DigiDic

Anleitung zur digitalen Selbstverteidigung

Klaudia Zotzmann-Koch

IMA
INSTITUT FÜR MEDIENARCHÄOLOGIE

DigiDic

Anleitung zur digitalen Selbstverteidigung

Klaudia Zotzmann-Koch
Elisabeth Schimana [Hg.]

IMA
INSTITUT FÜR MEDIENARCHÄOLOGIE

Unsere aktuelle Empfehlungsliste findet ihr unter
[https://ima.or.at/de/extra/empfehlungen]

IMA
INSTITUT FÜR MEDIENARCHÄOLOGIE

Inhalt

VOR WORT

Digitale Selbstverteidigung

Gegenüber den vielfältigen Problemen im Digitalen ist es nur menschlich, sich überwältigt und machtlos zu fühlen. Doch man muss nicht einen Weltkonzern eigenhändig zerschlagen, um selbst etwas Sinnvolles zu tun.

Digitale Selbstverteidigung ist für euch, weil Ihr wisst, dass jede:r von uns etwas zu verbergen und ein Recht auf die eigene Privatsphäre hat. Und damit helft Ihr nicht nur euch selbst, sondern auch euren Familien und euren Freunden. Denn digitale Selbstverteidigung ist auch ein Teamsport.

Wo wir uns im physischen Leben gegen Raub, sexuelle Belästigung, gewalttätige Betrunkene usw. wappnen, ist es im Netz undurchsichtiger, wer die Akteur:innen und was die tatsächlichen Bedrohungen sind.

Bei digitaler Selbstverteidigung geht es darum, den Blick zu schärfen, wo es im Digitalen brenzlig werden kann.

Damit ihr wisst, was ihr tun könnt, bekommt ihr einen praktischen Leitfaden an die Hand, damit es erst gar nicht kritisch wird.

Dabei ist dieses Buch als Einstiegslektüre gedacht und geht nicht in allen Bereichen weit in die Tiefe. Wir zeigen euch, an welchen Stellen ihr weiter recherchieren könnt.

Wie im physischen Leben braucht alles Zeit und Übung und geht nicht von heute auf morgen. Manches aus dem Leitfaden werdet ihr sofort umsetzen können, Anderes in ein paar Wochen oder erst in einem Jahr.

Wichtig ist, bewusster mit dem Netz und den unterschiedlichen Akteur:innen umzugehen. Und wenn ihr bis hier gelesen habt, habt ihr den ersten Schritt schon getan.

VERTRAUEN

Wir vertrauen täglich verschiedenen Akteur:innen: Familie und Freund:innen, den Verkehrsbetrieben, den Anbietern unserer Kommunikationsdienste und Geräte, dem Staat und den politischen Entscheidungsträger:innen, den Hersteller:innen unserer Kleider und den Menschen in unserem Umfeld. Ohne Vertrauen würde unsere Gesellschaft nicht funktionieren. Wir lernen üblicherweise in jungen Jahren Vertrauen in uns bekannte Menschen. Fremden gegenüber muss Vertrauen erst wachsen. Verspielt ist es aber in Sekunden.

Vertrauen ist nicht nur zentraler Baustein menschlichen Zusammenlebens, sondern auch die Grundwährung im Internet, eine geldwerte Handelsware.

Vertrauen im digitalen Kontext hat unterschiedliche Ebenen.

Vertrauen in Plattformen und deren User:innen

Wir haben Vertrauen, dass die Anbieter sich sorgfältig um die Programme, Messenger, Plattformen und Dienste kümmern und z. B. keine Unbefugten einfach mitlesen können. Wir posten Bilder im Vertrauen, dass sie auf der Plattform bleiben und unsere Follower:innen sie nicht als ihre eigenen ausgeben, speichern, verändern, Deepfakes daraus erstellen oder anderweitig weiterverwenden.

Vertrauenswürdige Quellen

Vertrauenswürdige Quellen sind z. B. Stiftung Warentest und unabhängige Medien oder auch Einzelpersonen, die als Expert:innen für ihr Fachgebiet bekannt sind. Wir vertrauen auf ihren guten Ruf, die redliche Recherche und ihr unbefangenes, auf aktuellem Wissen fußendes Urteil.

Ein guter Hinweis, dass Vertrauen in Informationen gerechtfertigt ist, ist ein Blick auf die Finanzierung von Studien oder dem Medienhaus, durch das Informationen veröffentlicht werden. Das alte Sprichwort »Wessen Brot ich ess, dessen Lied ich sing« trifft auch im Internet zu. Wenn nicht ersichtlich ist, wer eine Studie beauftragt, bezahlt oder wer sie durchgeführt hat, sind Skepsis und Faktenchecks angebracht. Und nur, weil eine Person in einem Bereich berühmt ist, heißt das nicht, dass sie sich auch in anderen Bereichen gut auskennt.

Vertrauen in Freunde und Bekannte

Wenn jemand, den wir kennen, uns einen Rat gibt, wiegt dieser meist schwerer als ein Rat aus einer uns unbekannten Quelle. Oft genug treffen wir intuitive Entscheidungen für oder gegen etwas auf Basis unseres Vertrauensverhältnisses zu den Ratgebenden. In Situationen, in denen es schnell gehen soll, sind selten gut fundierte Recherchen vertrauenswürdiger Quellen ausschlaggebend.

Ein Offline-Beispiel: Eine Person menstruiert zum ersten Mal und hat jetzt das konkrete Problem. Sie geht in einen Drogeriemarkt und steht vor dem Regal. In dieser Situation vertrauet sie auf das, was sie a) von zu Hause kennt, b) was eine befreundete Person empfiehlt oder c) was die ansprechendste Verpackung hat. Für die spontane Kaufentscheidung ist so gut wie nie ausschlaggebend, welches Produkt nachhaltig, unparfümiert oder plastikfrei ist. Erst viel später setzen wir uns – wenn überhaupt – mit den Hintergründen dessen auseinander, was wir verwenden.

Genauso verfahren wir üblicherweise auch bei Anbietern für E-Mail, Cloud-Office ... Wir vertrauen dem »guten Tipp«, statt uns selbst mit den ethischen, politischen, sozialen und ökologischen Hintergründen einzelner Lösungen auseinander zu setzen.

Vertrauen und Internetkriminalität

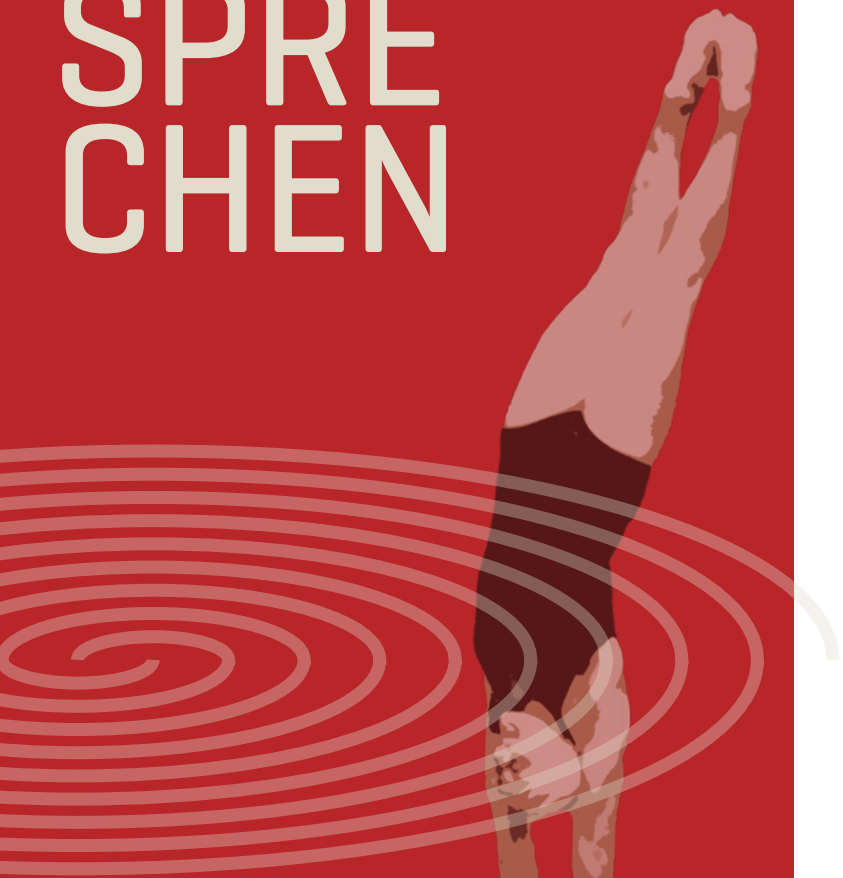
E-Mails oder Social-Media-Posts von Menschen, die wir kennen, haben einen Vertrauensvorschuss, weil sie für uns aus einer subjektiv verlässlichen Quelle kommen. Das macht beides zu einem lukrativen Angriffsziel für Kriminelle und Verbreiter:innen von Fakenews, weil wir dazu neigen, die Inhalte zu glauben und weiterzuverteilen. So bedienen wir selbst das Schneeballsystem. Wir dienen als Sprung-

brett, wenn unser Name und unsere E-Mail-Adresse als Absender zum Beispiel in Phishing-Mails stehen. Menschen öffnen sie im guten Glauben, eine Nachricht von uns zu erhalten. Stattdessen laden sie sich dadurch eine Malware auf ihr Gerät und werden Minuten später Opfer von Erpresser:innen. Woher die Kriminellen unsere Namen und Mailadressen haben? Aus den zahlreichen Datenlecks, bei denen Internetplattformen, Shops oder Spieleseiten ihre Kundendatenbank an Kriminelle verlieren.

Vertraut nicht blindlings den Anbietern eurer Apps und Plattformen. Und auch nicht auf alles, was Freunde und Verwandte sagen oder posten. Wir irren uns alle. Jeden Tag.

Überlegt bei allem, was ihr nutzt, welche Interessen der Anbieter dahinter stehen. Lest euch die AGB und Datenschutzerkläungen durch, auch wenn es mühsam ist. Seid euch bewusst, dass viele Anbieter euch und eure Entscheidungen zu ihren Gunsten oder denen zahlungskräftiger Unternehmen manipulieren.

VERSPRECHEN



Ewige Liebe, schlanke Taille, ethische Datenverarbeitung; Uns wird etwas versprochen und unser Vertrauensmechanismus damit ausgelöst. Im persönlichen Umfeld können wir noch einschätzen, ob Versprochenes auch gehalten wird. Bei allem anderen müssen wir entweder selbst recherchieren, uns auf eine vertrauenswürdige Quelle verlassen oder einfach glauben, dass wir nicht angelogen werden.

Als soziale Wesen sind wir geneigt, Versprechen zu glauben. Sie geben uns ein gutes Gefühl, das wir gleichsetzen mit »Sicherheit«.

Alles ist so leicht und einfach

Die vielen bunten Oberflächen, die unsere digitale Alltagswelt ausmachen, gaukeln uns dieses Gefühl vor, ihre Mechanismen sind aber alles andere als selbsterklärend. Das ist generationsübergreifend gleich. Der »Digital Native« ist ein Mythos, der durch nichts belegt ist. Junge Menschen verwenden das heute Vorhandene selbstverständlicher, Funktion und Auswirkungen verstehen sie deshalb aber längst nicht besser.

UNSER GROSSES PROBLEM

Werbeindustrie und Konzerne investieren laufend Milliarden, um herauszufinden, wie wir denken, Entscheidungen treffen, klicken, uns on- und offline bewegen und wie unsere Aufmerksamkeit möglichst lang gebunden werden kann. Unsere Hirnfunktionen werden zur Profitmaximierung gegen uns eingesetzt.

Die großen Versprechen – Werbung

Werbung mit ihren bunten Bildern wird gern verharmlost. Dabei gehen wir von der Annahme aus, Werbung funktioniere im Netz genauso wie bei Werbe-Prospekten. Doch nur selten geht es um wirkliche Lösungen. In den meisten Fällen wird das Problem durch die Werbung erst kreiert. Letztlich geht es fast immer um unser Geld. »Zwei plus eins gratis« ist nicht sparen; Sparen ist, gar keins davon zu kaufen.

Werbung ist schon seit vielen Jahren deutlich perfider geworden. Sammeln und Ausnutzen der über uns bekannten Informationen gehen Hand in Hand, online wie offline. »Crossmedia Advertising« ist das Marketing-Fachwort dazu. Über verschiedene Medien hinweg: Werbe-E-Mail, Bushaltestelle, Magazine und Social-Media-Posts können Teil einer einzigen Kampagne sein. Wenn wir oft genug Werbebotschaften sehen oder hören, werden wir mit ihnen vertraut. Irgendwann werden sie normal und wir glauben sie.

Genau darum geht es bei Werbung. Die Werbeindustrie weiß genau, wie lange unser Gehirn braucht, um den Wechsel des Deos in Betracht zu ziehen oder einer anderen politischen Richtung zu folgen. Daher gibt es sich immer weiter aufbauende und zuspitzende Kampagnen, die über Wochen und Monate laufen. Ziel ist die für uns unmerkliche Veränderung unserer Wahrnehmung und unseres Verhaltens. Das ist das Produkt, für das viele Milliarden bezahlt werden. Die Milliarden bekommen sie von uns. Werbung ist nicht gratis, sie kostet unser Geld, dadurch, dass wir Produkte kaufen. Wir werden in das Verhalten hinein manipuliert, das Werbetreibende von uns haben wollen. Im besten Fall kaufen wir ein Paar Schuhe, das wir nicht brauchen und das nicht im Budget ist. Im schlechtesten Fall gehen wir nicht wählen.

Das Bewusstsein dafür, dass wir durch Werbebotschaften aktiv manipuliert werden, hilft uns, vorsichtiger zu sein.

Vertraut nicht unhinterfragt dem, was auf Werbetafeln, in Advertorials, also als redaktionelle Inhalte getarnten Werbeanzeigen, oder Social-Media-Posts steht.

Seid skeptisch bei Botschaften, die starke Emotionen in euch auslösen. Diese sollen euch in ein bestimmtes Verhalten bringen. Die Versprechen haben zum Ziel, an unser Geld zu kommen oder unsere Meinung zu beeinflussen. Seid achtsam bei Inhalten im Netz und bei Werbung allgemein. Lest bei Artikeln oder Social-Media-Posts nach, ob ihr dieselbe Information auch bei z. B. öffentlich-rechtlichen Medien findet. Prüft bei Artikeln, ob ihr es mit Advertorials zu tun habt. Verwendet beim Surfen im Netz grundsätzlich einen Werbeblocker. Dieser blockiert den Großteil der Werbebotschaften. So spart ihr auch noch viel Strom und schont die Umwelt.

VERANTWORTUNG

Angesichts des bisher Gelesenen schauen wir erwartungsvoll oder betrübt auf »die Großen«, wenn es um Verantwortung geht. Auf ihnen lastet die große Bürde, unsere Daten mit Argusaugen zu hüten. Das sind die Hersteller:innen unserer Geräte, die ihre Cloud-Lösungen darin fest hinterlegen und uns so ganz automatisch in ihre Systeme ziehen. Es sind die Konzerne, die ihre ethischen Werte vielleicht erst noch finden müssen. Und es sind die Betreiber:innen der sozialen Medien, denen wir unser gesamtes Leben mit allen kleinen und großen Geheimnissen verraten und unsere Kontakte anvertrauen. Sie alle werden fürstlich dafür entlohnt. Nur nicht von uns, sondern von anderen, die für unsere Aufmerksamkeit bezahlen.

Bei all dem empören wir uns zu Recht. Wir sehen, wie Vertrauen missbraucht und Versprechen gebrochen werden. Aber wir haben ebenfalls Verantwortung.

Empowerment

Wir alle tragen Verantwortung uns selbst gegenüber, nicht blind den schönen Versprechen zu vertrauen. Wir tragen zumindest eine Teilschuld, wenn unsere Daten gegen uns verwendet werden. Natürlich haben wir nie gelernt, die Strategien der Werbeindustrie zu hinterfragen. Aber wir haben in der Schule auch nicht gelernt, wie man ein Haushaltsbuch führt und müssen uns trotzdem darum kümmern. Die Verantwortung einzugestehen und zu übernehmen

bringt uns in die eigene Wirkmächtigkeit. Das englische »Empowerment« ist ein schönes Wort dafür.

Akzeptieren wir, dass wir Verantwortung tragen, werden uns viele Vorgänge anders vorkommen. Unsere Freizeitgestaltung, unsere Kommunikation, unsere politische Einstellung, unser Kaufverhalten, Suchanfragen, unsere Finanzen, unser Modestil … Alles ist mit allem verbunden – auch für Unternehmen wie Google, die das auswerten und die Schlüsse daraus ziehen, welche Werbetreibenden uns was anzeigen sollen. Diese Verknüpfungen zu erkennen, ermöglicht es uns, freie und selbstbestimmte Entscheidungen zu treffen.

Die Verantwortung gegenüber Anderen

Andererseits haben wir auch eine Verantwortung gegenüber all denen, die uns vertrauen und von denen wir Daten haben. Sehr offensichtlich ist das bei Bildern, Videos, Geburtsdaten, Nummern und Nachrichten, die wir von anderen gespeichert haben. Nicht ganz so offensichtlich ist es bei unserem Verhalten wie Lesen, Liken, Kommentieren, Nachrichten senden … Mit allem, was wir tun, geben wir Informationen über uns preis, aber auch über andere und darüber, in welcher Beziehung wir zu ihnen stehen. Wir sind nie allein, wir sind immer in Beziehung zu anderen. Daher sind Datenschutz und Privatsphäre ein Teamsport.

Zur Verantwortung gegenüber Anderen gehört auch, dass wir keine Lügen im Netz posten, keine Fakenews verbreiten und Fakten checken.

Verantwortung als Grundlage demokratischer Gesellschaft

Eine demokratische Gesellschaft kann nur funktionieren, wenn wir uns aufeinander verlassen können. Wenn es um die politischen Verhältnisse geht, ist unser Dreieck »Vertrauen – Versprechen – Verantwortung« zwar etwas anders gelagert, aber das Grundprinzip ist noch immer dasselbe. Wir haben Rechte, aber wir haben auch Pflichten, die wir als Bürger:innen in Demokratien erfüllen sollten. Wählen gehen ist eine Sache, aber Verantwortung übernehmen kann jede:r, auch ohne für ein politisches Amt zu kandidieren. Man kann sich engagieren, indem man Ehrenämter in Vereinen und Organisationen übernimmt, zum Beispiel den in der Ausstellung genannten wie Tactical Tech, CCC e. V., Center for Humane Technology und einige mehr. Wir alle sind soviel stärker, wenn wir gemeinsam an einem Strang ziehen.

Schiebt nicht alle Verantwortung auf die anderen, auch wenn es schmerzhaft ist, sich der eigenen Verantwortung bewusst zu werden.

Nehmt eure Verantwortung an und werdet euch eurer Selbstwirksamkeit bewusst. Ihr könnt etwas verändern. Für euch selbst, aber auch für andere. Ihr habt Möglichkeiten, Dinge zu bewegen. Informiert euch darüber und nutzt sie.

ANLEITUNGEN

Bevor ihr euch ins Abenteuer stürzt, euer Onlineverhalten bewusster zu gestalten, wollen wir euch eine Erklärung an die Hand geben, die euch helfen wird, über dieses Handbuch hinaus Apps, Programme, Geräte und Angebote im Netz zu beurteilen.

Wie funktioniert das Internet?

Die Grundfunktion im Internet ist Datenübertragung. Das folgende Prinzip ist quasi überall dasselbe. Wenn wir die Inhalte einer Webseite anschauen, werden Daten vom Server, auf dem die Webseite gehostet ist, zu unserem Gerät und dem Browser darauf übertragen. Der Browser interpretiert diese Daten und zeigt uns die Inhalte der Seite an.

Wichtig: Um Daten von einem Server zu bekommen, müssen wir dem Server immer unsere IP-Adresse verraten. Wie bei der Post: ohne Adresse keine Pakete. Der Server muss wissen, wohin er die Daten schicken soll. Daher überträgt der Browser, ebenso wie jedes Programm und jede App, die mit dem Internet kommuniziert, immer die IP-Adresse unseres jeweiligen Gerätes.

IP steht für Internet Protocol. IP-Adressen sind nicht dasselbe wie eine physische Adresse mit Straßenname und Hausnummer, aber sie lassen auf den Internetanbieter schließen, über den wir den Zugang beziehen. Bei vielen großen Anbietern lassen IP-Adressen auch auf die Stadt und bei einigen auf den Bezirk innerhalb der Stadt schließen.

