EINE KURZE ANLEITUNG ZUR DIGITALEN SELBSTVERTEIDIGUNG

WOZ
DIE WOCHENZEITUNG

PROWOZ

Dieser Ratgeber wurde ermöglicht durch den Recherchierfonds des Fördervereins ProWOZ. Der Fonds unterstützt Recherchen und Reportagen, die die finanziellen Möglichkeiten der WOZ übersteigen. Er speist sich aus Spenden der WOZ-LeserInnen.

Förderverein ProWOZ, Postfach, 8031 Zürich, PC 80-22251-0

Wenn Sie weitere Exemplare dieses Ratgebers wünschen, melden Sie sich bitte bei der WOZ unter Tel. 044 448 14 14 oder bei woz@woz.ch. Sie finden ihn auch auf www.woz.ch/verteidigung

IMPRESSUM

Erstmals erschienen als Beilage der Wochenzeitung WOZ Nr. 35 vom 31. August 2017; leicht überarbeitet und ergänzt im Oktober 2018.

Redaktion: Jan Jirát, Donat Kaufmann, Christoph Laszlo, Hernani Marques, Arian Sanusi ***Abschluss:*** Armin Büttner, Dinu Gautier ***Gestaltung:*** Franziska Meyer
Korrektorat: WOZ-Korrektorat ***Verlag:*** Genossenschaft infolink
2. Auflage: 3500 ***Online***: Georg Bauer
Adresse: WOZ Die Wochenzeitung, Hardturmstrasse 66, 8031 Zürich. Telefon 044 448 14 14, Fax 044 448 14 15, woz@woz.ch, www.woz.ch

INHALTSVERZEICHNIS

MITHERAUSGEBER

Digitale Gesellschaft
Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich seit 2011 für Grund-, Menschen-, BürgerInnen- sowie Konsument-Innenrechte im Internet einsetzt. Das Ziel sind der Erhalt und die Förderung einer offenen und nachhaltigen Gesellschaft.
www.digitale-gesellschaft.ch

Chaos Computer Club Schweiz
Der Chaos Computer Club Schweiz (CCC-CH) setzt sich für das Recht auf Privatsphäre und Informationsfreiheit ein. Regionale Hackerspaces sind für alle Interessierten offen.
www.ccc-ch.ch

Konsumentenschutz
Der Konsumentenschutz bietet unabhängige Information und Beratung. Er vertritt die Interessen der KonsumentInnen gegenüber Anbietern, Gesetzgeber und Behörden. Im Zug der Digitalisierung kämpft er für die Wahrung der Privatsphäre und mehr Schutz vor Cyberkriminalität.
www.konsumentenschutz.ch

EDITORIAL

«Mit der Seilbahn!» lautete eine häufige Antwort, als der Bundesrat in der Volkszählung von 1980 wissen wollte, wie die BürgerInnen den Weg zur Arbeit zurücklegten. Landauf, landab sabotierten Menschen die Umfrage mit Falschangaben. Sie fürchteten um ihre Privatsphäre.

Hätte man sie mit den heutigen Verhältnissen konfrontieren können, wären sie wahrscheinlich in Schockstarre verfallen.

Mithilfe der im ***Nachrichtendienstgesetz (NDG)*** verankerten ***Kabelaufklärung*** kann der Schweizer Geheimdienst sämtliche Telekommunikationsverbindungen ins Ausland nach definierten Stichwörtern durchsuchen. Da der grösste Teil unserer alltäglichen Kommunikation über Server ausserhalb der Schweiz abgewickelt wird, entgeht dem Geheimdienst praktisch nichts mehr. Darüber hinaus ermöglicht es die ***Vorratsdatenspeicherung,*** das Kommunikationsverhalten und das Kontaktnetz sämtlicher BürgerInnen für sechs Monate zu speichern: Wer hat wann, wo, wie und mit wem kommuniziert? Gegen die Vorratsdatenspei-

cherung hat die Digitale Gesellschaft Klage erhoben, die beim Europäischen Gerichtshof für Menschenrechte hängig ist. Zudem hat sie eine Beschwerde gegen die Kabelaufklärung ans Bundesverwaltungsgericht weitergezogen. Der Entscheid steht noch aus.

Staatliche Überwachung in diesem Ausmass wäre undenkbar ohne die Infrastruktur der US-amerikanischen Techkonzerne. Die Geräte von Apple, die Programme von Microsoft, die Dienste von Google sind so konstruiert, dass Daten im grossen Stil gesammelt, analysiert und verkauft werden können. Die Datenabsauger in dieser gigantischen staatlich-privatwirtschaftlichen Überwachungsmaschinerie sind uns bestens bekannt: Sie heissen Whatsapp, Gmail, Facebook, Google Docs … Tagtäglich füttern wir sie mit Informationen.

Dabei gibt es Alternativen, die uns vor Eingriffen in unsere Privatsphäre besser schützen als die datenhungrigen Konzerne. In diesem Ratgeber stellen wir sie vor.

Die Alternativen versprechen Anonymität, geben weniger oder keine Daten an Dritte weiter, verschlüsseln Nachrichten, legen den Quellcode offen und schaffen damit Transparenz über die Funktionsweise des Programms. Sie betreiben ihre Server in Staaten mit strengen Datenschutzgesetzen oder sichern Informationen dezentral.

Absolute Datensicherheit können auch sie nicht gewährleisten. Aber ihre Nutzung verhindert, dass immer mehr Informationen bei immer weniger Instanzen zusammenfliessen. Und sie helfen uns, die Hoheit über unsere Daten zurückzugewinnen.

