

Einige Add-ons sind zwar beliebt, aber nicht unbedingt zu empfehlen.
Zwei Anwendungen die Du nicht verwenden solltest sind *Ghostery* und *Web of Trust (WOT)*.
Ghostery ist eine Art Ad-Blocker, der aber viel Tracking erlaubt und mit Verkäufen von Nutzerdaten Schlagzeilen gemacht hat. Ähnliches gilt für *WOT*. Im Herbst 2016 deckte der Norddeutsche Rundfunk auf, dass Millionen Internetnutzer von ihren Add-ons ausgespäht und ihre Daten an Dritte verkauft wurden.
Es ist also immer wichtig, dass Du Dich über ein Programm informierst, bevor Du es installierst.

Wenn Du testen möchtest, wie gut Dein Browser eingestellt ist, solltest Du Dir das Projekt *Panopticlick* (www.panopticlick.eff.org) von der *EFF* ansehen. Hier bekommst Du nach einem kurzen Test ein Ergebnis und Vorschläge zur Verbesserung.

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

JOHN PERRY BARLOW

Tor Browser

Selbst wenn Du alle genannten Tools installierst, kann Deine Identität beim Surfen immer noch festgestellt werden. Wenn Du Dich unerkannt im Internet bewegen möchtest, solltest Du den *Tor Browser* nutzen.

Wenn Du mit ihm ins Internet gehst, verbindet sich Dein Computer nicht direkt mit dem Server einer Webseite. Stattdessen wird eine zufällige und verschlüsselte Verbindung zu einem Rechner des *Tor Netzwerkes* aufgebaut. Von diesem Rechner aus wird dann eine zweite Verbindung aufgebaut und anschliessend noch eine Dritte. Der dritte Computer greift anschliessend auf den Server der Webadresse zu. Durch die mehrfache Umleitung der Verbindung bist Du zwar anonym, jedoch ein wenig langsamer unterwegs, als gewohnt.
Der *Tor Browser* ist der Eingang ins "Deep Web", das wegen seiner Anonymität oft auch "Dark Web" genannt wird.

Eine etwas schnellere, aber weniger sichere Alternative sind *Virtuelle Private Netzwerke (VPN).* Dein Computer kommuniziert verschlüsselt mit einem Server, der dann auf das Internet zugreift. Die Webseite, auf der Du bist, sieht dann als Absender die Adresse des *VPN* Servers, den mehrere Leute benutzen. Der Betreiber des *VPN* kennt jedoch Deine IP-Adresse. Insofern musst Du diesem Dienst dann vertrauen.

Shortfacts

Was ist der Tor Browser?
Ein Browser, um anonym im Internet zu surfen.

Wo bekomme ich den Tor Browser?
www.torproject.org

Lizenz: Open Source

Zeitaufwand: 5 Minuten

Die Grossen des Internets

Um die Grossen des Internets wie *Google*, *Apple*, *Facebook* und *Microsoft* kommst Du kaum herum.
Teil des Kerngeschäfts dieser Konzerne ist der Verkauf der Daten ihrer Nutzer. Genau wie bei staatlicher Überwachung, werden Deine Daten von Dritten gelesen und ausgewertet. Auf dieser Basis erstellen die Unternehmen Nutzerprofile und versuchen möglichst massgeschneiderte Werbung zu platzieren. Auch Strafverfolgungsbehörden haben auf diese Daten Zugriff.

Doch nur weil Du *Google* oder *Facebook* nutzt, verlierst Du nicht Dein Recht auf Privatsphäre. Du kannst zumindest einstellen, wer welche Informationen von Dir sehen kann. Achte darauf, welche Daten Du im Internet preisgibst. Auch Dein Smartphone ist durch die Bündelung vieler Funktionen eine grosse Datensammelmaschine. Vermutlich begleitet Dich Dein Handy auf Schritt und Tritt und sammelt eine Menge Informationen über Dich. Es erzählt *Google* und *Facebook*, wo Du gestern Abend warst, wie Du nach Hause gekommen bist, welche Musik Du hörst, mit welchen Freunden Du am liebsten Selfies machst und wie gut Dein Schlaf ist.
Darüber hinaus reichen schon vier zufällig ausgewählte Apps Deines Smartphones aus, um es mit 95 Prozent Wahrscheinlichkeit zu identifizieren. Doch auch hier kannst Du einige Einstellungen zum Schutz Deiner Freiheit vornehmen.

Daten bei Google und Facebook

In den *Anzeigeneinstellungen* Deines *Google-Profils* findest Du ein grobes Nutzerprofil mit Alter, Sprachen, Geschlecht und Interessen. Du kannst einstellen, ob Du personalisierte oder zufällige Werbung bekommen möchtest. Hier wird Transparenz suggeriert, allerdings werden durch Änderungen in den Einstellungen weder weniger Daten gespeichert, noch bekommst Du weniger Werbung.
Im *Standortverlauf* speichert *Google* alle Ortsdaten, die es von Deinen Geräten erhält. Es wird eine persönliche Karte mit Orten erstellt, die Du häufig besuchst. Diese Funktion lässt sich abstellen, sodass keine neuen Standortdaten mehr gesammelt werden.
Im Bereich *Aktivitätsanzeige* speichert *Google* alle Deine Suchanfragen, welche Links Du angeklickt und welche Bilder oder Videos Du Dir angesehen hast. Du kannst Deinen Suchverlauf löschen und die Speicherung deaktivieren. Darauf zu vertrauen, dass *Google* nach dem Deaktivieren der verschiedenen Funktionen keine Daten mehr über Dich speichert, wäre aber fahrlässig.