Euch ist sicher aufgefallen, dass viele Webseiten auf mobilen Geräten anders aussehen, als auf Desktopcomputern. Das liegt daran, dass unsere Browser auf Anfrage des Servers auch verraten, welches Betriebssystem auf dem Gerät läuft, was für ein Gerät es ist, oft auch die eindeutige Kennnummer des eingebauten Internetmodems (»Mac-Adresse«), welcher Browser oder welche App beim Server anfragt, welche Fensterbreite und Ausrichtung verwendet wird: Desktop oder mobile, Hoch- oder Querformat. Anhand dieser Informationen sendet der Server die Inhalte inklusive der Art, wie sie angezeigt werden sollen, passend für unser Gerät zurück.

So praktisch das auch ist, sind diese Informationen verräterisch und werden von der Werbeindustrie zu Personalisierung sowie eurer Wiedererkennung verwendet. Das nennt sich »Targeting«, also das »ins Ziel nehmen«.

Wenn ihr euch auf einer Webseite oder bei einem Service einloggt, werden diese Informationen zu eurem Gerät im Hintergrund eurem Nutzer:innen-Profil zugeordnet. Und wenn ihr euch von mehreren Geräten aus einloggt, liegen diese Informationen für alle eure Geräte vor. So werdet ihr über verschiedene Geräte hinweg wiedererkannt mit dem Ziel, mehr über euch und eure Vorlieben zu erfahren und euch vielleicht doch noch dieses Paar Schuhe zu verkaufen, das ihr vorhin auf dem anderen Rechner angesehen habt.

Open Source

Der Entschluss, offene Protokolle und freie Software zu verwenden, ist eine Philosophie, eine Grundhaltung zu Demokratie auch in den Technologien, die wir nutzen und die unsere Gesellschaft prägen. Das Gegenteil davon ist sogenannte proprietäre, also hersteller:innengebundene Software. Solche, die nur die Hersteller:innen kennen und in die niemand anders reinschauen kann, wie sie im Detail funktioniert. Proprietäre Software ist wie ein moderner Toaster. Alles ist verklebt und man kommt nirgends mehr dran. Dadurch kann man nichts reparieren und es wird kein nachhaltiges Produkt.

Die Open-Source-Community, also Menschen die Open-Source-Software nutzen und sich an ihrer Entwicklung und Verbreitung beteiligen, trägt dazu bei, dass die Software sicher ist und es auch bleibt. Zum Einen dadurch, dass sie gefundene Fehler öffentlich melden können, zum Anderen dadurch, dass die Macher:innen jederzeit einer ganzen Community von Menschen sowie auch der Öffentlichkeit gegenüber Rechenschaft ablegen (müssen).

Open-Source-Software kann auch von anderen Menschen mit entsprechender Fachkenntnis angepasst und weiterentwickelt werden. Hier können alle den Toaster reparieren und ihm weitere Funktionen wie Brötchengitter etc. hinzufügen.

Sollten Menschen ihre Projekte nicht weiter betreiben können oder wollen, können andere leicht daran weitermachen. Nicht wie bei Closed-Source-Software, die nach der Pleite einer Firma einfach nicht mehr nutzbar ist.

Bei Open Source können auch weitere, ganz neue Abzweigungen einer Software entstehen. Es herrscht viel Kreativität in dem Bereich.

Open Source ist so gesehen eine Demokratisierung der Software-Landschaft. Zum Anderen sorgt Open Source für Nachhaltigkeit im Bereich Software. Ein konkretes Beispiel dafür sind alternative Android-Betriebssysteme wie LineageOS oder eOS, die einige Android-Geräte unterstützten, die von den Hersteller:innen schon seit Jahren keine Sicherheitsupdates mehr bekommen. So können die Geräte nicht nur einige Jahre länger verwendet werden, sondern sind auch noch frei von Tracking.

Die meisten unserer Empfehlungen sind Open Source. Aus Überzeugung.

OPEN SOURCE

Open Source bedeutet, dass der Programmcode einer Software öffentlich einsehbar ist und weitergegeben werden darf. So können alle, die sich damit auskennen, sich davon überzeugen, dass die Software gut und sicher programmiert ist.

Die Schlüssel zum Erfolg

Das Hauptproblem hinter einem Großteil von Onlinekriminalität ist, dass viele von uns überall dasselbe Passwort verwenden. Teilweise über Jahre hinweg. Auch im Jahr 2022 gibt es noch immer Betreiber, die ihre Kundendatenbanken nicht ordentlich verschlüsselt und sicher ablegen. Solche Datenbanken sind für Kriminelle ein gefundenes Fressen, denn so bekommen sie tausende, manchmal Millionen Kombinationen aus Benutzername, E-Mail und Passwort, die sie für ihre Zwecke einsetzen. Sie sitzen nicht da und haben es auf genau euch abgesehen. Ihr, genauer: Eure Accounts, sind geldwerter Beifang.

Sie sitzen auch nicht da und geben jede dieser Kombinationen bei unterschiedlichen Plattformen, Shops etc. ein, um zu sehen, ob sie reinkommen. Die Kundendatenbanken aus den Datenlecks werden in ein kleines Programm gefüttert, das binnen Sekundenbruchteilen alle Kombinationen aus der Datenbank bei einer Vielzahl an Shops, Plattformen, Services etc. ausprobiert. Vollkommen automatisiert. Wo sie reinkommen, da schauen sie dann, was sie kriegen können. Hinterlegte Kreditkarteninformationen beispielsweise und das Gold des Internets: Eure Kontakte, die sie verwerten können.

Wenn ihr seit Jahren überall dieselbe E-Mail-Adresse und dasselbe Passwort verwendet, ist die Wahrscheinlichkeit, dass diese Zugangsdaten frei im Internet verfügbar sind und von Kriminellen bereits verwendet werden, bei nahezu 100 Prozent. Eure Accounts sind dann »owned« (engl. to own = besitzen), sie sind also im Besitz anderer Leute.

Have I been Pwned?

Wenn ihr herausfinden wollt, ob eure Zugangsdaten bereits irgendwo Teil eines Leaks, eines Datenlecks, geworden sind, könnt ihr euch auf [https://haveibeenpwned.com] informieren. Das P anstelle des O ist Absicht. Es rührt von einem Vertipper her, der in der Folge zu einem geflügelten Wort wurde. Gebt auf der Seite eure E-Mail-Adresse ein und schaut, in welchen Datenlecks der vergangenen Jahre sie schon dabei war.

Wenn ihr jetzt feststellt, dass eure E-Mail-Adresse schon in Datenlecks vorhanden ist, dann solltet ihr sofort handeln. Falls eure Adresse noch nicht in einem bekannten Datenleck vorkommt, bedeutet das nur, dass es noch kein bekanntes Datenleck gibt, nicht aber, dass eure E-Mail-Adresse und der Rest eurer Zugangsdaten sicher sind.

Die Lösung ist sehr simpel: Verwendet für jedes einzelne Login ein eigenes Passwort. Selbst wenn ihr überall dieselbe E-Mail-Adresse und denselben Benutzernamen habt, könnt ihr mit unterschiedlichen Passwörtern doch verhindern, dass andere Leute oder automatisierte Programme sich in eure Accounts einloggen.

Nein, ihr müsst euch keine 137 oder mehr Passwörter merken. Auch nicht in ein Büchlein schreiben, das eventuell bei einem Einbruch mitgenommen werden könnte. Es gibt hilfreiche Passwortmanager, die euch das Leben sehr erleichtern werden.

PASSWORTMANAGER

Gute Passwörter sind vor allem lang. Macht euch für jedes Login, für jeden Service ein eigenes Passwort. So verhindert ihr, dass Kriminelle Zugriff zu all euren Accounts haben, wenn bei einem Anbieter die Kundendatenbank leakt. Ein Passwortmanager hilft euch, die Passwörter sicher auf euren Geräten zu verwahren.

Das alles klingt komplizierter als es ist.

Gebrauchsanleitung

1. Installiert euch einen Passwortmanager. Wir empfehlen KeepassXC. Das XC hinten ist wichtig, das ist die aktuelle Version, die auch weiterentwickelt wird. Ihr ladet ihn einfach von der Webseite [https://keepassxc.org/] herunter und installiert ihn. Falls ihr Linux benutzt, findet ihr ihn ganz normal in der Anwendungsverwaltung.

2. Wenn ihr das Programm das erste Mal startet, richtet es euch automatisch einen Tresor für alle eure Passwörter ein. Dazu müsst ihr ein Passwort für den Tresor benennen. Dieses Passwort müsst ihr euch tatsächlich merken, denn es öffnet den Tresor, in dem dann alle eure anderen Passwörter liegen.

   Pro-Tipp: Nehmt auch hier ein langes Passwort, falls euer Gerät mal gestohlen wird. Ihr könnt aber gern etwas Nettes verwenden wie eine Zeile aus einem Lied, das ihr gerne hört, inklusive der Zeichensetzung. Wenn ihr mehrere Sprachen mischt, wird das Passwort mit heutiger Technologie quasi unknackbar.

3. Schreibt euch dieses wichtige Passwort für den Anfang auf. Am besten auf einen Zettel, den ihr später vernichten könnt, sobald ihr euch daran gewöhnt habt. Verwahrt ihn gut in einer Schublade. Keinesfalls als Klebezettel am Monitor oder an anderen Stellen, wo andere es sehen und abfotografieren könnten.

4. Installiert das Browser-Plugin für euren Passwortmanager. Das macht nicht nur das Login auf den unterschiedlichen Seiten sehr komfortabel, es bringt sogar noch mehr Sicherheit. Wenn euer Passwortmanager die Seite, auf der ihr euch versucht, einzuloggen, nicht kennt, wird er euch die Zugangsdaten nicht anbieten. Das hilft vor allem bei gut gemachten Fake-Seiten, die vielleicht nur einen Buchstabendreher in der URL haben, den unser Gehirn einfach überliest. So verhindert der Passwortmanager, dass ihr versehentlich eure Zugangsdaten an Dritte weitergebt.

5. Jetzt geht ihr einfach der Reihe nach vor. Wenn ihr euch irgendwo das nächste Mal einloggt, tauscht ihr bei der Gelegenheit das Passwort aus. Das sind pro Shop oder Plattform ... vielleicht zwei bis fünf Minuten Aufwand, die sich extrem lohnen.

Und das war es. Ihr könnt für euer Mobilgerät auch einen Passwortmanager verwenden. Keepass2Android und Strongbox (iOS) können beide mit KeepassXC-Tresor-Dateien umgehen.

Pro-Tipp: Legt für unterwegs einen eigenen Tresor an, in dem ihr dann nur die Handvoll Passwörter speichert, die ihr auf eurem Mobilgerät auch zwingend braucht. Sollte euer Telefon gestohlen werden oder verloren gehen, könnt ihr diese paar Passwörter vorsorglich einfach ändern.

Euer wichtigstes Passwort

Ein guter Anfang, euch mit Zwei-Faktor-Authentifizierung auseinanderzusetzen, ist euer E-Mail-Account. Denn falls Dritte Zugang zu euren E-Mails haben, können sie sehr einfach alle anderen Passwörter zurücksetzen, da die Bestätigungen in eurem E-Mail-Account landen. Dort können sie schnell geklickt und gelöscht werden, ehe ihr davon etwas seht. Ein zweiter Faktor zusätzlich zu eurem Passwort verhindert, dass jemand einfach mit Benutzernamen und Passwort in den Account reinkommt. Beispielsweise wird euch noch ein sechsstelliger Code per SMS geschickt, der zusätzlich für das Login gebraucht wird.

Wenn ihr damit fertig seid, alle eure alten Passwörter auszutauschen, schaut euch die Zwei-Faktor-Authentifizierung an und richtet diese bei euren wichtigsten Accounts ein. Euer Passwortmanager hilft euch dabei.

Wenn ihr euch nur zwei Tipps aus diesem Buch mitnehmt, dann bitte diese: Nutzt für jedes Login, für jeden Service ein eigenes Passwort. Und verwendet einen Passwortmanager, um die vielen Passwörter sicher auf euren Geräten zu verwahren. Danke.

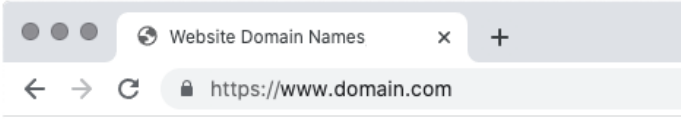
Verwendet auf keinen Fall überall dasselbe Passwort.

Installiert euch einen Passwortmanager wie KeepassXC und auf eurem Mobilgerät ebenfalls. Strongbox (iOS) oder Keepass2-Android bieten sich an. Tauscht nach und nach alle eure Passwörter gegen lange (14-35 Zeichen) aus. Verwendet für jedes Login und jeden Service ein eigenes Passwort.

Browser & Browser-Add-ons

Wenn wir im WWW, dem World Wide Web, unterwegs sind, nutzen wir dazu auf dem Desktoprechner genauso wie auf Mobilgeräten einen Browser. Viele von uns verwenden einfach den, der beim Gerät vorinstalliert mitgeliefert wurde. Andere verwenden bekannte Programme wie Google Chrome, der im April 2022 einen Marktanteil von immerhin 64,53% abdeckt; unter Desktop-Systemen sogar 67,29% [https://gs.statcounter.com/browser-market-share].

Grundsätzlich sollte jeder Browser gut abgesichert sein und eine ganze Reihe an Sicherheitsfunktionen mitbringen, denn seine Hauptfunktion ist es, mit dem Internet verbunden zu sein. Dort begegnet er nicht nur den eigentlichen Inhalten, sondern auch allerhand Gefahren wie verschiedensten Sorten von Schadsoftware bis hin zu Tracking und Targeting.



Was jeder Browser heute kann, ist »httpS«, also »hypertext transfer protocol«, das Protokoll, wie Webseiten und Informationen im WWW übertragen werden. Das »s« am Ende steht für »secure« und bedeutet, dass eine sichere Verbindung zwischen eurem Gerät und dem Server aufgebaut wird. Ihr könnt euch das wie einen Tunnel von eurem Browser bis zum Server der Webseite vorstellen. Niemand kann von außen auf das Innere des Tunnels schauen, etwas wegnehmen oder etwas anderes hinzufügen. Die Inhalte, die euch angezeigt werden, kommen dank des Tunnels also wirklich vom Server der Seite und nicht von irgendwo auf dem Weg dazwischen.

Es bedeutet leider nicht, dass die Inhalte auch sicher sind, denn auf dem Server selbst kann auch Schadsoftware hinterlegt sein, die über den Browser dann auf euer Gerät gelangt.

Wichtig ist https insbesondere bei allen Login-Seiten, wo ihr eure Zugangs- oder auch Zahlungsdaten eingebt, damit diese nicht von irgendwem zwischen eurem Browser und dem Server mitgeschrieben werden und dann anderweitig verwendet werden können.

Aber auch bei allen Inhalten gibt https die Gewissheit, dass die Informationen wirklich von der Seite, beispielsweise einem öffentlich-rechtlichen Nachrichtenportal kommen und nicht »von der Seite« eingeschleust wurden.

COOKIES

Cookies sind kleine Dateien … Ja, alles schon gelesen, aber das ist tatsächlich wichtig. Cookies sind Dateien, die auf euren Geräten von z. B. Webseitenbetreibern hinterlegt werden. Cookies sind nicht grundsätzlich schlecht, sie nehmen beispielsweise Informationen über die in den Warenkorb gelegten Produkte auf, wenn ihr nicht bei der Seite eingeloggt seid oder noch keinen Account habt. Allerdings werden Cookies auch in der Werbeindustrie verwendet, um darin Informationen über euer Surfverhalten, angeschaute Seiten, Produkte... zu speichern.

Cookies bei jedem Beenden des Browsers zu löschen ist eine kleine Änderung, die euch viel Souveränität wiedergibt. Das solltet ihr übrigens auch immer tun, wenn ihr Zug- oder Flugtickets oder Hotelzimmer buchen wollt, denn dass ihr immer wieder nach Verbindungen zu einem bestimmten Ziel schaut, mit welchen (teuren?) Geräten ihr das tut und dass die Abstände eurer Suchanfragen kürzer werden, wird ebenfalls in Cookies hinterlegt. Cookies löschen führt zu günstigeren Preisen.

Browser Add-ons

Mit Browser Add-ons könnt ihr eurem Browser nützliche Funktionen hinzufügen.

Adblocker, also Werbeblocker, sind eine dringende Empfehlung. Im Frühjahr 2022 sind das die Adblocker uBlock origin und EFF Privacy Badger.

Auch https everywhere ist eine gute Ergänzung. Das Add-on erzwingt überall wo möglich eine httpS-Verbindung zum Server, beispielsweise bei falsch konfigurierten Webservern.

Cookie AutoDelete ist nützlich, um Cookies direkt zu löschen, ohne den Browser dafür neu zu starten oder sie händisch in der Liste hinterlegter Cookies in den Einstellungen herauszusuchen.

Außerdem empfehlen wir euch das Browser-Add-on, das euer Password-Safe mitbringt. Falls ihr noch keinen verwendet, schaut in das Kapitel zu Passwörtern, dort findet ihr alle Infos dazu.

Last but not least: Snowflake. Das Add-on des Torprojekts, das auch den Tor-Browser zur Verfügung stellt, macht euren Browser zur Brücke ins Tor-Netzwerk. So helft ihr Menschen in Gebieten mit Medien- und Internetzensur wie beispielsweise Russland und China, dennoch an freie und unzensierte Medienberichte zu gelangen.

Browser auf Mobilgeräten

Auch auf euren Mobilgeräten könnt ihr alternative Browser verwenden und seid nicht an das gekettet, was die Hersteller auf euren Geräten vorinstalliert haben. In den AppStores oder auch dem F-Droid-Store findet ihr Alternativen wie den mobilen Firefox Browser oder auch Firefox klar, eine noch privatsphäreschonendere Version des Firefox Browsers. Dieser »vergisst« immer sofort nach dem Schließen alle Cookies und legt keine History an.

Firefox klar kann seine Funktionalitäten als Werbeblocker auf iOS auch mit dem hauseigenen Safari Browser teilen, falls eine App doch einmal den Safari aufrufen sollte. Dazu geht ihr auf Einstellungen -> Safari -> Erweiterungen und wählt dort Firefox klar aus.

Auch der DuckDuckGo Browser ist einen Versuch wert. Dieser hat die gleichnamige Suchmaschine allerdings fest eingebaut.

In den Geräteeinstellungen könnt ihr auch einen alternativen Browser als Standardbrowser festlegen. Das trägt viel zu eurer Privatsphäre bei.

Fallt nicht auf die Default-Falle hinein. Wenn etwas vorinstalliert ist, stecken oft genug kommerzielle Interessen dahinter. Seid nicht zu bequem.

Installiert euch einen anderen Browser statt dem mitgelieferten oder Google Chrome. Wir schlagen Firefox vor. Nutzt Werbeblocker, um euren Browser sicherer zu machen. Tauscht auch auf euren Mobilgeräten die Browser gegen sicherere Alternativen aus und verwendet auch dort Werbeblocker wie Firefox klar.

Das Problem mit Google

Es ist nicht so, dass Google nur schlechte Dinge tut, allerdings müssen wir die schiere Menge an Informationen, die bei Google zusammenlaufen, kritisch betrachten. Insbesondere, da Google diese kommerziell verwertet und auch an andere weitergibt und weiterverkauft.

Google bekommt alle Informationen, die wir in die Google Suche eingeben. Hier sind wir immer ehrlich, denn wir wollen ja Antworten auf unsere Fragen haben.

Google bekommt auch alles, was über Google-Mailadressen ausgetauscht wird. Von persönlichen Nachrichten bis zu Rechnungen, Mahnungen oder Arztterminvereinbarungen. Und wenn ihr einen großen Mailverteiler habt und eine einzige Person davon eine Gmail-Adresse hat, bekommt Google auch die ganze Konversation, in der diese eine Adresse mit drin hängt.

Google bekommt auch alle Informationen darüber, was wir uns auf YouTube anschauen, mit welchem Gerät, wie oft, welche Stellen mehrfach, wo wir Pausen machen, ...

Google stellt auch Services wie »Google Analytics« für private Webseitenbetreiber gratis und für Firmen sehr günstig zur Verfügung und erreicht damit, dass in sehr vielen Webseiten Google Analyseprogramme eingebaut sind, die mitschneiden, was wir auf all diesen verschiedenen Webseiten tun, was wir uns anschauen, was wir wegklicken, was wir uns wiederholt anschauen... Google stellt auch »Google Fonts« bereit. Das sind Schriftarten, die man auf der eigenen Webseite oder dem eigenen Blog einbauen kann, um die Webseite mit besonderen Schriftarten auszustatten. Natürlich wäre es möglich, diese auch direkt auf dem Server der jeweiligen Webseite zu hinterlegen, aber es wurde Menschen er-

folgreich eingeredet, dass die Seite schneller lädt, wenn einzelne Bestandteile von anderen Servern, also extern, geladen werden. So bekommt Google also auch unsere IP-Adresse, denn da müssen sie die Schriftart-Pakete ja hinschicken. So erfahren sie ebenfalls, wann wir eine Seite und deren Unterseiten aufrufen oder wiederkehren, selbst wenn auf dieser Seite kein Google Analytics aber eben Google Fonts eingebettet sind.