WOZ, DIGITALE GESELLSCHAFT, CCC-CH UND STIFTUNG FÜR KONSUMENTENSCHUTZ

P.S: Wichtige und weniger alltägliche Begriffe erläutern wir im Glossar (ab Seite 41). Im Text sind sie ***unterstrichen.***

01_GRUNDLAGEN

DATENSPARSAMKEIT

Mit dem Internet verbunden zu sein, bedeutet, Spuren zu hinterlassen. Da wir nur schwer überprüfen können, ob jemand (und wer) im Hintergrund mitliest, lautet das wirksamste Datenschutzprinzip noch immer: Weniger ist mehr. Daten, die nicht ins Netz gelangen, brauchen erst gar nicht geschützt zu werden. Personenbezogene Angaben wie Name, Adresse, Geburtstag, Telefon-, Konto- oder Versicherungsnummern, aber auch Fotos und Videos sind für Datenhändler besonders lukrativ und sollten ausschliesslich bei vertrauenswürdigen Diensten hinterlegt werden. Ist ein Angebot «gratis», ist davon auszugehen, dass sich der Dienst mitunter durch den Verkauf von Daten finanziert. Das gilt in besonderem Mass für die sozialen Medien wie Facebook, Instagram oder Twitter.

Zudem vergessen wir oft, dass wir Entscheidungsmacht haben: Nicht alles, was übers Internet erledigt werden kann, muss auch übers Internet erledigt werden. Wir müssen unsere Bücher nicht bei Amazon, unsere Schuhe nicht bei Zalando kaufen. Deren Produkte sind auch deshalb so günstig, weil wir mit unseren Daten ein grosszügiges Trinkgeld bezahlen.

Wichtig: Wenn man sich via Smartphone mit dem Internet verbindet, geschieht das in der Regel über ***Apps***. Lädt man sich eine neue App auf das Smartphone, fragt sie bei der Installation nach Zugriffen. Auf die Kontakte, den Ortungsdienst, auf die Kamera, das Mikrofon, auf die Bildergalerie. Grundsätzlich sollten die Zugriffe auf das Minimum reduziert und wann immer möglich deaktiviert werden.

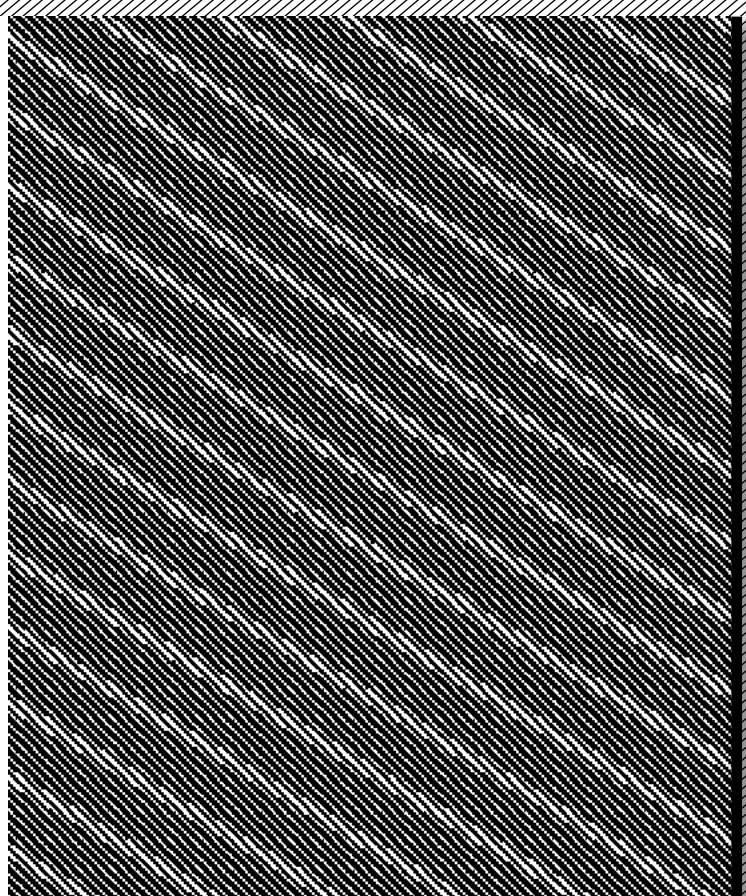
MÄCHTIGE TECHKONZERNE

Fünf US-Giganten dominieren das Internet: Google (Alphabet), Amazon, Facebook, Apple und Microsoft. Sie halten monopolartige Stellungen in etlichen Geschäftsbereichen wie den sozialen Netzwerken (Facebook) oder den Suchanfragen (Google). Gemeinsam steuern und überwachen sie den Informationsfluss im Internet. Sie unterhalten Infrastruktur wie Serverfarmen und Glasfasernetze, sie bauen die Geräte, mit denen wir kommunizieren, sie sind im Besitz der Programme, die wir nutzen. Dabei sammeln sie praktisch uneingeschränkt Daten über uns. Diese Daten verknüpfen sie zu komplexen Persönlichkeitsprofilen und verkaufen sie an Kunden aus Wirtschaft und Politik. Darüber hinaus werden diese Informationen von Geheimdiensten abgeschöpft, wie der Whistleblower Edward Snowden belegt

hat. Immer wieder kommt es auch zu Fällen von wirtschaftlichem Missbrauch. Im Juni 2017 wurde Google von der EU zu einer Strafe von 2,4 Milliarden Euro verurteilt, weil der Konzern konsequent Suchresultate manipuliert hatte. So nützlich die Dienste der Giganten auch sind: Sie haben eine Macht entwickelt, die sowohl wirtschaftlich als auch demokratisch bedenklich ist. Um ihre Dominanz nicht weiter zu stärken, sollten sie wo immer möglich umgangen werden.