Google

Anzeigeneinstellungen:
www.google.com/settings/ads

Standortverlauf:
www.google.com/maps/timeline

Aktivitätsanzeige:
myactivity.google.com

Zeitaufwand: 5 Minuten

Auch *Facebook* ermöglicht Dir einen Teil der gespeicherten Daten abzurufen. Dazu gehst Du auf "Einstellungen" und dort auf den Reiter "Allgemein". Auf dieser Seite findet sich ganz unten ein Button "Lade eine Kopie Deiner Facebook-Daten herunter". Wenn Du den Anweisungen folgst, bekommst Du eine E-Mail mit einem Downloadlink Deiner Daten. Dort findest Du unter anderem alle Deine Gespräche, alle Schlagworte, zu denen Du Werbung bekommst, Deine Bilder und Posts, sowie die IP-Adressen von denen aus Du Dich eingeloggt hast. Allerdings handelt es sich dabei nur um circa 40 Prozent

der Daten, die *Facebook* über Dich speichert. Du kannst auch eine schriftliche Anfrage zur Herausgabe aller Deiner Daten stellen. Ausführliche Anleitungen dafür finden sich im Internet.

Facebook

Datensatz herunterladen:
Klicke auf
"Einstellungen"
"Allgemein"
"Lade eine Kopie deiner Facebook-Daten herunter"

Zeitaufwand: 5 Minuten

Anleitung für eine komplette Anfrage:
www.europe-v-facebook.org

Smartphone

Wenn Du beim Surfen oder bei der Nutzung von Apps keine personalisierte Werbung bekommen möchtest, kannst Du die Funktion *Kein Ad-Tracking* aktivieren. Diese ist sowohl für *iOS* als auch für *Android* verfügbar. Weniger Werbung bekommst Du trotzdem nicht angezeigt.
Auch der Menüpunkt "Ortungsdienste" (*iOS*) bietet einige Möglichkeiten. Dort kannst Du einstellen, welche Apps auf Deinen Standort zugreifen dürfen. Die Funktionen *Ortsabhängige Apple Ads*, *Häufige Orte* sowie mehrere Optionen zur *Produktverbesserung* kannst Du ausschalten. Diese erfassen Daten, bringen Dir aber für die Nutzung keinerlei Vorteile. Bei *Android* finden sich ähnliche Einstellungsmöglichkeiten im Menüpunkt "Standort".
Ausserdem kannst Du auch auf dem Smartphone die Option *Do Not Track* für Deinen Browser einstellen und einen Ad-Blocker installieren.

Die gute Nachricht ist:
Wir sind nicht paranoid.

Die schlechte Nachricht ist:
Wir werden alle überwacht.
Jederzeit und überall.

MARKUS BECKEDAHL

Wer macht denn sowas?

Für die Digitale Selbstverteidigung ist es wichtig, dass Du Dich informierst und diejenigen unterstützt, die sich für ein offenes Internet engagieren.

Eine sehr gute Informationsquelle ist das Blog *netzpolitik.org*. Die Bandbreite der Inhalte reicht vom tagesaktuellen netzpolitischen Geschehen, über Live-Blogs aus dem NSA-Untersuchungsausschuss bis hin zu Hintergrundinformationen und Expertenwissen. Da *netzpolitik.org* sich ausschliesslich durch die Spenden seiner Leser finanziert, kann die Redaktion unabhängigen Journalismus mit Haltung betreiben. Wenn Du ihre Arbeit unterstützen möchtest, geht das mit einer Spende.

Schon kleine Beträge können viel bewirken. Weitere Anlaufpunkte in Deutschland sind die *Digitale Gesellschaft* und der *Chaos Computer Club*.

Die international wohl bekannteste Organisation, die sich für ein freies Internet einsetzt, ist die *Electronic Frontier Foundation (EFF)*. Seit 1990 setzt sie sich für Grundrechte im digitalen Zeitalter ein. Auf ihrer Webseite findest Du umfangreiche Informationen über alles, was mit dem Internet zu tun hat. Es gibt auch einen eigenen Bereich für Schritte zur Digitalen Selbstverteidigung. Eine Mitgliedschaft bei der *EFF* kann man gegen eine kleine Spende abschliessen.

Auch bei Wahlen solltest Du auch auf

netzpolitische Themen achten. Es gibt Günther Oettinger und es gibt Politiker, die sich für das Internet als Ort der Freiheit und Gleichheit einsetzen.

Shortfacts

Electronic Frontier Foundation
www.eff.org

Tipps zur Digitalen Selbstverteidigung von der EFF
ssd.eff.org

Netzpolitik.org
www.netzpolitik.org

Chaos Computer Club
www.ccc.de

Digitale Gesellschaft
www.digitalegesellschaft.de

PROTECT YOUR DIGITAL IDENTITY!

Impressum

Das Heft ist im Rahmen des Moduls “Meet Me At The Market” im Herbstsemester 2016 an der Zürcher Hochschule der Künste im Bachelor “Style & Design” entstanden. Ich bedanke mich bei allen, die mich bei der Gestaltung und Umsetzung des Produkts unterstützt haben. Besonderer Dank gilt *soomz.io*, die die zum Set gehörenden Kameraabdeckungen bereitgestellt haben, *netzpolitik.org* für die inhaltliche Unterstützung, *Alexander Katzmann* für das umfassende Lektorat und *Salomon Hörler* für die Layoutberatung.

Herausgeber:
Clemens Kommerell

Gesetzt aus:
Monsterrat, Courier Code und Glacial Indifference

Kontakt:
c.kommerell@udk-berlin.de

1. Auflage

Das aus Gründen der besseren Lesbarkeit vornehmlich verwendete generische Maskulin schliesst gleichermassen weibliche und männliche Personen ein, es sei denn das Geschlecht wird explizit hervorgehoben.