Wer in sein Google Konto eingeloggt ist oder sich, ohne die angesammelten Cookies zu löschen, in den Google Account einloggt, bei dem werden all diese Informationen auch mit diesem Account verknüpft.

Google kennt dank vieler Google-Kalender-Nutzer:innen alle unsere Termine, die Geburtsdaten von uns, unseren Freunden und Verwandten inkl. aller Tags und Nicknames, die wir für die Menschen oder Termine verwenden. Auch medizinische Eingriffe, Therapiesitzungen oder »3. Mahnung fällig« werden gespeichert – nicht dass sie das durch die Nachrichten in Gmail-Ordnern nicht ohnehin schon wüssten.

Google bekommt, kurz gesagt, alles mit, was wir im Internet tun. Und falls wir eine Webseite aufrufen sollten, die tatsächlich weder Google Analytics noch Google Fonts eingebaut haben sollte, wir aber den Google Chrome Browser verwenden, bekommen sie diese Information am Ende dennoch. Das Sammeln von Daten in den Google Accounts haben wir schon angesprochen. Zusätzlich sammelt Googles Browser den Browserverlauf der jeweiligen IP-Adresse und kann euch gegebenenfalls über Logins in andere Plattformen oder Services wie den Login mit eurem Google-Konto identifizieren.

Google stellt zudem den Kern seines eigenen Chrome-Browsers, Chromium, als OpenSource-Version für andere Entwickler:innen zur Verfügung. Auch als eigenständigen Browser, den man mit etwas Geschick ohne Google-Dienste als Ungoogled Chromium installieren kann.

Beinahe alle Hersteller verwenden Chromium als Basis für ihre eigenen Browser: Google Chrome, Microsoft Edge, Opera, Vivaldi, Brave, Epic, Blisk… So kommt es, dass 2022 neben Apples Safari-Browser, nur noch Firefox als Browser ohne Google-Technologie im Innern auf dem Markt ist.

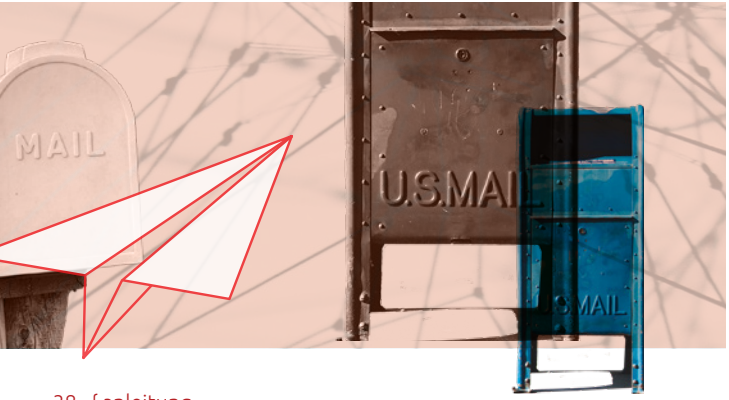
Nur wenige wirklich Google-freie Alternativen

Grundsätzlich funken alle Browser statistische Daten nach Hause, auch Edge und Safari. Wenn einem der Google-Kern egal ist, in dem hoffentlich das direkte Funken zum Mutterhaus unterdrückt wird,

hat man noch Alternativen wie Vivaldi und Brave zur Auswahl, die insgesamt viel Wert auf Privatsphäre und Datensicherheit legen.

Wenn ihr einen wirklich freien Browser verwenden möchtet, so können wir – Stand Frühjahr 2022 – nur Firefox empfehlen. Wobei anzumerken ist, dass dessen Hersteller Mozilla auch von Google Geld bekommt und dafür die Google Suchmaschine als Standard im Firefox Browser einstellt, was sich aber zum Glück in den Browsereinstellungen mit einem Klick ändern lässt (mehr dazu im Kapitel über Suchmaschinen).

Firefox kommt mit einer Menge sinnvoller Funktionen daher. Er blockiert schon in der Werkseinstellung Tracking-Cookies von Drittanbietern und man kann mit weniger als zwei Minuten Aufwand die Datenschutzeinstellungen auf »streng« stellen. Außerdem kann man dafür sorgen, dass Cookies immer bei Beenden des Browsers gelöscht werden und hat damit schon viel für die eigene Privatsphäre getan. Wenn zusätzlich noch Werbeblocker, sogenannte Adblocker, als Browser-Add-ons hinzugefügt werden, kann man das meiste Tracking von sich fernhalten.



Messenger: Alles eine Frage des Anwendungsfalls

Messenger haben in vielen Bereichen Kommunikationsformen wie E-Mail oder SMS erfolgreich abgelöst. Sie sind praktisch, meist kosten sie kein Geld und die Funktionsbreite macht sie für fast alle Einsatzgebiete von kurzen Textnachrichten, über Sprachnachrichten bis hin zum Teilen von Fotos interessant. Wie fast überall wird auf Grund von Gewohnheit, Gruppenzwang oder sofortigem Einsatz entschieden. Die Beschäftigung mit den technischen und ethischen Hintergründen oder der Frage, wer bei unseren Unterhaltungen alles mithört bzw. liest kommt meist zu kurz. Dabei sind gerade dies die entscheidenden Kriterien. Denn unsere Kommunikation geht grundsätzlich niemanden etwas an. Und zu Werbezwecken schon mal gar nicht.

Neben den bekannten Zentral-Messengern großer Konzerne und der Möglichkeit, auf Social Media Direktnachrichten an andere User:innen zu senden, gibt es verschiedene freie Messenger, die im Wesentlichen zwei unterschiedliche Schwerpunkte haben: Sicherheit oder Unabhängigkeit von Unternehmen.

Die Unabhängigen

Für die Einen ist Unabhängigkeit das Steckenpferd. Dazu zählen beispielsweise die Messenger, die das Matrix-Protokoll unterstützen wie etwa Element. Jede:r kann einen eigenen Server hosten, man kann sich aber auch einen Account auf einem bestehenden Server erstellen. Der Verbund aus vielen einzelnen Servern bildet das Rückgrat, auf dem die Kommunikation aller Teilnehmenden stattfindet. Allerdings ist dabei nie klar, wer alles mitliest, da ja jede:r einen eigenen Server betreiben kann. Sind Teilnehmende dieses Servers in eine Kommunikation involviert, läuft eventuell alles bei den jeweiligen Administrator:innen durch. Man sollte also tunlichst immer die Ende-zu-Ende-Verschlüsselung bei allen Matrix-Chats aktivieren. Allerdings verhindert diese nicht, dass die Metadaten der Konver-

sation – also wer mit wem, wann, mit welchem Programm... – den Server-Admins bekannt wird.

Matrix ist kein sicherer Messenger, sondern nur ein autonomer, also mit vielen unabhängig betriebenen und nicht an große Konzerne gebundenen Servern. Man muss den Betreibern genauso vertrauen, wie sonst den Konzernen. Tut ihr das nicht, ist Matrix nicht der richtige Messenger für euch.

Die Sicheren

Dagegen stehen Messenger wie Threema oder Signal, die zwar eine zentrale Server-Infrastruktur haben, deren Fokus aber auf Sicherheit und Integrität der Kommunikation liegt. Sie sind beide nicht auf eine Finanzierung durch Werbetreibende angewiesen. Während Threema einmalig knappe € 3,- kostet und sich somit über Einnahmen durch die Nutzer:innen finanziert, wird Signal durch Regierungen und verschiedene NGOs finanziert. Beide haben es somit gar nicht nötig, Kundendaten zu erheben, zu analysieren, zusammenzuführen und zu verkaufen. Es ist schlicht nicht ihr Businessmodell.

SICHERE MESSENGER

Sichere Messenger nutzen grundsätzlich Ende-zu-Ende-Verschlüsselung. Sie finanzieren sich nicht durch Werbung sondern über Beiträge der Nutzenden oder Spenden.

Der Blick in den Programmcode

Der Code von Threema ist proprietär, also nicht öffentlich einsehbar. Man nennt es auch »Closed Source«, also das Gegenteil von Open Source. Stattdessen haben die Macher ihre Software mehreren Sicherheits-Audits unterziehen lassen. Die Ergebnisse dieser Prüfungen durch unabhängige Expert:innen bestätigen, dass es sich bei Threema um einen sicheren Messenger handelt.

Der Programmcode von Signal ist Open Source und gut dokumentiert. Die Funktionsweise von Signal ist auch im Blog unter signal.org beschrieben. Dort kann man sich auch als Laie einlesen und erfahren, dass Signal nicht die echten Telefonnummern als Identifikation für die Accounts speichert, sondern nur Hashwerte davon – sowas wie Quersummen aus einer bestimmten mathematischen Funktion und der jeweiligen Telefonnummer. Wenn man nach Kontakten auf Signal sucht, wird auch nicht das ganze Adressbuch hochgeladen, sondern nachgeschaut, ob es schon Accounts zu den Telefonnummer-Hashwerten gibt. Und man erfährt auch, dass auf den Servern von Signal keine Daten der täglich vielen Millionen Kommunikationen liegen, das passiert alles nur auf den Geräten der Nutzer:innen. Die einzigen Informationen, die tatsächlich auf den Servern vorhanden sind, sind ob es einen Account zu diesem Hashwert gibt, wann dieser erstellt wurde und das Datum der letzten Verbindung zu den

Signal Servern. Selbst wenn also Behörden Zugang zu Signal-Servern haben sollten, werden sie darauf nichts sehen, außer ob ein Account vorhanden ist. Signal geht mit Behördenanfragen im Übrigen sehr transparent um, wie ihr unter [https://signal.org/bigbrother] nachlesen könnt.

Welchen Messenger – oder auch welche, Plural – ihr verwenden möchtet, richtet sich meistens danach, wozu ihr die Mehrheit eurer Kontakte überreden könnt oder wo vielleicht die meisten bereits Accounts haben. Denkt daran, wirklich kritische Informationen wie Fluchtrouten für Menschen aus Kriegsgebieten oder Ähnliches ausschließlich auf sicheren Messengern zu besprechen.

Nehmt nicht stillschweigend hin, wenn »alle« eben WhatsApp haben. Auch wenn es unbequem ist, sich in einer Gruppe zu äußern und Menschen euch Gegenwind geben. Hier spricht ihre eigene Unsicherheit und vor allem Bequemlichkeit.

Verwendet selbst sichere Messenger und schlagt diese auch immer wieder in Gruppen vor. Bessert Menschen beim Reden aus, wenn ganz automatisch »WhatsApp« gesagt wird, beispielsweise durch »Nachricht« bzw. »Messenger«, um auch sprachlich klarzumachen, dass es sich um nur eine von vielen Lösungen handelt.

Postkarten im Netz

Aus irgendeinem Grund denken wir bei E-Mails an Briefe: gute alte Papierbögen, gefaltet, in Umschläge gesteckt, zugeklebt, mit Briefmarke versehen, abgestempelt und verschickt. Der Geschmack von Briefmarkenkleber liegt uns beim Gedanken an E-Mails förmlich auf der Zunge. Vielleicht, weil alles, was früher in dicken Briefen kam, mittlerweile per E-Mail zugestellt wird; vom Kaufvertrag für eine Immobilie über Rechnungen bis hin zu ärztlichen Gutachten und Befunden.

Doch so einfach ist es leider nicht, wenn es um elektronische Post geht. Wie beim Surfen im Netz passiert auch bei E-Mails eine Datenübertragung. Und genauso kann vorab nicht gesagt werden, wo der Datenverkehr langgehen wird. An jedem Knotenpunkt kann mitgelesen werden, was genau übertragen wird, denn E-Mails sind grundsätzlich nicht verschlüsselt. Es sind Klartext-Nachrichten im Netz. Von der trügerischen Idee zugeklebter Umschläge müssen wir uns – leider! – verabschieden. E-Mails sind nur Postkarten im Netz. Jede:r auf dem Weg zwischen Sender:in und Empfänger:in kann lesen, was auf der Postkarte steht. Und die Anhänge natürlich ebenso.

Wer zahlt für den E-Mail-Account?

Das Mitlesen fängt dabei schon bei den E-Mail-Betreibern an. Gmail, GMX, web.de, Microsoft, Yahoo und alle anderen »Gratis«-Anbieter müssen die tausenden Server und den Strom dafür genauso wie ihre Angestellten von irgendwas bezahlen. Die einfachste Art ist durch Werbung. Und dafür lesen sie mit, was ihr schreibt oder bekommt. Sie werten diese Informationen aus und verkaufen euer Personenprofil und den passenden Werbeplatz an Werbetreibende. Bekommt ihr eine Rechnung von Stromanbieter A, kriegt ihr Werbung für Anbieter B am Rand eures Postfachs angezeigt oder bekommt sie als E-Mail direkt in euer Postfach. Manche blenden auch Werbung in E-Mails ein, die ihr versendet. Dann sehen eure Freunde

in eurer Nachricht Werbung für irgendein Produkt oder eine Dienstleistung, worauf ihr keinen Einfluss habt. Anders gesagt: Die Anbieter manipulieren eure Inhalte zu ihrem Profit. Ihr zahlt kein Geld für das Konto, weil andere ihnen Geld für eure Informationen, eure Aufmerksamkeit und den Zugang zu euren Augen und Ohren geben. Einige Lösungen dafür zeigen wir euch weiter unten.

VERTRAUENSWÜRDIGE E-MAIL-ANBIETER

Vertrauenswürdige Anbieter, die nicht eure gesamte Kommunikation auswerten, gibt es glücklicherweise immer mehr. Posteo.de, Mailbox.org und Tutanota sitzen alle in Deutschland und sind ab € 1,- pro Monat zu haben. So finanziert ihr den Dienst mit einem überschaubaren Beitrag und könnt sicher sein, dass auch bei E-Mails eure Inhalte euch gehören. Kalender und Adressbuch sind bei allen Anbietern gleich mit dabei und werden auf den Servern der Anbieter auch sicher verwahrt.

Achtung! Wenn in der Konversation Menschen mit Accounts bei Gmail, GMX und Co. dabei sind, liegen eure Gespräche, ebenso wie die Anhänge dann doch wieder auch bei diesen Anbietern.

Sprecht mit den anderen darüber. Nur durch stetiges Zursprachebringen können wir etwas bewegen.

Der Weg einer E-Mail

Wir stellen uns bei E-Mails vor, dass wir auf Senden klicken und am anderen Ende macht es Pling. Dazwischen liegt Magie. Oder wahlweise auch einfach Nichts. Dabei müssen auch die Bits und Bytes einer E-Mail und ihrer Anhänge ganz physisch von A nach B kommen. Üblicherweise über viele Kabel und einer Menge strombetriebenen Blechs in verschiedenen Rechenzentren irgendwo auf dem Planeten.

Gehen wir den Weg einer E-Mail einmal mit: Ihr schreibt sie auf eurem Gerät im E-Mail-Programm oder eurem Browser und von dort wird sie losgeschickt. Als nächstes kommt sie in den Postausgangsserver bei eurem Anbieter. Der schickt sie über eine vorab unbekannte Route von Kabeln und verschiedenen Servern durch das Internet zum Posteingangsserver beim Anbieter des oder der Empfänger:innen. Von dort kommt sie dann wieder auf das Gerät der Empfänger:innen.

Alles zwischen den Postausgangs- und -eingangsservern ist El Dorado, Wilder Westen für alle, inklusive Krimineller. Hier kann es viele »Men in the Middle« oder »Machines in the Middle« geben, die alles mitlesen, was ihr schickt oder bekommt. Wer dahinter steckt, kann sich ändern, je nachdem, welchen Weg eure E-Mail nimmt.

Alles ehrlich transportverschlüsselt

Manche E-Mail-Anbieter werben mit »TLS-Verschlüsselung«, wodurch die E-Mails bei ihnen sicher übertragen würden. Aber TLS ist nur eine Transportverschlüsselung. Sie greift nur auf der »ersten

und letzte Meile«. Damit meinen wir den Weg zwischen dem Gerät der Absender:innen und dem Postausgangsserver und dann wieder zwischen dem Posteingangsserver der Empfänger:innen und deren Gerät. Hier wird die Postkarte quasi getunnelt wie eine Rohrpost, bei der niemand von außen darauf zugreifen kann. Aber alles dazwischen, das ganze El Dorado, bleibt davon völlig unbeeindruckt und unberührt. TLS hat mit echter E-Mail-Verschlüsselung nichts zu tun.

DAS SCHLÜSSELPAAR

Das Schlüsselpaar könnt ihr euch so vorstellen: Der eine schließt immer nur in die eine Richtung ab, der andere immer nur in die andere Richtung auf.
Der private Schlüssel ist der, der aufschließt. Wichtig: Der private Schlüssel bleibt immer bei euch. Den braucht ihr, um E-Mails an euch entschlüsseln zu können.
Der öffentliche Schlüssel ist, wie der Name verrät, für die Öffentlichkeit bestimmt. Das ist der, der zuschließt und den andere brauchen, um Nachrichten an euch »zuschließen«, also verschlüsseln zu können. Den könnt ihr beispielsweise auf eure Webseite stellen, damit andere, die euch verschlüsselte Nachrichten schicken möchten, diesen öffentlichen Schlüssel runterladen und in ihrem E-Mail-Programm verwenden können.

E-Mail-Verschlüsselung

Bei echter E-Mail-Verschlüsselung wird der Inhalt der E-Mail ebenso wie eventuelle Anhänge in Zeichensalat verwandelt, der nur durch den passenden Schlüssel auf Seiten der Empfänger:innen wieder in lesbaren Text zurückübersetzt werden kann. Das bedeutet, dass noch immer auf dem Weg alle in die E-Mail hineingucken können, aber sie sehen nur noch den Zeichensalat und keinen lesbaren Text mehr. Aber das Problem ist, dass eben alle Kommunikations-Parteien bei sich E-Mail-Verschlüsselung im Mailprogramm installiert und eingerichtet haben müssen.

Falls ihr es ausprobieren möchtet, empfehlen wir Mozilla Thunderbird als E-Mail-Programm zu verwenden. Das hat E-Mail-Verschlüsselung bereits fest eingebaut und ihr müsst nichts extra installieren. Ihr findet die Funktion unter Extras und dann OpenPGP Schlüssel einrichten.

Die Einrichtung von E-Mail-Verschlüsselung läuft recht einfach. Euer E-Mail-Programm erstellt für euch ein Schlüsselpaar: einen privaten und einen öffentlichen Schlüssel. Für das Schlüsselpaar vergebt ihr ein Passwort. Wenn ihr dann noch die öffentlichen Schlüssel der anderen Gesprächsteilnehmer:innen habt, seid ihr auch schon startklar.

Wichtig: Speichert das Passwort für euer Schlüsselpaar in eurem Passwortmanager. Exportiert die Schlüssel als Datei und speichert sie nochmal extra auf einem passwortgesicherten USB-Stick, damit ihr sie jederzeit habt, auch falls euer Rechner kaputtgeht. Ihr braucht die Schlüssel und das Passwort, um E-Mails zu entschlüsseln, die ihr verschlüsselt bekommen habt.

Wenn ihr in eurem E-Mail-Programm eine E-Mail schreibt, könnt ihr dort mit einem Klick anhaken, dass diese Nachricht nun verschlüsselt an die Empfänger:innen verschickt werden soll. Bei den meisten Mailprogrammen müsst ihr das auch nur beim ersten Mal anhaken Sobald für die Empfänger:innen öffentliche Schlüssel im Mailprogramme hinterlegt sind, ist die Option für verschlüsselte E-Mails an diese Empfängerinnen vorausgewählt. Allerdings wird eine E-Mail nur dann verschlüsselt versendet, wenn für alle Empfänger:innen öffentliche Schlüssel vorliegen. Ein Misch-Versand ist nicht möglich. Zum Absenden gebt ihr das Passwort für das Schlüsselpaar ein und das war es.

Wenn ihr verschlüsselte Nachrichten bekommt, läuft es ähnlich unspektakulär: ihr werdet aufgefordert, das Passwort für das Schlüs-

selpaar einzugeben und daraufhin wird euch der Inhalt der E-Mail angezeigt.

Pro-Tipp: Erstellt gleich zu Beginn auch ein Widerrufszertifikat für euer Schlüsselpaar und sichert es in eurem Passwortmanager und auch auf dem USB-Stick mit euren Schlüsseln. Sollte euer Laptop gestohlen werden oder Dritte auf andere Art eurer E-Mail-Schlüssel habhaft werden, braucht ihr dieses Widerrufszertifikat, um das Schlüsselpaar für ungültig zu erklären. So wird Empfänger:innen von verschlüsselten E-Mails mit diesem Schlüsselpaar eine Warnung angezeigt, dass sich möglicherweise jemand fälschlich als euch ausgibt.

Die schnelle, vermeintliche Gratislösung kann weitreichende Folgen haben, immerhin gebt ihr dem Anbieter eurer Wahl meist eure gesamte Kommunikation in die Hand. Verwendet nicht blindlings das, was alle anderen nehmen oder den schnellen Tipp zwischen Tür und Angel.