PASSWÖRTER

Passwörter sind wie Hausschlüssel. Wer sie hat, dem öffnen sich die Türen zu unseren Daten. Für den Schutz der Privatsphäre sind sie zentral. Jedes Gerät, jede Festplatte, jeder Account, jedes Netzwerk sollte mit je einem eigenen Passwort gesichert werden. Ein hinreichend sicheres Passwort ist mindestens fünf zufällige Wörter oder zwölf Zeichen lang, beinhaltet Klein- und Grossbuchstaben, Zahlen und Sonderzeichen und lässt sich nicht herleiten aus personenbezogenen Angaben wie Name, Geburtstag oder Wohnort. Profile auf sozialen Netzwerken sind für BetrügerInnen dankbare Quellen, um an Pass-



worthinweise zu gelangen (Name des Haustiers, Zitat der Lieblingsband). Auf keinen Fall sollten Standardkombinationen wie «12345», «admin» oder der Name des Netzwerks gewählt werden.

Apropos Hausschlüssel: Immer wieder kommt es zu Wohnungseinbrüchen, weil DiebInnen über Facebook in Erfahrung bringen, dass die BewohnerInnen gerade Ferien im Ausland machen.

BETRIEBSSYSTEME

Auf den allermeisten Geräten ist eines der fünf folgenden Betriebssysteme installiert: Android (Google) oder iOS (Apple) bei mobilen Geräten wie Smartphones oder Tablets; Windows (Microsoft), MacOS (Apple) oder ***Linux*** (unabhängig) bei PCs. Grundsätzlich gilt: Kein Betriebssystem garantiert vollständige Sicherheit.

Die Sicherheitsupdates der Hersteller helfen, Lücken zu schliessen. Sie halten Betriebssysteme auf dem aktuellsten Stand und sollten jeweils schnellstmöglich installiert werden. Wie verhängnisvoll veraltete Betriebssysteme sein können, zeigte die Cyberattacke Wannacry im Mai 2017. Damals drangen Kriminelle durch «alte» Sicherheitslücken im Windows-Betriebssystem in Tausende von Computern ein und erpressten Lösegeld.

Während Apple regelmässig Sicherheitsupdates für seine Betriebssysteme liefert und die NutzerInnen zur Aktualisierung auffordert, sind die Hersteller von Android-Geräten nachlässiger.

LINUX ANDROID WINDOWS

iOS MacOS

BACK-UP

Festplatten können kaputtgehen, Handys oder Computer gestohlen werden. Daher ist es unverzichtbar, eine Kopie (Back-up) der wichtigsten Daten zu besitzen. Am besten legt man sie auf einer persönlichen externen Festplatte ab, die nicht mit dem Internet verbunden ist. Onlinespeicher bergen das grössere Risiko, Ziel von Kriminellen und staatlichen Akteuren zu werden. Da aber auch die persönliche Festplatte entwendet (Einbruch) oder zerstört (Feuer, Wasser) werden kann, sollte sie an einem sicheren Ort aufbewahrt werden.

02_DIE ALTERNATIVEN

WEBBROWSER

Der Webbrowser ist das Fenster zum Internet. Er bestimmt, was wir sehen – und wie viel von uns zu sehen ist. Vom Browser und seinen Einstellungen hängt ab, ob unser Surfverhalten systematisch erfasst werden kann und welche Spuren wir auf den einzelnen Websites hinterlassen. Da auch die Browserbetreiber Daten sammeln können, lohnt sich ein Blick auf ihr Geschäftsmodell.

Standardmässig ist auf jedem Gerät der Browser des Herstellers vorinstalliert. Bei Windows der Internet Explorer und sein Nachfolger Edge, bei Apple-Geräten Safari, bei Android (Google) Chrome. Alle diese Browser arbeiten im Dienst ihrer Hersteller. Da der ***Quellcode*** nicht vollständig offen, die Bauweise des Programms also nicht geklärt ist, lässt sich nicht überprüfen, welche Informationen im Hintergrund gesammelt werden.

MOZILLA FIREFOX

Mozilla Firefox gilt als die Alternative zu Chrome und Internet Explorer. Der Browser der gemeinnützigen Mozilla Foundation hat sich dem «sicheren Surfen» verschrieben. Er ist schnell und vielseitig. Der Quellcode ist offen und wird von einer aktiven Community ständig weiterentwickelt. Zudem können zahllose Erweiterungen (Add-ons) installiert werden, um den Datenschutz zu erhöhen.

Zwei Firefox-Erweiterungen können besonders empfohlen werden:

HTTPS Everywhere, entwickelt von der US-Bürgerrechtsorganisation Electronic Frontier Foundation (EFF), stellt – wenn immer möglich – eine verschlüsselte Verbindung zwischen Gerät und Website her.

Die Erweiterung *uBlock Origin* blockiert Werbeanzeigen und erschwert damit das systematische Erfassen von Informationen über unser Surfverhalten. Werbeblocker können auch vor Schadsoftware schützen.

www.mozilla.org

BRAVE

Brave wurde 2016 lanciert. Der Browser basiert auf Chromium, der Open-Source-Variante von Google Chrome. Brave hat sich ganz dem Datenschutz verschrieben. Im Unterschied zu Firefox sind bei diesem Browser Erweiterungen wie *HTTPS Everywhere* bereits vorinstalliert.

Auch Werbeblocker sind standardmässig aktiviert. Websites werden dadurch schneller aufgerufen, aber unter Umständen nicht vollständig angezeigt.

Brave bietet zwar auch Werbeflächen an, verspricht jedoch, keine Daten zu erheben. Stattdessen können NutzerInnen über ein integriertes Zahlungssystem Websites mit Mikrobeträgen direkt unterstützen.

www.brave.com

TOR

Tor ist der mit Abstand sicherste, wenn auch langsamste Browser. Da die Verbindung zwischen dem Gerät der NutzerInnen und der aufgerufenen Website über drei zufällige Knoten des Tor-Netzwerks hergestellt wird, lässt sich kaum mehr zurückverfolgen, wer auf die Website zugreift.