Nehmt euch ein paar Minuten Zeit und überlegt, welchem E-Mail-Anbieter ihr vertrauen möchtet. Vergleicht die Angebote von Posteo, Tutanota und Mailbox.org und entscheidet euch aufgrund ethischer und sozialer Kriterien.

Die magische Wolke, die all unsere Probleme löst

Anbieter versprechen uns die beste Erfindung seit geschnittenem Brot: Zu wenig Festplattenplatz? Cloudspeicher! Zu schwachbrüstiger Computer zum Zocken aber halbwegs schnelles Internet? Cloudgaming! Mit anderen an ein und demselben Textdokument arbeiten, ohne es ständig per E-Mail hin und her schicken zu müssen? Cloud-Office! Keine teure Grafik-Suite kaufen wollen? Software as a Service – natürlich ebenfalls in der Cloud. Dazu noch lückenlose Synchronisation all unserer Adressbücher, E-Mails, Podcatcher, Nachrichten-Apps und Fotos? Cloud-Services machen es möglich!

Aber was ist diese magische Wolke, die all unsere Probleme löst? Wo gehen die vielen Milliarden Gigabyte an Daten, die auf unseren Geräten »zuviel« sind, denn hin? Irgendwo in eine ominöse Wolke, die man nicht sieht und die man nicht fühlt. So wie die Daten selber auch. Aber wohin genau? Und wem gehören sie denn, wenn sie nicht oder nicht mehr auf unseren Rechnern liegen?

Alles, was so klingt, als wäre es zu gut, um wahr zu sein, ist es üblicherweise auch. Das haben wir vermutlich alle schon von unseren Großeltern gelernt. Und so ist es auch im Falle der ominösen Wolke.

Knapp gesagt: »Die Cloud« gibt es nicht. Es liegt alles auf massivem Blech irgendwo in Rechenzentren auf diesem Globus und wir greifen über tausende Kilometer lange Kabel unter Aufwand von viel Strom darauf zu. Die Cloud ist ein Mythos, ein Werbeversprechen.

THERE IS NO CLOUD
»There is no Cloud, just other people's computers.«
(Free Software Foundation Europe)

Rechner anderer Leute

»Es gibt keine Cloud, nur die Rechner anderer Leute«, wie es die Free Software Foundation Europe so treffend formulierte. Wenn unsere Daten nicht bei uns, sondern auf den Rechnern anderer Leute liegen, dann kann es schnell problematisch werden. Alle US-Cloud-Speicher beispielsweise scannen automatisiert unsere Daten, da die Betreiber verpflichtet sind, sich an amerikanisches Recht zu halten, das besagt, dass in den USA illegale Inhalte nicht auf ihren Servern gespeichert werden dürfen. So passierte es 2018, dass der Fall einer Pornodarstellerin durch die Medien ging, deren Werbematerial, das sie zum leichteren Teilen in die Google Cloud gelegt hatte, von Google gelöscht worden war [https://www.pcwelt.de/article/1169692/google-pornografische-inhalte-aus-drive-geloescht.html]. Pornographie ist in den USA illegal, also werden die Inhalte automatisiert gelöscht, da sich auch der Betreiber der Cloud-Dienste rechtlich absichern muss. Für uns heißt das, dass all unsere Daten automatisiert gescannt und auf ihre Inhalte analysiert werden. Deren Rechner, deren Regeln.

Meine Daten, deren Daten

Daher solltet ihr auch immer vorsichtig sein, wenn ihr Daten von Anderen irgendwo hochladet. Sei es euer Adressbuch, die Fotos und Videos oder auch Textnachrichten. Was brisante Inhalte sind oder nicht, entscheidet meist nicht ihr, sondern im Zweifelsfall die Rechtsprechung in dem Land, in dem eure Daten liegen. Und wem sie dort gehören, ist nochmal eine ganz andere Frage. Hier in Europa sind wir sehr verwöhnt, was Dateneigentum angeht. Hier gehören die Daten uns und wir haben die Möglichkeit, zumindest zu klagen, falls die Daten abhanden kommen oder missbräuchlich verwendet werden, falls wir es denn merken oder gesagt bekommen. In den USA ist die Lage anders. Da gehören die Daten den Unternehmen und durch das Akzeptieren der AGB stimmt ihr zu, dass sie die Daten auch kommerziell verwenden, an Dritte weitergeben oder weiterverkaufen etc. Wenn Meta, ehemals Facebook, eines eurer Instagram-Bilder nimmt, es abdruckt und damit Geld verdient, muss der Konzern euch weder Bescheid geben, noch dafür entlohnen, denn ihr habt die Lizenz zur kommerziellen Nutzung bereits erteilt. Und in China gehören die Daten dem chinesischen Staat; das betrifft Apps wie TikTok.

Eure eigene Cloud

Es gibt für einen Teil der unterschiedlichen Cloud-Services gute und praktikable Alternativen. Ganz vorne weg: eine eigene NextCloud. Die gibt es für kleines Geld um die drei bis fünf Euro im Monat und sie erschlägt euch mit einem Streich eine ganze Menge Probleme. Mieten könnt ihr sie bei europäischen Anbietern wie Ausstellungs-Koop, oder auch Windcloud.de. Falls ihr selbständig seid und die NextCloud auch beruflich benutzt, bekommt ihr bei diesen Anbietern auch einen Auftragsverarbeitungsvertrag (AVV) nach DSGVO.

Eure NextCloud ist euer eigener Cloud-Speicher, hat aber noch eine ganze Menge weiterer Funktionen. Ihr könnt wie bei den datenschnorchelnden Konkurrenzprodukten Ordner auf eurer Festplat-

te automatisch synchronisieren lassen. Oder alle Fotos und Videos vom Telefon automatisch sichern. Ihr könnt große Dateien über eure NextCloud mit anderen teilen und damit Dienste wie WeTransfer ersetzen.

Die NextCloud bietet auch ein eingebautes Adressbuch, das ihr statt dem vom Hersteller voreingestellten ebenfalls zum Synchronisieren eurer Kontakte verwenden könnt. Einen eingebauten Kalender gibt es ebenfalls, der alle Funktionen wie Kalenderfreigabe etc. ebenso anbietet wie die bekannten Konzern-Produkte.

Mit ein paar Klicks könnt ihr eurer NextCloud auch Umfragen und Formulare hinzufügen. Das geht mit sogenannten Plugins, also Zusatzfunktionen, die man einfach installieren kann. Es gibt auch ein Plugin, das eurer NextCloud ein ganzes Cloud-Office vergleichbar mit Google Workspace hinzufügt. Das kostet keinen Euro mehr und alle Dokumente sowie eure und auch die Daten aller, die mit euch gemeinsam an Texten arbeiten, bleiben auf eurem eigenen Server.

Verwendet nicht unhinterfragt alles, was ohne Geldzahlung vermeintlich gratis im Netz an Services zu kriegen ist.

Schaut einmal, was in eurer Umgebung alles Cloud-Services sind und wo bei denen die Daten liegen. Überlegt, ob euch dies recht ist. Schaut euch die meist vorhandenen datensparsamen Alternativen an, bei denen die Daten in jedem Fall euch gehören. Und besorgt euch eine große Festplatte für ein Backup eurer Daten, das dann in einer Schublade liegt und nicht »irgendwo in der Cloud«.

Suchen und Finden

Zu unserer Suchmaschine sind wir immer ehrlich, denn wir wollen ja passende Ergebnisse angezeigt bekommen. Dabei geben wir allerlei höchstpersönliche Informationen preis. »Wo gibt's ...“, Testberichte, Adressen, Erdbeeren richtig gießen, sexuelle Vorlieben, Familienanwalt, Schuldnerberatung, psychologischer Notfalldienst, Symptome, Verläufe und Heilung von Krankheiten.

Unsere Suchmaschine weiß eine Menge über uns. Und in den allermeisten Fällen ist das Google, was mit über 90 Prozent Marktanteil eine deutliche Monopolstellung hat [https://gs.statcounter.com/search-engine-market-share]. Google weiß durch unsere Suchanfragen so einiges von der Gesellschaft, das sich in den Trends der Suchanfragen spiegelt. Aber sie wissen auch verdammt viel über jede:n Einzelne:n von uns. Wenn wir ein Google-Konto haben, werden unsere Suchanfragen damit verknüpft. Haben wir keines, erstellt Google von sich aus ein Schattenprofil über uns und ordnet diesem unsere Suchanfragen zu [https://reclaimthenet.org/google-is-building-shadow-profiles-of-its-users-tech-company-oracle-claims].

Was alles nur aus unseren Suchanfragen über uns und unser Leben rekonstruiert werden kann, zeigt die Dokumentation »Made to Measure« sehr eindrücklich. Sie ist eine echte Empfehlung.

The Power of Default

Wie es dazu kommt, dass Google fast alle unsere Suchen bekommt? Weil Menschen gar nicht mehr wissen, dass es andere Suchmaschinen gibt. Das ist ein sich selbst verstärkender Effekt. Dazu geführt hat, dass Google als Standardsuchmaschine fast überall voreingestellt ist. In Googles eigenen Chrome und Chromium Browsern. Auf den Google Android Telefonen, die den Großteil aller Smartphones in der Welt ausmachen, ohnehin. Aber auch in anderen Browsern wie Safari auf MacOS und in iOS Geräten. Und im Firefox Browser;

durch das Geld, das Mozilla von Google für diese »Kooperation« erhält, kann der Firefox Browser überhaupt betrieben und weiterentwickelt werden.

Was passiert, wenn wir »googlen«?

Wenn wir eine Suche auf Google oder in eines der vielen Google-Suchfelder irgendwo eingeben, verlässt diese Suchanfrage den Google-Server nie. Wir machen einfach eine Datenbankabfrage bei Google. Die Ergebnisse sind nicht objektiv. Oben bekommen wir »Ergebnisse«, für die andere bezahlen, dass sie uns angezeigt werden (nicht, weil sie so super zu unserer Anfrage passen). Weiter unten sehen wir, was inhaltlich laut Google Algorithmen wohl zu unserer Frage passt. Dieses Ergebnis wird kombiniert mit dem Profil, das Google über uns hat. Deshalb kann es sein, dass euch andere Ergebnisse angezeigt werden als euren Freund:innen oder Familienmitgliedern, auch wenn ihr nach den selben Stichworten gesucht habt.

Suchmaschinen – was gibt es eigentlich?

Suchmaschinen unterscheiden sich durch den Suchablauf. Das ermöglicht uns eine Unterteilung in verschiedene Typen.

Indexsuchmaschinen

Google ist eine Index-Suchmaschinen, so wie alle »großen« Anbieter, die es heute im Netz gibt. Sie pflegen seit vielen Jahren einen eigenen Suchindex, also eine eigene Datenbank. Indizes aufzubauen und zu pflegen ist sehr aufwändig und teuer. Daher gibt es sehr wenige Suchindizes auf der Welt. Und große noch weniger.

Proxysuchmaschinen

Proxysuchmaschinen haben keinen eigenen Suchindex. Das bedeutet, sie nehmen unsere Anfragen auf ihrer eigenen Webseite oder in ihrem Suchfeld entgegen, geben diese aber an einen der großen Suchindex-Anbieter weiter. Häufig sind das Google oder Bing von Microsoft. Das Ergebnis zeigen sie uns dann wieder auf ihrer eigenen Webseite an. Dazu zählen beispielsweise Ecosia und Startpage. Vom Standpunkt des Datenschutzes haben sie einen Vorteil. Durch die Proxy-Funktion, also die Vertretungs-Funktion, geben diese Suchmaschinen nur ihre und nicht unsere IP-Adressen weiter. Nachdem sie ihre Anfragen aber an Google weiterleiten, befeuern sie trotzdem das Geschäftsmodell des Konzerns.

Metasuchmaschinen

Es gibt Suchmaschinen, die reichen die Suchanfrage nicht an eine einzige Suchmaschine weiter, sondern an mehrere. Das macht die Ergebnisse vielfältiger und somit in der Zusammenstellung auch tendenziell objektiver. Hierunter fällt beispielsweise Metager.

Hybride Suchmaschinen

Einige Betreiber bauen mittlerweile eigene Suchindizes auf. Da dies aber nicht nur Kosten verursacht, sondern auch lange dauert, nutzen sie ein hybrides Modell. Sie durchsuchen ihren eigenen, wachsenden Index und geben die Anfrage auch an andere Suchmaschinen weiter. Die Ergebnisse sind dann aus beiden Quellen kombiniert. Dies trifft auf z. B. DuckDuckGo zu, die mit DuckDuckBot einen eigenen Crawler haben, der das Internet indexiert. Gleichzeitig bedienen sie sich am Suchindex von Bing, u. a. auch für die Übersetzungsfunktion. Auch Qwant baut einen eigenen Suchindex auf. Allerdings zeigen sie auch die bezahlten

»Treffer« von Bing und arbeiten dem US-Konzern Microsoft zu [https://news.microsoft.com/europe/features/qwant-and-microsoft-announce-an-exclusive-partnership-for-a-unique-internet-research-experience].

Weitere Suchmaschinen
Darüber hinaus gibt es auch noch verteilte bzw. föderierte sowie Peer-to-Peer-Suchmaschinen als dezentral gedachte Ansätze. Außerdem existieren Spezialsuchmaschinen für Bilder, Adressen, Preise, Flug- & Bahnverbindungen...

Der Index macht's

Letztlich greifen alle Suchmaschinen auf die ein oder andere Weise auf einen oder mehrere Suchindizes zu. Allerdings gibt es davon nur vier große auf der Welt: Google und Bing in den USA, Yandex in Russland und Baidu in China. In Europa haben wir keinen eigenen Suchindex. Das sollte uns immer bewusst sein, wenn wir uns auf Suchergebnisse verlassen. Denn die uns angezeigten Treffer sind immer durch die kulturelle und politische Brille des Landes gefärbt, in dem der jeweilige Betreiber sitzt. Und was in ihren Datenbanken verzeichnet und zum Anzeigen freigegeben ist, ist nicht nur eine Frage der darunterliegenden Technik, sondern auch unternehmerischer und politischer Interessen.

SUCHINDIZES

Auf der Welt gibt es nur vier große Suchindizes:

- *Google (Alphabet, USA)*
- *Bing (Microsoft, USA)*
- *Yandex (Russland)*
- *Baidu (China)*

Es stimmt, es gibt keinen europäischen Suchindex. Einige kleinere Betreiber bauen eigene Indizes auf, greifen aber zugleich – voraussichtlich noch über Jahre – auch auf mindestens einen der Großen zurück.

Grundsätzlich tun wir gut daran, unsere Suchanfragen nicht oder nur zu einem kleinen Teil an Google zu geben, schon allein, um der Monopolstellung etwas entgegen zu setzen. Allerdings: Die eine perfekte Suchmaschine gibt es nicht. Je nach Anwendungsfall oder Suchbegriff kann es sinnvoll sein, auf mehreren Suchmaschinen danach zu suchen. Beispielsweise, wenn es um Faktenchecks geht.

FAKTENCHECKS

Faktenchecks haben einen anderen Fokus als privatsphäreschonendes Suchen. Hier geht es darum, die Quellen bestimmter Nachrichten zu finden, Bilder zu vergleichen, herauszufinden, ob ein Bild wirklich von einem bestimmten Ort und aus einer bestimmten Zeit stammt oder ob es vielleicht schon viel älter (oder auch jünger) ist etc. Bei Faktenchecks werden Suchen über verschiedene Anbieter und Indizes verteilt, um eine möglichst breite Faktenbasis zu erschließen.

Mehrere Suchmaschinen benutzen

Privatsphäreschonendes Suchen ist möglich. Ihr könnt sowohl in eurem Browser als auch auf euren Mobilgeräten die Standardsuchmaschine ändern. Beispielsweise auf DuckDuckGo, die zumindest keine Personenverknüpfung eurer Suchanfragen vornimmt und es damit auch keine Such-History über euch gibt. Das geht in jedem Browser, wir erklären es hier anhand des Firefox Browsers.

Zum Ändern der Standardsuchmaschine geht ihr beim Desktop-System in die Einstellungen und dort auf Suche. Ihr könnt aus einigen vorinstallierten Suchmaschinen auswählen und auch weitere hinzufügen.

Um eure Suchen auf verschiedene Anbieter anlassbezogen zu verteilen könnt ihr im Firefox die Suchleiste zur Symbolleiste hinzufügen und dort mit einem Klick eine eurer eingestellten Suchmaschinen einmalig für die jeweilige Suche verwenden.

Auf Mobilgeräten könnt ihr die Suchmaschine in den Einstellungen der jeweiligen Browser-App ändern. Beispielsweise im mobilen Firefox unter Einstellungen und dann Suchmaschine.

Ausnahme ist der DuckDuckGo Browser, bei dem ist die gleichnamige Suchmaschine fest eingebaut.

Vertraut nicht blind den Voreinstellungen eurer Geräte. Nutzt nicht unhinterfragt Suchmaschinen, weil sie hübsch aussehen oder irgendwelche Versprechen machen.

Hinterfragt die Geschäftsmodelle der Suchmaschinen, die ihr verwendet, und wen sie wirklich stärken. Überlegt euch, welche eine gute Standardsuchmaschine für euch sein kann und stellt diese als Standard auf all euren Geräten ein. Überlegt euch weitere Suchmaschinen, die in speziellen Fällen für euch interessant sein können, und richtet auch diese in eurem Browser damit ein.

Social Media

Soziale Medien sind aus der heutigen, globalisierten Welt kaum mehr wegzudenken. Abgesehen von allen Problemen wie Hatespeech, Mobbing, sich immer schneller überschlagenden Diskussionen, Trollen …, können wir uns zumindest darauf einigen, dass soziale Medien die Art, wie wir als Gesellschaft kommunizieren, nachhaltig verändert haben. Kommunikation ist – zumindest von der Idee her – demokratischer geworden. Menschen können mitreden, können auch mit »den ganz Großen« auf Social Media kommunizieren.

Allerdings haben soziale Medien neben den genannten gesellschaftlichen Problemen, noch einen Rattenschwanz weiterer Tücken.

Wer sind die Kunden?

»Wenn Du für einen Service nichts zahlst, bist Du das Produkt.« Diesen Satz haben wir alle schon gehört. Aber er ist schwammig, das Problem nicht greifbar.

Dass soziale Medien ohne Betriebskosten wie Rechenzentren, Strom für die Server, Lohn für die Menschen, die sich um den Betrieb kümmern etc. nicht laufen können, dürfte allen klar sein. Irgendwoher muss das Geld also kommen, das die Maschinerie am Laufen hält und dafür sorgt, dass sie weiter wächst und einzelne Menschen damit unermesslich reich werden.

»Werbefinanziert« sagt sich schnell, doch was bedeutet das? Das €10-Budget für die Werbung des Garagenflohmarkts im Dorf wird es wohl nicht sein; oder nur zu einem verschwindend geringen Teil. Im Kapitel »Versprechen« sprachen wir schon von den Kampagnen, bei denen Social Media Advertising, also Werbung in sozialen Medien, ein Baustein ist. Manche Werbung läuft vorwiegend oder auch ausschließlich in sozialen Medien. Hier sitzt das große Geld. Bei der Werbeindustrie, den Unternehmen und Konzernen, die diese Klaviatur bedienen. Und bei denjenigen, die politische Werbung machen. Sie sind diejenigen, die Geld für die Services der Social-Media-Plattformen zahlen. Sie sind die Kunden.

Einarmige Banditen

Wir Nutzer:innen sind das – Verzeihung – Klickvieh, das ihr Geschäftsmodell am Laufen hält. Wir werden auf den Plattformen gehalten in der Illusion, uns dort selbstbestimmt zu unterhalten. Unsere grundlegenden Hirnfunktionen werden gegen uns ausgespielt. Der kleine Kick für neue Follower und Likes. Gamification, alles ist ein Spiel, nur dass es eben keines ist, sondern wir als menschliche Wesen den Kampf gegen die Algorithmen der Werbeindustrie und Social-Media-Plattformen längst verloren haben, noch ehe wir wussten, dass es ihn gibt. Im Wettlauf der Industrie gegen uns geht es darum, wer

von ihnen noch tiefer in unser Stammhirn dringt, noch weiter vorn in unserer unbewussten Entscheidungskette ansetzt. Unser menschliches Gehirn ist den Mechanismen, die gegen uns eingesetzt werden, nicht gewachsen. Und während wir noch ein Mittagessen-Foto liken, das Paar rote Schuhe in der Seitenleiste für ein Schnäppchen halten und nächsten Monat das neue Mobiltelefon, sind wir schon lang schachmatt. Wir wischen für das schnelle Glücksgefühl immer wieder nach unten, als wären unsere Geräte einarmige Banditen und nichts, was uns eigentlich unterstützen sollte.

Dark Patterns

Wir Menschen sind an sich ja nicht doof. Menschen haben die Mathematik erfunden, bauen Jahrhunderte überdauernde Bauwerke, komponieren hochkomplexe Musikstücke und fliegen ins Weltall. Was also macht uns so dumm, das Spiel mitzuspielen und es nicht einmal zu merken? Dahinter stecken sogenannte Dark Patterns, versteckte Muster oder auch Tricks, die uns zum Klicken oder auch unüberlegten Zustimmen bewegen. Vorab angehakte Checkboxen bei Cookie-Bannern sind ein Beispiel dafür. Oder auf mehreren Unterseiten von Cookiebannern versteckte vorausgewählte Zustimmungen für »berechtigte Interessen«. Es geht aber noch perfider:

Werbebildchen, die auf Mobilgeräten ausgespielt werden und die so aussehen, als wäre ein Haar auf dem Display. Das soll uns zum Klicken bzw. Wischen des Telefon-Touchscreens bringen [https://twitter.com/rcalo/status/1519019029494571010].

Die Dokumentation des Centers for Humane Technology: »The Social Dilemma« / »Das Dilemma mit den sozialen Medien« ist eine ganz große Empfehlung. Sie macht uns deutlich, wie weitreichend das Problem tatsächlich ist.

DAS PRODUKT

»Das Produkt ist die allmähliche, leichte, unmerkliche Veränderung unseres eigenen Verhaltens und unserer Wahrnehmung. […] Es ist das einzig mögliche Produkt. […] Das ist das Einzige, mit dem sie Geld verdienen können: Ändern, was wir tun, wie wir denken, wer wir sind. Es ist eine sachte, allmähliche Veränderung. Wenn Sie zu jemandem gehen und sagen: »Geben Sie mir 10 Millionen Dollar, und ich werde die Welt um ein Prozent in die Richtung verändern, in die Sie sie verändern wollen …« Das ist die Welt! Das kann unglaublich sein, und das ist eine Menge Geld wert.« (Jaron Lanier, in: »The Social Dilemma«/»Das Dilemma mit den sozialen Medien«, 2020)

Bewusster und verantwortungsvoller Umgang

Auf Social Media zu verzichten ist für viele keine Option und die Möglichkeit der Partizipation ist ein gewichtiger Grund dagegen. Wenn uns nichts anderes übrig bleibt, als auf den Zentralplattformen wie Instagram, Twitter oder Facebook zu bleiben oder auch YouTube zu verwenden, dann sollten wir uns der Probleme dieser Plattformen bewusst sein. Die algorithmisch gesteuerten Timelines formen unsere Welt, unser soziales Gefüge und sie bestimmen, mit wem wir in Kontakt sind und mit wem vielleicht auch nicht mehr.

Vor dem gedankenlosen Teilen von Inhalten – seien es aufregend klingende Überschriften oder auch lustige Psychotests – macht drei Sekunden Pause, atmet tief durch und fragt euch, ob ihr das wirklich teilen wollt. Macht Faktenchecks, geht sicher, dass ihr nicht nur Opfer und Weiterbetreiber einer Schneeball-Maschinerie werdet.

Alternativen

Wir haben aber auch die Möglichkeiten, Alternativen zu verwenden. Seit Elon Musks Angebot Twitter zu kaufen, kam ein regelrechter #Twexit in Gang und das schon seit 2016 bestehende Fediverse [https://de.wikipedia.org/wiki/Fediverse] erfreute sich schlagartig ungeahnter Beliebtheit. Tagelang waren alteingesessene Fediverse-Nutzer:innen damit beschäftigt, den Neuankömmlingen Hilfestellung zu leisten, sich in diesem doch recht anderen Netzwerk zurecht zu finden.

Das Fediverse funktioniert ein bisschen wie E-Mail: Egal, auf welchem Server ihr euren Account habt, ihr könnt mit allen anderen kommunizieren, ihnen folgen, kommentieren...

Alle Fediverse-Plattformen haben ausdrücklich keine algorithmisch gefilterte Timeline. Das heißt, alle Posts und Meinungen stehen damit gleichberechtigt nebeneinander und die Diskussion wird nicht von denen dominiert, die die meisten Follower und die größte Reichweite haben. Bei Befragungen wird dies immer wieder positiv hervorgehoben und ist der Hauptgrund, warum Menschen das Fediverse nutzen. Klassische Werbung ist verpönt. Die Menschen dort sind an echtem Austausch und gegenseitigem voneinander Lernen interessiert. Social Media, aber eben wirklich sozial.

Finanziert werden die einzelnen Server zum Großteil durch Spenden der Community. Einige werden auch von Universitäten, Stadtverwaltungen und öffentlichen Stellen betrieben. Der Großteil wird allerdings durch Freiwillige organisiert und betreut, die das in ihrer Freizeit tun.

FEDIVERSE

Das Fediverse ist ein Verbund verschiedener sozialer Netzwerke. Mit einem einzigen Account kann man allen anderen folgen und bekommt die Posts von all den unterschiedlichen Plattformen in der eigenen Timeline angezeigt.

Es gibt Alternativen für die meisten beliebten Plattformen:

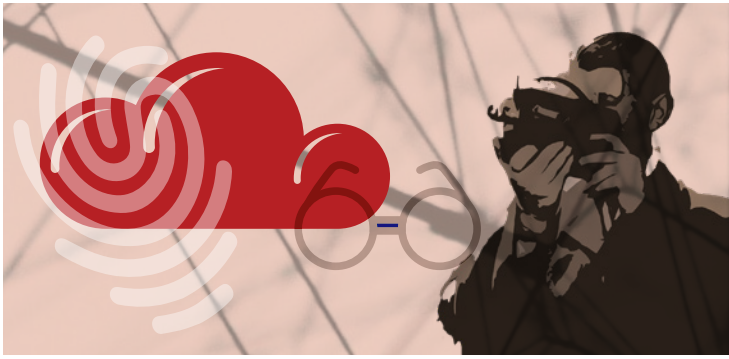
- *Mastodon (statt Twitter/Facebook)*
- *Pixelfed (statt Instagram)*
- *Funkwhale (statt Soundcloud)*
- *Peertube (statt YouTube/Vimeo)*
- *Mobilizon (statt Facebook-Gruppen & -Events)*
- *Bookwyrm (statt Goodreads/Lovelybooks)*
- *Blogs im Fediverse: WriteFreely, Plume & ActivityPub Plugin für WordPress*
- *Podcast-Hosting im Fediverse: Castopod*

Verwendet nicht unhinterfragt die großen Plattformen mit klar kommerziellen Interessen und algorithmisch gefilterter Timeline.

Seid Euch der stetigen Manipulation bewusst. Überlegt Euch, wo und wie Ihr Eure Zeit verbringen möchtet. Legt Euch versuchsweise einen Fediverse-Account an und probiert, ob dies für Euch eine lohnende Alternative darstellt. Ein guter Einstieg dazu ist ein Account auf einem der zahlreichen Mastodon-Server [https://joinmastodon.org/communities].

Es streamt so schön …

… wenn wir Vertrauen in die Anbieter haben können.



Streamingdienste beherrschen die Medienwelt. Musikstreaming hat in den letzten Jahren sowohl lineares Radio als auch CDs weitenteils verdrängt. Aber vor allem Videoinhalte sind beliebt, wie Nachrichten, Anleitungsvideos, Video-Blogs/Vlogs, Serien, Filme, Dokumentationen, Lernvideos, Musikvideos, Videos zu Gesundheitsthemen, Testberichte und mehr.

Streamingdienste wie Netflix, Amazon Prime, Apple TV+, Disney Plus, die Video-on-Demand-Dienste der Internetanbieter etc. sind mittlerweile die Haupt-Unterhaltungsquelle für Viele. Lineares Fernsehen hingegen scheint auszusterben, während die Mediatheken der Sender, insbesondere auch der öffentlich-rechtlichen, sich großer Beliebtheit erfreuen. Dass Video Trend ist, zeigt nicht zuletzt auch der Umschwung, den der Facebook-Mutterkonzern vor einer Weile seinem bis dahin reinen Bilderdienst Instagram zukommen ließ und ihn kurzerhand zur Videoplattform ernannte.

Doch wie überall, haben auch Streamingdienste einen ziemlichen Rattenschwanz. Denn was wir uns anschauen – oder im Falle von Musik oder »Pod-casts« hören–, verrät auch eine Menge über uns. Von Lebensabschnitt, Hob-bies und Interessen über Beziehungsstatus, medizinische Indikationen bis hin zur politischen Einstellung.

Aber es geht noch weiter. Denn die Anbieter wissen nicht nur genau, was wir uns wann angeschaut oder angehört haben, sondern auch, wo wir Pause gemacht haben, welche Stellen wir uns mehrfach angeschaut haben, vielleicht mit einer kurzen Pause dazwischen … ihr wisst, was wir meinen.

Wer uns über die Schulter schaut

Allen voran ist da YouTube als größte Video-Content-Plattform. YouTube gehört zum Google-Imperium. Das bedeutet, was immer wir auf YouTube tun, es füttert unser Google-Profil mit Informationen über uns.

Es gibt viele gute Gründen, das nicht zu wollen, angefangen bei der schieren Datenmasse und der Marktmacht, die bei Google zusammenlaufen. Allerdings haben wir das Problem, dass sehr viele Menschen, die Inhalte nur auf YouTube zur Verfügung stellen. Viele Livestreams werden über Facebook Live bzw. Googles YouTube gemacht oder sie finden auf Twitch statt, das zu Amazon gehört.

Und Spotify? An sich wäre es mit Sitz in Schweden ein europäisches Unternehmen. Allerdings haben sie vor einigen Jahren die Podcast-App Anchor gekauft, was ein US-Unternehmen ist. Seither haben sie einen Unternehmensbezug in die USA und fallen somit eigentlich auch unter den CLOUD-Act.

Auch Smart-TVs dürfen nicht unerwähnt bleiben, wenn es darum geht, wer uns beim Streamen von Inhalten aus dem Netz beobachtet. Die Geräte sind auch nur Computer mit großem Bildschirm, die den ganzen Tag am Internet hängen. Allerdings sind Smart-TV-Geräte oft technisch vernachlässigt, bekommen kaum Sicherheitsupdates und werden immer wieder Opfer von Schadsoftware, insbesondere Spyware, also Spionage-Software. Ob das Gerät Kamera und Mikrofon hat, die von solcher Spyware ausgenutzt werden können, kann man sich beim Kauf eventuell noch aussuchen. Es gab schon Fälle, bei denen durch eingebaute Kameras Privatwohnungen von Unbefugten ausspioniert wurden.

Und von Alexa-Geräten mit Kamera und stets auf's Aktivierungswort lauschenden Mikrofonen und den Möglichkeiten, die Amazon dadurch hat, mal ganz zu schweigen.

CLOUD-ACT

Der CLOUD-Act hat nur sehr begrenzt mit »der Cloud« zu tun. CLOUD steht für »Clarifying Lawful Overseas Use of Data«. Es handelt sich um ein US-Gesetz [https://www.justice.gov/dag/cloudact] von März 2018, das besagt, dass alle US-Unternehmen verpflichtet sind, Behörden Zugang zu ihren Servern zu geben, ganz egal, wo die Server stehen. Ob auf US-Boden oder ganz woanders in der Welt. Das betrifft auch alle Firmen, die einen Firmenbezug wie Mutter- oder Tochtergesellschaft in den USA haben. Es können auch andere Länder mit den USA nach CLOUD-Act kooperieren und dann bekommen die Behörden dieser Länder ebenfalls Einsicht in die Server der US-Unternehmen, und umgekehrt die US-Behörden Einsicht in die Server der Unternehmen dieser Länder.

Freie Sicht für alle

Aber es gibt sie auch hier, die datensparsameren Alternativen. Wenn ihr nicht umhin kommt, YouTube-Videos zu schauen, vielleicht, weil eine Organisation ihre Inhalte ausschließlich dort zur Verfügung stellt, könnt ihr euch mit Proxy-Apps behelfen. So bekommt Google nicht alles von euch mit.

Auf Android-Geräten könnt ihr beispielsweise NewPipe verwenden. Diese App nimmt neben YouTube auch verschiedene Mediatheken als Quellen an.

Für Desktop-Rechner ist FreeTube eine gute Möglichkeit, nicht all eure Seh-Gewohnheiten an Google zu verraten.

Selbst Inhalte zur Verfügung stellen

Wenn ihr nicht nur Inhalte konsumieren, sondern auch selbst Videos, Audio... ins Netz stellen oder Livestreams machen wollt, habt ihr einige Möglichkeiten. Überlegt euch nicht nur, wem ihr eure eigenen Daten geben möchtet, sondern auch, ob ihr das für euer Publikum verantworten könnt.

Videos & Livestreams

Eine Möglichkeit, Videos ins Netz zu stellen, ist Vimeo, das allerdings bei mehr als einer Handvoll Videos schnell teuer wird.

Stattdessen schlagen wir euch vor, einen Blick auf PeerTube zu werfen. Der Fediverse-Video-Dienst hat eine rege Community, die sich sehr um die Weiterentwicklung kümmert. Die Server sind alle gratis oder auf Spendenbasis betrieben. Peertube ist recht einfach zu bedienen und auch Livestreams laufen damit für Streamer:innen sehr entspannt.

Insbesondere für Organisationen ist ein eigener Peertube-Server eine lohnende Investition. Er ist sehr überschaubar in Wartung und Pflege und bietet neben Videohosting eben auch die Möglichkeit für Livestreams an.

Podcasts

Falls ihr Podcasts macht, denkt daran, dass Spotify einen »Gartenzaun« hat. Daher hatten die oben erwähnten »Podcasts« auch Anführungszeichen. Denn wenn ihr keinen frei verfügbaren RSS-Feed habt, habt ihr keinen Podcast, sondern ein Audioformat für Spotify-User:innen. Das Internet ist aber viel größer als nur Spotify.

Podcasthosting geht auch einfach über ein eigenes, möglicherweise ohnehin schon vorhandenes WordPress mit Podlove Plugin. Alternativ könnt ihr euch Castopod, die Podcast-Plattform im Fediverse an-

schauen. Und StudioLink für eure Aufnahmen mit Gästen über das Internet, wo wir schon dabei sind.

Falls ihr mehr über Podcasting und die Möglichkeiten abseits der kommerziellen erfahren möchtet, schaut gern in das Buch »Podcasting« von Klaudia Zotzmann-Koch.

Vertraut nicht all eure Gewohnheiten und Interessen den kommerziellen Streamingdiensten an, die diese Informationen auswerten und an Werbetreibende weiterverkaufen.

Schaut euch die Alternativen wie PeerTube an. Wenn es YouTube-Videos sein müssen, probiert eine Proxy-App wie FreeTube aus. Denkt bei euren eigenen Inhalten auch an eure Zuschauer:innen und Hörer:innen und achtet darauf, dass euer Format auch wirklich überall im Netz verfügbar ist. Ihr könntet auch ganz verwegen mal einen Abend ganz offline sein und einen Film von DVD oder BluRay schauen oder Musik von CD oder Schallplatte hören. Oder ein Buch lesen …

Von Angesicht zu Angesicht: Videokonferenzen

Während Corona ist unsere Welt zunehmend zweidimensional geworden. Vieles, was sonst irgendwo vor Ort stattgefunden hätte, wanderte kurzerhand ins Netz. Die Videokonferenzdienste bekannter US-Anbieter wie Zoom, Cisco WebEx, Microsoft Skype und Teams waren plötzlich heiß begehrt. Dass US-Dienste durch die Pandemie nochmal Milliarden Datensätze mehr bekamen als sonst, könnte uns in späteren Jahren noch teuer zu stehen kommen. Denn Videokonferenzen übertragen unsere Gesichter und Stimmen. Beides sind biometrische Merkmale, die zur eindeutigen Identifikation eingesetzt werden können. Außerdem verraten beide extrem viel über unsere körperliche sowie geistige Verfassung.

BIOMETRISCHE DATEN

Biometrische Daten sind Körper-Identifikationsmerkmale. Unser Gesicht, die Iris, Fingerabdrücke, Handvenen und auch unsere Stimme können uns eindeutig identifizieren. Juristisch gelten Fotos und auch unsere Stimme zwar nur dann als »biometrisch«, wenn sie zur Identifikation verwendet werden, der Technik hingegen ist das völlig egal. Ein einmal aufgenommenes Foto, Video oder auch eine Stimmaufnahme können jederzeit entsprechend eingesetzt werden. Das geht unter Einsatz entsprechender Algorithmen auch in Echtzeit während wir uns unterhalten.

Freie Alternativen

Wir sind nicht gezwungen, US-Lösungen zu verwenden. Es gibt auch freie Open-Source-Alternativen wie Jitsi Meet und Big Blue Button (BBB). Beide haben in den letzten Jahren einen ordentlichen Sprung nach vorn gemacht und es lohnt, sich damit zu befassen. Nicht zuletzt, weil beide im Browser laufen und keinerlei extra Programme benötigen.

Etwas unterschiedlicher Ansatz

Während Jitsi seinen Werdegang vor vielen Jahren in der Chat- und Messenger-Szene begann, kommt BBB aus dem Bildungsbereich. Das spiegelt sich beispielsweise darin, dass es bei BBB ein oder mehrere Moderator:innen gibt, die Rechte z. B. für Bildschirmfreigabe an Andere vergeben können, während bei Jitsi von Beginn an alle Teilnehmenden gleichberechtigt sind.

Frei verfügbare Videokonferenz-Server

Es gibt sowohl für Jitsi als auch für BBB frei verfügbare Server, die ihr für eure Videokonferenzen nutzen könnt.

Unter beispielsweise meet.scheible.it findet ihr einen gut gepflegten öffentlichen Jitsi-Server. Der Betreiber bietet auch eine Liste weiterer öffentlicher Server an [https://scheible.it/liste-mit-oeffentlichen-jitsi-meet-instanzen]. Einen Jitsi-Server habt ihr bei einem E-Mail-Postfach bei mailbox.org übrigens auch dabei, allerdings erst beim mittleren Paket um die 3€ pro Monat. Dafür bekommt ihr dort dann auch einen Auftragsverarbeitungsvertrag nach DSGVO (AVV) und könnt den Jitsi-Server dann auch beruflich nutzen.

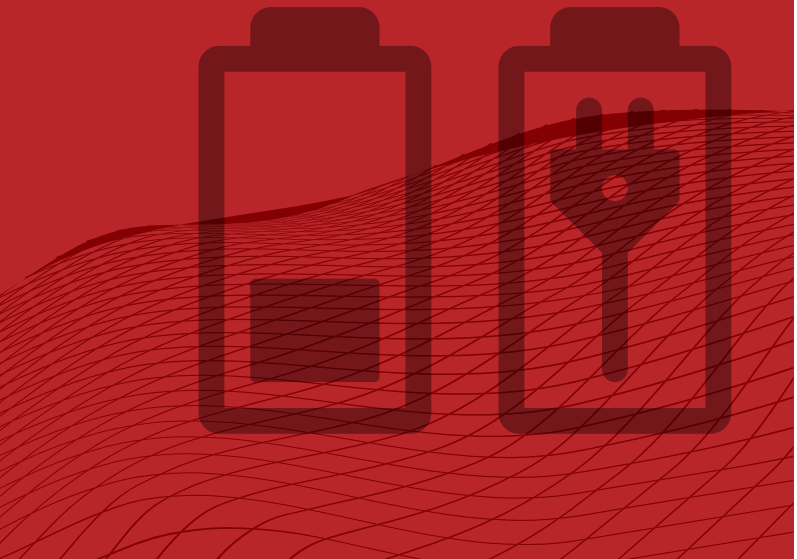
Für freie BBB-Konferenzen empfehlen wir euch Senfcall.de. Das Projekt wurde von Student:innen der Unis Darmstadt und Tübingen gestartet und ist über Corona zu einem eigenen Verein herangewachsen.

Senfcall bietet auch die Möglichkeit, einen AVV zu bekommen, wenn ihr deren BBB-Server z. B. als Verein nutzen wollt. Komplett kommerzielle Nutzung ist bei Senfcall nicht vorgesehen und widerspricht den Vereinsregeln.

Verwendet nicht einfach die US-Lösungen, nur weil euer Verein, eure Schule, eure wöchentliche Plauderrunde das schon immer so gemacht hat.

Gebt Jitsi oder BigBlueButton eine Chance. Auf z. B. Senfcall könnt ihr schnell und gratis einen Raum eröffnen und einfach loslegen.

NACH WORT



Wir hoffen, ihr habt ein paar Anregungen bekommen und konntet euch einige Tipps für euren digitalen Alltag mitnehmen. Vor allem wollten wir euch einen schnellen Einstieg bieten und Dinge an die Hand gegeben, damit ihr selbständig weiter recherchieren könnt. Zum Beispiel die vielen Themengebiete, die es aus Platzmangel nicht mehr hier in dieses Buch geschafft haben wie IoT, also das Internet der Dinge, GPS-, WiFi- und Bluetooth-Tracking und noch Vieles mehr.