Der Tor-Browser wird auch genutzt, um versteckte Websites (Darknet) aufzurufen oder um Internetsperren zu umgehen, wie es sie etwa im Iran, in der Türkei oder in der Schweiz gibt.

www.torproject.org

VPN

Eine weitere Möglichkeit, relativ sicher im Internet zu surfen, ist der Zugang über ein Virtual Private Network (VPN). Die installierte VPN-Software stellt eine verschlüsselte Verbindung zum Server des VPN-Anbieters her. Von dort aus wird die gewünschte Website aufgerufen – und nicht wie normalerweise direkt über die eigene ***IP-Adresse***, mit der das benutzte Gerät im Internet identifiziert wird.

Besonders empfehlenswert ist ein VPN bei der Nutzung von offenen WLAN-Netzen etwa in Cafés oder Bahnhöfen. In solchen offenen Netzen tummeln sich möglicherweise Akteure, die Daten absaugen: Behörden, Datenhändler oder Kriminelle.

Gerade in Ländern wie Russland, China, dem Iran oder der Türkei, wo Teile des Internets gesperrt sind, können sich NutzerInnen über VPN im Internet gesperrte Informationen beschaffen.

Viele Firmen und Hochschulen bieten einen eigenen VPN-Service an. Zudem gibt es eine Vielzahl unabhängiger Anbieter, die jedoch vorgängig auf ihre Verlässlichkeit geprüft werden sollten.

SUCHMASCHINEN

Wer im Internet nachschaut, googelt. Öffnungszeiten, Rezepte, Übersetzungen, Musik, Wegbeschreibungen, Krankheiten … die Suchmaschine findet alles. Im Internet etwas suchen heisst - seit 2004 auch nach Duden - «googeln». Der Konzern aus dem Silicon Valley hat in Europa einen Marktanteil von über neunzig Prozent. Die geheimen ***Algorithmen*** von Google bestimmen, was wir im Netz zu Gesicht bekommen und was nicht.

Die enorme Menge an gesammelten Daten nutzt der Konzern nicht nur, um Suchresultate zu liefern. Das Suchverhalten wird zusammen mit Daten anderer Google-Dienste wie Youtube, Gmail oder Google Docs zusammengeführt und ausgewertet. Die Profile bilden die Grundlage für personalisierte Werbung. Damit erzielte der Konzern allein im Jahr 2017 mehr als hundert Milliarden US-Dollar Umsatz. Die Profile sind auch für staatliche und private Geheimdienste zugänglich und relevant.

Es lohnt sich, seine Fragen an vertrauenswürdigere Dienste zu richten. Denn wer unsere Fragen kennt, der kennt uns.

STARTPAGE

Die Suchmaschine Startpage greift zwar auf den Suchindex von Google zurück, liefert dem Konzern aber weder die Suchdaten der NutzerInnen, noch speichert sie die Suchabfragen.

Die niederländische Firma, die Startpage betreibt, finanziert den Dienst ebenfalls über Werbung, diese ist jedoch nicht personalisiert.

www.startpage.com

DUCK DUCK GO

Duck Duck Go ist eine eigenständige US-amerikanische Suchmaschine, die das Suchverhalten der NutzerInnen nicht speichert. Finanziert wird Duck Duck Go über Spenden und nichtpersonalisierte Werbung.

www.duckduckgo.com

MESSENGER

Für unsere alltägliche Kommunikation nutzen wir heute häufig Messenger. Der beliebteste wie auch zweifelhafteste Nachrichtenübermittler ist Whatsapp. Seit 2014 gehört er zu Facebook. Mit dem Kauf von Whatsapp hat sich das Unternehmen von Mark Zuckerberg Zugang zu Millionen von Adressbüchern (Telefonnummern, E-Mail-Adressen) verschafft und diese ausgewertet - obwohl das Unternehmen anfangs das Gegenteil behauptet hatte.

Zwar sind Nachrichten zwischen Whatsapp-NutzerInnen nach Angaben des Unternehmens durch eine ***Ende-zu-Ende-Verschlüsselung*** gesichert, doch das lässt sich nicht unabhängig überprüfen.

Dass Whatsapp hierzulande weitgehend konkurrenzlos ist, liegt daran, dass sich viele NutzerInnen von alternativen Diensten abwenden, wenn sie dort keine FreundInnen antreffen. Umso wichtiger ist es, im Freundeskreis Überzeugungsarbeit zu leisten, auf andere Messenger zu setzen.

Die Digitale Gesellschaft veröffentlicht jährlich einen Messenger-Test:
www.digitale-gesellschaft.ch/messenger

THREEMA

Aussehen und Handhabung von Threema sind stark an Whatsapp angelehnt. Der Schweizer Messenger kann aber ohne Angabe der eigenen Telefonnummer verwendet werden. Zentral gespeichert wird nur eine zufällig erzeugte ID, nicht aber persönliche Daten wie Telefonnummer, Adresse, Profilbild oder TeilnehmerInnen von Gruppen. Alle Nachrichten sind durch eine Ende-zu-Ende-Verschlüsselung gesichert. Der Quellcode ist zwar nicht offen, doch wurde er von einer unabhängigen Stelle geprüft.

Die Softwareentwicklung und der Betrieb der Server in der Schweiz wird durch die NutzerInnen (einmalige Gebühr) finanziert.

www.threema.ch

iOS

SIGNAL

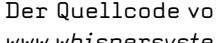
Dieser Messenger von Open Whisper Systems ist eine weitverbreitete Gratis-App, finanziert von einer gemeinnützigen Stiftung in den USA und empfohlen von Edward Snowden.

Signal umfasst alle wichtigen Messenger-Funktionen wie Gruppenchats und (Video-)Telefonie, wobei alle Nachrichten und Gespräche

verschlüsselt werden. So lässt sich der Messenger auch als sichere Alternative zu Skype nutzen. In Kombination mit dem Chromium-Browser kann Signal auch auf PCs verwendet werden.

Der Quellcode von Signal ist offen.

www.whispersystems.org



SOZIALE NETZWERKE

Mehrere Stunden verbringen wir täglich im Internet, sehr viel Zeit davon auf sozialen Netzwerken wie Twitter, Instagram, Snapchat, Linkedin - und natürlich Facebook: Mehr als zwei Milliarden aktive NutzerInnen zählt die Plattform mittlerweile. Ein Viertel der Menschheit teilt persönlichste Details mit Facebook - eine unvorstellbare Konzentration von Macht.

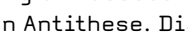
Der Einfluss von Facebook auf das gesellschaftliche Kommunikationsverhalten und die Informationsbeschaffung ist enorm. Auf der Plattform hat sich quasi eine eigene Öffentlichkeit gebildet. Was dort erlaubt ist und was nicht, bestimmen die BetreiberInnen weitgehend selbst, respektive deren geheime Algorithmen. Einer demokratischen Kontrolle unterstehen sie nicht. Zudem sind die Algorithmen so programmiert, dass wir auf Facebook kaum noch mit Meinungen konfrontiert werden, die nicht unserer eigenen entsprechen. Dies kann zu einem sehr verzerrten Realitätsbild führen. Man spricht in diesem Zusammenhang oft von Filterblasen.

Die Nutzung alternativer sozialer Netzwerke hilft, diese Blasen zum Platzen zu bringen. Leider haben auch sie damit zu kämpfen, dass sich viele NutzerInnen abwenden, weil sie wenig FreundInnen antreffen.

DIASPORA

In seiner Funktion ist das 2010 lancierte, dezentral aufgebaute Netzwerk eine Anlehnung an Facebook. Als Idee jedoch ist es dessen Antithese. Diaspora basiert auf ***freier Software.*** Verwaltet und weiterentwickelt wird die Plattform von der Community.

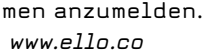
www.diasporafoundation.org



ELLO

Die werbefreie Plattform hat sich vor allem in der Kunst-, Foto- und Modeszene etabliert. Sie garantiert, keine Daten von NutzerInnen an Dritte weiterzugeben. Zudem zwingt Ello seine NutzerInnen nicht, sich mit dem richtigen Namen anzumelden.

www.ello.co



GNU Social

Eine Alternative zu Twitter ist GNU Social. Der Mikrobloggingdienst ist Teil des sogenannten GNU-Projekts, das massgeblich von der Freie-Software-Bewegung getragen wird.

www.gnu.io/social

MASTODON mastodon

Mastodon ist ein aufstrebender Kurznachrichtendienst, der mit GNU Social kompatibel ist.

www.joinmastodon.org

E-MAILS

Jeden Tag werden Milliarden von E-Mails verschickt. Ohne E-Mail-Adresse ist es praktisch unmöglich, sich im Internet zu bewegen. Noch. Bei vielen Diensten oder Anwendungen läuft die Registrierung nämlich zunehmend per Facebook- oder Google-Account. Das ist bequem, aber schlecht für die Datensicherheit. Dann doch lieber eine E-Mail-Adresse nutzen. Aber natürlich nicht irgendeine. Die meisten Schweizer NutzerInnen setzen auf Dienste wie Gmail (Google, USA), GMX (D) oder Bluewin (Swisscom, CH).

Alle diese Anbieter sind eng verbandelt mit der Werbeindustrie. Ihre E-Mail-Dienste betreiben sie in erster Linie aus kommerziellem Interesse. Der Schutz unserer Privatsphäre bleibt hingegen zweitrangig und ist entsprechend schwach. Posteingänge werden nach Schlagwörtern durchsucht, um Werbedaten zu sammeln; E-Mails werden nicht automatisch verschlüsselt.

Gerade diese Funktion ist für den Datenschutz aber unerlässlich. Niemand würde Briefe ohne Couvert versenden. Genauso wenig sollten elektronische Nachrichten unverschlüsselt verschickt werden.

Es gibt eine Reihe von E-Mail-Diensten, die dem Schutz der Privatsphäre hohe

Priorität geben und auf eine verschlüsselte E-Mail-Kommunikation setzen. Automatisch klappt die verschlüsselte Übertragung von E-Mails allerdings nur zwischen NutzerInnen des gleichen Anbieters.

KOLAB NOW (CH):

www.kolabnow.com

TUTANOTA (D):

www.tutanota.com

POSTEO (D):

www.posteo.de

IMMERDA

Der Dienst des Kollektivs Immerda (CH) richtet sich in erster Linie an AktivistInnen. Wer ihn nutzen will, braucht eine persönliche Einladung von Leuten, die bereits bei Immerda sind.

www.immerda.ch

E-MAIL-PROGRAMME

In den meisten Fällen verwalten wir unsere E-Mails im Webmail, also direkt auf der Website des Anbieters - etwa auf gmail.com oder gmx.ch.

Bei der Verwendung von Webmail sind die Daten auf dem Server des Anbieters gespeichert, nicht aber lokal auf dem benutzten Gerät.

E-Mails sollten aber immer auch auf dem eigenen Rechner archiviert werden - als Backup. Es kann nämlich sein, dass ein Dienst Ziel einer Cyberattacke wird oder Konkurs geht, was zum Verlust sämtlicher Daten führen kann.

Die Programme für die lokale E-Mail-Verwaltung greifen auf den Webserver zu und laden automatisch die gesamten Inhalte auf den eigenen Rechner. Apple Mail und Microsoft Office Outlook sind die bekanntesten, aber nicht die einzigen Mailprogramme.