Beginnt einfach mit den kleinen Dingen, die ihr direkt in eurem Leben ändern könnt und versucht nicht zuviel auf einmal. Wenn ihr ein Gebiet sicher beherrscht wie zum Beispiel eure Passwortmanager, dann schaut euch das nächste Thema an. So könnt ihr Schritt für Schritt die Dinge besser verstehen und damit auch gute und informierte Entscheidungen treffen. Wir haben gesagt, dieses Thema ist wie ein Teamsport. Es geht nur zusammen. Deshalb: Redet darüber. Sprecht die Themen an. Nur so können wir gemeinsam etwas bewegen.

Danke

GLOSSAR

Adblocker, Werbeblocker

Ein Ad- oder Werbeblocker ist eine Funktion innerhalb von Browsern, die verhindert, dass Werbeinhalte geladen werden. Somit verhindern Adblocker, dass Trackingsoftware innerhalb der Werbung ausgelöst wird, die euch durch das Netz verfolgen, euer Internetverhalten analysieren und euch identifizieren kann. Adblocker sind eine sinnvolle Ergänzung zu euren Browsern, auch auf mobilen Endgeräten.

Android

Betriebssystem für Mobilgeräte. Ursprünglich von Google gebaut, ist Android an sich Open Source, abzüglich der Google-spezifischen Teile wie dem Playstore oder dem Google-Android Swipe-Keyboard. Android ist auf dem überwiegenden Teil aller Smartphones installiert.

Auftragsverarbeitungsvertrag (AVV)

Ein Auftragsverarbeitungsvertrag nach DSGVO, kurz AVV, ist eine schriftliche Vereinbarung. Diese wird zwischen Verantwortlichem und Auftragsverarbeiter geschlossen. Beispiel: Ihr seid Blogger:in und versendet auch einen Newsletter. Der Newsletteranbieter verarbeitet in eurem Auftrag die personenbezogenen Daten anderer Menschen für euch. Er ist der Auftragsverarbeiter. Als Blogger:in seid ihr verantwortlich dafür, dass mit den Daten eurer Leser:innen auf eurem Blog und auch bei euren anderen Angeboten passiert. Ihr seid die:der Verantwortliche. Um euch rechtlich abzusichern, schließt ihr einen Auftragsverarbeitungsvertrag mit dem Newsletteranbieter. Sollte bei denen etwas schiefgehen, seid allerdings dennoch immer noch ihr dafür verantwortlich.

Backup

Das Einzige, das euch wirklich vor Datenverlust schützt, sei es wegen einer kaputten Festplatte oder einem Verschlüsselungstrojaner. Backups sind wichtig. Das kann und soll euch niemand abnehmen.

Moderne Betriebssysteme haben dafür praktische Automatismen entwickelt, die z. B. immer, wenn eine bestimmte Festplatte angeschlossen wird, automatisch alle neuen oder geänderten Dateien dort ablegen.

Betriebssystem

Ein Betriebssystem ist die Basis-Software, mit der ein Computer ausgestattet ist. Microsoft Windows ist noch immer das am weitest verbreitetste Betriebssystem, neben dem Apple MacOS und die verschiedenen Linux-Versionen nur einen kleinen Marktanteil haben. Linux ist Open Source und auf dem Großteil aller Server im Einsatz. Entgegen der weitreichenden Meinung, man würde auf einem Computer mit dem Betriebssystem arbeiten, sind es vielmehr die jeweils installierten Programme. Das darunter liegende Betriebssystem bemerkt man eher selten und Umgewöhnungsphasen fallen in der Regel kürzer aus, als anfangs gedacht.

Bits & Bytes

Ein Bit ist die kleinste Daten-Maßeinheit; Null oder Eins, aus oder an. Ein Byte ist eine Abfolge von Bits, die gemeinsam ein Zeichen wie beispielsweise einen Buchstaben ergeben. Üblicherweise sind das 8 Bit. Ein Byte ist daher in den meisten Computersystemen die kleinste adressierbare Einheit.

Browser

Ein Browser ist eine Software, die zum Surfen im Internet verwendet wird. Browser gibt es auf allen Betriebssystemen, auch für mobile Endgeräte.

Browser-Add-on

Add-ons fügen einer Software – in diesem Falle einem Browser – Funktionen hinzu. Beispielsweise Adblocker, also Werbeblocker wie uBlock origin, sind sinnvolle Erweiterungen für Eure Browser.

Cloud

Kunstwort für gemietete Server, die bei anderen Leuten stehen. Auch Software as a Service Produkte wie Cloud-Gaming, Cloud-Office... laufen auf Rechnern, die irgendwo auf der Welt stehen. Zu beachten ist die Rechtslage in den Ländern, in denen die jeweiligen Betreiber sitzen. Deren Rechner, deren Regeln.

CLOUD-Act

US-Gesetzgebung von März 2018. CLOUD steht für »Clarifying Lawful Overseas Use of Data«. Der CLOUD-Act besagt, dass alle US-Unternehmen verpflichtet sind, Behörden Zugang zu ihren Servern zu geben, ganz egal, wo die Server stehen. Das betrifft auch alle Firmen, die einen Firmenbezug wie Mutter- oder Tochtergesellschaft in den USA haben. Es können auch andere Länder mit den USA nach CLOUD-Act kooperieren. Dann bekommen die Behörden dieser Länder ebenfalls Einsicht in die Server der US-Unternehmen und umgekehrt.

Darknet

--> siehe Tor-Netzwerk

Dark Pattern

Dark Patterns sind versteckte Muster, die uns zum Klicken oder auch unüberlegten Zustimmen bewegen sollen. Beispielsweise vorab angehakte Checkboxen oder auf mehreren Unterseiten von Cookiebannern versteckte vorausgewählte Zustimmungen für »berechtigte Interessen«.

DSGVO

DSGVO ist die Kurzform von Datenschutzgrundverordnung. Das ist eine EU-Verordnung, die in allen EU-Mitgliedsstaaten gilt. Die DSGVO gilt seit 2016, im Mai 2018 lief die zweijährige Übergangsfrist zur Rechtsdurchsetzung aus. Seither werden Verstöße geahndet. Die Datenschutzgrundverordnung regelt, was mit den personen-

bezogenen Daten von Menschen passieren darf und was nicht. Vor allem gibt sie uns als Verbraucher:innen Werkzeuge an die Hand, um uns zu informieren und ggf. auch unser Recht einfordern zu können.

E-Mail

Technologie zum Senden und Empfangen von Nachrichten über das Internet. Seit 1989 sind E-Mails bereits technisch ausgewachsen. Die Möglichkeit, E-Mails in html anzuzeigen, hat die Darstellung bunter gemacht, allerdings auch alle Nachteile von Werbetracking in unsere Postfächer gebracht.

E-Mail-Verschlüsselung

Echte E-Mail-Verschlüsselung bewirkt, dass der Inhalt der E-Mails verschlüsselt wird. Würde die E-Mail auf dem Weg mitgelesen, sähen die Mitlesenden nur Zeichensalat. Die Verschlüsselung wird mittels extra Ersteller Schlüssel im E-Mail-Programm vollzogen und kann nur mit dem passenden Schlüssel auf Empfänger:innen-Seite wieder entschlüsselt werden.

Fediverse

»Fediverse« ist ein Kofferwort aus »federated« und »universe«, also föderiertes Universum. Es bezeichnet ein Netzwerk verschiedener Plattformen, die alle auf dem ActivityPub Protokoll aufbauen und somit »dieselbe Sprache sprechen«. Es gibt ganz unterschiedlich gelagerte Fediverse-Services und Alternativen zu verbreiteten Plattformen wie Mastodon (Alternative zu Twitter), Pixelfed (Alternative zu Instagram), Mobilizon (Alternative zu Facebook-Events und -Gruppen) und viele mehr. Mit einem Account auf Mastodon kann man nicht nur anderen Mastodon-Nutzern folgen und mit ihnen interagieren, sondern auch Nutzer:innen aller anderen Fediverse-Services. Die Fediverse-Services sind alle Open Source und können grundsätzlich von jedem:r gehostet werden. So stellen nicht nur Unis, Vereine und öffentliche Stellen Server für z. B. Mastodon zur Verfügung, sondern auch viele Privatmenschen. Die einzelnen Server, Instanzen genannt, sind üblicherweise durch Spenden der jeweiligen Nutzer:innen finanziert.

Gamification

Von englisch »game«, also »Spiel«. Bezeichnung für die Gestaltung von Oberflächen und Mechanismen wie ein Spiel, mit kleinen Belohnungen, Teasern (Stupser oder Anreize)... Gamification ist die Grundlage auf der Geräte wie Smartphones und deren Software, aber auch Social Media Plattformen gestaltet und organisiert sind, um uns möglichst lang zu beschäftigen. Sie ist der Grund, warum viele Angebote wortwörtlich süchtig machen.

Hassrede, Hatespeech

Hassrede oder englisch »hatespeech« meint verschiedene sprachliche Äußerungen von Hass, die einzelne Menschen oder auch Menschengruppen herabwürdigen und / oder verunglimpfen. Derlei anstachelnde Äußerungen sind illegal. In Österreich fallen sie unter den Verhetzungsparagraphen, in Deutschland unter Volksverhetzung und in der Schweiz unter die Rassismus-Strafnorm.

Hosting

Das Wort leitet sich vom Englischen »host« ab, was »Wirt« oder »Gastgeber« bedeutet. Im Kontext des Internets bedeutet Hosting, dass man sich auf einem Server »einmietet«. Der Anbieter (»Hosting-Provider«) bietet meist verschiedene Dinge an. Es gibt Webseiten-Hosting, wo man einen eigenen Blog betreiben kann und dazu etwas Platz auf deren Festplatten, eine Domain und innerhalb des gebuchten Pakets meist auch ein bestimmtes Volumen für Zugriffe auf den Blog bekommt. Außerdem gibt es Lösungen wie NextCloud, wo der Festplattenplatz viel größer sein kann.

html

html steht für Hyper Text Transfer Protocol. Das ist »die Sprache«, dank derer das WWW, das World Wide Web, funktioniert.

ID
»ID« steht kurz für »Identifyer«, also »Identifizierungsmerkmal«. Im Kontext des Internets ist damit häufig auch ein Pseudonym wie beispielsweise ein Nickname oder auch eine E-Mail-Adresse gemeint.

Internet
Unendliche Weiten. Physisch sind es Milliarden Kilometer Kabel, tausende Tonnen an Blech und diverse Gigawatt an Strom, die täglich für den Betrieb aufgewendet werden müssen. Inhaltlich gibt es verschiedene Bereiche. Das WWW ist der Bereich, der typischerweise mit »dem Internet« assoziiert wird: der Großteil dessen, was mit Browsern erreichbar ist, also Webseiten, Social-Media-Plattformen, Onlineshops etc. Videostreaming ist ein eigener Bereich des Internets, ebenso Internettelefonie (VoIP, Voice over IP), E-Mail und noch einige andere mehr.

iOS
iOS ist der Name des Betriebssystems der Apple Mobiltelefone (iPhone). »OS« steht für »Operating System«, also »Betriebssystem«. Für Tablets von Apple (iPad) heißt das Betriebssystem seit 2019 iPadOS. Fast alle Apps sind sowohl für iOS und iPadOS verfügbar.

IP-Adresse
»IP« steht für »Internet Protocol«. Eine IP-Adresse ist für jede Datenübertragung notwendig. Unsere Geräte bzw. die Apps und Browser darauf, schicken immer eine IP-Adresse an den jeweiligen Server, damit dieser weiß, wohin er die anzuzeigenden Informationen zurückschicken soll. IP-Adressen sind die Grundbausteine, auf denen der gesamte Internetverkehr basiert.

Malware
Das Wort Malware ist ein Kofferwort aus »malicious« und »software«. Das deutsche Wort ist »Schadsoftware« oder manchmal auch »Schadcode«. Es ist Software, die bösartige Ziele verfolgt wie beispielsweise die Verschlüsselung aller Daten auf dem System. Kommt oft in Kombination mit Lösegeldforderungen oder böswilliger Veröffentlichung erbeuteter Daten.

Messenger
Messenger sind Smartphone-Apps zur Kommunikation. In gewisser Weise sind sie die Nachfolger von SMS und MMS. Ihre Funktionen gehen über den reinen Nachrichtenversand meist weit hinaus und umfassen neben Text- und Bildversand meist auch Telefonie und Videoanrufe. Viele Messenger haben neben den Smartphone- und Tablet-Apps auch Desktop-Programme, was die Verwendung auf dem Rechner sehr komfortabel macht. Es gibt Messenger mit dem Ziel, zentrale Infrastrukturen zu vermeiden und durch viele verbundene Server die Kommunikation zu dezentralisieren. Dazu zählen Element und alle anderen Messenger, die das Matrix-Protokoll sprechen. Sichere Messenger sind Signal und Threema.

Mobbing
Das Wort stammt vom »Mob«, also einer wütenden Menge. Meist sind es Gruppen, die sich auf Einzelpersonen eingeschossen haben. Bei Mobbing sind negative Gruppendynamiken zu beobachten, die bei den Mobbenden oft unterbewusst ablaufen, was die Konsequenzen für die gemobbte Person keinesfalls rechtfertigen oder besser machen. Mobbing ist strafbar und kann zur Anzeige gebracht werden. Es gibt heutzutage auch schon kostenfreie Hilfsangebote, in Österreich beispielsweise von der Familienberatungsstelle.

Modem
Gerät, das eine Verbindung zum Internet herstellt. Die Funktion kann mittlerweile auf sehr kleinen Bauteilen stattfinden und so haben auch z. B. Mobiltelefone eingebaute Modems für mobiles Internet. Daheim haben wir heute meist Geräte, die sowohl Modemfunktion haben, als auch einen Router, der den Internetanschluss hinter

dem Modem dann innerhalb der Wohnung an die verschiedenen Geräte per Kabel oder auch WLAN verteilt.

Open Source
Open Source bedeutet, dass der Programmcode einer Software öffentlich einsehbar ist.

Passwort, Passphrase & PIN
Ein Passwort ist ein Wort oder heutzutage eine Buchstaben-Zahlen-Zeichen-Kombination. Eine Passphrase ist eine Abfolge mehrerer Wörter. Moderne Passwörter können statt ellenlanger Zeichenketten durchaus auch aus fünf oder sechs Wörtern bestehen. Es erhöht die Sicherheit, wenn diese aus unterschiedlichen Sprachen stammen. PIN sind persönliche Identifikations-Nummern. Das sind meist kurze Zahlenfolgen, die für sich genommen schon durch die Kürze nicht sonderlich sicher sind.

Passwortmanager, Passwordsafe, Passwordkeeper
Passwortmanager sind Programme, die bei der Verwaltung der eigenen Passwortsammlung helfen. Sie legen einen verschlüsselten Tresor an, in dem dann alle Passwörter hinterlegt werden. Das Passwort zum Öffnen dieses Tresors muss man sich gut merken. Moderne Passwortmanager unterstützen Zwei-Faktor-Authentifizierung. Meist gibt es zu den Desktop-Passwortmanagern auch passende oder kompatible Apps für Mobilgeräte. Wir empfehlen, für den mobilen Einsatz einen eigenen Tresor anzulegen, in dem dann nur die Passwörter liegen, die Ihr wirklich unterwegs braucht.

Phishing
Vom englischen »Angeln«, also Fischen. Tatsächlich meist eher vergleichbar mit dem Auswerfen sehr großer Netze, beispielsweise in Form von Millionen Spam-E-Mails, die zeitgleich ausgesendet werden. Wenn z. B. 200 Menschen auf solch eine Betrügerei reinfallen und Geld zahlen, kommt Einiges zusammen. Phishing-Kampagnen können aber auch zum Ziel haben, nicht Geld, sondern Zugangsdaten zu erbeuten. Dazu werden oft gefälschte Webseiten mit ebenso falschen Loginfeldern eingesetzt. Eine Spezialform ist das sogenannte »Spearphishing«, also »Speerfischen«, wo es wortwörtlich um einen gezielten Fisch geht. Das sind Betrugskampagnen, die sich gegen Einzelne, wie beispielsweise jemanden in der Chefetage oder auch die Finanzabteilung einer bestimmten Firma richten.

Podcast
»Podcast« ist ein Kofferwort aus »iPod« und »Broadcast«. Der Hinweis auf das Musikabspielgerät von Apple ist beabsichtigt, denn Apple erfand diese Möglichkeit für Menschen, um nicht nur schriftliche Inhalte wie Blogs zu veröffentlichen, sondern auch Audio-Tagebücher bis hin zu privaten »Sendungen« selbst zu gestalten und ins Internet zu stellen. Für die Reichweite eines Podcasts ist wichtig, dass es einen frei verfügbaren RSS-Feed gibt, über den Menschen die jeweiligen Podcasts abonnieren können.

Podcatcher
So nennt man Apps und Programme, mit denen man Podcasts abonnieren und hören kann.

RSS-Feed
Die Magie hinter Blogs und Podcasts: RSS-Feeds, oder kurz: Feeds, machen es möglich, Aktualisierungen eines bestimmten Blogs oder Podcasts zu abonnieren. Kommt eine neue Folge, wird man benachrichtigt und je nach Einstellung wird die Folge auch gleich heruntergeladen und bei den zu hörenden Folgen eingereiht.

Server
Durchgehend laufender, mit dem Internet verbundener Rechner, der neben einem Betriebssystem Programme installiert hat, die beispielsweise Webseiten darstellen (»Webserver«) oder E-Mails senden und empfangen können (E-Mail-Server).

Server-Administrator

Server sollten nie einfach allein gelassen im Internet hängen. Üblicherweise gibt es Menschen, die sich um die Rechner kümmern, Updates von Betriebssystem und Programmen einspielen, sich eventuell um die Hardware kümmern und aufpassen, dass die Server keine Opfer einer der vielen verschiedenen Schadsoftwares werden, die im Internet kursieren. Solche Menschen nennt man Administratoren, kurz: Admins. Diese haben systembedingt Einsicht in die Datenbanken der verschiedenen Dinge, die auf dem Server installiert sind. Das ist nicht nur bei kleinen Open-Source-Lösungen so, sondern auch bei großen Plattformen, E-Mail-Anbietern etc. Alles, was nicht sicher verschlüsselt auf Servern abgelegt ist, kann von Administrator:innen grundsätzlich ausgelesen werden; und gegebenenfalls auch an z. B. Behörden weitergegeben werden.

Suchindex, Suchindizes

Datenbanken, auf die Suchmaschinen zugreifen. Sie sind die Quellen der Suchtreffer.

Streaming, Streamingdienste

Streaming bezeichnet die Übertragung von Medieninhalten wie Video oder Musik. Eine übliche Form sind On-Demand-Angebote, bei denen man die Inhalte jederzeit von den Servern der Anbieter abspielen kann. Daneben gibt es auch Livestreams, die in Echtzeit übertragen werden; entweder von großen Anbietern, von Konferenzen oder Events, aber auch von Privatpersonen. Meist stehen die Aufzeichnungen dieser Livestreams im Anschluss auch zum zeitsouveränen Nachschauen bereit. Ein reines Herunterladen der Mediendateien auf unsere Endgeräte ist bei kommerziellen Streamingangeboten nicht vorgesehen, die Dateien verbleiben bei den Anbietern und wir mieten nur den Zugang dazu. Anders bei Open Source Angeboten wie PeerTube.

Suchmaschine

Suchmaschinen gibt es einige. Sie unterscheiden sich in Indexsuchmaschinen, Proxy-, Meta- und Spezialsuchmaschinen. Erstere haben einen eigenen Suchindex, der als Quelle ihrer Suchergebnisse dient. Proxy-Suchmaschinen leiten unsere Suchanfragen weiter an einen der großen Suchindizes. Meta-Suchmaschinen leiten die Anfrage an mehrere Indizes weiter, manche nehmen noch weitere Quellen für ihre Ergebnisseiten hinzu. Spezialsuchmaschinen sind auf kleine Bereiche wie Bildersuche, Preissuche, Flug- oder Bahnverbindungen etc. ausgerichtet.

Tag, Tags

Englisch für »Schildchen« wie in »price tag«, Preisschild oder auch »Schlagwort«.

Targeting

Der Begriff kommt vom Englischen »target«, auf Deutsch »Ziel« oder als Verb »targeting« im Sinne von »ins Ziel nehmen«, »anvisieren«. Targeting ist ein Überbegriff verschiedener Technologien, die verwendet werden, um Personen spezifisch mit Werbebotschaften zu versorgen, um ein bestimmtes Verhalten zu erreichen. Die Person ist das Ziel, das »target«. Es ist auch möglich, auf eine Gruppe von Menschen abzuzielen. Diese nennt man dann »target group«.