THUNDERBIRD

Thunderbird ist neben Firefox das bekannteste Produkt der Mozilla Foundation. Das Programm ermöglicht die lokale Archivierung von E-Mails. Wie für den Browser Firefox gibt es für Thunderbird Add-ons, um die Privatsphäre

besser zu schützen. Ein Beispiel dafür ist *Enigmail*. Es erlaubt die verschlüsselte Kommunikation zwischen E-Mail-Adressen **aller** Anbieter. Voraussetzung ist jedoch, dass sowohl Absender wie auch Empfängerinnen eine Verschlüsselungssoftware benutzen.

www.mozilla.org/de/thunderbird

KALENDER / ADRESSBUCH

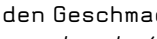
Kalender und Adressbuch sind zwei unverzichtbare Anwendungen - im privaten wie im beruflichen Alltag. Beide speichern jede Menge persönliche und sensible Informationen, die Rückschlüsse auf unsere Arbeit, unseren Freundeskreis, unsere Interessen, im Extremfall sogar auf unsere Krankheitsgeschichte zulassen.

Die Standardprogramme für die Verwaltung dieser Daten kommen von Apple und Google (iCal und Google Calender). Diese bieten einen durchaus sinnvollen Service: Sie erlauben die Synchronisation von Terminen und Kontakten zwischen Laptop und Handy. Trotzdem stellt sich die Frage, ob man seinen Arzttermin Google oder Apple mitteilen will.

Die beiden E-Mail-Anbieter Posteo und Kolab Now (siehe Kapitel E-Mails) bieten auch gute und sichere Kontaktverwaltungen und Kalenderfunktionen an. Beide Dienste sind allerdings kostenpflichtig.

Und hey! Noch immer gibt es Papeterien. Noch immer gibt es da physische Agenden für jeden Geschmack.

posteo.de // kolabnow.com



ZUSAMMENARBEITEN IM NETZ

Viele Dokumente und Publikationen entstehen als Gemeinschaftswerk (wie dieser Ratgeber) über Dienste, die ein gleichzeitiges Bearbeiten eines Dokuments durch mehrere Personen ermöglichen. Mit Google Docs kommt der bekannteste solche Dienst einmal mehr von Google.

Aber auch in diesem Bereich gibt es alternative kollaborative Tools. In der Regel können NutzerInnen ganz simpel per Link eingeladen werden, was den Vorteil hat, dass diese keinen Account brauchen. Die meisten

Tools ermöglichen es aber auch, dass man einzelnen NutzerInnen gewisse Rechte geben oder verwehren kann. Das setzt dann aber je einen eigenen Account voraus.

ETHERPAD

Die Software Etherpad ermöglicht es, Textdokumente zu erstellen, die via Webbrowser gemeinsam bearbeitet werden können. Wie bei Google Docs lassen sich die Dokumente über einen Link (nach Wunsch passwortgeschützt) erreichen. Ein eigener Account ist nicht nötig.

Auf *piratenpad.de* oder *pads.ccc-ch.ch* kann man direkt loslegen.

ETHERCALC

Das Tabellenkalkulationsprogramm Ethercalc ist in seiner Handhabung angelehnt an das Vorbild Excel. Es verfügt allerdings nicht über all dessen Funktionen.

www.ethercalc.net

CLOUDDIENSTE UND ONLINESPEICHER

Unzählige NutzerInnen bewahren ihre Daten und Programme nicht mehr auf dem eigenen Computer auf, sondern in gigantischen Serverfarmen. Die Festplatte entmaterialisiert sich, sie ist von überall und jederzeit abrufbar - und damit Tausende von privaten Fotos, Texten, Mails oder Songs.

Mit Nextcloud gibt es eine Software, mit der sich jedeR eine eigene Cloud bauen kann - auf eigenen Servern oder auf Servern von Anbietern, die auf Nextcloud setzen: *Eqipe* (eqipe.ch) und *Wölkli* (woelkli.com) beispielsweise. Beide Anbieter kann man kostenlos testen, die Nutzung der jeweiligen Cloudspeicher ist dann aber kostenpflichtig.

Gerade auch für die Verwaltung von Kalendern und Adressbüchern ist die Nutzung von Nextcloud sinnvoll. Ermöglicht wird die Synchronisation dieser Daten, ohne dass sie direkt zu Google oder Apple fliessen.

KARTEN

Auch wenn wir das Internet nach dem Weg fragen, kommt die Antwort üblicherweise von Apple oder Google respektive ihren Kartendiensten Apple Maps und Google Maps. Standardmässig können diese Dienste unseren Standort permanent überprüfen und umfassende Bewegungsprofile erstellen. Ortungsdienste müssen manuell in den Programmeinstellungen deaktiviert werden.

Ist die Ortungsfuktion auf dem Smartphone aktiviert, werden zudem sämtliche mit dem Telefon gemachten Fotos mit Informationen über Standort und Zeit der Aufnahme, sogenannten ***Metadaten,*** versehen. So können Dienste, die Zugriff auf Fotos haben, jederzeit rekonstruieren, wo und wann ein Foto gemacht wurde.

Die Ortungsfunktion sollte also wenn immer möglich deaktiviert werden.

OPEN STREET MAP

Die Open Street Map kann es bezüglich Genauigkeit und Informationsgehalt mit den Grossen aufnehmen. Nicht nur die geografischen Daten sind frei verfügbar, die NutzerInnen können die Karte auch erweitern – ähnlich wie beim Onlinelexikon Wikipedia.

Dank der offenen Struktur wächst die Open Street Map stetig und bringt verschiedenste Anwendungen hervor. Dazu gehören der Routenplaner *routing.osm.ch* oder die App *osmand.net.*

MAP.GEO.ADMIN.CH

Die frei zugängliche Karte der Bundesverwaltung ist ebenfalls empfehlenswert. Neben dem Kartenmaterial lassen sich viele weitere Informationen abrufen, etwa zu ÖV-Haltestellen oder Wanderwegen, zu lokal verfügbaren Internetbandbreiten, zur Lärmbelastung oder zur Gewässerqualität. Neben normalen Landkarten sind auch Luftbilder und historische Karten verfügbar. Über die offizielle App ist auf dem Smartphone der Zugriff auch offline möglich. Gerade bei WanderInnen ist dieses Angebot deswegen zu einem Standardwerkzeug geworden.

www.map.geo.admin.ch

INTERNET SERVICE PROVIDER

Die Internet Service Provider (ISP) bieten den Internetzugang. Wie und unter welchen Bedingungen sie das tun, hängt massgeblich vom Provider ab. Swisscom beispielsweise sammelt anonymisiert KundInnendaten und gibt diese der Werbefirma Admeira weiter, einem Joint Venture von Swisscom, Ringier und der SRG. Wer das nicht will, muss das Swisscom selber mitteilen (Opt-out) oder zu einem anderen Provider wechseln, wobei auf zwei Kriterien besonderes Augenmerk gelegt werden sollte: die ***Netzneutralität*** und den verantwortungsvollen Umgang mit Daten.

Ein Schweizer Provider, der sich der Netzneutralität verpflichtet, lokal verankert und eher an neuer und nachhaltiger Technologie als an Renditevorgaben orientiert ist, ist *Init7*. Der Provider setzte sich laut eigenen Angaben «für ein monopolfreies, liberales Internet» ein, «das Usern und Service-Providern ohne Einschränkungen offen steht».

Grundsätzlich gilt: Unbedingt lokale Angebote prüfen.

HOSTING

Wenn NutzerInnen eigene Inhalte ins Internet stellen wollen - Texte, Fotos, Videos et cetera -, sind sie auf Hostingdienste angewiesen, deren Rolle mit jener eines Gastgebers vergleichbar ist.

Die Website der WOZ beispielsweise wird über den Schweizer Hostingdienst *Netzone* aufgeschaltet. Einerseits, weil dessen Server in der Schweiz stehen, andererseits, weil er eine verschlüsselte Nutzung unserer Website anbietet. Das entsprechende Verschlüsselungsprotokoll sorgt dafür, dass der Datenaustausch zwischen dem Server, auf dem die Website läuft, und dem Browser der NutzerInnen verschlüsselt wird. Serverstandort und verschlüsselte Nutzung der Website sind die zentralen Kriterien bei der Auswahl eines Hostingdiensts. Mit *cyon.ch, nine.ch, hosttech.ch, hostpoint.ch* oder auch *amazee.io* gibt es zahlreiche sinnvolle lokale Anbieter.

03_GLOSSAR

GLOSSAR

Ein ***Algorithmus*** beschreibt grundsätzlich eine Folge von Anweisungen, mit denen ein bestimmtes Problem gelöst werden kann. Heutzutage wird der Begriff häufig im Zusammenhang mit der Verarbeitung riesiger Datensätze (Big Data) gebraucht: Algorithmen durchforsten diese Datenberge nach Mustern und Zusammenhängen. Konkret: Ein (nicht öffentlicher) Algorithmus bestimmt, welches Buch mir Amazon empfiehlt oder welche FreundInnen mir Facebook vorschlägt.

App ist die Kurzform des englischen Wortes Application (Anwendung) und beschreibt - zumindest im deutschsprachigen Raum - softwarebasierte Anwendungsprogramme auf mobilen Endgeräten (Smartphones und Tablets). Das berühmteste Beispiel ist wohl Whatsapp.

Die ***Ende-zu-Ende-Verschlüsselung*** ist das Couvert der digitalen Post. Durch die Verschlüsselung werden Nachrichten wie E-Mails auf dem Gerät des Absenders verpackt und mit einem «Schloss» versehen. Den Schlüssel zu diesem Schloss hat ausschliesslich die Empfängerin dieser Nachricht; nur sie kann sie wieder öffnen. So lässt sich verhindern, dass

Nachrichten auf dem Weg vom Absender zur Empfängerin mitgelesen werden.

Freie Software ist Software, die die Freiheit und Gemeinschaft der NutzerInnen respektiert. Sie können Programme ausführen, kopieren, verbreiten, ändern und verbessern und erhalten so die Möglichkeit zur Eigenkontrolle über die genutzte Software und die Datenverarbeitung.

Eine ***IP-Adresse*** wird jedem Gerät (Computer, Smartphone, Server et cetera) zugewiesen, das mit dem Internet verbunden ist. Eine IP-Adresse ist analog zu einer Postanschrift. Das heisst, Datenpakete werden mit einer IP-Adresse versehen, die den Empfänger eindeutig identifiziert.

Linux ist ein Sammelbegriff für unabhängige, quelloffene und kostenlose Betriebssysteme. Den Kern von Linux hat der damalige finnische IT-Student Linus Torvalds 1991 entwickelt. Linux basiert auf freier Software, das heisst, ProgrammiererInnen auf der ganzen Welt können das Betriebssystem erweitern und verbessern. Linux ist bei Smartphones (Android) und bei Servern das global führende Betriebssystem.

Die ***Kabelaufklärung*** ist verankert im neuen Nachrichtendienstgesetz (NDG). Sie erlaubt dem Geheimdienst, sämtliche von der Schweiz ins Ausland führende Telekommunikationsverbindungen nach definierten Stichwörtern zu durchsuchen. Gescannt werden Facebook-Nachrichten genauso wie Suchanfragen bei Google oder Einkäufe bei Onlineshops.

Die Vorratsdatenspeicherung umfasst die Sammlung der ***Metadaten*** unserer Kommunikation: Wer hat wann wen angerufen? Wie lange dauerte das Gespräch? Wer hat sich wann ins Internet eingeloggt oder auf ein E-Mail-Postfach zugegriffen? Auch Standortinformationen des Mobiltelefons werden gespeichert.