TLS-Verschlüsselung

TLS steht für Transport Layer Security, also »Transport Sicherheit«. Das ist eine Transportverschlüsselung, die einen »Tunnel« um die Verbindung eines bestimmten Streckenabschnitts macht. TLS-Verschlüsselung ist keine Inhaltsverschlüsselung. Die übertragenen Inhalte sind noch immer im Klartext lesbar für alle, die außerhalb des getunnelten Streckenabschnitts in die Übertragung reingucken.

Tor-Netzwerk

Die Bezeichnung »Tor« kommt vom Englischen »The Onion Router«. Der Name ist ein Hinweis auf das Zwiebelschalenmodell, die Art, wie die Verbindungen innerhalb des Tor-Netzwerks funktionieren (onion = englisch für Zwiebel). Das Tor-Netzwerk wird umgangssprachlich auch »Darknet« genannt. Es ist kein besonderes Modem notwendig. Das Tor-Netzwerk ist ein Bereich des Internets, der auf speziell konfigurierten Servern liegt. Ihr könnt diesen Bereich mit dem Tor-Browser, einer Unterart des Firefox-Browsers, aufrufen. Verbindungen im Tor-Netzwerk sind nie direkt vom Browser zum Server, sondern gehen immer über drei verschiedene Tor-Server, von denen nur der erste eure echte IP-Adresse sieht. Der letzte davon sieht nur noch, wohin die Verbindung aufgebaut werden soll und der Server, zu dem die Verbindung dann stattfindet, sieht nicht mehr eure Adresse, sondern nur die des letzten Tor-Servers des Dreiergespanns, über das eure Verbindung aufgebaut wurde. So wird euer Weg durch das Netz verschleiert. Aber Achtung, nur weil ihr eine Verbindung über das sogenannte Darknet habt, seid ihr nicht automatisch anonym. Es wird nur eure IP-Adresse verschleiert.

Tracking

Vom Englischen »track«, also »Spur« oder »Fährte« rührt diese Bezeichnung für die Verfolgung von Menschen für Werbezwecke durch's Netz. Eine eindeutige Zuordnung von Geräten, Browsern oder Apps zu bestimmten Personen wird durch unterschiedliche Merkmale erreicht. Darunter zählen die Geräte-ID, die eindeutige ID des Modems, die IP-Adresse, die Konfiguration des Browsers inkl. Bildschirmgröße und welche Add-ons installiert sind.

Trojaner

Ein Trojaner leitet sich vom mythischen Holzpferd aus den Sagen der griechischen Antike ab. Die Griechen belagerten die Stadt Troja und wollten sie einnehmen. Aber deren Stadtmauern und Vorräte waren zu gut. Schließlich schoben die Griechen ein Holzpferd vor die Stadt. Die Menschen drinnen öffneten die Stadttore, holten das Pferd herein und machten flugs die Tore wieder zu. In der Nacht kamen griechische Kämpfer aus dem Pferd hervor, die von innen die Stadttore öffneten. So konnten die Griechen mit dieser List die Stadt doch noch einnehmen. Genau so verhält es sich auch in unserem Kontext. Ein Trojaner ist eine Schadsoftware, die wir uns meist im Glauben, etwas anderes zu klicken oder herunterzuladen, selbst auf unser Gerät holen. Bekannte Beispiele sind die verbreiteten Verschlüsselungstrojaner.

Troll, Trollen, Trolling

Ein Troll ist eine Person die, wie die Trolle der Mythen und Legenden, auf alles draufhaut, was ihr nicht passt. Meist mit dem Ziel, eine konstruktive Diskussion gänzlich unmöglich zu machen und die Diskussionsparteien komplett zu spalten.

WLAN, WiFi

WLAN ist kurz für »wireless LAN«, wobei LAN für »local area network« steht, also kabelloses lokales Netzwerk. WiFi ist die englischsprachige Bezeichnung, die vom Modewort »Wireless Fidelity« kommt, das sich am »HiFi« der 1980er und 90er im Bereich Musik orientiert.

WWW

Das World Wide Web ist der Teil des Internets, der durch Browser erreicht und navigiert werden kann. Dazu gehören Webshops, Social-Media-Plattformen, Blogs und Webseiten... Bei E-Mails gehören beispielsweise nur die Weboberfläche eures Postfachs zum WWW, falls ihr euer Postfach im Browser öffnen könnt. Die verschlungenen Pfade, auf denen E-Mails durch's Netz gehen, gehören nicht zum WWW.

Zwei-Faktor-Authentifizierung

Zwei-Faktor-Authentifizierung (2FA) bedeutet, dass ihr beispielsweise zum Login mit eurem Usernamen zusätzlich zum Passwort einen zweiten Faktor benötigt, damit der Loginvorgang durchgeführt werden kann. Varianten sind das Zusenden von SMS oder Hardware-Tokens wie Yubikey oder die Open-Source-Variante von Nitrokey. Am weitesten verbreitet ist der sogenannte Google-Authenticator oder auch TOTP/OTP genannt. Das Verfahren wurde ursprünglich von Google entwickelt, ist aber Open Source und wird von verschiedenen Projekten angeboten. TOTP/OTP steht für Timebased One Time Password, im Deutschen meist »Einmalpasswort« genannt. Dies ist ein sechsstelliger Zahlencode, der jede Minute neu erstellt wird. Einmalpasswörter werden von allen modernen Passwortmanagern unterstützt.

STATE MENTS

Zwei kalifornische Träume

Marek Tuszynski

I

Ich beende einen Vortrag über Drohnen als Beispiel für problematische Technologien, die unsere Erfahrung der Welt abstrahieren. Ich befinde mich an einem Ort namens Occupy San Francisco, der, wie sich bei meiner Ankunft herausstellt, nichts mit der Occupy Bewegung zu tun hat – es handelt sich um eine nur weitere Aneignung, einen nur weiteren aufstrebenden Startup-Space. Es kommt zu Missverständnissen. Ich mache dennoch weiter, bewahre die Ruhe, etliche Leute verlassen vorzeitig den Raum, meine perfekten Folien sind keine Hilfe. Immerhin bleibt eine hoffnungsvolle Gruppe bis zum Schluss, es werden Drinks gereicht, wir reden. Eine junge Person ist von meinem Vortrag besonders angetan – aus den gänzlich falschen Gründen. Ich stehe da, überlege, wie ich mit dieser offenkundigen Dissoziation umgehen soll. Wir sprechen beide über dieselben Dinge, allerdings mit ganz unterschiedlichen Vorstellungen von der Zukunft.

Später spiele ich die Situation im Kopf noch einmal durch und muss dabei an Amitav Ghosh und sein Buch Uncanny And Improbable Events (Unheimliche und unwahrscheinliche Ereignisse) denken. Darin schreibt er, während er sich die Frage stellt, warum so wenige Schriftsteller:innen in ihren Romanen den Klimawandel aufgreifen, folgendes: „Kultur schafft Wünsche – nach Fahrzeugen und Geräten, nach einer bestimmten Art von Gärten und Häusern –, die zu den Haupttreibern der Kohlenstoffwirtschaft zählen. Ein schnelles Cabrio lässt unsere Herzen nicht deshalb höherschlagen, weil wir eine Liebe für Metall und Chrom hegen oder ein abstraktes Verständnis für Ingenieurswissenschaften haben; es erregt uns, weil es in uns das Bild von einer Straße weckt, die wie ein Pfeil durch eine unberührte Landschaft schneidet. Wir denken dabei an Freiheit und an den Wind in unseren Haaren.“ Ein paar Passagen weiter fügt er hinzu: “ (…) die Fragen, mit denen Schriftsteller:innen und Künstler:innen

heute konfrontiert sind, drehen sich nicht nur um die Politik der Kohlenstoffwirtschaft; viele beziehen sich auch auf unsere eigenen Praktiken und die Art und Weise, wie wir an der Komplettierung dieser Kultur im weiteren Sinne mitschuldig sind. Zum Beispiel: Wenn der Trend in der zeitgenössischen Architektur selbst in Zeiten sich beschleunigender Kohlenstoffemissionen in Richtung funkelnder Glas- und Metalltürme geht, müssen wir uns dann nicht fragen: Nach welchen Mustern wird der Wunsch durch die Gesten befeuert?"

Darüber denke ich also nach. Natürlich gibt es Gründe, warum wir uns Technologie nur auf bestimmte Weisen vorstellen können, und insofern bin ich um nichts besser als die aufgeregte junge Person im Space des Occupy-Startups. Ich unterliege meinen eigenen Verwirrungen. Mit dem Design und der Nutzung digitaler Technologien erfüllen wir uns unsere Wünsche; wir können sie nicht verändern, ohne nicht die Kultur zu hinterfragen und umzugestalten, die unsere Vorstellungskraft fixiert. Ich frage mich – ist Big Tech ein Produkt unserer Träume und unseres Wahns?

II

Ich chille am Pier von San Francisco und überlege, ob ich zum ersten Mal einen Impossible Burger essen soll, entscheide mich dann aber doch für Pommes und gegen das Kunstfleisch. Auf dem Rückweg zur Straßenbahn, die mich den Hügel hinauffährt, komme ich an einer ebenerdigen Ausbildungsstätte von Google vorbei. Ich werfe einen Blick hinein. Auf dem Whiteboard steht: „PROBLEM OBDACHLOSIGKEIT – WIE WIR ES BEHEBEN". Ich stehe davor, spüre die Leere des Raums, die Leere ihres Universums.

Zurück in Berlin, ein paar Monate später. Ich gehe zu einem Vortrag, Covid befindet sich noch in der Frühphase, in der Woche darauf wird alles geschlossen sein. Es herrscht eine unbehagliche Stimmung, die wenigen Leute, die gekommen sind, halten Abstand, wissen aber noch nicht so recht, warum.

Den Vortrag hält Didier Debaise. Er handelt von der Natur – beziehungsweise vom Begriff von Natur. Der Sprecher ist charmant, unaufgeregt, ein wenig fragil, aber selbstsicher. Er beschreibt seine Denkweise, ist dabei angenehm strukturiert und nachvollziehbar. Ich werde aufmerksam, als er davon spricht, wie der moderne Mensch die Natur als eine Reihe von operativen Vorgängen erfand. Wie er zu der Vorstellung von „Natur als passiv und mechanisch – als endloser Bewegung von belanglosen Dingen" gelangt. Damit sagt er, jedenfalls in meiner Erinnerung, dass unsere Sichtweise der Natur sie als ein Ding definiert, zu dessen Sezierung, Demontage und Ausbeutung wir berechtigt sind. Ich überlege, ob ich eine Frage stellen soll (was ich, wie ich weiß, nicht tun werde), aber mich würde interessieren, wie der Vortragende über die fortschreitende Abstrahierung der Natur durch die Technologie denkt. Die Natur wird zu einem Ding, das wir mit Sensoren ausstatten können. Ein Knäuel aus Geolocations. Können wir uns Natur ohne Koordinaten vorstellen?

III

Zwei California Dreams, betrachtet durch das Prisma zweier Denker, überzeugen mich, dass es unmöglich ist, unsere unmittelbaren Probleme technologisch zu lösen. Unsere Technologien sind das Produkt unserer Kulturen. Wir können Technologie nicht reparieren, ohne nicht ihren Zweck neu zu konzipieren.

Marek Tuszynski *ist Kreativdirektor und Mitbegründer von Tactical Tech. Seit 25 Jahren arbeitet er an der Schnittstelle von Technologie und Politik, Information und Aktivismus und den Folgen des Lebens in einer quantifizierten Gesellschaft. [https://tacticaltech.org/]*

Quellen:
1. Gosh Amitav, Uncanny And Improbable Events, Penguin classics series Penguin Ideas ISBN9780141996905; [https://www.penguin.co.uk/books/444078/uncanny-and-improbable-events-by-ghosh-amitav/9780141996905]
2. Debaise Didier, Nature and Its Others. The Invention of a Political Force, Vortrag, 24 Feb 2020,19:30; veranstaltet vom ICI Berlin; [https://www.ici-berlin.org/events/didier-debaise]

Digitale Inklusion

Martina Eigelsreiter

Digitale Inklusion umfasst benachteiligte Menschen, die durch Digitalisierung weiteren Ausschluss erfahren könnten, also ältere Personen, Personen mit Behinderungen, Menschen aus niedrig qualifizierten und bildungsferneren Schichten, benachteiligte Jugendliche sowie Frauen.

Wir wissen: Frauen-Domänen sind digitalisierungs- & rationalisierungsanfällig. Allein die Pandemie hat aufgezeigt, dass Gleichstellung, Chancengleichheit und Inklusion schnell zu Luxusproblemen werden. Durch die COVID-19 Krise waren digitale Kompetenzen sehr gefragt. Sei es für die Arbeit im Homeoffice oder für das Lehren und Lernen im Homeschooling. Die Pandemie hat vorhandene, gesellschaftliche Schwachstellen sichtbarer gemacht und überdeutlich gezeigt, dass die Ressourcen für die Teilhabe an der digitalen Welt ungleich verteilt sind. Ein Teil der Kinder und Jugendlichen konnten schwer bis gar nicht am Homeschooling teilnehmen, da viele Familien weder einen Computer noch einen Internetanschluss besitzen. Hinzu kommt, dass viele Lehrplattformen und Lernangebote nicht barrierefrei zugänglich waren und sind.

Es ist nach wie vor so, dass digital angepasste Angebote für benachteiligte Personen entwickelt werden, aber nicht mit ihnen. Das bedeutet, dass abweichende Lebensrealitäten nicht umfassend genug berücksichtigt werden. Zudem wird bei der Gestaltung digitaler Prozesse und automatisierter Entscheidungsfindungen (Algorithmen, künstliche Intelligenz) viel zu wenig bedacht, wie sie auf benachteiligte Menschen wirken.

Folgen für die Gesellschaft

Der Philosoph Richard David Precht warnt nicht ohne Grund davor, dass es nichts nützt, sich damit zu beruhigen, dass sicherlich nicht alles digitalisiert wird, was man digitalisieren kann. Es reicht schon aus, wenn 20 Prozent der bisherigen Beschäftigungsverhältnisse wegfallen. Das wird reichen, um unglaubliche Auswirkungen auf unsere Gesellschaft zu haben.

Wie wird also die Zukunft der nächsten 20 Jahre aussehen? Sich nicht sofort damit intensiv auseinanderzusetzen ist grob fahrlässig! Wir müssen uns jetzt ein ungefähres Bild dieser Zukunft machen, um wichtige Maßnahmen setzen zu können. Bleiben wir beim Strukturwandel am Arbeitsmarkt: Digitalisierung in der Arbeitswelt ist keine Naturkatastrophe, sie bricht nicht plötzlich auf uns herab, sondern muss aktiv gestaltet werden. Digitalisierung kann ein Hilfsmittel sein, um Beschäftigung und Beratung sowie Abläufe und Prozesse in Unternehmen inklusiver zu gestalten. Das setzt eine aktive Entscheidung voraus, die getroffen und von Anfang an mitbedacht werden muss. Nichtsdestotrotz bleiben Fragen, wie zum Beispiel: Verbessert oder verschlechtert Digitalisierung Chancen von Menschen am Arbeitsmarkt? Geht es nur um die Verfügbarkeit entsprechender Technologien? Wer entwickelt diese Technologien für wen?

Digitale Alphabetisierung

Die Teilhabe an der digitalen Welt setzt einiges an Wissen, digitalen Kompetenzen, Geldmitteln und eben die Möglichkeit einer barrierefreien Nutzung voraus. Um eine explosionsartig ansteigende Arbeitslosigkeit in den nächsten Jahrzehnten zu verhindern, sollte es aber im Interesse des Staates sein, Schulungen im Bereich digitale Kompetenzen günstig oder kostenlos anzubieten, und zwar für alle Altersklassen und alle Bevölkerungsgruppen. Die Politik ist gefragt: sie muss gesellschaftliche und wirtschaftliche Rahmenbedingungen vorgeben, die faire Arbeitsbedingungen, Entlohnung und soziale Absicherung sicherstellt – auch für die digitale Arbeitswelt.

Zusätzlich zur digitalen Alphabetisierung der Bevölkerung muss aber gleichzeitig ein Paradigmenwechsel stattfinden: nicht nur Menschen müssen sich an Erfordernisse der Digitalisierung anpassen, sondern neue Technologien müssen sich auch an die Menschen anpassen. Den Nutzer:innen dieser neuen Technologien muss auf Augenhöhe begegnet werden. Dafür steht auch Digitaler Humanismus.

KI und Big Data

Ein politisches Regelwerk braucht es auch für den generellen Umgang mit Digitalisierung und Künstlicher Intelligenz (KI). Doch der politische Diskurs hinkt den technologischen Möglichkeiten und der geschäftstüchtigen Wirtschaft hinterher. Entscheidungen in der Arbeitswelt und anderen Sektoren werden immer öfter an Algorithmen übergeben, nicht nur weil sie schneller arbeiten und Entschlüsse treffen können, sondern auch im Glauben sie würden objektiver entscheiden. Ihre Entscheidungsfindung hängt jedoch von den Trainingsdaten ab, mit denen sie von Menschen gefüttert werden. Wenn diese Diskriminierungen beinhalten, zeigt sich dies auch in den Entscheidungen des Algorithmus.

Die Nutzer:innen werden durch Bewegungs- und Suchprofile, Eingaben auf sozialen Medien, Konsumverhalten, dem Tragen von intelligenten Uhren und ähnlichen Produkten (die den Blutdruck, den Schlafrhythmus, die Herzfrequenz, ... überwachen), immer transparenter. Unternehmen, Technologiegiganten und Versicherungskonzerne werden jedoch in ihren Zielen und im Umgang mit diesen von ihnen gespeicherten, riesigen Datenmengen (Big Data) immer intransparenter. Demokratiepolitisch ist das sehr bedenklich.

Auch im Gesundheitssystem, wo die Künstliche Intelligenz stark unterstützend wirkt, da sie viel schnellere Analysen liefert, muss die Letztverantwortung bezüglich Diagnose und Behandlung bei den Ärzt:innen liegen. Dasselbe gilt für Pflegeroboter. Denn man kann in die Künstliche Intelligenz kein Verantwortungsbewusstsein programmieren, nur Entscheidungspfade und Regeln. Im Unterschied zu Menschen hat die Künstliche Intelligenz keine ethischen Impulse und ist nicht auf Ausnahmefälle programmierbar. Diese Eigenschaften bleiben (noch) dem Menschen vorbehalten.

Martina Eigelsreiter *leitet das Büro für Diversität der Stadt St. Pölten. Das Büro für Diversität ist eine Verwaltungsstelle für Vielfaltmanagement am Magistrat St. Pölten und bündelt die Aufgabenbereiche Frauen, Menschen anderer Herkunftsländer, Menschen mit Behinderung, sexuelle Identität und den Bereich Weltanschauung & Weltreligionen.*

Vertrauen im Internet schaffen

Lisa Kostrzewa, Roland Alton-Scheidl

Was ist Vertrauen?

„Vertrauen [stellt] immer das Resultat einer Interaktion zwischen den Eigenheiten einer spezifischen Vertrauenssituation und den individuellen Charakteristiken der vertrauenden Person [dar].“ (Wertheimer; Birbaumer 2016, S.13). Auch Bernd Blöbaum beschreibt innerhalb seiner Forschung am Alfred Wissenschaftskolleg Greifswald zwei Einheiten für die Entstehung von Vertrauen. Demnach bedarf es eine:n Vertrauensgeber:in und eine:n Vertrauensnehmer:in. Vgl. (Blöbaum 2015). Vertrauen ist somit das Resultat einer Interaktion zweier Einheiten. Die individuellen Charakteristiken der vertrauenden Person fallen aufgrund vielfältiger Variationen stets unterschiedlich aus und variieren bei jeder Vertrauenssituation. Anders verhält es sich mit den Eigenheiten der spezifischen Vertrauenssituation.

Im Internet spielt sich die Vertrauenssituation zwischen dem/der Nutzer:in als vertrauende Person bzw. Vertrauensgeber:in und dem Server bzw. dem Dienst, welcher genutzt werden soll und sich auf dem Server befindet, als Vertrauensnehmer:in ab. Hinter dem Server steht immer ein:e Betreiber:in, welcher den Dienst zur Verfügung stellt. Der Server bzw. der Serverbetreiber bestimmt als Vertrauensnehmer die Vertrauenssituation mit. Vertrauen wird im Internet zunächst auf technischer Ebene realisiert. Um Daten oder Informationen von einem Server abrufen zu können, benötigt der Client (Webbrowser, Mail- oder Chatprogramm) dessen IP-Adresse. Die Auflösung einer Webadresse auf eine IP-Adresse erfolgt über DNS Server, welche also auch Kenntnis haben, welche Webseiten vom Client besucht werden.

Der/die Internetnutzer:in darf demnach einen Dienst nutzen bzw. die entsprechenden Daten vom Server abrufen und hinterlässt im Gegenzug dazu dem Dienst und dem DNS die eigene IP-Adresse. Der Vertrauensgeber gibt dem Vertrauensnehmer also einen Hinweis auf dessen Identität und dieser übertragt dafür die Daten. Der Vertrauensgeber weiß in den meisten Fällen jedoch nicht, was im Moment der Datenübertragung mit den eigenen Daten passiert. Wo werden die Daten hinübertragen? Wer hat Zugriff darauf? Wo, wie und wie lange werden die Daten gespeichert? Was sagen die Daten über den/die Internetnutzer:in aus? Kann ein/eine Nutzer:in anhand der Daten im Internet wiedererkannt und dadurch ganze Wege der Datenübertragung nachverfolgt werden? Für den/die Internetnutzer:in sind die Antworten auf diese Fragen zunächst nicht ersichtlich, sondern die Situation der Datenübertragung erfordert Vertrauen in den Server und dessen Betreiber:in.

Die Datenschutzgrundverordnung

„Vertrauen ist nur dann notwendig und entsteht nur dann, wenn Informationen über die Absichten des Gegenübers fehlen, wenn man also das Verhalten des Gegenübers nicht vorhersagen kann.“ (Wertheimer; Birbaumer 2016, S.13). Im Hinblick auf das Thema Vertrauen soll die Datenschutzgrundverordnung Aufschluss über die Absichten des Gegenübers geben, indem dessen Verhalten bzw. die Möglichkeiten, wie personenbezogene Daten weitergegeben werden dürfen, eingeschränkt werden. Die Datenschutzgrundverordnung soll Nutzer:innen Transparenz geben, wie das Gegenüber mit personenbezogenen Daten umzugehen hat. Das Problem ist aber, dass die Datenschutzgrundverordnung in vielen Fällen nach wie vor missachtet wird.

Das Privacy Shield war eine informelle Absprache, welche im Jahr 2015 von der EU-Kommission mit den Amerikanern ausverhandelt wurde. Die Übereinkunft sollte die Erfüllung europäischer Datenschutznormen bei der Datenübermittlung in die USA gewährleisten.

Das Privacy Shield sollte als Nachfolger des bereits zuvor gekippten Safe-Harbor-Abkommens dienen und einen angemessenen Datenschutz für die europäische Bevölkerung sicherstellen. Am 16. Juli 2020 stellt der Europäische Gerichtshof im entsprechenden EuGH Urteil fest, dass das Privacy Shield, unter dem die Datenübertragung in die USA zulässig war, nicht mehr gilt.

Das bedeutet, dass der Transfer von personenbezogenen Daten auf Basis des Privacy Shield nicht zulässig ist und nur anhand von Standardvertragsklauseln erfolgen darf, wenn der Staat, in welchen die Daten transferiert werden, über ein Datenschutzniveau verfügt, welches den Bürger:innen dieselben Rechte wie in der EU gewährleistet. Damit scheidet die USA als Staat, in welchen personenbezogene Daten auf Basis von Standardvertragsklauseln transferiert werden dürfen, in den meisten Fällen aus, da das Datenschutzniveau der USA nicht an jenes der EU heranreicht. Um dies zu umgehen, haben amerikanische Großkonzerne, wie beispielsweise Microsoft, vor einigen Jahren damit begonnen, sogenannte Serverfarmen, also riesige Datencenter, in Europa aufzubauen. Dadurch müssen die Daten europäischer Bürger:innen nicht mehr in die USA transferiert werden.

Der Foreign Intelligence Surveillance Act, kurz FISA, ist ein US-amerikanisches Gesetz. Das Gesetz verpflichtet alle amerikanischen Anbieter von Kommunikationsdiensten dazu, die Daten ausländischer Bürger:innen zu sammeln, zu speichern und den Behörden zur Verfügung zu stellen. Die US-amerikanischen Anbieter unterliegen diesem Gesetz, unabhängig davon, was mit europäischen Unternehmen in Verträgen vereinbart wurde. Hinzu kommt der Cloud Act, ein Gesetz, welches 2018 von der amerikanischen Regierung erlassen wurde. Das Gesetz verpflichtet alle amerikanischen Unternehmen dazu, den Behörden auch dann Zugriff auf gespeicherte Daten zu gewähren, wenn diese außerhalb der USA gespeichert werden. Dies bedeutet, auch wenn amerikanische Unternehmen Daten in Europa speichern, muss der Zugriff auf diese Daten für US-Behörden gewährleistet sein. Dies steht im Widerspruch zur europäischen Datenschutzgrundverordnung.

Wie schafft fairkom Vertrauen?

An dieser Stelle wird beispielhaft die fairkom Gesellschaft porträtiert, welche auch für private Nutzer:innen ein alternatives Portfolio an Internetdiensten bereithält. Dazu zählen faircloud, fairchat, fairmeeting, fairteaching, fairsuch, fairmailing oder fair.tube – alle über das fairapps.net Portal erreichbar und mit einem fairlogin Konto nutzbar. fairkom Anwendungen werden ausschließlich auf Servern innerhalb der EU betrieben und sind somit DSGVO konform.

fairkom Anwendungen sind Open Source. Open Source Software bedeutet, dass der Code offen zugänglich ist. Damit gibt es keine Geheimnisse bei Algorithmen oder Möglichkeiten einer versteckten Überwachung. Der Code ist über Dienste zur Versionsverwaltung von Softwareprojekten, wie beispielsweise GitLab oder GitHub, öffentlich einsehbar.

fairkom ist Teil der Open Source Community und verfügt über ein weitläufiges Netzwerk. Software Code wird innerhalb der Community regelmäßigen Reviews unterzogen und jede:r kann Fehler im Code beheben. Dadurch wird der Code stetig optimiert und Bugs werden schnell gefixt. Änderungen können dank der Versionsverwaltung bis ins Detail nachverfolgt werden.

fairkom Dienste arbeiten datensparsam. Es werden nur technisch notwendige Cookies, die ausschließlich von eigenen Servern kommen, verwendet und keine Cookies für Webtracking gesetzt. Anfragen an fremde Server werden nicht gestellt. Alle fairkom Anwendungen funktionieren im Browser, die Installation eines Programms oder einer App wird optional angeboten, ist aber nicht zwingend erforderlich. Den Nutzer:innen ist es freigestellt, ob beispielsweise die

Teilnahme an einer Videokonferenz browserbasiert erfolgen oder das Programm auf dem Computer installiert werden soll.

Die Nutzung der meisten fairkom Anwendungen erfolgt nach dem fair-use Prinzip. Die Videokonferenz-Anwendung fairmeeting kann für den privaten Gebrauch ohne Anmeldung sofort verwendet werden. Nach der Konferenz erscheint eine Spendenseite, die erfreulicherweise auch rege genutzt wird. Bei den angebotenen Paketen wird nicht nach Anzahl der Teilnehmenden oder Nutzungsdauer abgerechnet, sondern es werden Richtwerte für die Verwendung angegeben. fairkom ist eigenkapitalfinanziert und unterliegt keinen kurzfristigen Gewinnerwartungen von Shareholdern. Gewinne werden in Open Source und Commons Projekte investiert.

fairkom entwickelt neue Features für Open Source Anwendungen und gibt diese an die Community zurück. So zum Beispiel fairblue, eine Erweiterung für BigBlueButton, welche eine Simultanübersetzung während einer Konferenz ermöglicht.

fairkom ist kein anonymer Dienstleister, sondern jede:r kann einfach zum Hörer greifen oder bei unserem Hauptsitz in Dornbirn, Vorarlberg vorbeikommen. Mit speziellem Support oder Consulting Paketen zu einzelnen Open Source Anwendungen unterstützt fairkom auch zahlreiche Organisationen mit ihren Bedürfnissen nach vertrauensvoller IT.

Roland Alton-Scheidl *ist Vorstandsmitglied der fairkom Gesellschaft und Unabhängiger Berater für Kommunikation und Informatik.*
Lisa Kostrzewa *ist Konzeptionerin bei der fairkom Gesellschaft.*
[https://www.fairkom.eu/]

Quellen
Wertheimer, Jürgen; Birbaumer, Niels (2016): Vertrauen. Ein riskantes Gefühl. Wals bei Salzburg: Benevento Publishing.
Blöbaum, Bernd (2015): Vertrauen und Journalismus. Wie Medien durch Misstrauen das Vertrauen des Publikums gewinnen. Online im Internet: [https://www.wiko-greifswald.de/storages/wiko-greifswald/Mediathek/PDF_Dateien/Fellows/2014_15/Studienjahr_2014_2015_Bloebaum.pdf] (Zugriff am: 27.07.2022)

Suchmaschinen

Wolfgang Sander-Beuermann

Das wichtigste Kriterium, nach dem Suchmaschinen und am besten jedes Programm beurteilt werden sollte, ist das folgende: Ist diese Software oder dieses Programm Quellcode-offen? Viele Nutzer:innen können mit dem Begriff „Quellcode-offen" nicht so richtig etwas anfangen. Darum zunächst eine kurze Begriffserklärung.

Auch wenn sie Maschine heißt: eine Suchmaschine ist nichts weiter als ein Programm. Wenn auch meist ein sehr langes, was letztlich dann natürlich von Computern, also Maschinen, ausgeführt wird. Jedes Programm besteht aus Anweisungen an Prozessoren und Chips, eine Reihe von digitalen Befehlen auszuführen, die im Allgemeinen in einer höheren (= verstehbaren) Programmiersprache formuliert und von Menschen geschrieben wird. Beim Quellcode-offenen Programm wird letzteres - dieses von Menschen geschriebene Programm - öffentlich gemacht. Somit auch die Gedanken, die zu diesem Programm geführt haben. Jede:r kann es lesen und prinzipiell auch verstehen.

Die meisten Programme sind aber nicht Quellcode-offen, sondern sogenannte proprietäre Software. Also eine Software, die jemandem gehört der/die nicht zulässt, dass andere die Details verstehen können, was programmiert wurde. Dies aus den verschiedensten Gründen: Er/sie möchte das Programm verkaufen, ohne zu verraten, wie es funktioniert (Geschäftsgeheimnis). Oder er/sie möchte nicht, dass jede:r verstehen kann, was das Programm genau und in allen Einzelheiten tut. Weil darin einiges geschieht, was kaum jemand akzeptieren würde, wenn er/sie es wüsste und verstünde.

Wenn ich nun Menschen frage, die Google & Co benutzen, warum sie ihre Privatsphäre so deutlich sichtbar machen, sagen sie meist

im Brustton der Überzeugung „ich habe doch nichts zu verbergen". Doch es sollte sie sehr misstrauisch machen, dass diejenigen, deren Programme sie gerade benutzen, das genaue Gegenteil im Schilde führen: nämlich ihr Programm und ihre Gedanken dahinter zu verstecken! Sie, diese Anbieter, wollen einiges verbergen. Seltsamerweise stört die meisten Menschen das aber nicht - vielleicht sehen oder verstehen sie diesen Gegensatz nicht. Da SIE diesen Text lesen, vermute ich das bei Ihnen anders: ich gratuliere!

Unter den Suchmaschinen gibt es nur wenige, die ihre Programme öffentlich gemacht haben; die großen tun es sowieso nicht. Denn sie wollen vor allem eines: Geld verdienen. In Deutschland sind nur zwei größere Suchmaschinen bekannt, die ihren Programm-Quellcode veröffentlichen: metager.de, ab 1996 entwickelt an der Uni-Hannover, 2012 outgesourced zum gemeinnützigen SUMA-EV, und YaCy.net seit 2003 auf der Basis einer breiten Community.

- Metager.de ist wie jede Suchmaschine zu bedienen. Ihr Quellcode ist öffentlich: [https://gitlab.metager.de/open-source/MetaGer]. Dort kann jede:r sehen, wie sie funktioniert oder Verbesserungsvorschläge einbringen. Wenn bei metager.de gesucht wird, bleibt nichts gespeichert. Dazu gibt es noch etliche weitere Anonymisierungs-Möglichkeiten (inkl. Tor). Siehe: [https://metager.de/hilfe]

- YaCy.net funktioniert anders als die hier genannten Alternativen. Sie basiert auf einem Netz nach dem Peer-to-Peer Prinzip [https://de.wikipedia.org/wiki/Peer-to-Peer]. Dieses Netzwerk bildet gemeinsam die Suchmaschine. Im Unterschied zu den anderen beiden Alternativen hängt YaCy nicht von wohlgesonnenen Daten-Zulieferern ab! Einzelheiten & Quellcode via: [https://de.wikipedia.org/wiki/YaCy]

- Als größeren dritten im Bunde gibt es seit 2014 noch eine Quellcode-offene internationale Meta-Suchmaschine: searx.org [https://en.wikipedia.org/wiki/Searx]. Nutzer:innen sind aufgerufen eigene Instanzen dieses Programms zu installieren. Da diese z.T. auch Google abfragen, werden solche oftmals von Google blockiert.

Ein paar Schlussworte noch zu folgendem: Viele Menschen sagen, dass sie den Quellcode eines Programms eh nie verstehen könnten; darum sei es ihnen egal, ob Quellcode-offen oder nicht. Sie vergessen dabei, dass das Internet sehr groß ist: es gibt dort immer Expert:innen oder Freaks, die ALLES bis zum letzten Komma auseinander nehmen. Spätestens diese Expert:innen würden auch gut versteckte Datenkrakereien finden und öffentlich machen - sie könnten die Monetarisierung deutlich erschweren.

Wolfgang Sander-Beuermann *war vom Juli 2004 bis Januar 2019 geschäftsführendes Vorstandsmitglied des Vereins Suma e.V., der die Metasuchmaschine MetaGer betreibt. [https://suma-ev.de]*

Die Normalisierung von Überwachung im Bildungswesen und digitale Selbstverteidigung als Antwort

Daniel Lohninger

Das Bildungsministerium in Österreich scheitert an der Einhaltung der einfachsten Datenschutzvorgaben und riskiert damit massive, lebenslange Benachteiligungen der österreichischen Schüler:innen. Man ist schon lange falsch abgebogen und verlässt sich auf US-amerikanische Big Tech Firmen bei der Nutzung von Software im Schulbereich und wohl auch darüber hinaus. Microsoft ist vorherrschend, und auch Google kommt oft zum Einsatz. Neben der Präsenz im Lehrplan werden diese Produkte auch für Mails mit den Schüler:innen, Eltern und für dienstliche Kommunikation der Lehrenden verwendet. Trotz großer Datenschutzbedenken von Expert:innen werden diese Anbieter von offizieller Seite als datenschutzrechtlich unbedenklich angepriesen.

Die „Fundgrube" an sensiblen Informationen, die während der Schulzeit durch das Bildungssystem gesammelt werden, wird zunehmend mit Datensätzen Dritter über Personen und Haushalte verknüpft. Diese Daten werden von Datenbrokern gekauft, um basierend auf algorithmisch vorhergesagtem Verhalten frühzeitig einzugreifen und prädiktive Modelle in Klassenzimmern zu entwerfen.

Die globale Pandemie hat einen fruchtbaren Raum für Überwachungsunternehmen und Ed-Tech-Plattformen geschaffen. Aber auch über die Krisenreaktion hinaus führt die stetige Verbreitung dieser Technologien zu einem zunehmend dokumentierten, bewerteten und profilierten Lernraum. Die Schüler:innen werden im Dunkeln gelassen, während ihr Verhalten und ihre Bildungsbiografie ohne ihr Wissen erfasst und von angeblich die Zukunft vorhersagenden Technologien genutzt wird.

Wir, als NGO für digitale Grundrechte, sehen schon lange wie sehr es an digitaler Grundbildung im Bereich Datenschutz fehlt. Meine Kolleg:innen und ich halten seit Jahren Vorträge, Workshops und Schulungen zu digitaler Selbstverteidigung für unterschiedlichstes Publikum. Der Bedarf und der Wunsch Datenschutz, IT-Sicherheit und das Internet besser zu verstehen und Lösungsmöglichkeiten kennenzulernen ist groß. Wir wollen das gezielt angehen und beginnen damit ein Bildungsprojekt aufzubauen. Neben der inhaltlichen Qualität sind OER (Open Educational Ressources), möglichst gute Barrierefreiheit, von uns ausgebildete Trainer:innen und ein zielgruppenorientiertes Workshopangebot zentrale Elemente um Wissen effektiv in die Breite tragen zu können. Unser erstes Projekt „Digitale Selbstverteidigung für Lehrlinge" richtet sich an junge Menschen in der Berufsausbildung und wird von der Arbeiterkammer Niederösterreich gefördert. Neben Workshops an Berufsschulen gibt es auf einer Webseite ein frei nutzbares E-Learning zu den wichtigsten Themen Digitaler Selbstverteidigung: [https://epicenter.academy/e-learning]

Daniel Lohninger *ist Mitarbeiter der NGO epicenter.works – Plattform Grundrechtspolitik und hat 2021 die Projektleitung des Bildungsbereichs im Verein übernommen. [https://epicenter.works/]*

Arbeitswelt & Schule

Alexander Sommer, Felix Wendt

Arbeitswelt & Schule umfasst ein breitgefächertes Angebot der AK Niederösterreich, welches Lehrkräfte bei ihrem Unterricht an Schulen unterstützt und bestehende Lehrplaninhalte zielgerichtet und kompetenzorientiert ergänzt. Ziel ist es, Schüler:innen optimal auf den Einstieg in die Arbeits- und Berufswelt vorzubereiten. Das Angebot reicht von Expert:innenvorträgen und Webinaren zu Themen des Arbeits- und Sozialrechts, Inhalte der Verbraucher:innenbildung, Bewerbungstrainings mit speziell geschulten Coaches, eine breite Palette gesellschaftspolitischer Workshops und wirtschaftspolitischer Planspiele bis hin zu Lehrkräftefortbildungen und ergänzenden Unterrichtsmaterialien.

Diese Unterstützungsangebote, die sich an alle Schüler:innen und Jugendlichen in Niederösterreich richten, werden seitens der AK Niederösterreich unter der Jugendmarke *AK Young* zusammengefasst. Neben den oben beschriebenen Leistungen stellen zusätzlich Infomaterialien, Broschüren, zahlreiche Veranstaltungen und (Berufsorientierungs-)Messen sowie eine eigene Website [https://www.akyoung.at] ein breites Angebot dar, welches Lehrkräfte, Schüler:innen und deren Erziehungsberechtigte kostenfrei nutzen können.

Digitalisierung bei Arbeitswelt und Schule

Bei zahlreichen Angeboten von *Arbeitswelt & Schule* ist das Thema Digitalisierung ein wichtiger und an Bedeutung gewinnender Bestandteil: Sei es bei Bewerbungstrainings, welche u.a. den Blick auf die Bedeutung digitaler Bewerbungsprozesse legen, oder bei Berufsorientierungsworkshops, bei denen aktuelle Inhalte wie Apps zur Berufs- und Bildungsorientierung sowie virtuelle Berufslexika thematisiert und ausprobiert werden.

Als kooperatives, sozialpartnerschaftliches Projekt seitens der AK Niederösterreich und der WK Niederösterreich wurde bspw. die Berufsorientierungs-App BoToGo entwickelt, um Eltern einen Wegweiser für die weitere Berufs- und Bildungswegsentscheidung ihrer Kinder zur Verfügung zu stellen.

Auch bei Schulvorträgen, wie bspw. Verbraucher:innenbildung für Jugendliche, klären AK-Expert:innen über Gefahren und Herausforderungen im Umgang mit digitalen Medien im Kontext von Konsumentscheidungen auf (z. B. Einkäufe im Internet, Fake-Shops, In-App-Käufe etc.) und geben Tipps & Tricks für einen richtigen und sicheren Umgang mit eben diesen.

Herausforderungen wie Fakes im Netz, (Cyber-)Mobbing und Hatespeech:

Die Nutzungsintensität und -dauer von digitalen Medien durch Jugendliche stieg in den letzten Jahren stetig an. Es häufen sich somit auch die Berührungspunkte mit zwei dominierenden Phänomenen der digitalen Welt wie Fakes und Hass im Netz. Die gezielt dazu entwickelten Workshops *#Click_Trust_Like* und *#Digital_Courage* widmen sich genau diesen Themen, sollen Jugendliche sensibilisieren und im Umgang mit diesen Erscheinungen stärken (Empowerment).

Alexander Sommer *und* ***Felix Wendt*** *sind Mitarbeiter der AK Niederösterreich im Bereich Arbeitswelt & Schule.*
[https://noe.arbeiterkammer.at/aws]

Impressum

Redaktion: **Elisabeth Schimana**
Übersetzungen: **Jacqeline Csuss**
Lektorat: **Judith Strußenberg, Elisabeth Schimana**
Grafik: **Andreas Rathmanner, Nora Bischof**

Erste Auflage November 2022
© IMA Institut für Medienarchäologie
© der Texte bei den Auitor:innen

Mit Unterstützung von
Niederösterreich Kultur
Bundesministerium für Kunst, Kultur, öffentlicher Dienst und Sport
Stadt St. Pölten

Bundesministerium
Kunst, Kultur,
öffentlicher Dienst und Sport

KULTUR
NIEDERÖSTERREICH

st.pölten

IMA
INSTITUT FÜR MEDIENARCHÄOLOGIE