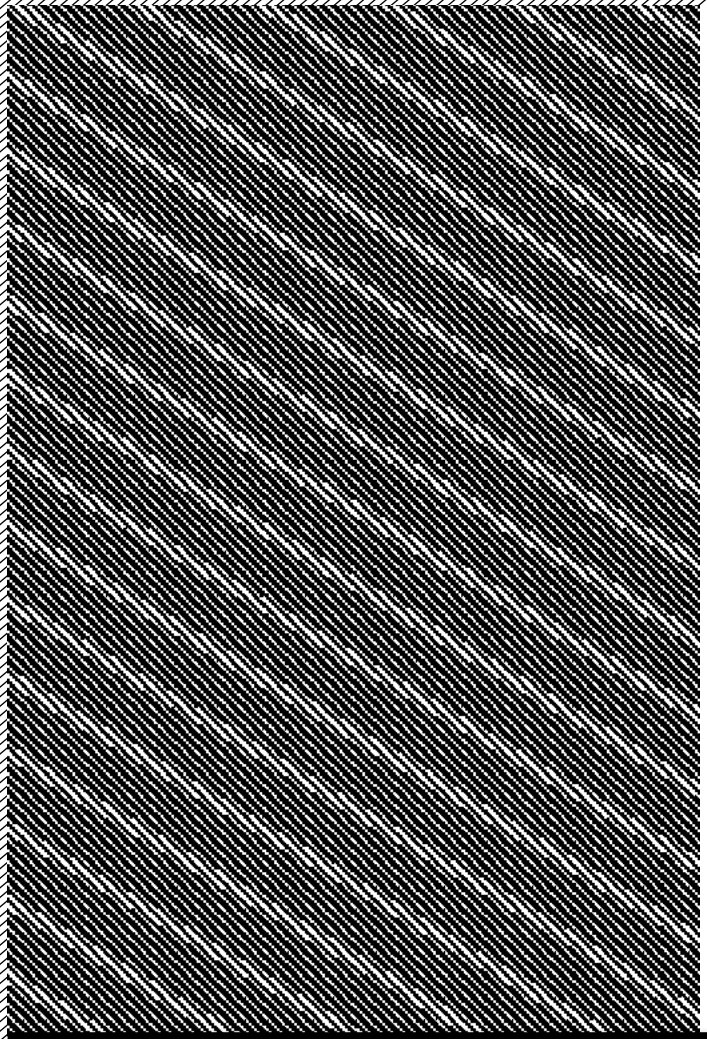
Im ***Nachrichtendienstgesetz (NDG)*** sind die Tätigkeiten des Schweizerischen Geheimdiensts geregelt. Mit der Einführung des Gesetzes am 1. September 2017 erhält der Geheimdienst massiv mehr Kompetenzen: Er darf Telefone abhören, Briefe und E-Mails mitlesen, Wohnungen verwanzen, per Trojaner in fremde Computer eindringen und sämtliche Datenströme durchsuchen, die über das Schweizer Glasfasernetz ins Ausland fliessen (vgl. «Kabelaufklärung»). Kurzum: Mit dem Gesetz erhält der Geheimdienst ein Instrument zur Massenüberwachung.

Netzneutralität bezeichnet die gleichberechtigte Übertragung von Daten im Internet. Netzneutralität ist dann erreicht, wenn sämtliche Daten - unabhängig von Absenderin, Empfänger, Dienst oder Inhalt - von den Telekommunikationsanbietern (Providern) in gleicher Qualität und gleicher Geschwindigkeit weitergeleitet werden.

Die ***Vorratsdatenspeicherung*** ist zentraler Bestandteil des neuen Nachrichtendienstgesetzes (NDG). Sie verpflichtet sämtliche Anbieter von Post-, Telefon- und Internetdiensten, das Kommunikationsverhalten ihrer KundInnen aufzuzeichnen und für sechs Monate zu speichern. Zuständig für die Vorratsdatenspeicherung ist der Dienst für die Überwachung des Post- und Fernmeldeverkehrs.

Der ***Quellcode*** ist der Bauplan eines Programms. Er wird in einer Programmiersprache wie C, Python oder Java verfasst. HerstellerInnen, die den Quellcode offenlegen, schaffen Transparenz über die Funktionsweise ihrer Software. So kann etwa überprüft werden, ob sogenannte Backdoors (Hintertüren) eingebaut wurden, um Daten abzusaugen. Grundsätzlich gilt deshalb die Regel: Wenn immer möglich Programme mit offenem Quellcode verwenden.

04_ADRESSEN



NÜTZLICHE ADRESSEN

ZUR PRIVATSPHÄRE IM DIGITALEN RAUM:

Digitale Gesellschaft
www.digitale-gesellschaft.ch

Chaos Computer Club Schweiz *www.ccc-ch.ch*

Netzpolitik *www.netzpolitik.org*

Konsumentenschutz *www.konsumentenschutz.ch*

Melde- und Analysestelle Informations-sicherung Melani
www.melani.admin.ch/melani/de/home.html

Eidgenössischer Datenschutz- und Öffentlich-keitsbeauftragter *www.edoeb.admin.ch*

ZUR DIGITALEN SELBSTVERTEIDIGUNG:

Prism Break *www.prism-break.org*
Electronic Frontier Foundation *www.eff.org*
Privacy Tools *www.privacytools.io*
Cracked Labs *www.crackedlabs.org*

FÜR BERATUNG, REPARATUR VON HARD UND SOFTWARE:

Revamp-it *www.revamp-it.ch*
Itopie *www.itopie.ch*, Revendo *www.revendo.ch*
Hackerspaces *www.ccc-ch.ch*


BY
SA